22 декабря 2021

Председателю

Специального комитета по разработке всеобъемлющей международной конвеции о противодействии использованию информационно-коммуникационных технологий в преступных целях

Госпоже Фаузии Бумайза Мебарки

Ваше Превосходительство,

Мы, нижеподписавшиеся организации и ученые, занимаемся защитой и развитием прав человека в онлайн и офлайн пространстве. Мы озабочены предпринимаемыми мерами в сфере борьбы с киберпреступностью не только потому, что преступления в киберпространстве сами по себе нарушают права человека и угрожают нормальной жизнедеятельности, но и потому что законы, правила и инициативы в данной сфере в настоящее время используются для ущемления прав человека. В связи с этим мы просим включить в работу Специального комитета представителей гражданского общества на всех этапах разработки и составления конвенции, и чтобы любая предлагаемая конвенция включала материальные и процессуальные гарантии прав человека.

Справочная информация

Предложение о разработке всеобъемлющей "международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях" выдвигается в то самое время, когда правозащитные механизмы ООН бьют тревогу по поводу злоупотребления законами о киберпреступности по всему миру. В своем докладе за 2019 год специальный докладчик ООН по правам на свободу мирных собраний и объединений Клемент Ньялецосси Вуле отметил: "Активизация деятельности по разработке законов и стратегий, направленных на борьбу с киберпреступностью, также открыла дверь для использования цифровых технологий как инструмента наказания и слежки за активистами и участниками протестов во многих странах мира". В 2019 году и еще раз в этом году Генеральная Ассамблея ООН выразила серьезную обеспокоенность тем, что законодательство о киберпреступности неправомерно используется для преследования правозащитников, препятствует их работе и ставит под угрозу их безопасность, что противоречит международному праву. Этому предшествовало множество сообщений неправительственных организаций о нарушениях прав человека, связанных со слишком широкой формулировкой законов о киберпреступности.

Когда принятие конвенции было предложено впервые, более 40 ведущих организаций и экспертов в области цифровых прав и прав человека, включая подписавших данное письмо, призвали делегации проголосовать против резолюции, предупреждая, что данная конвенция угрожает правам человека.

В преддверии первой сессии Специального комитета мы вновь обращаем внимание на наши опасения. Если конвенция ООН по киберпреступности будет принята, ее целью должна стать борьба с использованием информационно-коммуникационных технологий в преступных целях без ущерба основным правам тех, кого она призвана защищать: у людей должна сохраниться возможность свободно пользоваться и осуществлять свои права как в сети, так и вне ее. Любая предлагаемая конвенция должна включать в себя четкие и надежные гарантии прав человека. Конвенция без таких гарантий или послабляющая обязательства государств в области прав человека подвергнет риску отдельных людей и сделает наше цифровое присутствие еще более небезопасным, что угрожает фундаментальным правам человека.

Поскольку в ближайшие месяцы Специальный комитет приступит к разработке проекта конвенции, жизненно важно применить правозащитный подход, чтобы гарантировать, что предложенный проект не станет инструментом ограничения свободы слова, нарушения неприкосновенности частной жизни и персональных данных, а также не подвергнет риску отдельных лиц и сообщества.

Работа по борьбе с киберпреступностью должна соответствовать обязательствам государств в области прав человека, изложенным во Всеобщей декларации прав человека, Международном пакте о гражданских и политических правах и других международных документах и стандартах. Другими словами, усилия по борьбе с киберпреступностью должны защищать, а не подрывать права человека. Мы напоминаем государствам, что те же права, которые люди имеют вне Интернета, должны быть защищены и в онлайн-пространстве.

Сфера применения основных положений уголовного права

Не существует единого мнения о том, как бороться с киберпреступностью на глобальном уровне, а также общего понимания или определения того, что представляет собой киберпреступность. С точки зрения прав человека, необходимо, чтобы сфера применения любой конвенции по киберпреступности была ограниченной. Тот факт, что преступление может быть связано с технологией, не означает, что оно должно быть включено в предлагаемую конвенцию. Например, расширительные законы о киберпреступности зачастую просто увеличивают санкции за использование компьютера или устройства при совершении уже существующего преступления. Такие законы особенно проблематичны, когда они включают преступления, связанные с информационным наполнением (контентом). Нечетко сформулированные законы о киберпреступности, направленные на борьбу с дезинформацией и онлайн-поддержкой или пропагандой терроризма и экстремизма, могут быть использованы для тюремного заключения блогеров или блокировки целых платформ в той или иной стране. Такие законы не соответствуют международным стандартам свободы выражения мнений и подвергают опасности журналистов, активистов, исследователей, представителей ЛГБТ-сообществ и диссидентов, а также могут оказывать сдерживающее воздействие на общество в целом.

