

**Генеральная Ассамблея**

Distr.: General  
24 April 2015  
Russian  
Original: English

**Совет по правам человека**

Двадцать девятая сессия

Пункт 3 повестки дня

**Поощрение и защита всех прав человека,  
гражданских, политических, экономических,  
социальных и культурных прав,  
включая право на развитие**

**Доклад Специального докладчика по вопросу  
о внесудебных казнях, казнях без надлежащего  
судебного разбирательства или произвольных казнях  
Кристофа Хейнца**

**Использование информационно-коммуникационных  
технологий в целях обеспечения права на жизнь**

*Резюме*

В настоящем докладе, представленном Совету по правам человека согласно резолюции 26/12, Специальный докладчик по внесудебным казням, казням без надлежащего судебного разбирательства или произвольным казням рассматривает влияние информационно-коммуникационных технологий (ИКТ) на защиту права на жизнь.

Специальный докладчик проводит обзор существующих возможностей применения ИКТ в интересах поощрения, защиты и мониторинга прав человека. Отмечая, что задействование "гражданских свидетелей" может потребовать изменения порядка документирования нарушений прав человека и создать трудности с использованием собираемых и передаваемых ими доказательств, в частности в связи с их проверкой, Специальный докладчик разбирает, каким образом такие материалы помогают в работе различным международным правозащитным механизмам. Он вносит несколько рекомендаций, в том числе рекомендует Управлению Верховного комиссара Организации Объединенных Наций по правам человека назначить специалиста по цифровым доказательствам для оказания ему содействия в оптимальном применении ИКТ.

GE.15-08236 (R) 130515 150515



\* 1 5 0 8 2 3 6 \*

Просьба отправить на вторичную переработку 

## Содержание

	<i>Пункты</i>	<i>Стр.</i>
I. Деятельность Специального докладчика .....	1–34	3
A. Сообщения .....	3	3
B. Поездки .....	4–6	3
C. Пресс-релизы .....	7–22	4
D. Международные и национальные совещания .....	23–34	5
II. Использование информационно-коммуникационных технологий в целях обеспечения права на жизнь .....	35–106	6
A. История вопроса .....	35–43	6
B. Поощрение и пропаганда прав человека .....	44–48	9
C. Предупреждение и защита .....	49–66	10
D. Мониторинг и установление фактов .....	67–76	15
E. Оценка доказательств, собранных с использованием информационно-коммуникационных технологий .....	77–91	18
F. Использование информационно-коммуникационных технологий правозащитными механизмами .....	92–106	22
III. Заключение .....	107–113	26
IV. Рекомендации .....	114–125	27
A. Рекомендации Организации Объединенных Наций .....	114–116	27
B. Рекомендации региональным правозащитным механизмам .....	117	28
C. Рекомендации государствам .....	118–120	28
D. Рекомендации организациям гражданского общества и академическим кругам .....	121–122	29
E. Рекомендации донорам .....	123	29
F. Рекомендации корпорациям, занимающимся разработкой технологий и программного обеспечения .....	124–125	29

## **I. Деятельность Специального докладчика**

1. Специальный докладчик представил свой последний доклад Генеральной Ассамблее в октябре 2014 года. В этом докладе (A/69/265) он рассматривает четыре темы, связанные с защитой права на жизнь, а именно: роль региональных правозащитных систем; применение "менее смертоносных" и беспилотных оружейных систем для целей правоохранительной деятельности, возобновление смертной казни и роль статистических показателей.

2. В июне 2014 года Специальный докладчик представил свой предыдущий доклад Совету по правам человека. В этом докладе (A/HRC/26/36) он затронул вопросы защиты права на жизнь в ходе мероприятий по поддержанию правопорядка, а также необходимость приведения внутреннего законодательства о применении полицией оружия в соответствие с международными стандартами. Он также призвал Совет разработать общие контуры правового режима использования дистанционно-пилотируемых летательных аппаратов или боевых беспилотников и продолжать держать в поле зрения вопрос об автономных оружейных системах.

### **A. Сообщения**

3. Специальный докладчик высказал замечания по сообщениям, направленным в период с 1 марта 2014 года по 28 февраля 2015 года, а также по ответам, которые были получены в период с 1 мая 2014 года по 30 апреля 2015 года (A/HRC/29/37/Add.5).

### **B. Поездки**

4. С 3 по 7 ноября 2014 года совместно со Специальным докладчиком по вопросу о пытках и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания Хуаном Э. Мендесом Специальный докладчик посетил Гамбию (A/HRC/29/37/Add.2).

5. Доклады по итогам поездок Специального докладчика в Индию и Турцию содержатся в документах A/HRC/29/37/Add.3 и 4, а доклад о поездке в Папуа-Новую Гвинею приводится в документе A/HRC/29/37/Add.1

6. После представления Совету по правам человека своего предыдущего доклада Специальный докладчик направил просьбы о посещении их стран правительствам Йемена, Нигерии, Руанды и Украины. Он выражает признательность правительствам Гамбии, Ирака и Йемена за положительный отклик на его просьбы и призывает правительства Египта, Ирана (Исламской Республики), Нигерии, Пакистана, Руанды, Украины и Эритреи дать согласие на его просьбы о посещении этих стран.

## С. Пресс-релизы<sup>1</sup>

7. Приводимые ниже пресс-релизы были выпущены Специальным докладчиком в период с марта 2014 по март 2015 года.
8. 6 марта 2014 года Специальный докладчик выпустил совместное заявление по поводу утверждений о применении чрезмерной силы и насилия в отношении участников протестных акций, журналистов и сотрудников средств массовой информации в Боливарианской Республике Венесуэла.
9. 18 марта 2014 года он выпустил совместное заявление о событиях, которые стали причиной смерти китайского правозащитника.
10. 30 мая 2014 года он выпустил совместное заявление для печати о решении Совета Безопасности не передавать вопрос о положении в Сирийской Арабской Республике в Международный уголовный суд.
11. 12 июня 2014 года он выпустил заявление с призывом к правительству Мексики положить конец совершаемым в стране нарушениям права на жизнь.
12. 2 июля 2014 года совместно с другими мандатариями он обратился с призывом к правительству Шри-Ланки прекратить поощрять проявления ненависти по расовым и религиозным мотивам.
13. 4 июля 2014 года он выпустил совместное заявление, в котором обратился к правительству Непала с призывом внести изменения в законодательство об установлении истины, которое допускало возможность амнистирования виновных в случаях серьезного нарушения прав человека и гуманитарного права.
14. 8 августа 2014 года он выпустил совместное заявление с выражением глубокой озабоченности по поводу нарастания числа случаев ареста и тюремного заключения лиц в Исламской Республике Иран.
15. 12 августа 2014 года он выпустил совместное заявление с выражением обеспокоенности по поводу нависшей опасности массового уничтожения язидов и общин других меньшинств, подверженных нападениям со стороны "Исламского государства Ирака и Эш-Шама" (ИГИШ) в Ираке.
16. 29 сентября 2014 года он выпустил совместное заявление о возможном принятии законопроекта № 85 2013 года, направленного на реструктуризацию и расширение юрисдикции военных судов в Колумбии.
17. 29 сентября 2014 года он выпустил заявление, в котором настоятельно призвал правительство Мексики расследовать гибель 22 человек.
18. 10 октября 2014 года он выпустил совместное заявление с призывом к правительству Мексики расследовать исчезновение 43 студентов в штате Герреро.
19. 26 ноября 2014 года он выпустил совместное заявление с настоятельным призывом к президенту Соединенных Штатов Америки поддержать как можно более широкое опубликование доклада о методах допроса, применяемых Центральным разведывательным управлением.

---

<sup>1</sup> С пресс-релизами Специального докладчика можно ознакомиться по адресу [www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx?MID=SR\\_Summ\\_Executions](http://www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx?MID=SR_Summ_Executions).

20. 5 декабря 2014 года он выпустил совместное заявление о решениях большого жюри присяжных в Соединенных Штатах Америки не передавать в суд дела сотрудников полиции, причастных к двум резонансным убийствам.

21. 27 марта 2015 года он выпустил совместное заявление для печати с призывом к Испании выдать или привлечь к ответственности лиц, ответственных за нарушения прав человека.

22. В отчетный период Специальный докладчик также выпустил совместные заявления по вопросам смертной казни в Бангладеш, Египте, Индии, Индонезии, Иране (Исламской Республике), Пакистане, Саудовской Аравии, Соединенных Штатах Америки и Судане.

#### **D. Международные и национальные совещания**

23. Деятельность Специального докладчика в период с 26 марта по 22 июля 2014 года освещается в докладе, представленном Генеральной Ассамблее на ее шестьдесят девятой сессии (A/69/265).

24. 2 сентября 2014 Специальный докладчик выступил в Вене с заявлением по вопросу о смертной казни в Комитете по человеческому измерению Организации по безопасности и сотрудничеству в Европе.

25. 15 сентября 2014 года он выступил с лекцией об автономных системах оружия в Стелленбосском институте перспективных исследований в Южной Африке.

26. 18 и 19 сентября 2014 года он принимал участие в организованной Всемирной Организацией здравоохранения и Кембриджским университетом Глобальной конференции по снижению уровня насилия 2014 года в Королевском колледже, Кембридж, Соединенное Королевство Великобритании и Северной Ирландии.

27. 22 сентября 2014 года он участвовал в групповом обсуждении по теме "Обеспечение использования дистанционно-пилотируемых летательных аппаратов или ударных беспилотников в ходе контртеррористических и военных операций в соответствии с нормами международного права, включая международное право прав человека и международное гуманитарное право", которое было организовано Советом по правам человека в Женеве.

28. 25 сентября 2014 года он выступил в Осло на организованном парламентом Норвегии семинаре для парламентариев по вопросу применения беспилотников.

29. С 29 сентября по 3 октября 2014 года Специальный докладчик участвовал в 21-м ежегодном совещании мандатариев специальных процедур в Женеве.

30. 8 и 9 октября 2014 года он участвовал в международном рабочем совещании по теме "Укрепление сотрудничества между Организацией Объединенных Наций и региональными правозащитными механизмами", который был организован Управлением Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) в Женеве.

31. 20 октября 2014 года он принял участие в обсуждении, которое состоялась в Колумбийском университете, Нью-Йорк, под эгидой Института по правам человека Колумбийской юридической школы, "Rightlink", Института по изучению прав человека, факультета прав человека и гуманитарной политики

Школы международных отношений и публичной политики, а также журнала "Human Rights Law Review".

