Интервью: гуманитарные операции, распространение вредоносной информации и защита данных

Беседа с Дельфиной ван Золинге, советником МККК по вопросам защиты людей от цифрового риска в условиях вооруженного конфликта, и с Массимо Марелли, руководителем отдела защиты данных МККК

Сотрудники журнала побеседовали с Дельфиной ван Золинге и Массимо Марелли из Международного Комитета Красного Креста (МККК). Д. ван Золинге координирует в МККК изучение вопросов о том, как цифровые технологии и распространение вредоносной информации влияют на людей, живущих в условиях конфликта, и как это отражается на гуманитарной деятельности. С данной целью Д. ван Золинге по поручению МККК и в партнерстве с другими организациями проводит исследования

как способов снижения риска, который привносят в гуманитарную сферу цифровые технологии, так и возможностей разработки соответствующих защитных мер, необходимых в цифровую эпоху. М. Марелли руководит отделом защиты данных. За время его работы в МККК организация наметила новые пути осуществления своей основной деятельности с обеспечением надлежащей защиты данных не только пострадавших, которым она помогает, но и данных своих сотрудников.

В ходе интервью Д. ван Золинге и М. Марелли рассказывают о том, как их направления работы дополняют и укрепляют друг друга и составляют две стороны одной медали, поскольку информация и данные в электронном виде могут, с одной стороны, принести в гуманитарную сферу перемены к лучшему, а с другой — стать предметом злоупотреблений. М. Марелли поясняет, как гуманитарные организации обрабатывают, защищают и используют данные и информацию в электронном виде. Д. ван Золинге рассуждает о том, как можно манипулировать информацией и распространять с помощью цифровых технологий вводящие в заблуждение сведения, дезинформацию и риторику ненависти, особенно в эпоху COVID-19, когда люди сильнее зависят от цифровых коммуникационных технологий. В статье поднимаются такие вопросы, как перспективы надлежащего использования цифровых технологий, этические соображения, которые следует учитывать гуманитарным организациям, а также возможные направления сотрудничества государственного и частного секторов в данной сфере.

Ключевые слова: распространение вредоносной информации, вводящие в заблуждение сведения, дезинформация, риторика ненависти, социальные сети, COVID-19, защита данных, «не навреди», гуманитарные метаданные.

: : : : : : :

Как МККК понимает «превращение информации в оружие»? Чем оно отличается от злоупотребления информацией в ходе вооруженных конфликтов или других ситуаций насилия? Как принцип «не навреди» и работа отдела защиты данных связаны с «превращением информации в оружие»?

Дельфина ван Золинге: Прежде всего, важно отметить, что термин «превращение информации в оружие» имеет ряд недостатков как минимум с юридической точки зрения. Например, возникает вопрос о том, может ли информация стать оружием в правовом смысле, и если да, то как и когда? Поэтому МККК называет это явление распространением вредоносной информации, включая в это понятие вводящие в заблуждение сведения, дезинформацию и риторику ненависти во всех их проявлениях.

МККК уже давно обеспокоен случаями использования цифровой информации и систем коммуникации и связи таким образом, что уязвимые группы населения — например, внутренне перемещенные лица, мигранты, заключенные и представители меньшинств, а также сотрудники гуманитарных организаций и добровольцы — могут столкнуться с новым или возросшим риском гуманитарных последствий. За неимением более удачного термина МККК пользуется формулировкой «вводящие в заблуждение сведения, дезинформация и риторика ненависти» в качестве собирательного названия этого явления, но при этом признает, что информация может использоваться и для других целей или не приводить к возрастанию риска гуманитарных последствий (например, если операция имеет последствия исключительно для сил противника). В этом случае под гуманитарными последствиями могут пониматься перемещение, смерть, исчезновение людей, утрата или уничтожение имущества, потеря источника дохода, физический, моральный / психологический и социальный ущерб или травма, стигматизация, разлука с семьей или отказ в доступе к услугам, таким как образование, медицина, пропитание и кров. Кроме того, гуманитарные последствия могут характеризоваться возникновением или обострением существующих гуманитарных потребностей, в том числе в убежище, пропитании и непродовольственных товарах, медико-санитарной помощи, психологической и психосоциальной поддержке, экономической помощи, доступе к услугам и к оперативной и актуальной для данного места информации, юридическим консультациям и поддержке или в доступе к сети Интернет. К вводящим в заблуждение сведениям, дезинформации и риторике ненависти могут также относиться некорректная информация, вирусные слухи, выражение ненависти в виртуальном пространстве, пропаганда в интернете и так далее[1].

Сам по себе способ использования информации, как правило, не «причиняет» никакого вреда. Речь, скорее, о том, что на фоне соответствующей социальной, культурной и исторической динамики, существующей общественной или политической напряженности, отсутствия у людей цифровой грамотности или критического мышления при поиске информации в интернете, нехватки источников надежной и корректной информации и так далее «потенциал» нанесения вреда может возрасти.

Может возникнуть вопрос: а как было раньше и что изменилось? История знает множество примеров того, как информационно-коммуникационные системы могут причинять вред: один из них — «Радио тысячи

1 Подробнее об этой терминологии см.: Peter Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, MA, 2018, доступно по адресу: www.likewarbook.com; Mark Silverman, “Book Review: LikeWar: The Weaponization of Social Media”, *International Review of the Red Cross*, Vol. 101, No. 910, 2019, доступно по адресу: https://international-review.icrc.org/sites/default/files/reviews-pdf/2019-12/irrc_101_910_21.pdf; John Mingers and Craig Standing, “What is Information? Toward a Theory of Information as Objective and Veridical”, *Journal of Information Technology*, Vol. 33, No. 3, 2018, доступно по адресу: https://link.springer.com/article/10.1057/s41265-017-0038-6.

