



Генеральная Ассамблея

Distr.: General
17 October 2018
Russian
Original: English

Семьдесят третья сессия

Пункт 74 b) повестки дня

**Поощрение и защита прав человека: вопросы
прав человека, включая альтернативные подходы
в деле содействия эффективному осуществлению
прав человека и основных свобод**

Право на неприкосновенность частной жизни*

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад Специального докладчика Совета по правам человека по вопросу о праве на неприкосновенность частной жизни г-на Джозефа А. Каннатачи, представленный в соответствии с резолюцией [28/16](#) Совета по правам человека.

* Настоящий доклад был представлен с опозданием в связи с необходимостью отразить в нем последние события.



Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни

Резюме

Настоящий доклад состоит из двух частей: резюме деятельности, проведенной в период 2017–2018 годов, и окончательного доклада о работе целевой группы по вопросам использования больших объемов данных и открытых данных, которая была создана Специальным докладчиком.

I. Обзор деятельности Специального докладчика по вопросу о праве на неприкосновенность частной жизни

1. Период с октября 2017 года по октябрь 2018 года был крайне продуктивным для Специального докладчика по вопросу о праве на неприкосновенность частной жизни, поскольку он был ознаменован взаимодействием с гражданским обществом, правительствами, правоохранительными органами, разведывательными службами, управлениями по защите данных, разведывательными надзорными органами, академическими кругами, корпорациями и другими заинтересованными сторонами.
2. В марте 2018 года Специальный докладчик представил Совету по правам человека всеобъемлющий обзор его первого трехгодичного срока работы в качестве первоначального обладателя мандата, учрежденного Советом в марте 2015 года¹. В этом докладе он представил отчет о своей деятельности в каждой из тематических областей его мандата. Специальный докладчик хотел бы заявить, что для него большая честь видеть, что его срок полномочий продлен до 2021 года, и продолжать важную работу в рамках мандата.
3. График работы Специального докладчика был прерван, когда он перенес хирургическую операцию в апреле 2018 года. Он благодарит Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) за оказанную им поддержку и помощь в течение этого времени. Специальный докладчик полностью выздоровел и возобновил свою работу в июне 2018 года.

A. Работа целевой группы по вопросам конфиденциальности данных в сфере здравоохранения

4. Целевая группа по вопросам конфиденциальности данных в сфере здравоохранения занималась рассмотрением вопросов под руководством Стива Стеффенсена из Медицинской школы Делла, Техасский университет, Соединенные Штаты Америки. Хотя началась работа над проектом доклада, непредвиденные события привели к тому, что, консультации, запланированные на 2018 год, были перенесены на 2019 год. Заместитель Председателя Николаус Форго согласился взять на себя обязанности Председателя.

¹ [A/HRC/37/62](#).

В. Работа целевой группы по вопросам использования корпорациями персональных данных

5. Право на неприкосновенность частной жизни никогда не занимало такого ведущего места в политическом, судебном и личном самосознании, как в настоящее время, когда напряженность между вопросами безопасности, корпоративными бизнес-моделями и правом на личную жизнь продолжает находиться в центре внимания.

6. В ответ на происшедшие за прошедший год события, включая утечку данных в компании Cambridge Analytica, принятие законодательства, такого как Акт, разъясняющий законное использование данных за рубежом, в Соединенных Штатах, законопроект 2018 года о внесении поправок в законодательство в области электросвязи и другое законодательство в Австралии и дело *Соединенные Штаты против корпорации «Майкрософт»* в Верховном суде Соединенных Штатов, Специальный докладчик ускорил начало работы целевой группы по вопросам использования корпорациями персональных данных.

7. Первое заседание целевой группы состоялось на Мальте в сентябре 2018 года. Ее членский состав включает представителей крупных корпораций, занимающих ведущие места в цифровую эпоху, и ведущих субъектов, отстаивающих защиту права на неприкосновенность частной жизни в мире технологии. Она будет консультировать Специального докладчика относительно возникающих проблем и возможностей для поощрения права на неприкосновенность частной жизни, включая гендерные аспекты этих вопросов.

С. Работа целевой группы по вопросам более глубокого понимания концепции неприкосновенности частной жизни

8. Целевая группа по вопросам более глубокого понимания концепции неприкосновенности частной жизни анализирует факт признания Советом по правам человека права на неприкосновенность частной жизни как создающего возможности для развития личности, равно как и барьеры на пути реализации таких возможностей. Она будет сотрудничать с инициативами по всему миру, такими как инициатива Австралийской комиссии по правам человека по изучению воздействия цифровой эпохи на права человека².

9. Хотя все люди имеют право на пользование защитой, предоставляемой международным правом прав человека, поступают сообщения о том, что пользование правом на неприкосновенность частной жизни не является ни единообразным, ни универсальным. Гендерная проблематика — это одна область, в которой связанные с защитой и содействием последствия неприкосновенности частной жизни и нарушений такой неприкосновенности наряду с сопутствующим вредом могут ощущаться по-разному.

10. В этой связи Верховный суд Индии отменил раздел 377 индийского Уголовного кодекса, касающийся установления уголовной ответственности за консенсуальные сексуальные действия между взрослыми людьми в постановлении, признающем права сообщества людей нетрадиционной сексуальной ориентации в Индии. Это постановление окажет значительное воздействие на связанные с

² Australian Human Rights Commission, “Major project to focus on human rights and technology, 22 May 2018. URL: www.humanrights.gov.au/news/stories/major-project-focus-human-rights-and-technology.