32. 10 и 11 ноября 2014 года он принимал участие в третьем Джакартском диалоге по проблеме прав человека, посвященном праву на жизнь и мораторию на смертную казнь в странах Ассоциации государств Юго-Восточной Азии (АСЕАН), который был организован УВКПЧ, Европейским союзом и представителем Индонезии в Межправительственной комиссии АСЕАН по правам человека в Джакарте.

33. 10 декабря 2014 года он выступил на презентации доклада *The War Report 2013: Armed Conflicts and their Consequences* ("Доклад о войнах 2013 года: вооруженные конфликты и их последствия") Женевской академией международного гуманитарного права и прав человека в Женеве.

34. 6 февраля 2015 года он выступил на девятом заседании Форума по вопросам безопасности, который был посвящен теме "От беспилотников к роботам-убийцам", и организован Вебстеровским университетом в сотрудничестве с Институтом Организации Объединенных Наций по исследованию проблем разоружения.

## II. Использование информационно-коммуникационных технологий в целях обеспечения права на жизнь

### A. История вопроса<sup>2</sup>

35. В силу того что многие нормы международного права, касающиеся права на жизнь, в основном урегулированы, работа по защите этого права часто связана со спорными фактами и даже с наличием фактов. Люди нарушают право на жизнь не потому, что считают это правомерным, а поскольку надеются, что им не придется оправдываться. Это придает повышенное значение деятельности по установлению фактов и доказательствам.

36. Поскольку для установления фактов требуются специальные знания и соответствующие специалисты, разработка методов правозащитной деятельности проходила в тесной увязке с профессионализацией правозащитной деятельности<sup>3</sup>. Этот поступательный процесс развивался в рамках так называемых трех поколений сообществ, занимающихся международным мониторингом в области прав человека, каждое из которых использовало свои собственные методы. Во-первых, действуя в интересах международных организаций, группа видных юристов планомерно производила обзор имеющейся информации; во-вторых, при ведущей роли крупных международных неправительственных организаций по правам человека (НПО) в области установления фактов произошли кардинальные изменения, резко расширив ее рамки, но сохранив зависимость такой деятельности от опроса свидетелей, который позволяет получать из первых рук

<sup>2</sup> Специальный докладчик выражает признательность Центру по вопросам управления и прав человека Кембриджского университета, и в частности Элле Макферсон и Томасу Проберту, за их ценную помощь в проведении исследований. В качестве одного из элементов этих исследований были обобщены описания многих обсуждавшихся программ и проектов, с которыми можно ознакомиться в интернете по адресу <http://ictandhr.tumblr.com/>.

<sup>3</sup> Molly K. Land, "Networked activism", *Harvard Human Rights Journal*, vol. 22 (2009), pp. 205–43.

очень подробные сведения, но может требовать много времени и страдать от внешнего вмешательства и необъективности при отборе свидетелей. С течением времени методология второго поколения нашла свое отражение в практике первого поколения, включая специальные процедуры Совета по правам человека. Однако сегодня в этой сфере вновь происходят изменения под влиянием все более широкого круга самых разных оснащенных цифровыми технологиями субъектов, т.е. третьего поколения, включая свидетелей, наблюдателей и активистов, проявляющих более гибкие подходы к установлению фактов и добывающихся более значительных результатов<sup>4</sup>. Каждое поколение расширяет круг участников расследований нарушений прав человека. Ни одно поколение не отвергло ранее проделанную работу, однако важно, что каждое из них может использовать сильные стороны других, не ставя под сомнение собственные возможности.

37. Стало очевидно, что информационно-коммуникационные технологии (ИКТ), т.е. аппаратное и программное обеспечение, которое облегчает сбор, передачу, получение, архивацию и хранение информации, способны играть все более значимую роль в защите всех прав человека, в том числе права на жизнь. Получаемая с их помощью информация может использоваться в целях привлечения виновных к ответственности, однако они могут также обеспечивать гласность или мобилизацию усилий на поддержку лиц, которым угрожает непосредственная опасность.

38. В своей повседневной работе по выявлению незаконных казней и оценке утверждений о таких казнях Специальный докладчик подобно многим другим участникам деятельности в этой области испытывает все большую зависимость от информации, получаемой с помощью упомянутой технологии. В качестве примера можно сослаться на использование видеозаписей с мобильных телефонов, сделанных во время гражданской войны в Шри-Ланке, для оказания на государство и международное сообщество давления в интересах проведения более обстоятельного расследования предполагаемых широкомасштабных нарушений многих прав человека, включая право на жизнь (A/HRC/17/28/Add.1). Аналогичным образом при подготовке доклада Совету по правам человека по вопросу о безопасности журналистов стало понятно, какую широкую известность приобрели журналисты из числа гражданских лиц и социальные сети благодаря использованию этих технологий для освещения и документирования нарушений в различных районах мира (A/HRC/20/22 и Согг.1).

39. Расширение цифрового потенциала во многом повышает способность простых людей участвовать в мониторинге прав человека. Цифровые ИКТ создают возможности для формирования плюрализма мнений, способного демократизировать процесс установления фактов в области прав человека, а также предоставляют механизмы социальной подотчетности, которыми могут пользоваться граждане для привлечения к ответственности государств и других субъектов<sup>5</sup>. Социальные сети раскрывают перед гражданами широкий диапазон возможностей для придания огласке засвидетельствованных ими нарушений прав человека, зачастую минуя официальные межправительственные или неправительственные структуры. Это имеет далеко идущие последствия для устойчивейшей структуры распределения ролей в мониторинге прав человека, по-

<sup>4</sup> Philip Alston "Introduction: third generation human rights fact-finding", *Proceedings of the Annual Meeting of the American Society of International Law*, vol.107 (April 2013), pp. 61–62.

<sup>5</sup> Molly K. Land and others, *#ICT4HR: Information and Communication Technologies for Human Rights* (World Bank Institute, 2012).

сколькx ныне в этой работе принимают участие как никогда широкое сообщество наблюдателей-правозащитников. При этом также открываются новые возможности в таких условиях, которые иначе не допускают контроля. В обстоятельствах, когда физическое присутствие лиц, занимающихся расследованием нарушений прав человека, может быть затруднено, разумное применение ИКТ может помочь восполнить недостаток информации о ситуациях, представляющих повышенный интерес для правозащитного сообщества.

40. Вместе с тем с точки зрения защиты прав человека развитие ИКТ не следует рассматривать как безусловное благо. В цифровом пространстве возможности государств для слежки за гражданским обществом и вмешательства в его деятельность многократно возрастают, и Совет должен проявлять осмотрительность по отношению к опасностям и возможностям ИКТ<sup>6</sup>. Применение технологий правозащитниками и другими лицами может подвергать их разнообразным рискам, которые многие могут не осознавать.

41. Для полной реализации потенциала ИКТ в интересах правозащитной деятельности необходимо разобрать вопрос о цифровом неравенстве с точки зрения доступа к технологиям и цифровой грамотности. С одной стороны, ИКТ способствуют развитию плюрализма в сфере правозащитной деятельности, позволяя начинающим дополнять профессионалов; но – с другой, они могут служить новыми факторами интеграции сообщества или его размежевания, которые зачастую соответствуют таким ранее существовавшим препятствиям для доступа к ресурсам и власти, как знание языка, образование, финансовое благополучие или пол<sup>7</sup>. Кроме того, давая шанс высказывать свое мнение, плюрализм также позволяет и быть услышанным. Возможность быть услышанным структурами, занимающимися установлением фактов в области прав человека, может зависеть от способности того или иного лица добывать поддающуюся проверке информацию, каковая в свою очередь определяется его цифровой грамотностью и цифровыми следами<sup>8</sup>. Наличие более доступной цифровой информации о нарушениях прав человека в том или ином отдельно взятом контексте и регионе может обернуться тем, что таким нарушениям будет уделяться больше внимания, нежели другим более вопиющим, но менее заметным нарушениям.

42. Вполне очевидно, что в случае их рационального использования ИКТ могут способствовать более надежной защите прав человека, включая право на жизнь. Различные элементы более широкой системы Организации Объединенных Наций уделяют все больше времени и ресурсов интегрированию потенциала ИКТ в рамках своих методов работы. Управление по координации гуманитарных вопросов и Департамент операций по поддержанию мира разрабатывают перспективные методики кризисного мониторинга и картографирования. Международный уголовный суд проанализировал свои подходы к рассмотрению цифровых доказательств. Тем не менее представляется, что полный потенциал таких новых инструментов до сих пор систематически не изучался и не

<sup>6</sup> Специальный докладчик отмечает, что на своей двадцать восьмой сессии Совет по правам человека постановил назначить специального докладчика по вопросу о праве на неприкосновенность личной жизни в цифровой век.

<sup>7</sup> A. Trevor Thrall, Dominik Stecula and Diana Sweet, "May we have your attention please? Human rights NGOs and the problem of global communication", *International Journal of Press/Politics*, vol. 19, No. 2 (April 2014), pp. 135–59.

<sup>8</sup> Ella McPherson, "Advocacy organizations' evaluation of social media information for NGO journalism: the evidence and engagement models", *American Behavioral Scientist*, vol. 59, No. 1 (July 2014), pp. 124–48.



освоен международным правозащитным сообществом (см. A/65/321, пункты 3–10).

43. В настоящем докладе Специальный докладчик показывает, в частности, какие возможности и трудности создают ИКТ для основных аспектов правозащитной деятельности, т.е. для поощрения, защиты и мониторинга прав человека либо для установления фактов с целью обеспечения подотчетности в случае совершения того или иного нарушения. Хотя влияние ИКТ и социальных сетей на правозащитную деятельность рассматривается в других материалах, оно будет вкратце освещено в настоящем докладе, равно как и роль технологии в упрощении мер физической защиты и обеспечения безопасности в цифровой среде, которые имеют важное значение в контексте его мандата. Специальный докладчик затем разберет вопрос об использовании ИКТ для сбора информации о нарушениях в целях усиления подотчетности и об исследовании существующих проблем, включая проблему проверки. Наконец Специальный докладчик рассмотрит, в какой мере цифровые доказательства используются в тех или иных компонентах международного механизма защиты прав человека.