холмов» в Руанде[2]. Изменился лишь вид носителя, который используется для распространения информации на мировом уровне. Цифровые технологии, а особенно социальные сети, демонстрируют увеличение скорости, масштаба и воздействия распространяемой информации, которая влияет на самые разные виды аудитории. Рост использования интернета, доступность смартфонов и социальных сетей стали мощными инструментами обмена информацией и налаживания связей между людьми, но также привели к усугублению насилия и конфликтов, как в случае с распространением в Мьянме риторики ненависти через Facebook. Под воздействием этих новых переменных информация может рассматриваться как возможный способ причинения вреда в гражданском пространстве.

Массимо Марелли: На мой взгляд, то, чем мы занимаемся в отделе защиты данных, связано с тем, о чем сейчас сказала Дельфина. Мы подходим к своей работе во многом так же: все дело не только в самих данных, но и в том, как они используются или, может быть, становятся предметом злоупотреблений. Задача отдела защиты данных — позаботиться о том, чтобы персональные данные получателей помощи МККК, его посредников и сотрудников были надежно защищены и чтобы сохранялся необходимый уровень доверия как внутри организации, так и по отношению к ней. В таких условиях принцип «не навреди» означает, что неспособность защитить данные получателей помощи МККК, его посредников и сотрудников может нанести колоссальный ущерб как самим этим людям, так и всей деятельности МККК. Защита данных как инструмент «недопущения нанесения вреда в цифровом пространстве»[3] также связана с возможностью выстроить призму, через которую можно анализировать потоки данных, генерируемых за счет использования технологий, и определять, каких еще заинтересованных лиц можно привлечь к сотрудничеству, какой риск это повлечет и как можно снизить этот риск или избежать его. Таким образом, защита данных — это нечто большее, чем просто недопущение нанесения вреда; она позволяет соблюдать права и достоинство пострадавших людей при обработке их данных и ставить их интересы на первое место. Кроме того, защита данных позволяет обеспечить подотчетность перед пострадавшими по четким стандартам.

2 «Радио тысячи холмов» (Radio Mille Collines), также известное как «Свободное радио и телевидение тысячи холмов» (Radio Télévision Libre des Mille Collines), — работавшая в Руанде радиостанция, в эфирах которой с 8 июля 1993 года по 31 июля 1994 года распространялись дезинформация и вводящие в заблуждение сведения. Ложная пропаганда, которую транслировало радио, сыграла главенствующую роль в подстрекательстве к геноциду народа тутси в Руанде в 1994 году. Подробнее см.: Elizabeth Baisley, “Genocide and Constructions of Hutu and Tutsi in Radio Propaganda”, *Race and Class*, Vol. 55, No. 3, 2014, доступно по адресу: https://journals.sagepub.com/doi/abs/10.1177/0306396813509194.

3 ICRC, *The Humanitarian Metadata Problem: “Doing No Harm” in the Digital Era*, 2018, доступно по адресу: www.icrc.org/en/download/file/85089/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

Не могли бы вы подробнее рассказать о том, почему гуманитарным организациям стоит беспокоиться о распространении вредоносной информации и о защите данных?

Массимо Марелли: И защита данных, и борьба с распространением вредоносной информации составляют неотъемлемую часть общего мандата МККК по предоставлению защиты. Кроме того, оба направления работы важны для поддержания доверия к МККК со стороны пострадавших и тех, с кем он ведет конфиденциальные переговоры. В случае появления масштабной бреши в защите данных в МККК или другой гуманитарной организации, помимо серьезных последствий для субъектов данных, возможен подрыв доверия ко всему сектору и к его способности оценивать ситуацию и помогать тем, кто больше всего нуждается в помощи.

Примером того, какую роль играет защита данных в повседневной работе гуманитарной организации и почему гуманитарным организациям необходимо заботиться о сохранности данных, является использование биометрических данных в судебно-медицинской деятельности МККК и в программе по восстановлению семейных связей. В августе 2019 года была принята политика МККК в области использования биометрии, что позволило решить острые проблемы, связанные с защитой информации при использовании биометрических данных — отпечатков пальцев, систем распознавания лиц, ДНК и так далее, — которые являются особенно уязвимой информацией, поскольку, если хранить их после сбора, они позволят составить досье о человеке, с помощью которого его всегда можно будет опознать[4]. Это может создать проблемы в гуманитарной деятельности, поскольку люди могут воспротивиться тому, чтобы их личность можно было установить в любой момент, особенно если существует риск попадания этой информации не в те руки. Политика МККК была разработана в ответ на растущий внутри организации интерес к потенциалу использования биометрии в деятельности МККК и призвана обеспечить баланс между ее ответственным применением и снижением присущего ей риска, связанного с защитой данных. Сейчас эта политика помогает наладить различные аспекты перехода к цифровым технологиям в Центральном агентстве МККК по розыску, которое разрабатывает новые инструменты для наращивания наших возможностей, позволяющих устанавливать судьбу и местоположение пропавших людей и восстанавливать семейные связи в сотрудничестве с партнерами по Международному движению Красного Креста и Красного Полумесяца («Движение»). Сюда входит и возможное использование технологии распознавания лиц по фотографиям пропавших и разыскиваемых людей, а также применение искусственного интеллекта для поиска людей в базах данных МККК и его партнеров по гуманитарной деятельности. Беспрекословное соблюдение стандартов защиты данных

4 ICRC, “The ICRC Biometrics Policy”, 16 October 2019, доступно по адресу: www.icrc.org/en/document/icrc-biometrics-policy.

будет совершенно необходимо, чтобы сформировать доверие к этичности, безопасности и возможностям использования этих инструментов.