гендером и тайной личной жизни рассуждения в Индии, и оно вытекает из принятого в 2017 году постановления о праве на неприкосновенность частной жизни в деле *Путтасвами*³.

11. Специальный докладчик инициировал онлайн-консультацию о гендерных аспектах права на неприкосновенность частной жизни в цифровую эпоху, желая получить отклики по таким вопросам, как нижеследующие:

a) Какие гендерные вопросы возникают в цифровую эпоху? Какими проблемами нужно заниматься, и какой позитивный опыт можно более широко пропагандировать?

b) Привела ли цифровая эпоха к новому или существенно иному гендерному опыту (включая опыт с учетом сексуальной ориентации, гендерной идентичности, гендерного самовыражения и половых признаков) в плане неприкосновенности частной жизни? Если да, то в чем заключается такой опыт?

c) Каковы гендерные последствия вмешательства в частную жизнь для женщин и мужчин и для лиц иной сексуальной ориентации и гендерной идентичности, гендерного самовыражения и половых признаков, возникающие вследствие нарушения права на неприкосновенность частной жизни, включая вопросы здравоохранения, дискриминации в сфере занятости или в иных областях?

d) Какова передовая практика в области права и в моделях предоставления услуг, которая устраняет гендерные различия в пользовании правом на неприкосновенность частной жизни?

12. К 30 сентября 2018 года были запрошены материалы для представления доклада Совету по правам человека в 2019 году. Специальный докладчик рад принять запоздалые представления государств-членов вплоть до 30 ноября 2018 года.

13. Эта инициатива следует за консультациями на тему «Неприкосновенность частной жизни, правосубъектность и потоки информации», проведенными по всему миру в июле 2016 года, мае 2017 года и сентябре 2017 года. Четвертое мероприятие, посвященное гендерным аспектам, которое было запланировано на май 2018 года в Латинской Америке, было отложено из-за неспособности Специального докладчика совершить поездку, и вместо этого оно состоится в середине 2019 года.

D. Работа целевой группы по вопросам безопасности и слежения

14. После того как Эдвард Сноуден раскрыл детали программ слежки и обмена разведывательными данными, осуществляемых разведслужбами Соединенных Штатов и Соединенного Королевства Великобритании и Северной Ирландии, в Европейский суд по правам человека были поданы ходатайства относительно массового перехвата сообщений, обмена разведывательными данными с иностранными правительствами и получения передаваемых данных от поставщиков услуг связи на основании Закона Соединенного Королевства о правовом регулировании следственных полномочий 2000 года.

15. Недавно Суд постановил, что действующий в Соединенном Королевстве режим массового перехвата является нарушением статьи 8 Конвенции о защите прав человека и основных свобод (Европейской конвенции по правам человека),

³ Сообщение, полученное от Смиты Кришны Прасад, Национальный университет права, Дели, Индия, 24 сентября 2018 года.

касающейся права на уважение частной и семейной жизни/корреспонденции, ввиду недостаточного надзора за отбором Интернет-каналов для перехвата и фильтрации, поиска и отбора перехваченных сообщений для анализа, равно как и неадекватных гарантий отбора «соответствующих передаваемых данных» для анализа.

16. Суд счел, что режим получения передаваемых данных от поставщиков услуг связи стал нарушением статьи 8 и что режимы массового перехвата и получения передаваемых данных от поставщиков услуг связи являются нарушением статьи 10 Конвенции в силу недостаточных гарантий сохранения конфиденциальных журналистских материалов. Он далее постановил, что режим обмена разведывательной информацией с иностранными правительствами не является нарушением ни статьи 8, ни статьи 10⁴.

17. Хотя это постановление касалось предусмотренного законом режима слежения, ранее существовавшего в Соединенном Королевстве, его выводы важны и доводятся до сведения государств-членов на предмет проведения обзора их практики и их нормативных основ.

18. Что касается вынесенного в декабре 2016 года постановления Суда Европейского союза касательно сохранения передаваемых данных и консультации правительства Соединенного Королевства относительно его предлагаемого ответа, то в начале 2018 года Специальный докладчик внес свой вклад, который будет помещен на веб-странице УВКПЧ, посвященной этому мандатарю⁵.

19. В сентябре 2018 года правительство Австралии внесло законопроект о поправках в законодательство в области электросвязи и другое законодательство, который оказал глубокое воздействие на права человека и кибербезопасность на международном и национальном уровнях.

20. Законопроект страдает роковыми изъянами. Он представляет собой плохо продуманную меру национальной безопасности, которая может с таким же успехом ставить под угрозу безопасность; с технологической точки зрения сомнительно, может ли он достичь своих целей и при этом не добавлять уязвимости в кибербезопасность всех устройств, независимо от того, идет ли речь о мобильных телефонах, планшетных компьютерах, «умных» часах, автомобилях или замкнутых телевизионных системах, и он ненадлежащим образом подрывает права человека, включая право на неприкосновенность частной жизни. Заверения насчет того, что он не является «черным ходом» в зашифрованную связь, не вызывают доверия, поскольку, по сути дела, он может дать дополнительные ключи для «парадного входа» или даже создать больше парадных дверей.