## **В. Поощрение и пропаганда прав человека**

44. Расширение потенциала обмена информацией и поддержания связей открывает очевидные и уже широко используемые возможности для распространения информации о правах человека, как в порядке общего правозащитного просвещения, так и по линии целенаправленной информационно-пропагандистской работы в поддержку тех или иных законодательных изменений или политических преобразований, либо в интересах инициирования расследований по конкретным делам или привлечения к ответственности виновных. Правозащитные организации могут дополнять свои обычные стратегии поддержания связей по традиционным каналам прямыми обращениями к общественности.

45. Так, например, межправительственные и неправительственные организации, а также государства используют веб-сайты для донесения до как можно более широких кругов общественности информации о нормах и правовых стандартах в области прав человека. В своих предыдущих докладах Специальный докладчик подчеркнул важное значение четких и общедоступных правовых рамок для предупреждения произвольных казней в результате применения силы или смертных приговоров (A/HRC/26/36 и A/67/275)<sup>9</sup>. Благодаря ИКТ государства становятся заметно более открытыми для своего населения и международного сообщества.

46. Помимо распространения информации в цифровом формате многие правозащитные организации накопили опыт по оперативному использованию социальных сетей для прямых индивидуальных контактов с представителями общественности. За счет применения ИКТ могут быть открыты новые направления просветительской работы, которые способствуют формированию условий, благоприятствующих соблюдению прав человека. В Кении в рамках инициативы "PeaceTXT" зарегистрированным абонентам направлялись текстовые сообщения с призывами к укреплению мира с целью деэскалации потенциальных конфликтов. В других регионах НПО использовали методы съемки скрытой ка-

---

<sup>9</sup> См. также [www.use-of-force.info](http://www.use-of-force.info).

мерой для придания огласке проявлений крайней нетерпимости и преследований в интересах осведомления о них населения<sup>10</sup>.

47. Таким образом, цифровые ИКТ могут помочь в привлечении внимания к правам человека широкой общественности и, по крайней мере, пользователей социальных сетей. Такие приложения, как "Ai Candle" или "Pocket Protest", позволяют подписывать петиции, направлять сообщения по электронной почте или получать информацию о правах человека с помощью мобильных телефонов или смартфонов, которые особо полезны при возникновении потребности в срочной мобилизации<sup>11</sup>. Отправляемые послания могут быть расширены с использованием таких платформ, как "Thunderclap". В итоге, конечным результатом применения таких методов может стать ознакомление общественности с тем или иным конкретным случаем или проблемой<sup>12</sup>.

48. Остаются вопросы относительно того, позволяют ли упомянутые возможности заметно повысить эффективность информационно-пропагандистской деятельности. Информационные кампании соперничают за привлечение к себе внимания в условиях все более широкого распространения информации и, по крайней мере на начальном этапе, являются доступными только для тех, кто овладел навыками обращения с цифровой техникой<sup>13</sup>. Вместе с тем сжатость сообщений и культура общения в реальном времени в "Twitter" могут препятствовать освещению неоднозначных ситуаций или придавать ему упрощенный характер, а факторы мгновенного распространения информации могут быть плохо совместимы с правозащитными доказательствами<sup>14</sup>. Социальные сети доказали свою эффективность в расширение круга участников отчасти потому, что они снижают уровень необходимой для участия мотивации, что может привести к появлению бессодержательных или неустойчивых форм политической активности (так называемого "кликтивизма")<sup>15</sup>. Однако высказывались мнения, что такие на первый взгляд незначительные сдвиги в своей совокупности приобретают важное значение и способствуют созданию "благоприятной среды" и "повышению осведомленности"<sup>16</sup>.

### С. Предупреждение и защита

49. ИКТ можно различными способами использовать для предупреждения нарушений права на жизнь государственными или негосударственными субъек-

<sup>10</sup> Cynthia Romero, "What next? The quest to protect journalists and human rights defenders in a digital world", conference report, Freedom House, Mexico City, (February 2014), <https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf>.

<sup>11</sup> См. Amnesty International UK, "What is pocket protest?" (June 2013), [www.amnesty.org.uk/what-pocket-protest](http://www.amnesty.org.uk/what-pocket-protest).

<sup>12</sup> См. Jiva Manske "Case studies: concrete examples of compelling and strategic use of social media", *New Tactics in Human Rights* (9 May 2013), <https://www.newtactics.org/comment/6124>.

<sup>13</sup> Thrall, Stecula and Sweet, "May we have your attention please?" (см. чоксы 7).

<sup>14</sup> Dustin N. Sharp, "Human rights fact-finding and the reproduction of hierarchies" (6 June 2014), *Social Science Research Network*, <http://papers.ssrn.com/abstract=2341186>.

<sup>15</sup> Malcolm Gladwell, "Small change: why the revolution will not be tweeted", *The New Yorker* (4 October 2010), [www.newyorker.com/reporting/2010/10/04/101004fa\\_fact\\_gladwell](http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell).

<sup>16</sup> Stephanie Vie, "In defense of 'slacktivism': the Human Rights Campaign Facebook logo as digital activism", *First Monday*, vol. 19, No. 4 (April 2014), <http://firstmonday.org/ojs/index.php/fm/article/view/4961>.

тами. Во-первых, с помощью программ тревожной сигнализации может обеспечиваться физическая и цифровая защита потенциально уязвимых групп, включая правозащитников. Социальные сети используют преимущества цифровой связи, однако последняя сопряжена с риском для тех, кто уязвим по отношению к цифровой слежке или другим формам наблюдения. Во-вторых, ощущается потребность в проведении разъяснительной работы по вопросам цифровой безопасности и мер предосторожности. Однако наблюдение может также послужить превентивным механизмом, и ниже будут рассмотрены соответствующие тактические приемы – от потокового вещания о демонстрациях или полицейских операциях до использования спутниковых визуальных материалов.

## 1. Программные приложения тревожной сигнализации

50. Различные организации разрабатывают приложения тревожной сигнализации, которыми активисты, журналисты и прочие лица могут воспользоваться для подачи сигнала об угрожающей им опасности. Например, Международная амнистия разработала приложение "тревожная кнопка", закамуфлированное под обычную утилиту и позволяющее пользователям скрыто подать сигнал тревоги путем отправления текстового сообщения и, в качестве опции, данных геолокации, которые могут быть направлены заранее выбранным адресатам путем быстрого нажатия кнопки "питание" телефона. В случаях нападения на активистов или журналистов или их задержания у них часто отбирают телефоны для ознакомления с хранящимися в них списками абонентов. Скрытое приложение будет продолжать подавать сигналы тревоги, которые не только служат призывами о помощи, но и предупреждают абонентов задержанного о том, что им следует принять меры предосторожности<sup>17</sup>. С этой целью разрабатывались и другие приложения или устройства<sup>18</sup>.

51. Такие приложения дают возможность справиться с трудностями, которые возникают из-за недостатка информации или времени и могут ограничивать меры по защите находящихся в опасности лиц. По мнению практиков, полномасштабная реакция на задержание того или иного лица или на поступление в его адрес угрозы может быть наиболее эффективна в течение приблизительно 48 часов. По всему миру можно найти многочисленные примеры случаев, когда массовая реакция на задержание, скоординированная по социальным сетям или другими методами, заставила власти пересмотреть выгоды от ареста задержанного лица.

52. Таким образом новые технологии вписываются в более широкую и устойчивую практику установления контакта с надежной социальной сетью при возникновении угрозы или при необходимости мобилизации крупного сообщества на демонстративное выступление против произвольного акта в отношении того или иного лица. Однако важно помнить о потенциальных опасностях такой технологии, которая может использоваться для идентификации и сбора информации.

## 2. Важность цифровой информации

53. Предоставляя правозащитникам дополнительные возможности, ИКТ в то же время могут создавать целый ряд дополнительных рисков, и для их уменьшения лица, находящиеся под угрозой нарушений, включая правозащитников,

<sup>17</sup> См. <https://panicbutton.io/>.

<sup>18</sup> BBC News, "Smart bracelet protects aid workers" (5 April 2013), [www.bbc.com/news/technology-22038012](http://www.bbc.com/news/technology-22038012).

должны серьезно относиться к требованиям цифровой безопасности. К средствам ее обеспечения могут относиться приложения для сканирования компьютеров на предмет выявления шпионских программ или такие ресурсы, как "Security in-a-Box", а также линии помощи или форумы по вопросам цифровой безопасности<sup>19</sup>.

54. Активисты могут общаться в более надежно защищенных режимах, используя частные виртуальные сети, криптографические программы или браузер "Tor", предназначенный для повышения анонимности интернет-пользователей. Тем не менее, разработчики и инструкторы должны предупреждать пользователей о том, что в Интернете их неприкосновенность и анонимность никогда не может быть полностью гарантирована. Помимо этого, крупные международные межправительственные и неправительственные правозащитные организации должны также оценивать риски, связанные с незащищенностью в цифровом пространстве, в контексте их взаимодействия с небольшими организациями или отдельными лицами.

55. Оценка достоинств и недостатков режима защищенного цифрового кодирования напрямую не входит в мандат Специального докладчика. Однако в условиях поступления многочисленных требований о расследовании нарушений прав человека это, безусловно, составляет сложную проблему, вызывающую его, как мандатария, беспокойство в случаях, когда незащищенность цифровой связи является непосредственной причиной виктимизации, включая угрозы внесудебных казней или их совершение. Использование популярных платформ социальных сетей для обмена информацией по правам человека может ставить под угрозу безопасность "гражданских свидетелей" и лиц, о которых они дают показания.

### 3. Мониторинг в целях защиты

56. Распространение практики наблюдения и документирования информации с помощью ИКТ не только во многом расширяет возможности привлечения к ответственности отдельных лиц, о чем будет сказано ниже, но и предотвращает совершение нарушений. Осведомленность о том, что ведется наблюдение, может иметь действенный сдерживающий эффект в случае ее подкрепления сознанием неотвратимости ответственности, как это видно на примере использования телевизионных систем наблюдения замкнутого типа для предотвращения преступлений. Вера в такой сдерживающий эффект настолько сильна, что в стремлении не допустить своего ареста или похищения некоторые активисты, как стало известно, делали вид, что ведут съемку происходящего, хотя батарейка их телефона села<sup>20</sup>.

57. Пожалуй, наиболее убедительным примером сказанного, который относится к сфере основных интересов Специального докладчика, поскольку касается чрезмерного применения силы сотрудниками правоохранительных органов, является использование полицейскими нательных камер. Недавно проведенное в Калифорнии, Соединенные Штаты Америки, исследование по вопро-

<sup>19</sup> Ресурсы, предоставляемые через такие программы, как "New Tactics in Human Rights" ("Новая тактика в области прав человека") ([www.newtactics.org](http://www.newtactics.org)) служат площадкой для обмена в диалоговом режиме знаниями о различных аспектах правозащитной деятельности, в том числе о цифровой безопасности.