Дельфина ван Золинге: То же относится и к распространению вредоносной информации через вводящие в заблуждение сведения, дезинформацию, риторику ненависти и так далее. Такая практика и динамика могут иметь свои последствия для нашей гуманитарной деятельности, направленной на защиту людей. Сами по себе это не новые явления и их способность наносить вред относительно хорошо изучена, однако стремительная цифровизация — как в обычной деятельности МККК, так и вне ее — привела к увеличению скорости, с которой вредоносная информация может распространяться, находить отклик у разных видов аудитории и влиять на них. Слухи больше не ограничены географией, сфабриковать фотографии и видеоролики можно быстро и с минимальными накладными расходами; появилась возможность выявлять отдельных лиц и сообщества и направлять удар на них.

Мьянма, Южный Судан и Эфиопия[5] — вот несколько примеров, которые показывают, что явления, связанные с введением в заблуждение, дезинформацией и риторикой ненависти, особенно в социальных сетях, сейчас все чаще возникают в условиях насилия и войны. Что это значит? По большому счету, это значит, что гуманитарные организации стали чаще сталкиваться с такой практикой и динамикой применения информационно-коммуникационных систем, которые могут быть очень разрушительными. Подобная практика чревата дестабилизацией и без того неустойчивой среды и ростом уязвимости людей, а также повышает вероятность наступления гуманитарных последствий. Если мы не сможем понять и определить эти факторы риска при выработке ответных мер защиты, мы можем упустить из виду некоторые виды вреда или удовлетворить потребности пострадавших лишь частично.

Кроме того, мы должны понимать, что вводящие в заблуждение сведения, дезинформация и риторика ненависти могут непосредственно влиять на деятельность и на авторитет гуманитарных организаций. Что произошло бы, если бы МККК стал мишенью целенаправленной кампании по дезинформации в стране, истерзанной войной? Наш авторитет мог бы быть существенно подорван, вследствие чего мы могли бы потерять доверие пострадавших; нам могло бы быть отказано в доступе в зоны боевых действий, и тогда бы мы не смогли обеспечить защиту и помощь местному населению и даже могли бы стать объектом нападения.

Если мы согласны с тем, что распространение вредоносной информации может стать вектором или фактором, который способен усугубить уязвимость людей, спровоцировать нанесение вреда гражданскому населе-

5 В этих странах социальные сети, такие как Facebook и Twitter, использовались для распространения вводящих в заблуждение сведений, слухов и риторики ненависти, что усугубило напряженность и вызвало ряд проявлений насилия на местах.

нию или вызвать репутационные потери или угрозу безопасности гуманитарных организаций, нам, по всей видимости, необходимо следить за этим.

С какими трудностями сталкивается гуманитарный сектор из-за распространения вредоносной информации? Нам также много приходится слышать о проблемах, которые возникают у гуманитарных организаций в связи со сбором и защитой гуманитарных метаданных, — не могли бы вы рассказать нам об этих проблемах и о риске, сопутствующем сбору и защите таких метаданных?

Дельфина ван Золинге: Отвечу на ваш первый вопрос. Существует целый ряд проблем, связанных с распространением вредоносной информации, мы можем рассмотреть три из них.

Во-первых, угроза распространения вводящих в заблуждение сведений, дезинформации и риторики ненависти не локализована. Она не исходит от одной группы лиц, которые сидят в бункере и обладают уникальной способностью создавать вредоносный контент или изыскивать новые способы распространения ложной информации. В цифровую эпоху потреблять, создавать и распространять контент может любой человек, имеющий доступ в интернет, и в силу этого он, сам того не зная, может стать распространителем вредоносной информации. Кроме того, в некоторых случаях можно без больших трудозатрат добиться больших успехов в распространении дезинформации или вводящих в заблуждение сведений среди потенциально масштабной аудитории. Двухминутный видеоролик, снятый и смонтированный с помощью смартфона и размещенный в соцсетях, может дать колоссальный эффект. Все мы смотрели видеоролики с флешмобами, и здесь действует похожая концепция: одним сообщением можно заставить танцевать весь Центральный вокзал Антверпена[6]. Кроме того, доступность инструментов и хакерских программ по относительно низким ценам все больше облегчает работу злонамеренных пользователей. Это может вызвать целый ряд юридических вопросов, касающихся ответственности, подотчетности и участия в боевых действиях.

С этим связан и тот известный нам факт, что выявить вводящие в заблуждение сведения, дезинформацию и риторику ненависти или проверить их обычными средствами нелегко. Необходимы время и практика, чтобы научиться безошибочно ориентироваться в захлестывающем нас океане новостей и информации. К этой проблеме добавляется и сложность измерения воздействия вводящих в заблуждение сведений, дезинформации и риторики ненависти, которое иногда может быть размытым или неосязаемым. Например, как измерить последствия разрушения доверия? Или как определить взаимосвязь между действиями в интернете и их последствиями в реальном мире? Некоторые некоммерческие организации и ученые

6 Танцевальный флешмоб, о котором идет речь, можно посмотреть по адресу: www.youtube.com/watch?v=7EYAUazLI9k.

тщательно изучают различные аспекты превращения информации в оружие, но они редко обращают особое внимание на страны, пострадавшие от войны и насилия. Что касается гуманитарного сообщества, то оно начинает осознавать возможные виды риска, связанные с вводящими в заблуждение сведениями, дезинформацией и риторикой ненависти, а также с распространением вредоносной информации, но испытывает сложности, стараясь определить, как вписать это новое направление в свою работу.

Наконец, средства цифровой коммуникации вкупе с вводящими в заблуждение сведениями, дезинформацией и риторикой ненависти вводят в игру целый ряд новых участников с разнообразными функциями и обязанностями, таких как СМИ и частный сектор. Вопрос о том, как выстраивать с ними предметный диалог, помимо обычного содействия нашей гуманитарной деятельности, пока остается для нас в значительной степени открытым.