21. Законопроект предусматривает чрезмерно высокий уровень свободы действий в отношении использования исключительных полномочий. Ответственность возлагается не на парламент, а на учреждения и на Генерального прокурора. Законопроект не предусматривает судебного надзора или независимого мониторинга, крайнюю тревогу вызывает отсутствие транспарентности, а предлагаемая способность внедрять программное обеспечение, среди прочего, в устройства подозрительно схожа с правительственным хакерством. Он был вне-

⁴ European Court of Human Rights, First Section, *Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58170/13, 62322/14 and 24960/15, Information Note on Judgment of 13 September 2018. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22002-12080%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-12080%22]}).

⁵ www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

сен в парламент после недостаточного периода консультаций и, несмотря на получение, как сообщалось, свыше 14 000 обращений и материалов, всего лишь через две недели после закрытия консультаций⁶.

22. Обеспокоенность Специального докладчика усугубляется позицией правительства Австралии относительно средств правовой защиты от серьезных посягательств на неприкосновенность частной жизни и ограниченных мер защиты прав человека и частной жизни в стране: в ней не предусмотрена конституционная защита неприкосновенности частной жизни; в ней нет никакого билля о правах, закрепляющего неприкосновенность частной жизни; и, в отличие от ее соседа — Новой Зеландии, — ее Закон о неприкосновенности частной жизни не прошел европейскую оценку на достаточность предусмотренных мер.

23. Требуется новый подход для решения проблем, возникающих вследствие кодирования сообщений для правоохранительных органов и органов национальной безопасности. Хотя технология создает проблемы для правоохранительных учреждений и разведывательных служб и хотя важно бороться с онлайн-сексуальными надругательствами над детьми и нейтрализовать угрозы терроризма, защита прав человека граждан является также законной и необходимой в демократическом обществе. Технологии, позволяющие преступникам и террористам избегать обнаружения или предпринимать злобные нападки, также приносят огромную пользу с точки зрения кибербезопасности, неприкосновенности частной жизни и экономики⁷. Ослабление технологии шифрования ставит под угрозу безопасность современной информационной экономики⁸.

24. Устранение осложнений, вызываемых шифрованием для правоохранительных расследований и сбора разведывательных данных, требует подхода, исключающего ослабление принципов шифрования и, следовательно, национальной безопасности других стран.

25. Я рекомендую государствам-членам подход, используемый правительством Нидерландов, которое признало, что национальные действия не могут рассматриваться отдельно от их международного контекста, равно как и отсутствие вариантов, которые позволяли бы ослабить программное обеспечение шифрования, не ставя под угрозу безопасность цифровых систем, применяющих шифрование⁹.

26. Международный форум по надзору за деятельностью разведывательных служб с участием Специального докладчика соберется на Мальте в конце ноября 2018 года. Интерес к форуму настолько велик, что количество потенциальных участников уже превысило намеченные цифры.

⁶ Justin Hendry, "Decryption laws enter parliament", IT News, 20 September 2018.

URL: www.itnews.com.au/news/decryption-laws-enter-parliament-512867?eid=1&edate=20180921&utm_source=20180921_AM&utm_medium=newsletter&utm_campaign=daily_newsletter.

⁷ James A. Lewis, Denise E. Zheng and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (Washington, D.C., Center for Strategic and International Studies, 2017). URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.r.rE.

⁸ New America, "Coalition raises serious concerns about Australian draft bill and encryption backdoors", press release, 10 September 2018; Michelle Mosey and Adam Henschke, "Defining thresholds in law – sophisticated decryption and law enforcement", National Security College Policy Options Paper, No. 8 (Australian National University, April 2018).

⁹ G.A. Van der Steur, Minister of Security and Justice, and H.G.J. Kamp, Minister of Economic Affairs, The Netherlands, "Cabinets view on encryption", position letter provided to the President of the House of Representatives of the States General, 4 January 2016.

Е. Сообщения

27. За период с 22 сентября 2017 года Специальный докладчик направил 17 сообщений, включая 8 «писем с информацией о предполагаемых нарушениях», 7 «прочих писем» и 2 «срочных призыва». Из 17 сообщений 15 были направлены совместно с другими мандатариями специальных процедур, а 2 сообщения — одним Специальным докладчиком.

Ф. Promoting право на неприкосновенность частной жизни

28. Специальный докладчик сотрудничал с другими мандатариями специальных процедур посредством выпуска совместных пресс-релизов и заявлений и обмена советами и информацией. Специальный докладчик подтверждает конструктивные консультации со Специальным докладчиком по вопросу о насилии в отношении женщин, его причинах и последствиях.

29. Специальный докладчик выпустил 11 пресс-релизов и заявлений. Два из них были выпущены совместно с другими мандатариями: один — о правах эко-активистов на предстоящей двадцать четвертой сессии Конференции сторон Рамочной конвенции Организации Объединенных Наций об изменении климата¹⁰; и второй — о проекте закона Мексики по вопросам безопасности¹¹.