<sup>20</sup> Stephanie Hankey and Daniel Ó Clunaigh, "Rethinking risk and security of human rights defenders in the digital age", *Journal of Human Rights Practice*, vol.5, No. 3 (November 2013), p. 543.

сам использования такой аппаратуры показало, что после оснащения полицейских такими камерами применения ими силы сократились на 59%, а число жалоб на применение чрезмерной силы упало почти на 90%<sup>21</sup>. В Бразилии, Кении и Южной Африке осуществляются другие экспериментальные проекты, связанные с использованием смартфонов в качестве нательных камер с функциями передачи видео-, аудио- и геолокационной информации<sup>22</sup>.

58. Подобно тому, как превентивное воздействие замкнутых телевизионных систем достигает наибольшего эффекта, когда известно об их существовании, по мнению некоторых, нательные камеры предотвращают противоправные действия, поскольку порядок их применения определяется регламентами, согласно которым полиция обязана предупреждать о видеозаписи происходящего, в результате чего и полицейские и гражданские лица сознают, что за ними ведется наблюдение<sup>23</sup>.

59. Существуют опасения по поводу возможных нарушений права на неприкосновенность частной жизни вследствие использования нательных камер, в связи с которыми их предлагается отключать при входе в дом или при беседе с жертвами. Другие считают, что сотрудники полиции не должны самостоятельно контролировать работу своих камер, что позволит сократить возможности для выборочной регистрации событий<sup>24</sup>. Определенная обеспокоенность выражается и в отношении доступа к отснятому материалу и его ответственного хранения. Хотя эти вопросы пока остаются без ответа, многие считают, что сдерживающее воздействие нательных камер сотрудников полиции оправдывает их дальнейшее использование<sup>25</sup>. Проблема потенциальных преимуществ видеозаписи полицией своих собственных действий связана с не менее важной темой защиты права граждан на регистрацию действий полиции.

60. Если с одной стороны нательные камеры позволяют осуществлять наблюдение на микро уровне межличностного взаимодействия, то с другой стороны существенные возможности для наблюдения открывают дистанционно-управляемые системы видеозаписи со спутников или беспилотников. Такие инициативы, как проект "Satellite Sentinels" ("Спутниковые часовые") и организованная Международной амнистией компания "Eyes on Darfur" ("Взгляд на Дарфур") высветили потенциал таких механизмов. Повышение осведомленности возможных правонарушителей о том, что уязвимые места взяты под наблю-

<sup>21</sup> Barak Ariel, William A. Farrar and Alex Sutherland, "The effect of police body-worn cameras on use of force and citizens' complaints against the police: a randomized controlled trial", *Journal of Quantitative Criminology* (November 2014).

<sup>22</sup> Graham Denyer Willis and others, "Smarter policing: tracking the influence of new information technology in Rio de Janeiro", *Igarapé Institute Strategic Note 10* (November 2013); see also the Smart Policing initiative, <http://en.igarape.org.br/smart-policing/>.

<sup>23</sup> Пожалуй, наиболее убедительно об эффекте осознания слежки писал Джереми Бентам, однако его криминологические последствия, а также потенциальная опасность до последнего времени не были реализованы в технологическом отношении.

<sup>24</sup> Bracken Stockley "Public support for police body cameras – but who controls on/off switch?" *The justice gap* (March 2014), <http://thejusticegap.com/2014/03/body-worn-video-cameras-scrutiny/>.

<sup>25</sup> Robert Muggah, "Why police body cameras are taking off, even after Eric Garner's death", *IPI Global Observatory* (11 December 2014), <http://theglobalobservatory.org/2014/12/police-body-cameras-eric-garner/>; см. также Alexandra Mateescu, Alex Rosenblat and Danah Boyd, "Police body-worn cameras", *Data & Society Research Institute Working Paper* (February 2015), [www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf](http://www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf).

дение, может предотвратить противоправные действия или, по крайней мере, те из них, которые можно наблюдать дистанционно<sup>26</sup>. Однако такое наблюдение связано с большими затратами и может быть сопряжено с довольно произвольными решениями при выборе в качестве объекта наблюдения тех или иных конкретных общин или мест. Как и при других методах наблюдения сдерживающее воздействие упомянутой техники объясняется как знаниями о ее существовании (повышая важность параллельного информационно-пропагандистского сопровождения в СМИ), так и реальной угрозой наказания<sup>27</sup>.

61. Такие методы наблюдения задействуют угрозу будущего наказания для корректировки поведения в текущий момент. Возможно также и применение ИКТ для использования информации о случившемся в (недавнем) прошлом для воздействия на происходящее. Анализ работы социальных сетей может помочь прогнозированию всплеск нарушений прав человека в реальном времени. Так, например, база данных "Hate base" осуществляет сбор информации о лексическом составе и частотности ненавистнических заявлений в социальных сетях путем соотнесения ненавистнических заявлений с угрозами геноцида и применяется для прогнозирования региональных очагов насилия<sup>28</sup>.

62. Однако подобно системам раннего предупреждения ИКТ имеют и свои ограничения. Хотя, как показывает практика, "сбор больших данных", т.е. крупных массивов информации с успехом используется для прогнозирования и предотвращения конфликтов, этот метод менее эффективен для анализа и передачи информации, предназначенной для принятия конкретных мер<sup>29</sup>.

63. Работа по анализу больших данных и дистанционному наблюдению, направленная на предотвращение нарушений прав человека, связана также с вопросами методологического и этического порядка. Так, например, дистанционная съемка может поставить под угрозу уязвимые группы населения с точки зрения распознавания их местонахождения и состояния<sup>30</sup>. Кроме того, при статистическом анализе данных о правах человека могут возникнуть определенные неточности вследствие необъективности выборки, дублирования данных и трудностей с их сбором<sup>31</sup>.

#### 4. Обеспечение должной осмотрительности в цифровом пространстве

64. Практика наблюдения с целью предотвращения нарушений прав человека может быть настолько эффективна, что обладающие соответствующим потенциалом государства просто обязаны ее применять. Камеры устанавливаются в полицейских автомобилях и в помещениях для допросов, но при этом может

<sup>26</sup> Nathaniel A. Raymond and others, "While we watched: assessing the impact of the satellite sentinel project", *Georgetown Journal of International Affairs* (26 July 2013), <http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/>.

<sup>27</sup> Patrick Meier, "Will using 'live' satellite imagery to prevent war in the Sudan actually work?" *iRevolutions* (30 December 2010), <http://irevolution.net/2010/12/30/sat-sentinel-project/>.

<sup>28</sup> См. <http://www.hatebase.org/>.

<sup>29</sup> Sheldon Himelfarb, "Can big data stop wars before they happen?" (United States Institute of Peace, 25 April 2014), [www.usip.org/publications/can-big-data-stop-wars-they-happen](http://www.usip.org/publications/can-big-data-stop-wars-they-happen).

<sup>30</sup> См., например, проект Гарвардской гуманитарной инициативы "The Signal Program on Human Security and Technology" (2013), <http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program>.

<sup>31</sup> См. материалы о работе Группы по анализу данных о правах человека по адресу <https://hrdag.org/coreconcepts/>.

быть рассмотрена возможность их использования и в других условиях, в которых такое наблюдение может оказывать превентивное воздействие (например, в тюрьмах), с учетом ограничений, возникающих в связи с осуществлением других прав, в частности права на неприкосновенность частной жизни.

65. В интересах выполнения своих обязанностей, связанных с предупреждением нарушений или проведением профилактических мероприятий, государства могут прибегать и к другим возможностям ИКТ. В частности, государства применяли текстовые сообщения или телефонные звонки для предупреждения гражданского населения о воздушных налетах. Установленные на некоторых современных видах оружия записывающие устройства позволяют повышать эффективность наблюдения, однако в этой связи необходимо обеспечивать более значительную транспарентность.

66. Вместе с тем обязанность проявлять должную осмотрительность в цифровом пространстве распространяется не только на государства. Организациям, осуществляющим мониторинг прав человека, включая межправительственные и неправительственные организации, следует ответственно относиться к последствиям их переписки или использования информации. При этом, вероятно, уместно было бы пересмотреть традиционное толкование концепции "осознанного согласия".

## **D. Мониторинг и установление фактов**

67. Как было указано выше, в силу особого характера нарушений, подпадающих под действие настоящего мандата, первостепенное значение приобретает деятельность по установлению фактов. Правозащитные организации разработали строгие методики установления фактов, причем не в последнюю очередь для защиты достоверности своих доказательств, а соответственно и своей репутации. ИКТ и генерируемый пользователями с их помощью контент расширяют и демократизируют процесс установления фактов за счет увеличения возможностей случайных и специально опрашиваемых "гражданских свидетелей". В этой связи наиболее сложным аспектом является поддержание баланса между демократизацией и неизменной, возможно завышенной, потребностью в контроле и соответственно в проверке цифровых доказательств.

### **1. Гражданские свидетели и видеодоказательства**

68. За несколько десятилетий, по крайней мере со времени произошедшего в начале 1990-х годов инцидента с Родни Кингом, активисты оценили преимущества видеодоказательств. Записи с камер замкнутых частных телевизионных систем стали повсеместно применяться в целях проведения публичных расследований<sup>32</sup>. На международном уровне обвинительное заключение по делу Тома Лубанги, которое вынес Международный уголовный суд, принявший в качестве доказательства видеозапись допросов детей-солдат, принудительно набранных в его военизированные отряды, продемонстрировало, что видеозаписи могут использоваться для восполнения пробелов в доказательной базе<sup>33</sup>. Разумеется,

<sup>32</sup> См., например: Daoud Kuttab, "Video technology exposing Israeli violations in the West Bank", *Al-Monitor* (8 July 2014), [www.al-monitor.com/pulse/originals/2014/07/israel-palestine-cctv-camera-footage-occupation-settlers.html](http://www.al-monitor.com/pulse/originals/2014/07/israel-palestine-cctv-camera-footage-occupation-settlers.html).