Массимо Марелли: На мой взгляд, аналогично проблеме распространения вредоносной информации существует ряд сложностей, с которыми сталкиваются гуманитарные организации в рамках защиты и хранения метаданных. Но для начала давайте определимся с терминологией. Метаданные — это данные о данных. К ним относятся информация о коммуникации — кто связался с кем и когда — и цифровой след, который оставляют компьютеры, приложения и сети при взаимодействии друг с другом.

Почему сбор и защита метаданных имеют такое большое значение? Да потому что метаданные раскрывают много информации о людях. Метаданными пользуются компании, которые занимаются рекламой в интернете, чтобы создать профили пользователей, а также ведомства в сфере разведки и безопасности, которые с помощью метаданных выявляют интересующих их лиц и группы людей. В гуманитарной ситуации трудности и опасности, присущие сбору метаданных, связаны с тем, что метаданные могут использоваться для отслеживания местонахождения, передвижений и взаимодействия между организациями и пострадавшими, — эта информация может привести к нарушению конфиденциальности и использоваться не для гуманитарных целей, например сторонами в конфликте. Однако в некоторых ситуациях метаданные могут быть чрезвычайно полезны для гуманитарных организаций, позволяя им лучше понять, как используются их услуги и где они нужнее всего. Метаданные также могут применяться для выяснения судьбы пропавших людей с помощью интернет-пространства. Тот факт, что эта информация присутствует везде, создает особые сложности для обеспечения защиты метаданных. С этой целью МККК вступил в партнерство с организацией Privacy International, чтобы содействовать повышению осведомленности о проблеме гуманитарных метаданных[7], а также в сотрудничестве с организацией Brussels Privacy Hub

7 ICRC, “Digital Trails Could Endanger People Receiving Humanitarian Aid, ICRC and Privacy International Find”, 7 October 2018, доступно по адресу: https://www.icrc.org/en/document/digital-trails-could-endanger-people-receiving-humanitarian-aid-icrc-and-privacy.

подготовил инструкцию по защите данных, призванную помочь справиться с этими видами риска[8].

Каким образом пандемии, подобные COVID-19, влияют на число случаев распространения вредоносной информации и на необходимость проявлять бдительность в отношении защиты данных в гуманитарном секторе?

Дельфина ван Золинге: Вспышка инфекционного заболевания часто приводит к всплеску вводящих в заблуждение сведений, дезинформации и риторики ненависти. Мысли о пандемии вызывают у нас самые глубокие и сильные эмоции, возбуждая страх и поднимая волны паники. С ростом неопределенности и тревоги люди начинают искать ответы на свои вопросы с помощью информационных ресурсов. В социальных сетях новости распространяются быстрее и шире, с минимальной цензурой. В таких условиях возможно манипулирование информацией ради экономической, идеологической или политической выгоды.

Во время COVID-19 вводящие в заблуждение сведения, вирусные слухи и дезинформация наблюдались на многих цифровых платформах и веб-сайтах. Распространение информации достигло такого уровня, что это явление получило название «инфодемия»[9]. Определенные непроверенные сведения об инфекционных заболеваниях, непреодолимых угрозах и смерти могут победить рациональное мышление и усугубить поляризацию общества. В некоторых случаях такой образ мыслей может проявляться в экстремальном, возможно, даже агрессивном поведении, в том числе в непосредственных физических нападениях на медицинский персонал или объекты здравоохранения, в забастовках, против которых полиция или военные применяют силу, и так далее. Например, распространенная в социальных сетях вводящая в заблуждение или ложная информация о местонахождении обсерваторов для прохождения карантина привела к росту неопределенности и страха среди общественности, в результате чего граждане стали нападать на транспортные колонны, в которых перевозили пациентов, и препятствовать эвакуации.

Распространение вводящих в заблуждение сведений или дезинформации в социальных сетях может расти и вследствие того, что модераторы контента, публикуемого на платформах, были упразднены, а удалением вводящего в заблуждение контента стали заниматься машины. Несмотря

8 ICRC, *Handbook on Data Protection in Humanitarian Action*, 23 August 2017, доступно по адресу: www.icrc.org/en/data-protection-humanitarian-action-handbook (Руководство по защите данных в ходе гуманитарной деятельности. Готовится к публикации на русском языке).

9 См., например: *Департамент глобальных коммуникаций ООН*. Киберпреступность и распространение дезинформации во время пандемии COVID-19, 31 марта 2020 года. Доступно по адресу: https://www.un.org/ru/coronavirus/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19; Farah Lalalni and Juraj Majcin, "Inside the Battle to Counteract the COVID-19 'Infodemic'", World Economic Forum, 9 April 2020, доступно по адресу: https://www.weforum.org/agenda/2020/04/covid-19-inside-the-battle-to-counteract-the-coronavirus-infodemic/.

на всю перспективность искусственного интеллекта и автоматизированных систем, их возможностей пока недостаточно для отслеживания сведений, которые могут вводить в заблуждение.

Вводящие в заблуждение сведения или дезинформация могут влиять на гуманитарные организации, особенно на те, которые связаны или считаются связанными со странами, где отмечается высокий уровень распространенности инфекции COVID-19. Население может полагать, что сотрудники зарубежных гуманитарных организаций являются переносчиками вируса. Это может иметь далеко идущие последствия с точки зрения безопасности и возможности выполнять свою работу.

Что уже предпринял МККК для борьбы с вводящими в заблуждение сведениями, дезинформацией и риторикой ненависти в плане своей гуманитарной деятельности и для применения принципа «не навреди» к своей работе в сфере защиты данных?

Дельфина ван Золинге: Для обсуждения обычной деятельности, связанной с вводящими в заблуждение сведениями, дезинформацией и риторикой ненависти, в декабре 2018 года МККК организовал в Лондоне симпозиум, посвященный цифровому риску[10]. Цель этого мероприятия состояла в том, чтобы понять, как цифровые технологии и способы их применения влияют на гражданское население в условиях вооруженных конфликтов и отражаются на деятельности гуманитарных организаций и на обеспечении защиты.