30. 19 и 20 февраля 2018 года Специальный докладчик выступил с презентацией о роли права на неприкосновенность частной жизни в рамках прав человека и в связи с защитой возможностей для гражданской активности и был модератором на сессии, посвященной новым и формирующимся тенденциям, в ходе семинара-практикума экспертов по вопросу о праве на неприкосновенность частной жизни в цифровую эпоху, организованного в Женеве УВКПЧ.

Г. Посещение стран

31. В июне 2018 года Специальный докладчик посетил Соединенное Королевство. В его заявлении по окончании поездки он высказал предварительные замечания¹². Окончательный доклад будет представлен Совету по правам человека на его сороковой сессии.

32. В 2015 году Специальный докладчик высказал критические замечания по поводу законодательных предложений, усиливавших полномочия правительства Соединенного Королевства в области слежки. С тех пор произошли значительные улучшения в режиме надзора за деятельностью разведывательных служб, включая создание лучше обеспеченного ресурсами Управления Комиссара по вопросам следственных полномочий и системы «двойного запора», в рамках которых персонал, равноценный пяти работающим на полную ставку судебным уполномоченным, занимается обзором наиболее чувствительных решений о предоставлении разрешения, одобренных высокопоставленными правительственными чиновниками, такими как министр внутренних дел и министр ино-

¹⁰ Office of the United Nations High Commissioner for Human Rights (OHCHR), “UN experts urge Poland to ensure free and full participation at climate talks”, 7 May 2018. URL: www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23042&LangID=E.

¹¹ OHCHR, “Mexico draft security law threatens rights and should be rejected, UN rights experts warn”, 14 December 2017. URL: www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22535&LangID=E.

¹² См. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E.

странных дел. Одним позитивным аспектом является то, что эти гарантии против произвольной или незаконной слежки применяются в равной мере ко всем лицам, находящимся под наблюдением властей Соединенного Королевства в пределах его территории, без каких-либо различий по признаку национальности или места проживания.

33. Специальный докладчик по-прежнему обеспокоен возможными недоработками в новом Законе о следственных полномочиях 2016 года, включая требование о том, чтобы Управление Комиссара по вопросам следственных полномочий выполняло двойную задачу — разрешало слежку и вело надзор за той же слежкой. Это может ставить под угрозу независимость надзора постфактум.

34. Специальный докладчик выявил необходимость в ясных и твердых руководящих указаниях и в надзоре за любым соглашением об обмене данными в отношении Национальной службы здравоохранения и настоятельно рекомендовал, чтобы эти руководящие указания стали достоянием гласности при первой же возможности. Обсуждения с Хранителем национальных данных наводят на мысль о том, что это может произойти в ближайшие 12–24 месяца. Специальный докладчик рекомендовал, чтобы роль Хранителя данных была как можно скорее закреплена в законе.

35. Другие вопросы в его заявлении по окончании поездки касаются мер по борьбе с радикализацией и программы «Предотвращение» и их воздействия на мусульман; предложений об установлении уголовной ответственности за доступ к экстремистским материалам; и проблем, поднятых организациями гражданского общества.

Планируемые поездки в страны

36. Следующей официальной поездкой в страну будет поездка в Германию в период с 29 октября по 9 ноября 2018 года, которой будет предшествовать призыв к заинтересованным сторонам вносить взносы, который будет помещен на веб-странице УВКПЧ, посвященной этому мандатария.

Неофициальные поездки и международные мероприятия

37. Во время посещения Австралии для консультаций по вопросам больших данных и открытых данных Специальный докладчик побывал в трех штатах и встретился с организациями гражданского общества, одним из правительственных министров и теневым Генеральным прокурором, правительственными чиновниками, представителями корпораций и профессиональных ассоциаций, научными работниками и другими лицами. Он также встретился с австралийским Уполномоченным по правам человека и с Председателем Комиссии и выступил с публичными лекциями в Университете Нового Южного Уэльса, Сидней; Мельбурнском университете; Университете Ла Троба; и Университете Эдит Коуэн. Центр кибербезопасности корпорации «Оптус» и Университета Маккуори организовал брифинг с участием Специального докладчика и ведущих зарегистрированных компаний. Секция Австралии и Новой Зеландии Международной ассоциации специалистов по вопросам неприкосновенности частной жизни организовала встречи со специалистами-практиками, занимающимися вопросами неприкосновенности частной жизни.

38. Специальный докладчик также участвовал в шестнадцатой Международной конференции по вопросам киберпространства, состоявшейся в Чехии в ноябре 2017 года; одиннадцатой Международной конференции по вопросам компьютеров, неприкосновенности частной жизни и защите данных, состоявшейся в Брюсселе в январе 2018 года; семинаре-практикуме экспертов по вопросу о

праве на неприкосновенность частной жизни в цифровую эпоху, проведенном в Женеве в феврале 2018 года; Конференции по вопросам глобального Интернета и юрисдикции, состоявшейся в Оттаве в феврале 2018 года; и конференции в рамках проекта МАППИНГ, проведенной на Мальте в феврале 2018 года.

Н. Изменения, касающиеся права на неприкосновенность частной жизни

Способность обращаться к средствам правовой защиты

39. Специальный докладчик продолжал обращать внимание соответствующих государств-членов на утверждения о нарушениях права на неприкосновенность частной жизни, и в своем докладе 2018 года он проинформировал Совет по правам человека о нарушениях статьи 12 Всеобщей декларации по правам человека и статьи 17 Международного пакта о гражданских и политических правах.