<sup>33</sup> Matthew Shaer, "The media doesn't care what happens here: can amateur journalism bring justice to Rio's favelas?" *The New York Times* (18 February 2015), [www.nytimes.com/2015/02/22/magazine/the-media-doesnt-care-what-happens-here.html](http://www.nytimes.com/2015/02/22/magazine/the-media-doesnt-care-what-happens-here.html).

такие сведения могут быть получены не только от свидетелей нарушений или пострадавших от них лиц, но и от правонарушителей. Кроме того, эффективное использование информации в целях расследования нарушений прав человека не обязательно требует ее обнародования.

69. Поскольку информация гражданских свидетелей всегда служила основой работы по установлению фактов в области прав человека, ею традиционно занимались специалисты. В частности, они сами либо их доверенные лица обычно присутствуют при опросе свидетелей и передаче их информации миссии по установлению фактов. ИКТ позволяют гражданским свидетелям анонимно получать и сообщать информацию.

70. В самых непредвиденных обстоятельствах гражданские свидетели могут собирать информацию с помощью общедоступных потребительских устройств или платформ. Повсеместное использование смартфонов позволяет осуществлять видео- и аудиозапись, которая может быть легко передана по таким цифровым каналам, как платформы социальных сетей. Преимущество таких методов сбора и передачи информации состоит в том, что они не требуют каких-либо конкретных специальных знаний; в свою очередь их недостаток заключается в том, что они могут ограничивать объем метаданных (например, об источнике, месте и времени сбора данных), которые могут быть полезны для проверки информации. В то же время такие приложения, как "Informa Cam" и "Eye Witness" разработаны специально для дополнения метаданных, сопровождающих фото- и видеоматериалы, а также для отслеживания цепочки их передачи<sup>34</sup>.

71. Целый ряд НПО в настоящее время уже организовали учебные курсы для гражданских свидетелей и инструкторов по вопросам сбора и передачи материалов повышенной доказательной ценности. Такую работу на общемировом или региональном уровне проводят "WITNESS", Международная амнистия, "Tactical Tech" и инициатива "Справедливость в открытом обществе". В рамках такой подготовки могут затрагиваться как вопросы личной защиты, касающиеся цифровой безопасности, о которой говорилось выше, так и практическая информация о том, на какие именно детали следует обращать внимание при свидетельской видеозаписи (например, номерные знаки автомобилей, номера на форменной одежде или особые приметы местности), а также о методах обмена этими сведениями<sup>35</sup>.

## 2. Информация, полученная на основе "краудсорсинга"

72. Промежуточное место между традиционными методами получения сведений путем опроса гражданских свидетелей и спонтанным сбором и передачей информации такими свидетелями занимают методы "краудсорсинга" и "краудсиндинга". "Краудсорсинг" подразумевает возложение задач на не оговоренную конкретными параметрами крупную группу лиц, набранных посредством открытого призыва, которая, однако, необязательно является репрезентативной, поскольку при таком наборе предпочтение отдается лицам, обладающим такими ресурсами, как технологии, деньги и время. В свою очередь "краудсиндинг" является определенной формой лимитированного "краудсорсинга", в рамках которого допускается формирование репрезентативной выборки

<sup>34</sup> См. информацию о Informacam, <https://guardianproject.info/informa/>; и New Perimeter, "eyeWitness to atrocities", [www.newperimeter.org/our-work/access-to-justice/eyeWitness.html](http://www.newperimeter.org/our-work/access-to-justice/eyeWitness.html).

<sup>35</sup> См., например: Kelly Matheson, "Video as evidence: basic practices", *Witness blog* (16 February 2015), <http://blog.witness.org/2015/02/video-as-evidence-basic-practices/>.



методом случайного отбора участников, которые обеспечиваются необходимой техникой и средствами для сбора информации. Со временем между отобранными свидетелями и проектом устанавливаются определенные взаимоотношения со всей присущей им правдивостью и доверием<sup>36</sup>.

73. Помимо потенциального расширения рамок правозащитной деятельности привлечение гражданских свидетелей как единой массы людей может повысить действенность правозащитной пропаганды за счет увеличения круга участников и повышения их осведомленности, а также возможного сотрудничества<sup>37</sup>. При этом, однако, возникают определенные риски. Обнародуя информацию в привязке к конкретной местности, такие свидетели могут подвергаться опасности уязвимые группы населения. Эти методы могут также использоваться и против правозащитного сообщества, например для выполнения задач по сбору информации путем сопоставления лиц с фотографиями акций протеста<sup>38</sup>.

### 3. Спутниковые данные, используемые в качестве доказательств

74. Применение спутниковых записей может внести определенные изменения в правозащитную деятельность. В основе сдерживающего эффекта спутников лежит понимание того, что в случае совершения какого-либо нарушения, кто-то сможет использовать такую запись для его выявления. Так, например, в начале текущего года сотрудники Международной амнистии и "Хьюман Райтс Уотч", занимающиеся установлением фактов, проанализировали спутниковые изображения двух городов в северо-восточной части Нигерии с целью выявления произошедших изменений, и определили, что они сильно пострадали от пожаров. Эта информация была сопоставлена с показаниями свидетелей, и было установлено, что пожары возникли в ходе вооруженных нападений, в результате которых были убиты сотни человек. Хотя выявление такой взаимосвязи было важным, поскольку сами по себе спутниковые изображения мало помогают в установлении вины и причинно-следственных связей, данный случай подтверждает преимущества дистанционного наблюдения за труднодоступными районами<sup>39</sup>.

75. Полученные с помощью спутников доказательства можно сочетать с другими цифровыми процессами, например с анализом социальных сетей, для более эффективного донесения информации. Доклады о происхождении ракетных или артиллерийских ударов или о последствиях бомбардировок с беспилотников составлялись на основе спутниковых снимков<sup>40</sup>.

<sup>36</sup> Patrick Meier, "From crowdsourcing crisis information to crowdseeding conflict zones (updated)", *iRevolutions* (10 July 2012), <http://irevolution.net/2012/07/10/crowdsourcing-to-crowdseeding/>.

<sup>37</sup> Molly Beutz Land, "Peer producing human rights", *Alberta Law Review*, vol. 46, No. 4 (2009), p. 1115.

<sup>38</sup> Jonathan Zittrain, "The Internet creates a new kind of sweatshop", *Newsweek* (7 December 2009), [www.newsweek.com/internet-creates-new-kind-sweatshop-75751](http://www.newsweek.com/internet-creates-new-kind-sweatshop-75751).

<sup>39</sup> Christoph Koettl, "The story behind the Boko Haram satellite images", *Amnesty International UK/Blogs* (17 January 2015), [www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satellite-images](http://www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satellite-images).

<sup>40</sup> Bellingscat, "Origin of artillery attacks on Ukrainian military positions in Eastern Ukraine between 14 July 2014 and 8 August 2014" (17 February 2015), [www.bellingscat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/](http://www.bellingscat.com/news/uk-and-europe/2015/02/17/origin-of-artillery-attacks/); and Forensic Architecture, "Drone strikes: investigating covert operations through spatial media", [www.forensic-architecture.org/case/drone-strikes/](http://www.forensic-architecture.org/case/drone-strikes/).

76. В настоящее время большая часть спутниковых видеоматериалов, используемых в правозащитной деятельности, принадлежит коммерческим операторам. Это означает, что для их получения искомый район должен представлять коммерческий интерес, и в нем должна отсутствовать облачность; кроме того, такие снимки, как правило, имеют низкое разрешение. Спутниковые изображения военного назначения имеют более широкий угол охвата и более высокое разрешение, однако правозащитные расследователи зачастую наталкиваются на нежелание обмениваться с ними этой информацией (а не самими засекреченными изображениями), даже при отсутствии угрозы национальной безопасности.

## **Е. Оценка доказательств, собранных с использованием информационно-коммуникационных технологий**

77. Обильная информация, сообщаемая гражданскими свидетелями, может представлять доказательную ценность лишь при возможности ее обобщения и оценки. Поэтому важно, чтобы правозащитные организации могли интегрировать эту информацию в рамках своих традиционных методов проведения исследований и анализа, особенно с учетом значимости достоверности сообщаемых данных. Однако оценка получаемого от гражданских свидетелей цифрового контента может быть сопряжена с определенными трудностями, в том числе в отношении выявления представляющей интерес информации, ее проверки и хранения. Эти проблемы могут быть решены с помощью разработки новых технологий и совершенствования методов оценки информации.

### **1. Проблема объема данных**

78. Нарастание объемов поступления информации от гражданских свидетелей, собираемой и передаваемой с помощью цифровых технологий, означает, что выявление представляющих интерес данных может стать непосильной задачей. Одним из промежуточных шагов на этом пути может быть использование социальных сетей для фильтрации сведений методом "краудсорсинга", однако велика вероятность возникновения потребности в задействовании аналитических возможностей цифровых ИКТ для решения создаваемой ими же проблемы "коэффициента помех". Один из способов может состоять в автоматизированном просеивании больших массивов данных, содержащих потенциально значимую информацию. Так, например, платформа "CrisisNET" предназначена для сбора и стандартизации получаемых в режиме реального времени цифровых данных о кризисах из тысяч источников, что позволяет исследователям оперативно и эффективно осуществлять поиск<sup>41</sup>. Хотя машины не могут заменить человеческие знания и опыт при анализе правозащитной информации, поскольку оценка доказательной ценности информации в конечном итоге является субъективным актом, технологии способны помочь структурам, занимающимся мониторингом прав человека, сосредоточиться на наиболее важном материале. Эти вопросы требуют дальнейшего изучения.

79. Вероятно всегда будет существовать потребность в отборе цифрового контента для целей мониторинга и использования широким кругом заинтересованных сторон. Такой отбор будет состоять в сочетании автоматизированных и традиционных методов установления фактов или их проверки. Успешным примером в этом отношении может служить правозащитный канал "WITNESS",

<sup>41</sup> См. <http://crisis.net/about/>.

использующий материалы, которые проверяются в сотрудничестве с новостным агентством социальных сетей "Storyful".

## 2. Проблема быстротечности

80. Поскольку большинство материалов, представляющих интерес для проведения расследований в области прав человека, могут быть доступны в онлайн-режиме только ограниченное количество времени (из-за оказания на аплоудера или на платформу давления с целью воспрепятствования размещению определенного контента)<sup>42</sup>, весьма важно, чтобы занимающиеся расследованиями структуры были способны получать и надежно сохранять всю нужную им информацию. В этой связи приоритетной задачей становится разработка инструктивных материалов для национальных следственных органов и структур, осуществляющих мониторинг прав человека<sup>43</sup>.