Опираясь на некоторые из ключевых итогов мероприятия, МККК начал осуществлять программу борьбы с вводящими в заблуждение сведениями, дезинформацией и риторикой ненависти. Первый этап программы был реализован в 2019 году; основной задачей в этот период было выявление ключевых препятствий и трудностей, мешающих сотрудникам МККК учитывать в своей работе и анализе вводящие в заблуждение сведения, дезинформацию и риторику ненависти. Это исследование было проведено на примере двух делегаций МККК — на Шри-Ланке и в Эфиопии. Исходя из некоторых первоначальных потребностей, определенных в ходе исследования, мы разработали практическое руководство по вводящим в заблуждение сведениям, дезинформации и риторике ненависти для сотрудников МККК на местах, чтобы они лучше ознакомились с этим явлением и понимали, что делать.

Наконец, совместно с учеными и заинтересованными гуманитарными организациями мы начали создавать научное партнерство по исследованию вводящих в заблуждение сведений, дезинформации и риторики ненависти. Наша цель состоит в том, чтобы собрать основанные на фактических данных исследования этого явления и его гуманитарных последствий,

10 Доклад по итогам проведенного в Лондоне симпозиума, посвященного цифровому риску в условиях вооруженных конфликтов, можно найти по адресу: www.icrc.org/fr/publication/4403-symposium-report-digital-risks-armed-conflicts.

а затем разработать на их основе концепцию, необходимую гуманитарным организациям для решения этого вопроса. Это поможет определить последствия вводящих в заблуждение сведений, дезинформации и риторики ненависти для обеспечения защиты и гуманитарной деятельности. Кроме того, такие исследования помогут понять, как МККК и другим заинтересованным гуманитарным организациям лучше всего учитывать это явление в своем анализе и работе с пострадавшими.

Массимо Марелли: Наша работа в области защиты данных тоже основана на тщательной оценке риска причинения вреда в ходе определенных действий с последующим принятием мер для уменьшения такого риска, в том числе через отказ от проведения таких действий или пересмотр стратегии проведения операции. Что касается принципа «не навреди», мы уже приняли несколько конкретных мер защиты в рамках утвержденных в 2015 году Правил МККК по защите персональных данных; эти меры направлены на снижение риска несанкционированного доступа к персональным данным посредством введения стандартов защиты данных и требований к процедурам обработки данных для всей организации[11]. В тех случаях, когда МККК рассматривает возможность использования новых технологий или более рискованных операций по обработке данных, необходимо провести оценку последствий обработки данных, чтобы определить риск причинения вреда и принять меры для его уменьшения[12]. Кроме того, Правила предписывают МККК придерживаться подхода, основанного на «защите данных, обеспечиваемой на конструктивном уровне»[13], чтобы ограничить сбор персональных данных необходимым для работы минимумом и обеспечить соблюдение прав субъектов данных.

Что мы как гуманитарное сообщество можем сделать, чтобы начать решать проблемы, возникающие в связи с распространением вредоносной информации (вводящих в заблуждение сведений, дезинформации и риторики ненависти), и вопросы защиты данных?

Дельфина ван Золинге: Для того чтобы начать решать проблемы, возникающие в связи с распространением вредоносной информации, мы должны глубже понять само явление вводящих в заблуждение сведений, дезинформации и риторики ненависти и его гуманитарные последствия, сориентироваться в стратегии на основе проработанной концепции и проявить готовность взаимодействовать с новыми участниками этого процесса на доселе неизведанной территории.

11 *МККК*. Правила МККК по защите персональных данных, 2015. Доступно по адресу: https://www.icrc.org/ru/document/pravila-mkkk-po-zashchite-personalnyh-dannyh.

12 Там же; см. также: ICRC, “Policy on the Processing of Biometric Data by the ICRC”, 28 August 2019, доступно по адресу: www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf.

13 *МККК* (примечание 11 выше).

Однако для этого нам необходимо иметь в виду следующее. Если мы начнем работать над решениями в отрыве друг от друга, не определив общие приоритеты, результаты нашей работы будут несущественными, и мы лишь зря потратим силы. Проблема вводящих в заблуждение сведений, дезинформации и риторики ненависти волнует многих из нас, это сложная проблема, в которой переплетаются и взаимодействуют разные динамические процессы, системы и участники. Для решения данной проблемы необходимо придерживаться системного подхода.

Наконец, мы должны определить концептуальную основу распространения вредоносной информации. Для этого необходимо четко и тщательно разобраться в том, с какими видами риска и вреда могут столкнуться пострадавшие люди и гуманитарные организации в связи с цифровыми информационными технологиями и их применением и как можно реагировать на этот риск и способствовать его снижению. Следовательно, нам необходима теория вреда, причиняемого в связи с цифровыми технологиями, а для связи между теорией и практикой необходима концептуальная основа. Учитывая то, насколько обширна эта задача, мы должны формировать партнерства и объединяться друг с другом, например с другими организациями или учеными и научно-исследовательскими учреждениями.