40. Специальный докладчик по-прежнему убежден в том, что для возмещения вреда, причиненного нарушениями неприкосновенности частной жизни, необходима уверенность в получении доступа к справедливому слушанию дела и возможному средству правовой защиты. Способность получать доступ к средствам правовой защиты имеет ключевое значение для защиты прав человека и по-прежнему занимает видное место среди приоритетов Специального докладчика.

Искусственный интеллект

41. Поскольку все больше решений, сказывающихся на жизни всех людей, принимаются с использованием алгоритмов и машинного обучения, их воздействие на права человека требует тщательной и постоянной оценки.

42. Эти технологии являются настолько вездесущими, что на них даже полагаются в качестве доказательств в ходе судебных разбирательств. Однако то, как действуют сложные алгоритмы, остается большей частью неизвестным, так же как и прогрессия их развития в случае машинного обучения. Анализ этого с точки зрения всех прав человека необходим до выработки — или параллельно с выработкой — политики, стимулирующей и создающей возможности для разработки и использования продуктов, основанных на искусственном интеллекте¹³. Твердые правовые и этические основы крайне важны для защиты затрагиваемых прав человека.

Принятие законодательства о неприкосновенности частной жизни и защите данных на глобальном уровне

43. Значительно возросло число стран, принявших законы о неприкосновенности частной жизни или о защите данных¹⁴; 2018 год стал особенно активным годом в этом отношении по всему миру.

44. Следует особо отметить проект закона Индии, последовавший за решением, вынесенным Верховным судом по делу *Путтасвами*¹⁵. Законопроект,

¹³ Priyanar Bhunia, “Taskforce recommends establishment of national mission for coordinating AI-related activities across India”, Open Gov, 9 April 2018.

¹⁴ Graham Greenleaf, “Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey — 145 privacy laws and business international report 10, 2017”, University of New South Wales Law Research Series, No. 45 (2017).

¹⁵ Supreme Court of India, Civil Original Jurisdiction, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*, Writ Petition (Civil) No. 494 of 2012, Judgment, 24 August 2017. URL: [http://supremecourtfindia.nic.in/pdf/jud/ALL%20WP\(C\)](http://supremecourtfindia.nic.in/pdf/jud/ALL%20WP(C))

опубликованный в середине 2018 года, имеет много позитивных моментов, присутствующих также в Общем регламенте по защите данных № 2016/679 Европейского союза, таких как оценки воздействия на защиту данных, право быть забытым и неадекватные санкции в целях обеспечения соблюдения обязательств. Но в нем есть и вызывающие беспокойство моменты, такие как ограничения в отношении исследований на предмет потенциальной реидентификации людей в предположительно обезличенных наборах данных. Более того, хотя использование персональных данных правоохранительными органами должно быть «необходимым и пропорциональным», раскрытие информации в рамках процессуальных действий связано с широкими исключениями¹⁶. Специальный докладчик настоятельно призывает правительство Индии наладить взаимодействие с учеными, исследователями и организациями гражданского общества, которые поднимают такие вопросы.

45. В постановлении от 26 сентября 2018 года Верховный суд Индии поддержал конституционность Закона об уникальном идентификационном номере «Аадхаар», но при этом отменил: а) раздел 57, на основании которого частные компании могут просить у потребителей детальные данные за использование программы «Аадхаар» для целей идентификации; b) раздел 33 (2), касающийся обмена данными со службами безопасности по причинам национальной безопасности; и c) раздел 47, на основании которого только правительство может подавать жалобу в случае кражи данных системы «Аадхаар»¹⁷. Суд потребовал от правительства представления надежного законодательства о защите данных.

46. В рамках Европейского союза произошла существенная реформа. Общий регламент по защите данных вступил в силу 25 мая 2018 года, и специальная директива о защите данных в сферах полиции и правосудия стала применяться с 6 мая 2018 года. Директива о конфиденциальности и электронных сообщениях 2002/58/ЕС подлежит замене новым Постановлением об уважении неприкосновенности частной жизни и защите персональных данных в электронных сообщениях (ePrivacy)¹⁸. Постановление (ЕС) 45/2001 устанавливает правила по защите данных в учреждениях Европейского союза и определяет обязанности Уполномоченного Европейского союза по защите данных. Европейская комиссия приняла 10 января 2017 года предложение, отменившее это Постановление и приведшее его в соответствие с Общим регламентом по защите данных; предполагается, что обе эти меры будут применяться с конца 2018 года. Благодаря этой реформе Европейский союз завершит первую за 20 с лишним лет крупную модернизацию своей нормативно-правовой основы по защите неприкосновенности частной жизни и защите данных¹⁹.

47. Эти важные меры по упорядочению норм в рамках Европейского союза применяются ко всем секторам, за исключением частной жизни и «националь-

[%20No.494%20of%202012%20Right%20to%20Privacy.pdf](#).

¹⁶ Richard Chirgwin, “India mulls ban on probes into anonymized data use – with GDPR-style privacy laws”, The Register, 31 July 2018. URL: www.theregister.co.uk/2018/07/31/india_privacy_boffin_ban/.