81. Хранение материалов для организаций, занимающихся правозащитными расследованиями, может создавать угрозу для безопасности активистов. Такие приложения, как "Eyewitness" и "International Evidence Locker" разработаны с той целью, чтобы свидетели могли загружать доказательства в облачное файловое хранилище и использовать либо удалять их по своему усмотрению в зависимости от обстоятельств. Такие приложения также позволяют осуществлять безопасную передачу информации целевым аудиториям, сохраняя при этом метаданные информации, а также саму информацию. Тем не менее, жизненно важное значение по-прежнему будет иметь сотрудничество между проводящими расследования структурами и техническими корпорациями.

## 3. Проблема проверки

82. Хотя проверку иногда считают основным препятствием для использования цифровых доказательств, проблема проверки отнюдь не нова: она связана со стандартным нормативно-закрепленным требованием о подтверждении надежности источника и точности сообщаемых им сведений прежде, чем по ним будет принято решение или поставлена на кон репутация. В то время как характер проверяемой информации и используемые для проверки конкретные методы претерпевают быстрые изменения по мере развития ИКТ, основные элементы проверки остаются неизменными: идентификация и подтверждение контента, а также происхождения полученной информации.

83. Проверка обычно предполагает установление происхождения, источника, времени и места получения данной информации, а также цепочки ее передачи. Лица, занимающиеся установлением фактов, должны тщательно идентифицировать источник, проанализировать файл индексов метаданных, затем перепроверить их в сопоставлении с другими источниками. В настоящее время складывается новый комплекс методов, зачастую именуемый информационной криминалистикой, однако подобно традиционным расследованиям многие элементы этого процесса все еще предполагают участие специалистов и проведение доскональных проверок.

<sup>42</sup> Madeleine Bair, "Navigating the ethics of citizen video: the case of a sexual assault in Egypt", *Arab Media & Society*, vol. 19, (2014), <http://arabmediasociety.com/?article=844>.

<sup>43</sup> С имеющимися ресурсами, которыми могут руководствоваться активисты при архивировании своих материалов, можно ознакомиться, например, по адресу <http://archiveguide.witness.org/>. Канцелярия Прокурора Международного уголовного суда в настоящее время завершает подготовку руководящих материалов для расследователей.

84. Свидетель может сообщить сведения о времени, месте и контенте в ходе опроса или включить такие данные в файл. Согласно ранее применявшейся методике особое внимание уделялось важности сочетания сильных сторон второго и третьего поколений методологии установления фактов, а также тому, насколько источники информации одного поколения могут повысить достоверность источников другого, как на этапе сбора данных, например путем озвучивания места и даты события, так и в процессе передачи сведений. Информацию можно также получать путем анализа наземных ориентиров (например, дорожных знаков или геологических особенностей местности), погодных условий, одежды, оружия или диалекта, сведения о которых записаны в цифровой файл, либо выявлять ее на основе метаданных, которые автоматически заносятся в файл, как, например, временная метка. Такую информацию можно подтверждать и перепроверять путем сопоставления с другими цифровыми файлами и доказательствами, включая спутниковые видеоматериалы. Несколько видеозаписей одного и того же инцидента могут быть синхронизированы по времени для составления снятого с разных точек хронологического видеоряда<sup>44</sup>.

85. Ширится признание потребности в специальных знаниях о проверке цифровых данных. Чем более обширными знаниями по информационной криминалистике обладают занимающиеся установлением фактов правозащитники, тем более уверенно и оперативно они могут пользоваться цифровой информацией гражданских свидетелей. Изданный в 2014 году справочник "Verification Handbook" ("Справочник по проверке") быстро стал руководством для структур, занимающихся установлением фактов в гуманитарной и правозащитной областях<sup>45</sup>.

86. Углубление знаний гражданских свидетелей о проверке может облегчить ее процесс. Так, например, "WITNESS" дает рекомендации относительно того, какую именно информацию следует включать в видеозаписи нарушений прав человека<sup>46</sup>.

87. Еще одним направлением работы по упрощению проверки являются инициативы, направленные на облегчение процессов представления информации для целей ее проверки или на оценку такой информации. Такие инициативы упоминались как "вспомогательные компоненты проверки" и могут предусматривать участие людей или задействование специально разработанных технологий<sup>47</sup>. Такие приложения, как "InformaCam" позволяют в автоматическом режиме добавлять верификационные метки на стадии сбора информации и ускоряют их включение во время передачи сведений. Помимо этого ретроспективным образом может задействоваться потенциал больших групп, как, например, это делается с помощью платформы "Veri.ly"<sup>48</sup>. Кроме того, разработанная специально

<sup>44</sup> См., например, the Rashomon Project, <http://rieff.ieor.berkeley.edu/rashomon/about-rashomon/>.

<sup>45</sup> Craig Silverman (ed.) *Verification Handbook: An ultimate guideline on digital age sourcing for emergency coverage* (European Journalism Centre, 2014), <http://verificationhandbook.com/>.

<sup>46</sup> См.: "A field guide to enhancing the evidentiary value of video for human rights", <http://verificationhandbook.com/book/appendix.php>.

<sup>47</sup> Ella McPherson, "Digital civilian witnesses of human rights violations: easing the tension between pluralism and verification at human rights organizations" in Lind (ed.), *Producing Theory 2.0: The Intersection of Audiences and Production in a Digital World*, vol. 2 (forthcoming 2015).

<sup>48</sup> См. Victor Naroditskiy, "Veri.ly – getting the facts straight during humanitarian disasters", (August 2014), [www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitarian-disasters](http://www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitarian-disasters).

для индивидуальных новостных студий платформа "Checkdesk" позволяет проводить перекрестную и транспарентную проверку среди членов ограниченной группы.

88. Если технические трудности проверки не следует переоценивать, то ее важность невозможно переоценить. Использование правозащитной организацией непроверенных материалов может подорвать к ней доверие, но и ложные слухи могут также стать причиной возникновения взрывоопасных ситуаций, так называемых "цифровых пожаров", способных вылиться в проявления насилия<sup>49</sup>. Во многих странах уже действуют законы об ограничении свободы выражения мнений по таким мотивам, как подстрекательство к насилию или возбуждение паники, однако в настоящее время эти государства ищут способы эффективного применения таких законов по отношению к деятельности в виртуальном пространстве. Любое регулирование в этой сфере будет всегда оставаться многосложным и противоречивым; предлагалось, чтобы этот пробел восполнило само виртуальное сообщество при ведущей роли его кураторов и модераторов<sup>50</sup>. Специальный докладчик по вопросу о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости в 2014 году докладывал Совету по правам человека о том, что при выполнении своего мандата он сталкивается с комплексными проблемами, связанными с использованием Интернета и социальных сетей (A/HRC/26/49). Обратив внимание на политику некоторых ведущих сайтов социальных сетей, он также подчеркнул важность инициатив гражданского общества.

#### 4. Использование цифровых доказательств

89. Большинство сведений, которые можно получить по вышеупомянутым потоковым каналам, являются "данными общего назначения", однако их значимость для расследования нарушений прав человека не всегда удается сразу оценить. Кроме того, важно не заикливаться на видеоматериалах, поскольку многое можно подчерпнуть из блогов и микроблогов, к которым можно прибегать для подтверждения информации из других источников.

90. Вспомогательные компоненты проверки могут ускорить ее процесс, однако их применение требует наличия у лиц, занимающихся установлением фактов по правам человека, и гражданских свидетелей цифровой грамотности. Непонятно, каким образом знания об эффективном, безопасном и этичном сборе и передаче информации для использования ее в качестве доказательств будут распространяться среди гражданских свидетелей, особенно среди тех, которые действуют на самом деле спонтанно. Заблаговременные меры по подготовке лиц, занимающихся мониторингом прав человека, помогут подготовленным активистам, но зачастую действительно информативные материалы поступают от случайных свидетелей.

91. По этой причине такие организации, как "WITNESS" выступают за стандартное включение режима "eyewitness" ("свидетель") или ("proof") "доказательство", по подобию "InformaCam", в фото- и видеоприложения, устанавлива-

<sup>49</sup> Этот вопрос был затронут в докладе Всемирного экономического форума "Global Risks" ("Глобальные риски"), 8-е издание (2013 год), стр. 23–27 издания на английском языке.

<sup>50</sup> См. Lee Howell, "Only you can prevent digital wildfires" (8 January 2013), [www.nytimes.com/2013/01/09/opinion/only-you-can-prevent-digital-wildfires.html](http://www.nytimes.com/2013/01/09/opinion/only-you-can-prevent-digital-wildfires.html).

емые в смартфоны и платформы социальных сетей<sup>51</sup>. Интеграция этих функций в наиболее популярные приложения и платформы означает, что гражданские свидетели, скорее всего, будут о них знать и пользоваться ими.

## **Е. Использование информационно-коммуникационных технологий правозащитными механизмами**

92. В настоящем докладе выше шла речь о возможностях применения ИКТ в рамках общей правозащитной деятельности, а не об их использовании международными механизмами по защите прав человека. Важно чтобы международное сообщество было открыто по отношению к этим методологиям, поскольку в противном случае правозащитные организации и гражданские свидетели столкнутся с трудностями в полноценном использовании существующих механизмов обеспечения подотчетности. Как указывалось выше, полученные с помощью применения технологий доказательства не должны рассматриваться как окончательная цель, поскольку без эффективной подотчетности они останутся пустыми словами, и поэтому крайне важно, чтобы официальные каналы, предназначенные для содействия привлечению к ответственности за нарушения прав человека, были открыты для такого вида доказательств.

93. Более широкое сообщество Организации Объединенных Наций вкладывается в освоение потенциала ИКТ, особенно в области распространения информации в кризисных ситуациях (A/69/517). Управление информационно-коммуникационных технологий Организации Объединенных Наций в сотрудничестве с Фондом за использование ИКТ во имя мира координировали деятельность Консультативной группы по вопросам распространения информации в кризисной ситуации, которая стала форумом для обсуждения технологических новшеств в области управления гуманитарной помощью и распространения информации о кризисах<sup>52</sup>. Управление по координации гуманитарных вопросов (УКГВ) изучило влияние использующих ИКТ сетей по оказанию чрезвычайной гуманитарной помощи и с тех пор осуществило целый ряд совместных проектов по задействованию потенциала групп населения<sup>53</sup>. Следует также отметить, что проект "Global Pulse" ("Глобальный пульс") осуществляется как крупная программа по изучению гуманитарных последствий использования больших данных<sup>54</sup>.