Массимо Марелли: Я согласен с Дельфиной. Чтобы действенно решать проблемы распространения вредоносной информации и защиты данных, надо разрушить стоящие между нами стены и выявить несколько общих приоритетов для всего гуманитарного сектора. С точки зрения защиты данных внедрение гуманитарным сектором новых цифровых технологий и конкретные виды риска, которые принесли с собой эти технологии, побудили МККК серьезно задуматься над тем, что значит «недопущение нанесения вреда в цифровом пространстве». С этой целью мы стали активно формировать стратегические партнерства с организациями, которые ответственно относятся к защите данных[14], и поставщиками услуг, а также заниматься «цифровой дипломатией» для решения некоторых конкретных проблем, стоящих перед гуманитарным сектором. Помимо всего прочего, принимаются меры

14 Например, МККК сотрудничал с Brussels Privacy Hub в рамках проекта по защите данных в гуманитарной деятельности, который ориентирован на работников гуманитарных организаций, участвующих в обработке персональных данных в рамках гуманитарной деятельности, особенно тех, кто отвечает за консультирование по стандартам защиты данных и за их применение. По итогам проекта было, в частности, подготовлено Руководство по защите данных в ходе гуманитарной деятельности, доступное по адресу: www.icrc.org/en/data-protection-humanitarian-action-handbook (готовится к печати на русском языке). МККК сотрудничал и/или консультировался со специалистами из разных организаций по вопросам защиты данных, в том числе из таких как Brussels Privacy Hub, Швейцарское ведомство по защите данных, Европейский инспектор по защите данных, Управление Верховного комиссара ООН по делам беженцев, Международная организация по миграции, Международная Федерация Обществ Красного Креста и Красного Полумесяца, Управление ООН по координации гуманитарных вопросов, Йельский университет, Privacy International, Франкофонная ассоциация ведомств по защите персональных данных, Федеральная политехническая школа в Лозанне, «Врачи без границ», Сенегальское ведомство по защите данных и другие.

для защиты «цифрового гуманитарного пространства»[15], чтобы данные, собранные для гуманитарных целей, могли использоваться только в этих целях в соответствии с принципами нейтральности и независимости.

В дополнение к включению правил защиты данных в партнерские соглашения на операционном уровне МККК, например, тесно сотрудничал с Движением в целях разработки стандартов защиты данных для программы по восстановлению семейных связей, которые представлены в Кодексе поведения Движения[16]. Вопросы, связанные с защитой данных, активно поднимались и в ходе XXXIII Международной конференции Красного Креста и Красного Полумесяца в декабре 2019 года[17], где широко обсуждалась тема недопущения нанесения вреда в цифровом пространстве в контексте «смещения уязвимости» и «доверия к гуманитарной деятельности». В ходе этой конференции также была принята поворотная резолюция о восстановлении семейных связей и защите данных, в которой признается, что сбор и использование гуманитарных данных иначе чем для гуманитарных целей подрывают доверие к гуманитарным организациям и представляют угрозу для их деятельности. Резолюция «призывает государства и Движение сотрудничать, с тем чтобы гарантировать, что персональные данные не будут запрашиваться или использоваться в целях, несовместимых с гуманитарным характером деятельности Движения»[18].

Не могли бы вы привести несколько положительных примеров использования цифровых информационно-коммуникационных систем?

Дельфина ван Золинге: Цифровые информационные технологии открывают возможности для совершенствования оказания гуманитарной помощи пострадавшим, в том числе за счет налаживания двусторонней связи между сотрудниками гуманитарных организаций и людьми, пострадавшими от кризисов, или за счет применения инновационных способов сбора и использования информации о кризисе для выработки мер оказания помощи, а также за счет других технологий. Правозащитники и деятели гуманитарной сферы пользуются более совершенными методами оценки ситуации и получения практически значимой информации, которые доступны в цифровую эпоху. Тому есть много примеров, приведу

15 Более подробный анализ роли МККК в защите «цифрового гуманитарного пространства» приведен в статье Massimo Marelli, “Hacking Humanitarians: Moving Towards a Humanitarian Cybersecurity Strategy”, *Humanitarian Law and Policy Blog*, 16 January 2020, доступно по адресу: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/.

16 Сеть Международного движения Красного Креста и Красного Полумесяца по восстановлению семейных связей. Кодекс поведения в отношении защиты данных, ноябрь 2015 года. Доступно по адресу: https://www.icrc.org/ru/download/file/54719/ruscodedataprotection.pdf.

17 International Conference of the Red Cross and Red Crescent, “33rd International Conference: At a Glance”, доступно по адресу: https://rcrcconference.org/about/33rd-international-conference/.

18 International Conference of the Red Cross and Red Crescent, “Resolution: Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection”, 33rd International Conference, 9–12 December 2019, доступно по адресу: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

здесь несколько: они применяют дистанционные датчики в дополнение к инструментам раннего оповещения о нарушениях прав человека и документирования таких случаев. Они задействуют мобильные решения для отслеживания условий, характеристик и маршрутов транзита мигрантов и беженцев, используют метаданные из расшифровок звонков для исследования распространения инфекционных заболеваний, проводят анализ общественных настроений и сбор слухов в нестабильных районах с помощью социальных сетей и, разумеется, применяют воздушную робототехнику для наблюдения за пораженными объектами и за ключевой инфраструктурой.

В период пандемии COVID-19 цифровые инструменты, искусственный интеллект[19] и анализ больших данных используются в различных условиях для поддержки мер реагирования в системе здравоохранения. Они могут помочь собрать, проанализировать и передать ключевую информацию для распределения медицинских ресурсов и сил, ускорения работы медицинских, логистических цепочек и цепочек поставок или обеспечения общественной безопасности и порядка в условиях изоляции.

Цифровые информационные технологии могут очень пригодиться для обмена ключевыми сведениями и, следовательно, для содействия медицинско-эпидемиологическим лабораторным исследованиям. Во время кризиса, вызванного COVID-19, широко использовались информационные приложения для обмена актуальной и точной информацией с пострадавшими, которые были полезны для профилактики и повышения осведомленности. Эти приложения различались в зависимости от модели, интерфейса, содержания, а также уровня безопасности и соблюдения конфиденциальности. В целом, если эти приложения утверждаются и рекомендуются официальными государственными органами здравоохранения, они могут сыграть свою роль в повышении осведомленности и уровня информированности населения, благодаря чему люди оказываются лучше подготовлены к принятию соответствующих мер для профилактики и поддержания хорошего самочувствия.