¹⁷ Supreme Court of India, Civil Original Jurisdiction, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*; Economic Times, “This is what the Supreme Court did not like about Aadhaar”, 26 September 2018. URL: http://economictimes.indiatimes.com/articleshow/65961697.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

¹⁸ Cm. European Commission, “Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)”, 10 January 2017.

¹⁹ Cm. https://edps.europa.eu/data-protection/data-protection/legislation_en.

ной безопасности» — этот вопрос исключен из сферы компетенции Европейского союза на основании статьи 4.2 Договора о Европейском союзе. Слежение в рамках национальной безопасности, а не правоохранительной деятельности регулируется гораздо более разнородным образом в пределах Европейского союза вследствие усилий таких стран, как Бельгия, Нидерланды, Соединенное Королевство и Франция по обновлению своего законодательства.

48. В более широких региональных рамках отразить, что в июне 2018 года была доработана Модернизированная конвенция о защите физических лиц при автоматизированной обработке персональных данных (также известная как «Модернизированная конвенция 108»), и соответствующий подзаконный правовой акт (Протокол CETS 223) был открыт для подписания 10 октября 2018 года. Это — важная веха, поскольку, в отличие от Общего регламента по защите данных, Конвенция также охватывает вопросы национальной безопасности, ее ратифицировали более 55 государств-членов Организации Объединенных Наций, и к ней присоединяется все больше неевропейских государств.

49. В Бразилии Сенат одобрил общий закон о защите данных, который вступит в силу в феврале 2020 года. Ключевые элементы включают²⁰: трансграничную юрисдикцию; принципы неприкосновенности частной жизни и основанный на рисках подход; новые права для физических лиц; больше правовых основ для обработки персональных данных; картирование данных и оценки воздействия на защиту данных; обязательное уведомление о нарушениях и сотрудника по защите данных; и ограничения на трансграничную передачу персональных данных.

50. Штрафы за несоблюдение этих положений могут достигать 2 процентов валового объема продаж компании или группы компаний, либо максимальной суммы за одно нарушение в объеме примерно 12,9 млн долл. США.

Коренные народы и данные

51. Специальный докладчик изучал на протяжении многих лет культуру уважения частной жизни австралийских аборигенов. Ввиду того, что эта культура представляет собой одно из самых утонченных, жизненных выражений неприкосновенности частной жизни на уровне индивидуума, семьи и группы, реализуемых посредством норм поведения, обрядов и порядков, таких как личное и общественное пространство, Специальный докладчик рад тому, что в ходе консультаций по большим данным и открытым данным были рассмотрены, хотя и сдержанным образом, вопросы суверенитета коренных народов над данными.

52. Специальный докладчик рекомендует правительствам и корпорациям признать неотъемлемый суверенитет коренных народов в отношении данных о них или собранных от них, которые относятся к системам знаний, обычаям или территориям коренных народов.

II. Консультации относительно предыдущего доклада Специального докладчика Генеральной Ассамблеи

53. В своем докладе Генеральной Ассамблеи от октября 2017 года (A/72/540) Специальный докладчик рассмотрел проблемы на пути обеспечения права человека на неприкосновенность его частной жизни в контексте одной из определяющих характеристик цифровой эпохи: больших данных и открытых данных. С тех пор был принят Общий регламент по защите данных и имели место случаи

²⁰ См. www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/.

раскрытия информации, имеющие отношение к сети «Фейсбук» и к компании Cambridge Analytica.

54. Консультация с правительственными чиновниками, организациями гражданского общества, компаниями и физическими лицами по этому докладу была проведена в Австралии 26 и 27 июля 2018 года. Ей предшествовал призыв о представлении материалов, срок для подачи которых завершился 28 апреля 2018 года, и полученные материалы были резюмированы для целей консультации. Дальнейший вклад был получен за счет встреч организаций гражданского общества, проведенных Австралийским фондом защиты частной жизни, и материалов, полученных после проведения консультации.

А. Резюме полученных откликов

55. В ходе публичной консультации были рассмотрены истоки и виды использования больших данных и открытых данных; потенциальные выгоды и потенциальный вред от одних и от других; воздействие использования персональных данных на другие права человека; адекватность методов деидентификации; передовая практика в использовании персональных данных; важность прав человека и норм этики в технологиях автоматизированного принятия решений; суверенитет коренных народов над данными; потребительские и гендерные вопросы; и мнения неевропейских стран²¹. Обсуждения в основном касались открытых данных и последствий их взаимодействия с большими данными для неприкосновенности частной жизни.

В. Открытые данные

56. Анализ больших данных и методы вычислений, основанные на искусственном интеллекте, приносят пользу, но одновременно вызывают потенциальные риски с точки зрения защиты от несанкционированного доступа для индивидумов и общин, а также для самой структуры демократического общества. Открытие правительственной информации, в частности повторяющееся публичное разглашение наборов данных, содержащих личную информацию, требует более нюансированного и тщательного изучения²².

57. В ходе консультации было рассмотрено предположение о том, что аналитика больших данных может идентифицировать физических лиц, несмотря на их деидентификацию²³. Участники заслушали информацию о том, как установление того, содержат ли данные или результаты аналитической обработки данных персональную информацию, зависит от обстоятельств использования или раскрытия, и как это может меняться в зависимости от других факторов. Соответственно, реидентификацию лучше всего описывать с точки зрения уровней риска, а не как какое-то абсолютное понятие. Уровни риска основаны на том, кто имеет доступ к данным, насколько детализированными являются данные (размеры самой мелкой группы данных), какие другие наборы данных можно аккуратно связать с этими данными и соответствующим внешним контекстом.