94. В 2014 году Департамент операций по поддержанию мира просил Группу экспертов по технологиям и инновационной деятельности в рамках миссий Организации Объединенных Наций по поддержанию мира дать рекомендации относительно путей повышения их оперативной эффективности на основе технологий и инноваций. В феврале 2015 года Группа опубликовала свой окончательный доклад<sup>55</sup>, в котором, в частности, рекомендовала Совету Безопасности организовать специальную техническую миссию с целью использования технологий аудио- и видеозаписи, мониторинга и наблюдения в интересах информационного обеспечения процессов принятия решений.

<sup>51</sup> Sam Gregory "How an Eyewitness mode helps activists (and others) be trusted", *WITNESS Blog* (3 March 2014), <http://blog.witness.org/2014/03/eyewitness-mode-helps-activists/>.

<sup>52</sup> См. <http://ict4peace.org/crisis-information-management-advisory-group-cimag-retreat/>.

<sup>53</sup> OCHA Policy and Studies Series, *Humanitarianism in the Network Age: including world humanitarian data and trends 2012*, (2013), <https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf>.

<sup>54</sup> См. <http://www.unglobalpulse.org/>.

<sup>55</sup> См. <http://www.performancepeacekeeping.org/offline/download.pdf>.

95. Правозащитные механизмы Организации Объединенных Наций полностью не упускали из виду достижения в области ИКТ. Некоторые из них с успехом создали собственные платформы в социальных сетях в контексте информационно-пропагандистских стратегий и кампаний, ориентированных на миллионы пользователей по всему миру. Не умаляя важности ИКТ для пропагандистской работы, Специальный докладчик далее рассмотрит вопрос о привлечении различных международных и региональных правозащитных механизмов к использованию ИКТ для установления фактов и обеспечения подотчетности.

#### **1. Специальные процедуры и другие механизмы Совета по правам человека**

96. Настоящий доклад отчасти был составлен по итогам изучения Специальным докладчиком видеозаписей казней, совершенных на заключительном этапе гражданской войны в Шри-Ланке (см. A/HRC/17/28/Add.1, добавление). В данном случае Специальному докладчику удалось поддержать широкую коалицию, добивавшуюся привлечения к ответственности виновных, путем самостоятельного подбора технических экспертов, способных прокомментировать метаданные видеоматериалов, баллистические характеристики оружия, фигурировавшего в этих видеозаписях, а также движение тел. С учетом стремительного развития технологии в этой области сегодня, вероятно, стало легче найти таких экспертов, однако потенциал УВКПЧ практически не изменился. При отборе наилучших экспертов для выполнения конкретных задач мандатарии специальных процедур будут полагаться на технические знания своих сотрудников.

97. Как указано выше, проверка сгенерированного пользователями контента имеет принципиальное значение для эффективного использования преимуществ ИКТ с точки зрения расширения доступа к правозащитной деятельности и ее масштабов. Однако важно не считать проверку помехой для применения цифровых доказательств. Технические сложности проверки иногда преувеличиваются и используются как предлог для того, чтобы не заниматься такими доказательствами. Международный правозащитный механизм должен демистифицировать проверку в целях более полного использования преимуществ цифровых доказательств.

98. По поводу рисков, связанных с незнанием основ цифровой безопасности, уместно отметить, что многие механизмы Совета по правам человека поощряют индивидуальную переписку через незащищенные общие адреса электронной почты, не предупреждая о необходимости соблюдения мер безопасности и не предлагая альтернативные варианты поддержания связи. Хотя создание таких контактов само по себе является похвальным усилием по расширению доступа к механизмам Совета, последний, как утверждается, не выполняет свою обязанность по обеспечению должной осмотрительности, поскольку надлежащим образом не предупреждает отдельных лиц или группы лиц о потенциальных рисках, связанных с их действиями.

99. Разумеется, не должно создаваться впечатление, что специальные процедуры Совета закрыты для информации, которая проходит по новым потоковым каналам, рассматриваемым в настоящем докладе. По существу, многие поступающие от НПО сведения, на которые опираются сообщения специальных процедур, основаны на данных из таких источников. Однако, поскольку Совет до сих пор не готов оценивать такие доказательства или сообщения, возникает опасность того, что в предстоящие годы он может оказаться в изоляции от более широкого правозащитного сообщества, к сотрудничеству с которым он столь активно в прошлом стремился.

## 2. Национальные и международные комиссии по расследованиям

100. Цифровые доказательства использовались во многих национальных расследованиях. Заключение суда о том, что Ян Томлинсон стал жертвой незаконного убийства во время демонстрации в 2009 году в Лондоне, базировалось на видеозаписи свидетеля, которая была отслежена и передана Независимой комиссией по расследованию жалоб на действия полиции одним из журналистов-расследователей. Кроме того, в ходе расследования стрельбы на шахте Марикана, Южная Африка, были предположительно получены имеющие доказательную силу видеозаписи, которые были синхронизированы экспертом для Южноафриканской комиссии по правам человека<sup>56</sup>.

101. На международном уровне УВКПЧ на целевой основе сотрудничает с Программой Организации Объединенных Наций по применению спутниковой информации в оперативных целях и с различными внешними партнерами в интересах применения спутниковых и видеодоказательств в работе международных комиссий по расследованию<sup>57</sup>. Как указывалось выше, в сочетании с другими методами мониторинга в области прав человека спутниковые записи могут дать исключительно важную информацию, заслуживающую включения в доклады Совету по правам человека.

102. Комиссия по расследованию положения в области прав человека в Корейской Народно-Демократической Республике использовала спутниковые снимки и скрытно произведенные видеозаписи и фотографии для подтверждения существования нескольких лагерей для политических заключенных (см. A/HRC/25/63). Комиссия использовала эти видео- и фотоматериалы в той мере, в какой могла быть подтверждена их достоверность, а также спутниковые изображения, закупленные на коммерческой основе. По мнению Комиссии, спутниковые изображения высокого разрешения, получаемые технически развитыми государствами, по-видимому, могли бы содержать больше информации. К сожалению, несмотря на запросы, эти снимки не были предоставлены Комиссии (см. A/HRC/25/CRP.1, пункты 60–61).

103. Независимая международная комиссия по расследованию событий в Сирийской Арабской Республике также использовала определенное число спутниковых и цифровых материалов, предположительно поступивших от одной из организаций по мониторингу одного из наиболее полно задокументированных конфликтов в истории<sup>58</sup>. Например, при проведении специального расследования убийств в Эль-Хула Комиссия изучала спутниковые изображения для анализа пунктов доступа в район совершения убийств и заявлений опрошенных лиц, а также для оценки утверждений о том, что правительство полностью разрушило районы проживания гражданского населения в Дамаске и Хаме<sup>59</sup>. Комиссия упомянула о случаях, в которых она получала или находила видеодоказательства, подтверждающие утверждения о пытках или других формах жестокого обращения, либо съемки убийств, но при этом указывала, когда она не смогла их проверить<sup>60</sup>. Сбором видеоматериалов, которые упоминаются в до-

<sup>56</sup> См.: “Written submissions of the South African Human Rights Commission regarding ‘Phase One’” по адресу Комиссии по расследованию событий в Марикана (29 октября 2014 года) [www.sahrc.org.za/home/21/files/SAHRC%20PHASE%20ONE%20FINAL%20WRITTEN%20SUBMISSIONS.pdf](http://www.sahrc.org.za/home/21/files/SAHRC%20PHASE%20ONE%20FINAL%20WRITTEN%20SUBMISSIONS.pdf).

<sup>57</sup> См. <http://www.unitar.org/unosat/>.

<sup>58</sup> См. Marc Lynch, Deen Freelon and Sean Aday, *Syria’s Socially Mediated Civil War* (United States Institute of Peace, 2014).

<sup>59</sup> См. A/HRC/21/50, приложение IV; и A/HRC/22/59, приложение XIII, пункт 18.

<sup>60</sup> A/HRC/21/50, приложение VIII, пункт 31; A/HRC/22/59, приложение V, пункт 22.



кладах Комиссии<sup>61</sup>, непосредственно занималась также Миссия Организации Объединенных Наций по наблюдению в Сирийской Арабской Республике. Комиссия также провела предварительный обзор и криминалистический анализ 26 948 фотоснимков, которые предположительно были сделаны в период с 2011 по 2013 год в государственных пенитенциарных учреждениях<sup>62</sup>. В представленных в самое последнее время докладах Комиссия ссылалась на ряд видеозаписей, которые были сделаны и распространены ИГИШ; эти видеоматериалы не соответствовали нынешней практике использования видеозаписей только для подтверждения событий, в отношении которой имеются другие свидетельские показания, однако Комиссия признала их важными в качестве признаков<sup>63</sup>.

### 3. Международная уголовная ответственность

104. Полученная из цифровых источников информация приобретает все более важное значение для международных судов, включая некоторые из тех, которые были созданы в 1990-е годы, а ныне и для Международного уголовного суда. При оценке важности таких доказательств для своей деятельности Суд определил на будущее методы работы, позволяющие принимать к рассмотрению такие доказательства. В 2012 и 2013 годах Суд предлагал партнерам обмениваться мнениями и специальными знаниями о путях расширения потенциала расследователей и прокуроров для сбора и анализа цифровых доказательств применительно к тяжким международным преступлениям<sup>64</sup>.

105. Согласно одной из выдвинутых в этой связи рекомендаций, Канцелярии Прокурора следует "нанимать специалистов, которые прошли подготовку по передовым методам расследований с использованием Интернета и знакомы с самыми новыми технологиями", а также "обладают соответствующим опытом и квалификацией для осуществления расследований с применением цифровой техники, включая криминалистический анализ записей с компьютеров и смартфонов, расследование в режиме онлайн, хранение данных и управление ими, современные методы киберрасследований, а также глубокие знания вопросов цифровой безопасности". Предполагалось, что это будет "во многом способствовать формированию эффективного внутреннего потенциала для анализа цифровых данных и получения качественных доказательств"<sup>65</sup>. Следуя этой рекомендации, Канцелярия Прокурора назначила в состав своей группы расследователей с опытом юридической и правоохранительной деятельности специалиста по проверке цифровых материалов в качестве "киберрасследователя".