В целом существует много различных цифровых инструментов, которые продвигаются и обсуждаются в контексте реагирования на COVID. Они могут играть разные роли и выполнять разные функции в зависимости от своего назначения и конструктивных особенностей, а также от времени и места их развертывания и использования. Таким образом, цифровые технологии могут внести свой вклад в борьбу с COVID, однако их необходимо систематически анализировать с точки зрения их актуальности, соблюдения требований защиты данных и достаточности на основе оценки каждого конкретного случая и условий использования, поскольку их актуальность и добавочная стоимость могут сильно варьироваться.

19 Shana Lynch, “Artificial Intelligence and COVID-19: How Technology Can Understand, Track and Improve Health Outcomes”, *Stanford Institute for Human-Centered Artificial Intelligence Blog*, 1 April 2020, доступно по адресу: https://hai.stanford.edu/news/artificial-intelligence-and-covid-19-how-technology-can-understand-track-and-improve-health.

Массимо Марелли: На мой взгляд, цифровые информационно-коммуникационные системы могут быть полезны, если их надлежащим образом регулировать. Например, законодательство в сфере защиты данных предусматривает, что цифровые технологии могут использоваться таким образом, чтобы обеспечить «цифровое достоинство» или «информационное достоинство» с предоставлением субъекту данных всех необходимых сведений, возможности контроля и прав, которые нужны им для того, чтобы контролировать использование информации о них самих. В этих законах также предпринята попытка ограничить перечень действий, которые контролеры данных могут выполнять с нашей информацией, чтобы обеспечить нам справедливое обращение, без дискриминации и эксплуатации. Учитывая эти законы в своей работе, мы можем добиться того, чтобы положительное воздействие цифровых технологий перевешивало их отрицательные стороны. Исходя из этого понимания, эти фундаментальные принципы защиты данных легли в основу Правил МККК по защите персональных данных[20]. Конечно, легко сказать, что применение этих принципов к гуманитарной деятельности может осложняться условиями на местах или тем, что получателям нашей помощи все равно, но если мы всерьез намерены добиться того, чтобы общий итоговый эффект от применения цифровых технологий был положительным, и серьезно относимся к уважению достоинства пострадавших, стремясь не навредить им, обеспечить подотчетность и сохранить доверие, то этого недостаточно. У нас нет иного выбора, кроме как попытаться преодолеть эти трудности и обеспечить соответствие своих действий принципам, которые определяют гуманитарную деятельность в данной сфере.

Зачем гуманитарному сектору сотрудничать с частными технологическими компаниями?

Дельфина ван Золинге: Давайте я отвечу на этот вопрос. Стремительное развитие технологий, средств связи и данных приводит к изменениям в различных слоях общества, в нашей работе и общении. В условиях гуманитарного кризиса оно влияет не только на ожидания и потребности пострадавших и других участников, но и на возможные способы реализации гуманитарных программ и услуг.

Переход к цифровым технологиям открывает перед гуманитарным сектором новые перспективы осуществления и масштабирования ответных мер, но при этом создает новые виды риска для пострадавших от конфликта людей и/или усугубляет существующие опасности. В то же время от цифровой трансформации общества и бизнеса уже, на самом деле, нельзя отказаться. Она уже идет, и нам придется научиться жить и работать в этих условиях.

20 *МККК* (примечание 11 выше).

Гуманитарный сектор обязан одновременно оценивать актуальность цифровых решений и подбирать подходящий способ этичного взаимодействия с компаниями технологической отрасли. Первая причина этого состоит в том, что технологии и данные дают возможность усовершенствовать гуманитарную деятельность и, следовательно, помочь облегчить страдания людей, которых коснулась беда. Вторая причина: в зависимости от способа применения этих технологий или злоупотребления ими может возникать риск для людей и/или ущерб для авторитета гуманитарных организаций. Появившуюся возможность совершенствования гуманитарной деятельности за счет использования цифровых технологий необходимо проанализировать, понять, исследовать и ответственно реализовать, следуя принципу «не навреди» и соответствующим правилам защиты данных.

В том же ключе гуманитарный сектор может поучиться у технологических компаний планированию более эффективных ответных мер, а технологический сектор — заимствовать у гуманитарного способность думать и о том, как поведет себя технология вне лабораторных условий, осознавать возможные последствия техноколониализма[21] в реальном мире, которые могут влиять на жизнь и безопасность пострадавших, и совместными усилиями искать способы сокращения этих последствий.

Массимо Марелли: По-моему, Дельфина упомянула обо всем, что я мог бы сказать на эту тему. Я присоединяюсь к ее словам о том, что мы уже не можем «отказаться» от процессов цифровой трансформации, и мы видим это на примере господства частных технологических компаний. Со своей стороны, у гуманитарного сектора есть обязательство взаимодействовать с этими участниками игры и стремиться адаптировать методы своей работы таким образом, чтобы безопасность и доверие пострадавших оставались в нашей повседневной деятельности на первом месте.

Обязаны ли крупнейшие социальные сети внедрять политику, которая защищала бы пострадавших от широкого распространения вводящих в заблуждение сведений и дезинформации?

Массимо Марелли: Думаю, лучше на этот вопрос может ответить Дельфина.

Дельфина ван Золинге: Спасибо, Массимо. Я считаю, что это общая ответственность. Распространение вводящих в заблуждение сведений, дезинформации и риторики ненависти происходит не на пустом месте, оно коре-

21 По определению Мирки Мадиану, понятие «техноколониализм» описывает то, «как сближение новых цифровых технологий с гуманитарными структурами и рыночными силами оживляет и восстанавливает в иной форме отношения колониальной зависимости». См: Mirca Madianou, “Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises”, *Social Media and Society*, Vol. 5, No. 3, 26 July 2019, доступно по адресу: https://journals.sagepub.com/doi/full/10.1177/2056305119863146.