Даже те законы, которые более целенаправленно ориентированы на преступления с использованием кибертехнологий, используются для нарушения прав. Законы, криминализирующие несанкционированный доступ к компьютерным сетям или системам, используются для преследования ученых в области цифровой безопасности, информаторов, активистов и журналистов. Слишком часто эксперты, которые помогают обеспечить всеобщую безопасность, попадают под действие расплывчатых законов о киберпреступности и сталкиваются с уголовными преследованиями за выявление недостатков в системах безопасности. В некоторых государствах законы о несанкционированном доступе трактуются настолько широко, что фактически криминализируют любое доносительство; при таком толковании любое раскрытие информации в нарушение корпоративной или государственной политики может рассматриваться как "киберпреступление". Любая потенциальная конвенция должна включать ясный стандарт прямого умысла, не должна создавать уголовную ответственность в рамках корпоративной или государственной политики использования компьютеров, должна обеспечивать ясно сформулированную и обширную защиту общественных интересов, а также включать четкие положения, позволяющие специалистам в сфере безопасности выполнять свою работу без страха быть подвергнутыми уголовному преследованию.

Права человека и процессуальные гарантии

Наша частная и личная информация, которая раньше хранилась в ящике стола, теперь хранится на наших цифровых устройствах и в облаке. Полиция по всему миру использует все более интрузивный набор следственных инструментов для получения доступа к цифровым доказательствам. Зачастую их расследования пересекают границы без надлежащих гарантий и обходят защиту, предусмотренную договорами о взаимной правовой помощи. Во многих случаях судебный надзор отсутствует, а роль независимых регуляторов защиты данных ослаблена. Национальные законы, включая законодательство о киберпреступности, зачастую не обеспечивают адекватную защиту от непропорционального или ненужного наблюдения.

Любая потенциальная конвенция должна подробно описывать надежные процессуальные гарантии и гарантии прав человека, регулирующие уголовные расследования, проводимые в соответствии с такой конвенцией. Она должна обеспечить, чтобы любое вмешательство в право на неприкосновенность частной жизни соответствовало принципам законности, необходимости и пропорциональности, в том числе путем требования независимой судебной санкции на меры наблюдения. Она также не должна запрещать государствам принимать дополнительные гарантии, ограничивающие использование персональных данных правоохранительными органами, поскольку такой запрет подорвал бы принципы неприкосновенности частной жизни и защиты данных. Любая потенциальная конвенция должна также подтвердить необходимость принятия и применения государствами "сильного, надежного и всеобъемлющего законодательства о неприкосновенности частной жизни, включая неприкосновенность данных, которое соответствует международному праву в

области прав человека в плане гарантий, надзора и средств правовой защиты для эффективной защиты права на неприкосновенность частной жизни".

Существует реальный риск того, что в попытке убедить все государства подписать предлагаемую конвенцию ООН по киберпреступности, будут учтены неправомерные практики в области прав человека, что приведет к гонке на понижение. Поэтому очень важно, чтобы любая потенциальная конвенция четко закрепляла процессуальные гарантии защиты прав человека и противостояла упрощению соглашений о взаимопомощи.**Значимое участие**

В дальнейшем мы просим Специальный комитет активно привлекать к консультациям организации гражданского общества, в том числе занимающиеся вопросами цифровой безопасности, и объединения, оказывающие помощь уязвимым сообществам и лицам, чего не произошло ни в начале этого процесса в 2019 году, ни за прошедшее время.

В связи с изложенным мы просим Комитет:

● Своевременно и прозрачно аккредитовать заинтересованных академиков и экспертов в области технологий, а также неправительственные организации, включая обладающие соответствующим опытом в области прав человека, но не имеющие консультативного статуса при Экономическом и Социальном Совете ООН, и разрешить участвующим группам регистрировать нескольких представителей, чтобы обеспечить дистанционное участие в разных часовых поясах.

● Обеспечить, чтобы условия участия, учитывая разнообразие неправительственных заинтересованных сторон, предоставляли каждой группе заинтересованных сторон достаточное время для выступления, поскольку гражданское общество, частный сектор и академические круги могут иметь различные взгляды и интересы.