²¹ Amanda Lo, "The right to privacy in the age of big data and open data", The Allens Hub for Technology, Law and Innovation, University of New South Wales, 21 August 2018.

²² Материал, представленный М. Патерсоном, Университет Монаша, август 2018 года.

²³ См. Office of the Victorian Information Commissioner, "Protecting unit-record level personal information: the limitations of de-identification and the implications for the Privacy and Data Protection Act 2014", May 2018. URL: <https://ovic.vic.gov.au/resource/protecting-unit-record-level-personal-information/>.

58. «Личная информация» в структуре данных охватывает широкую область, и ее описания варьируются в разных юрисдикциях. Общим для большинства определений является то, что сфера личной информации может быть широкой и может иметь отношение к способности идентифицировать то или иное лицо, а не только то, что сами данные идентифицируют это лицо.

59. Два главных аспекта для выявления данных, содержащих личную информацию, сводятся к следующему: а) сами данные должны идентифицировать лицо; или б) должна иметься разумная возможность идентифицировать то или иное лицо.

60. Каждый из трех основных механизмов для обмена данными — явный, производный и логически выводимый — сопровождается соображениями относительно степени содержащейся личной информации и обязательств организации, которая собирает, использует и хранит эти данные.

61. Онлайн-просмотр и покупка данных могут использоваться для все большей персонализации услуг, не зная о личности пользователя. Вместе с тем высказывается обеспокоенность насчет того, составляют ли личную информацию узкоспециализированные анонимные идентификаторы. Данные мобильных сетей используются в целях, выходящих за рамки оптимизации сетей, позволяя прогнозировать отток клиентов или даже указывать на взаимосвязь с другими абонентами мобильной связи, не зная личность соответствующих индивидуумов²⁴.

62. Одна из главных проблем для обмена данными заключается в том, что сейчас нет никакого метода, позволяющего однозначно определить, имеется ли личная информация в рамках агрегированных данных или можно ли вновь агрегировать дезагрегированные данные. Риск реидентификации зависит от доступа к соответствующим наборам данных (и способности увязать их), методов, используемых для деидентификации, и уровня агрегирования или перемешивания данных. Следовательно, различные методы и уровни агрегирования данных используются разными организациями в зависимости от усматриваемого риска, связанного с совместно используемыми данными.

63. Разработка стандартов для определения того, что составляет «деидентифицированные данные», поможет решить проблемы, касающиеся неприкосновенности частной жизни. На международном уровне в настоящее время существует только руководство очень высокого уровня — и, разумеется, ничего количественного, — касательно того, что означает «деидентифицированный», и поэтому многие организации должны определять, что именно это понятие означает для них в каждом конкретном случае на основе различных наборов данных и того, как их можно разумно использовать или сочетать с другими данными.

64. В 2017 году Австралийское компьютерное общество выпустило технический информационный документ, в котором оно проанализировало проблемы с обменом данными и особо отметило то, что одной из фундаментальных проблем для создания интеллектуальных услуг является вопрос о том, содержит ли тот или иной набор данных личную информацию. Ответ на этот вопрос является сложной задачей, поскольку само объединение наборов данных порождает информацию. В документе также предлагался модифицированный вариант концепции «пяти безопасных компонентов» для обмена данными в целях количественного определения различных пороговых величин для «безопасного компонента». Эта работа продолжается при поддержке Австралийской организации по стандартам и имеет целью инициировать работу по выработке международных

²⁴ Материал, представленный Иэном Опперманом, Центр по аналитике данных, правительство Нового Южного Уэльса, Австралия, 31 августа 2018 года.

стандартов касательно сохранения неприкосновенности частной жизни и обмена данными. Второй информационный документ запланирован на октябрь 2018 года, и предполагается, что он заложит основу для международной деятельности по стандартизации с целью, в конечном итоге, определить надежную основу для сохранения неприкосновенности частной жизни и обмена информацией²⁵.

65. Примером ограничений деидентификации для целей защиты записей на уровне единичной записи была публикация в Интернете в августе 2016 года большого набора продольных данных в отношении 10-процентной выборки австралийцев, которые требовали возмещения по линии страховой программы «Медикэр» с 1984 года либо льготного лекарственного обеспечения с 2003 года²⁶. Это сказалось на медицинских сведениях в отношении примерно 2,9 млн австралийцев, включая рецепты, случаи хирургического вмешательства, анализы (исключая результаты) и визиты к врачам общей практики и специалистам (исключая справки от врача)²⁷. Указанный набор данных был скачан 1500 раз, прежде чем его удалили из Интернета после поступления сообщений о том, что производимую врачами идентификацию можно легко расшифровать²⁸, после чего можно идентифицировать пациентов²⁹. Эта публикация Министерством здравоохранения Австралии имела целью содействие медицинским исследованиям.