нится в истории, моделях поведения в обществе, хронических размолвках, политике и целом ряде других факторов.

Сами по себе платформы не являются причиной распространения вредоносной информации; конечно, они играют свою роль в расширении масштабов, повышении значимости и увеличении скорости ее распространения, но инициируют сообщение не они. Это не следует трактовать как позволение владельцам соцсетей «умыть руки» и ничего не предпринимать в связи с тем, что на их платформах плодится опасный контент. Поскольку они предоставляют людям эту прибыльную услугу, в которой алгоритмы, искусственный интеллект и анализ данных играют одну из главенствующих ролей в определении того, насколько заметным и доступным будет контент в зависимости от профиля пользователя, его интересов и/или поведения в обществе, эти компании несут ответственность за то, чтобы внедрить необходимую политику для снижения риска и технические меры для ограничения распространения информации, способной причинить вред людям.

Во время кризиса, вызванного COVID, многие социальные сети, такие как Facebook и Twitter, приняли меры для ограничения объема, например, вводящих в заблуждение сведений о методах лечения, которые явно способны привести к смертельному исходу, — то есть некорректных и потенциально вредоносных советов медицинского характера[22]. Хотя многие люди сказали бы, что эта информация очевидно и совершенно ложна, в условиях кризиса в области здравоохранения страх смерти может лишить людей способности мыслить рационально. В условиях вооруженного конфликта и даже латентного насилия можно легко играть на первобытных страхах и инстинкте выживания. Публикация и распространение тревожных или вырванных из контекста сведений в такой обстановке могут способствовать поляризации, усугублять стресс и страх, провоцировать неразумное поведение и в конечном счете насилие.

Поэтому так важно обращать внимание не только на сами платформы, но и на различных участников процесса, их роли и сферы ответственности. Политики, органы власти и гражданское общество, каждый на своем месте и со своим набором полномочий, должны внести свой вклад в то, чтобы помочь ограничить создание и распространение вводящих в заблуждение сведений, дезинформации и риторики ненависти в социальных сетях, и несут за это ответственность. Но мы все-таки должны быть реалистами: вводящие в заблуждение сведения и дезинформация глубоко укоренены в политике, власти и поведении в обществе, и в силу этого они будут

22 Например, Google удаляет ложную или вводящую в заблуждение информацию о COVID-19 со своих разнообразных платформ и из объявлений; см.: Sundar Pichai, “COVID-19: How We’re Continuing to Help”, *Inside Google*, 15 March 2020, доступно по адресу: https://blog.google/inside-google/company-announcements/covid-19-how-were-continuing-to-help/. Twitter теперь проверяет публикации и учетные записи на предмет достоверности содержащейся в них информации; компания также внедрила информативные подсказки для поиска по хештегу #KnowTheFacts; см.: “Coronavirus: Staying Safe and Informed on Twitter”, *Twitter Blog*, 3 April 2020, доступно по адресу: https://blog.twitter.com/en_us/topics/company/2020/covid-19.html.

и дальше использоваться разными способами, в разных формах и видах. Однако способ справиться с этой проблемой все же есть: мы можем повышать сопротивляемость людей этому явлению за счет содействия развитию цифровой грамотности, критического мышления и — если немножко побыть идеалистами — гуманитарных ценностей.

В чем состоят преимущества и недостатки расширения доступа пострадавших к цифровым платформам и инструментам?

Дельфина ван Золинге: Пусть Массимо ответит.

Массимо Марелли: Спасибо, Дельфина. Для начала позвольте заметить, что доступ к сети Интернет следует рассматривать как часть нашей жизни, а не просто как проблему или возможность. Поскольку общественная и материальная жизнь все больше перемещается в интернет, а мир становится все более связанным, у гуманитарных организаций не остается иного выбора, кроме как обеспечить свое присутствие в том виртуальном пространстве, где собираются пострадавшие, задействовать новые механизмы повышения устойчивости, появившиеся благодаря такому доступу, и учитывать это явление при подготовке своих программ. Это может быть относительно просто, например, в случае предоставления подключения к интернету как гуманитарной помощи, а может быть и сложнее, скажем, если речь идет о новых цифровых услугах. Помимо соблюдения требований в области защиты данных и поддержания полноценного реагирования на потребности тех, у кого нет доступа к Сети, основной трудностью здесь, на наш взгляд, является ответственное внедрение инноваций. Нам необходимо инвестировать в создание безопасных и защищенных цифровых гуманитарных пространств, где мы можем быть уверены в том, что не причиняем никому вреда и при этом работаем в цифровой среде, какой она является сегодня. Это далеко не так легко. Для этого необходимо проводить просветительскую работу среди партнеров, государств и поставщиков технологии, объясняя им, зачем нужны такие пространства, а также совместно с ними развивать инфраструктуру и приложения, которые требуются для ведения нейтральной, независимой и вызывающей доверие гуманитарной деятельности.

Каковы этические последствия использования цифровых технологий, например применения программ распознавания лиц для поиска пропавших людей? Как эти этические соображения влияют на работу МККК?

Массимо Марелли: Этика и защита данных часто пересекаются. Законодательство в области защиты данных, как и большинство других законов, в конечном счете является итогом размышлений над ответами общества на этические вопросы и сводом правил, которых оно решает придерживаться, чтобы соответствовать данным ответам. На мой взгляд,

ключевыми вопросами при применении технологий, о которых вы упомянули, являются следующие: могут ли эти технологии принести реальную пользу МККК и пострадавшим, с одной стороны, а с другой — можем ли мы использовать их в духе ответственности и подотчетности, чтобы интересы пострадавших стояли для нас на первом месте?