● Обеспечить эффективное участие аккредитованных участников, включая обеспечение устным переводом, возможность своевременно получать документы, выступать на сессиях Комитета (очно и дистанционно) и представлять письменные заключения и рекомендации.

● Обеспечить актуальным наполнением веб-страницу, специально посвященную указанным вопросам, с соответствующей практической информацией (подробности об аккредитации, времени/месте проведения и дистанционном участии), организационными документами (повестки дня, документы для обсуждения и т.д.), заявлениями и прочими выступлениями государств и других заинтересованных сторон, справочными документами, рабочими документами и итоговыми проектами, а также отчетами о заседаниях.

Противодействие киберпреступности не должно осуществляться за счет фундаментальных прав и достоинства тех, чьей жизни коснется предлагаемая Конвенция. Государства должны обеспечить соответствие любой предлагаемой конвенции по киберпреступности своим обязательствам в области прав человека

и выступить против любой предлагаемой конвенции, не соответствующей этим обязательствам.

Мы будем признательны, если Вы любезно распространите настоящее письмо среди членов Специального комитета и опубликуете его на сайте Специального комитета.

Подписи*:

1. Аксесс Нау — Международная
2. Альтернативная сеть АСЕАН по Бирме (Алтсеан) - Бирма
3. Альтернативы - Канада
4. Ассоциация альтернативной информатики - Турция
5. АквальтюнЛаб - Бразилия
6. Фонд Армсек - Армения
7. Статья 19 - Международная
8. Ассоциация гражданских прав (ADC) - Аргентина
9. Ассоциация Тринидад/ Радио Вива - Тринидад
10. Ассоциация по технологиям и Интернету (АпТИ) - Румыния
11. Ассоциация прогрессивных коммуникаций - Международная
12. Всемирная ассоциация публичных радиовещателей (Амарк Бразил) - Бразилия
13. Парламентарии АСЕАН за права человека (APHR) - Юго-Восточная Азия
14. Объединение НПО Бангладеш по радио и коммуникации (BNNRC) - Бангладеш
15. Информационная сеть БлюЛинк - Болгария
16. Бразильский институт публичного права - Бразилия
17. Камбоджийский центр по правам человека (CCHR) - Камбоджа
18. Камбоджийский институт демократии - Камбоджа
19. Ассоциация Альянс журналистов Камбоджи - Камбоджа
20. Дом цифровой культуры Порту-Алегри - Бразилия
21. Центр демократии и верховенства права - Украина
22. Центр за свободу слова - Канада
23. Центр многосторонних отношений - Уганда
24. Центр демократии и технологий - США
25. Гражданское общество - Европа
26. Коалиция Права в сети - Бразилия
27. Сотрудничество по международной политике в области ИКТ для Восточной и Южной Африки (CIPESA) - Африка
28. КиберХаб-АМ - Армения
29. Бразильская ассоциация по исследованию конфиденциальности данных - Бразилия
30. Dataskydd - Швеция
31. Цифровые права (Деречес Диджиталис) - Латинская Америка

32. Защита прав и инакомыслия - США
33. Цифровые граждане - Румыния
34. ДиджиталРич - Юго-Восточная Азия
35. Лаборатория цифровой безопасности - Украина
36. Državljan D / Гражданин Д - Словения
37. Фонд электронных рубежей (EFF) - Международный
38. Информационный центр электронной конфиденциальности (EPIC) - США
39. Elektronisk Forpost Norge - Норвегия
40. Эпицентр.воркс за цифровые права - Австрия
41. Европейский центр некоммерческого права (ECNL) Stichting - Европа
42. Европейский гражданский форум - Европа
43. Европейские цифровые права (EDRi) - Европа
44. Проект eQuality - Канада
45. Фонд Фанцуам - Нигерия
46. Коалиция за свободу слова - США
47. Фонд альтернативных медиа (FMA) - Филиппины
48. Фонд "Акцесо" - Центральная Америка
49. Фонд гражданства и развития - Эквадор
50. Фонд Конструир - Боливия
51. Фонд Харисма - Колумбия
52. Фонд ОпенлабЕС - Эквадор
53. Фундамедиос - Эквадор
54. Хакерский клуб Гароа - Бразилия
55. Глобал Партнерс Диджитад - Великобритания
56. ГринНэт - Великобритания
57. ГрейтФаер - Китай
58. Гипердеречо - Перу
59. Хомо Диджиталис - Греция
60. Права человека в Китае - Китай
61. Сеть защитников прав человека - Сьерра-Леоне
62. Хьюман Райтс Вотч - Международный
63. Институт Игарапе - Бразилия
64. IFEX - Международный
65. Институт политических исследований и правозащитной деятельности (ELSAM) - Индонезия
66. Инфлюенсер платформа - Украина
67. Сеть INSM по цифровым правам - Ирак
68. Интерньюс - Украина
69. Институт Бета: Интернет и демократия (IBIDEM) - Бразилия
70. Бразильский институт защиты потребителей (IDEC) - Бразилия
71. Институт Эдукадиджитал - Бразилия