106. Признавая преходящее значение большей части представляющих интерес материалов, Канцелярия Прокуратуры ввела практику анализа имеющихся цифровых доказательств на этапе предварительного расследования. Как указывалось выше, Суд разработал для проводящих расследования сотрудников инструктивные указания по передовой практике в области поиска, хранения и

<sup>61</sup> A/HRC/21/50, приложение V, пункт 14.

<sup>62</sup> A/HRC/27/60, пункт 26.

<sup>63</sup> A/HRC/28/69 и Согг.1, приложение II, пункты 21–25.

<sup>64</sup> См. Центр по правам человека, Университет Калифорнии: *Beyond Reasonable Doubt: Using scientific evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2012); and *Digital fingerprints: Using electronic evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2014).

<sup>65</sup> См. Human Rights Center, "Digital Fingerprints", стр. 11 текста на английском языке (см. сноску 64).

изучения цифровых доказательств, включая снятие информации с веб-сайтов и изъятие жестких дисков.

### III. Заключение

107. ИТК оказывают большое влияние на эффективность и характер правозащитной деятельности. Однако этот процесс не следует заводить слишком далеко, особенно в условиях дефицита информации, когда все сильнее придется бороться с искушением отдавать предпочтение цифровым материалам. Новые технологии могут породить повышенные ожидания в отношении получения информации, однако здесь следует помнить, что традиционный мониторинг в области прав человека и представление сообщений об их нарушениях не претендуют на полноту и что анализ новых каналов получения данных с помощью ИКТ также не должен считаться исчерпывающим. Такие каналы являются не кратчайшим путем к цели, а скорее частью дополнительного процесса, который вписывается в ранее применявшиеся правозащитниками стратегии.

108. Кроме того, не менее важно, чтобы освоение ИКТ осуществлялось на основе надлежащего понимания присущих им рисков. Во многих случаях технология может служить стимулом к развитию плюрализма, но при этом все равно остаются проблемы цифровой пропасти. Чтобы с успехом применять цифровые средства защиты, правозащитники должны о них знать. Поощрение прав человека с помощью цифровых средств может помочь формированию таких знаний, однако переключение на эти цели ресурсов с более традиционных каналов правозащитной деятельности повредит уязвимым группам, не являющимся участниками общения в киберпространстве.

109. Необходимо также признать важность владения цифровыми ИКТ и контроля над их механизмами. Применение цифровых доказательств часто зависит от готовности технологических корпораций размещать и хранить такую информацию, а также содействовать ее поискам. Кроме того, в некоторых государствах блокирован доступ к принадлежащим внешним структурам коммерческим платформам социальных сетей, в частности, к "Twitter", "Facebook" и "YouTube". В других странах для пресечения передачи информации отключаются целые коммуникационные сети.

110. Правозащитные организации могут испытывать трудности с повышением цифровой грамотности и оплатой новой технологии. Одним из способов решения этой проблемы могло бы стать сотрудничество между специалистами по ИКТ и экспертами по правам человека в деле разработки, применения и даже коммерциализации новых правозащитных приложений либо достижение договоренностей о предоставлении недорогих или бесплатных лицензий на применение существующих программ. Доноры заинтересованы в финансировании технологического развития, но якобы могут уделять больше внимания самой технологии, нежели необходимой для ее использования подготовке персонала. Однако без надлежащей подготовки технология может оказаться бесполезной или даже опасной. По словам од-

ного наблюдателя, "рано или поздно все технологические проблемы становятся проблемами обучения"<sup>66</sup>.

111. Сотрудничество может осуществляться и на более широкой основе. По существу, многие организации проявляют готовность помогать международным правозащитным механизмам в более эффективном использовании ИКТ. В этой связи предпринимались усилия по координации действий, но, как представляется, правозащитное сообщество еще намного отстает от других международных учреждений в деле полного освоения их потенциала, что наиболее ярко прослеживается на примере антикризисных мер<sup>67</sup>.

112. Для укрепления правозащитных механизмов системы Организации Объединенных Наций, которые напрямую участвуют в рассмотрении доказательств, зачастую собираемых третьими сторонами, необходим собственный потенциал для так называемого "просеивания" цифровых материалов в качестве первоначальной оценки возможной ценности источника до их передачи внешним экспертам для проведения полноценной проверки или другой технической оценки. Такой потенциал по выработке "первоначального мнения" и поддержания связей в рамках секретариата международных механизмов, включая специальные процедуры, способствовал бы более широкому использованию потенциально ценной информации.

113. Разумеется, технологические достижения в сфере сбора доказательств эффективны лишь настолько, насколько эффективны механизмы обеспечения подотчетности, для которых готовятся такие доказательства и большинство из которых не имеют прямого отношения к технологии. В этом смысле для более надежной защиты прав человека, включая право на жизнь, более эффективные каналы передачи информации на основе ИКТ являются необходимыми, но не достаточными. Это подчеркивает важность того, чтобы международные правозащитные механизмы, включая Совет по правам человека и его специальные процедуры, могли в полной мере использовать такие материалы. Некоторые правозащитные НПО, относящиеся к так называемому "второму поколению", соответствуют в своем развитии инновациям "третьего поколения". Крайне важно, чтобы "первое поколение" ликвидировало свое отставание.

## IV. Рекомендации

### A. Рекомендации Организации Объединенных Наций

114. В ближайшее возможное время УВКПЧ должно назначить на консультативной основе специалиста по цифровому контенту для выработки рекомендаций в отношении получаемой от гражданских свидетелей или собираемой ими информации, а также для выполнения функции по поддержанию связей с внешними экспертными сетями в этой области. Такое

<sup>66</sup> Christopher Neu, "Mobile applications for atrocity prevention require mobile students", *TechChange*, (19 February 2013), <http://techchange.org/2013/02/19/mobile-applications-for-atrocity-prevention-require-mobile-students/>.

<sup>67</sup> В контексте гуманитарного реагирования Цифровая сеть гуманитарного реагирования подготовила два доклада, предназначенных для обеих сторон такого партнерства: см. <http://digitalhumanitarians.com/content/guidance-collaborating-formal-humanitarian-organizations> и <http://digitalhumanitarians.com/content/guidance-collaborating-volunteer-technical-communities>.

назначение будет рассматриваться как временное решение, направленное на обеспечение ускоренного продвижения на данном направлении. При этом УВКПЧ при содействии назначенного им специалиста следует приступить к созданию долговременного потенциала.

115. Поскольку международные комиссии по расследованию и миссии по установлению фактов являются временными органами, которые могут получать большой и все нарастающий объем цифровых доказательств, в рамках их кадровых потребностей следует рассмотреть возможность привлечения специалистов для анализа таких материалов.

116. В более широком плане УВКПЧ надлежит принять меры для повышения осведомленности своего персонала и организационных структур всех уровней о требованиях цифровой безопасности и ознакомления с ними. Это предполагает разработку минимальных стандартов проявления должной осмотрительности в отношении цифровой безопасности источников. Следует также в консультации с соответствующими партнерами разработать руководящие указания для персонала Организации Объединенных Наций по этическим аспектам использования информации из открытых источников, особенно из социальных сетей.

## **В. Рекомендации региональным правозащитным механизмам**

117. Региональным правозащитным механизмам надлежит проанализировать свой потенциал в отношении получения и использования цифровых материалов, а также поощрять применение передовой практики в области цифровой безопасности. При необходимости в целях наращивания такого потенциала им следует входить в контакт с УВКПЧ.

## **С. Рекомендации государствам**

118. Государства должны соблюдать и, когда это необходимо, защищать права личности на регистрацию техническими средствами общественного мероприятия, в том числе поведения сотрудников правоохранительных органов, а также обеспечивать "обратную регистрацию" действий индивидуума государственным агентом.

119. Государствам следует рассмотреть возможные инновационные меры по использованию ИКТ с целью предотвращения нарушения права на жизнь своими агентами, особенно чрезмерного применения силы сотрудниками правоохранительных органов, или в условиях пенитенциарных учреждений. К их числу можно, в частности, отнести такую инновационную практику, как применение нательных камер с должным учетом необходимых гарантий права на неприкосновенность личной жизни.

120. Государства, обладающие развитым потенциалом для осуществления спутниковой съемки, должны изучить вопрос о предоставлении по крайней мере обобщенной информации нуждающимся в ней международным правозащитным механизмам, при необходимости, на конфиденциальной и анонимной основе.

#### **D. Рекомендации организациям гражданского общества и академическим кругам**

121. Оставаясь открытыми по отношению к достижениям в быстро развивающейся сфере технологических инноваций, организации гражданского общества должны применять основанный на доказательствах подход к оценке преимуществ новых механизмов, использующих ИКТ в своей работе. В сотрудничестве с академическими кругами они должны сосредотачивать ресурсы в тех областях, в которых ИКТ действительно открывают более широкие возможности, продолжая при этом свою жизненно важную работу на основе прочих более традиционных методов. Академические круги и правозащитные организации должны также сотрудничать с целью проведения в первоочередном порядке исследований в тех областях, в которых в них ощущается наибольшая потребность, например в деле решения "проблемы объема информации".

122. Органы, ответственные за разработку учебных планов и программ подготовки в области прав человека, должны рассмотреть возможность включения модулей об эффективном применении ИКТ для обеспечения прав человека. Более крупным организациям следует продолжать принимать меры по оказанию помощи организациям, которые обладают более ограниченными ресурсами в области цифровых технологий.

#### **E. Рекомендации донорам**

123. Доноры должны признать, что технологические решения проблем прав человека могут быть успешными, только если они подкрепляются эффективной подготовкой кадров. Полагаясь на строгую и беспристрастную оценку полезности и эффективности новых приложений или устройств, доноры должны также поощрять и поддерживать усилия по повышению цифровой грамотности и уровня осведомленности о цифровой безопасности среди наиболее нуждающихся в них сообществ.

#### **F. Рекомендации корпорациям, занимающимся разработкой технологий и программного обеспечения**

124. Разработчики должны в позитивном ключе изучить возможность включения в число основных опций камер функции "свидетель" или "доказательство", которая позволяет пользователям добавлять метаданные и обеспечивать неприкосновенность файла, повышая тем самым ценность видеодоказательств, без предварительной загрузки специализированного приложения.

125. Платформы социальных сетей должны разработать процесс, с помощью которого генерируемый пользователями контент, представляющий потенциальный интерес для расследований в области прав человека, но исключенный из этих платформ в соответствии с принятыми в сообществе стандартами, мог бы оставаться доступным для организаций, занимающихся установлением фактов.