72. Институт Нупеф - Бразилия
73. Институт Ресифи по исследованиям в области права и технологий (IP.rec) - Бразилия
74. Институт ссылок на Интернет и общество (IRIS) - Бразилия
75. Панамский институт права и новых технологий (IPANDETEC) - Панама
76. Институт общества информации и промышленной революции - Перу
77. Международная комиссия юристов - Международная
78. Международная федерация по правам человека (FIDH)
79. IT-Pol - Дания
80. JCA-NET - Япония
81. KICTANet - Кения
82. Корейская прогрессивная сеть Джинбонэт - Южная Корея
83. Лаборатория Данные и общество (Datysoc) - Уругвай
84. Лаборатория государственной политики и Интернета (LAPIN) - Бразилия
85. Латиноамериканская сеть исследований в области наблюдения, технологий и гражданского общества (LAVITS)
86. Центр юристов - Африка
87. Правовые инициативы для Вьетнама
88. Лига защиты прав человека (LDH) - Франция
89. Масаар - Сообщество технологии и права - Египет
90. Фонд Манушия - Таиланд
91. MINBYUN Адвокаты за демократическое общество - Корея
92. Фонд Открытая культура - Тайвань
93. Открытые медиа - Канада
94. Ассоциация открытой сети - Корея
95. ОпенНэт Африка - Уганда
96. Фонд Паноптикон - Польша
97. Инициатива Парадигма - Нигерия
98. Приваси Интернешнл - Международный
99. Радио Вива - Парагвай
100. Сеть в защиту цифровых прав (R3D) - Мексика
101. Региональный центр по правам и свободам - Египет
102. Исследование ИКТ Африка
103. Самуэльсон-Глушко Канадская клиника интернет-политики и общественных интересов (CIPPIC) - Канада
104. Фонд Share - Сербия
105. Биржа соцсетей (SMEX) - Ливан, Арабский регион
106. SocialTIC - Мексика
107. Сеть свободы выражения мнений Юго-Восточной Азии (SAFEnet) - Юго-Восточная Азия

108. Сторонники за здоровье и права работников полупроводниковой промышленности (SHARPS) - Южная Корея
109. Проект по надзору за технологиями наблюдения (STOP) - Соединенные Штаты Америки
110. Технологии, исследования и общество (TEDIC) - Парагвай
111. Тайская сеть нетизенов - Таиланд
112. Нежелательный свидетель - Уганда
113. Vrijschrift - Нидерланды
114. Западноафриканская сеть правозащитников - Того
115. Всемирное движение за демократию - Международное
116. 7amleh - Арабский центр развития социальных медиа - Арабский регион

Эксперты и ученые:
1. Жаклин Абреу, Университет Сан-Паулу
2. Чан-Мо Чунг, профессор юридического факультета Университета Инха
3. Данило Донеда, Бразильский институт публичного права
4. Дэвид Кайе, клинический профессор права, Школа права Университета Ирвайна, бывший Специальный докладчик ООН по вопросам свободы мнений и их выражения (2014-2020)
5. Вольфганг Кляйнвехтер, почетный профессор Орхусского университета; член Глобальной комиссии по стабильности киберпространства
6. Дуве Корфф, почетный профессор международного права, Лондонский университет Метрополитен
7. Фабиано Менке, Федеральный университет Рио-Гранде-ду-Сул
8. Кюн-Син Парк, профессор юридического факультета Корейского университета
9. Кристофер Парсонс, старший научный сотрудник, Citizen Lab, Школа глобальных дел и государственной политики Мунка при Университете Торонто
10. Мариетье Шааке, Стэнфордский центр киберполитики
11. Валери Стивз, доктор юридических наук, доктор философии, профессор кафедры криминологии Университета Оттавы.

*Список подписавших по состоянию на 13 января 2022 года