66. Такие примеры ставят важные вопросы, такие как следует ли публиковать для внешнего пользования имеющиеся у правительства наборы данных с персональной информацией, когда существуют все большие угрозы крупномасштабных нарушений неприкосновенности частной жизни в результате реидентификации, отчасти вследствие наличия другой обнародованной информации, и неадекватных технических возможностей организаций; и в чем заключаются соответствующие ответные меры, дабы предотвратить повторение таких инцидентов.

67. Из информации, собранной в ходе консультации, стало ясно, что публикация имеющейся в распоряжении правительства информации требует адекватных мер по защите неприкосновенности частной жизни и нормативно-правовому регулированию. Звучали твердые мнения о том, что неограниченный доступ к данным на уровне единичной записи, а также другим личным данным, которые не

²⁵ Ibid., including Australian Computer Society, *Data Sharing Frameworks*, Technical White Paper (Sydney, 2017). URL: www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf.

²⁶ Материал, представленный Ванессой Тиг Специальному докладчику во время консультаций по большим данным и открытым данным, 26 и 27 июля 2018 года, Университет Нового Южного Уэльса, Сидней, Австралия. См. также Office of the Australian Information Commissioner, “Publication of MBS/PBS data”, Commissioner-initiated investigation report, 20 March 2018, pp. 7–9. URL: www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data.pdf.

²⁷ Vanessa Teague, Chris Culnane and Ben Rubinstein, “The simple process of re-identifying patients in public health records”, University of Melbourne, Pursuit, 18 December 2017. URL: <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records>.

²⁸ Chris Culnane, Benjamin Rubinstein and Vanessa Teague, “Health data in an open world”, report on re-identifying patients in the MBS/PBS dataset and the implications for future releases of Australian Government data, University of Melbourne, 18 December 2017. URL: <https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf>.

²⁹ Управление австралийского Комиссара по информации установило, что врачи поддаются идентификации и что пациенты также могут быть идентифицированы, но не являются «в разумной степени идентифицируемыми», если использовать терминологию австралийского Закона о неприкосновенности частной жизни. Предполагается, что соответствующие люди не были уведомлены.

могут безопасно разглашаться в агрегированном виде, несовместим с правом на неприкосновенность частной жизни. Полученные комментарии и отзывы не поддерживали меры нормативно-правового регулирования, опирающиеся на установление уголовной ответственности за реидентификацию, предпринимаемую с целью проверить защищенность опубликованных наборов данных³⁰.

68. Участники рассказали о существующих механизмах, которые позволяют использовать поддающиеся идентификации личные данные в исследовательских целях³¹, указав, что их можно расширить, в зависимости от обстоятельств, для дальнейшего использования в общественных интересах³².

69. Вопрос, как представляется, заключается в том, добьемся ли мы более устойчивой практики, если полезные данные будут рассматриваться как ограниченный ресурс, а не как неограниченный неиспользуемый ресурс³³.

70. Нынешняя практика, отчуждающая субъект персональных данных сравнивалась, образно говоря, с ситуацией, когда «режут курицу, несущую золотые яйца», поскольку неверие в способность правительства или частных субъектов надлежащим образом распоряжаться персональной информацией приводит к тому, что люди либо не пользуются услугами — это, в свою очередь, создает угрозу негативного воздействия на общество, например, в сферах здравоохранения, — либо дают неполную или неточную информацию³⁴. Эти действия подрывают также качество данных и, в конечном итоге, точность алгоритмов для машинного обучения.

71. Мнение подавляющего большинства участников консультации сводилось к тому, что устойчивость порядка обращения с персональными данными увеличивается, если субъекты данных являются полноправными партнерами в операциях с данными³⁵. Участники услышали, что нигде это не является столь очевидным и важным, как в отношении коренных народов.

С. Суверенитет коренных народов над данными

72. Данные являются культурным, стратегическим и экономическим ресурсом для коренных народов. Но при этом коренные народы остаются в значительной степени оторванными от сбора, использования и применения данных о них самих, их землях и их культуре³⁶. Существующие данные и инфраструктура данных не признают и не отдают привилегию знаниям и мировоззрениям коренных

³⁰ Материалы, представленные, в частности, М. Патерсоном.

³¹ Эти механизмы обычно подлежат надзору со стороны комитетов по вопросам этики, причем доступ ограничивается исследователями, на которых лежат обязательства по сохранению конфиденциальности.

³² Например, на основе таких механизмов, как «пять безопасных компонентов»: см. Australian Bureau of Statistics, “Managing the risk of disclosure: the five safes framework”, Confidentiality Series, part 3, August 2017. URL: www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S.

³³ Материал, представленный Терезой Дирндорфер Андерсон, Технологический университет, Сидней, Австралия.

³⁴ Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey, 2017* (Canberra, 2017). URL: www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017; Australia, Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey: Research Report 2013* (Canberra, 2013). URL: www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf.

³⁵ Материал, представленный Терезой Дирндорфер Андерсон.

³⁶ Tahu Kukutai and Maggie Walter, “Recognition and indigenizing official statistics: reflections

народов и не соответствуют нынешним и будущим потребностям коренных народов в данных. Нынешняя практика касательно больших данных и открытых данных, под эгидой будь то правительств или корпораций, по-видимому, отодвигает интересы коренных народов в том, что касается данных, еще дальше от тех инстанций, на которых принимаются решения, затрагивающие данные коренных народов.

73. Суверенитет коренных народов над данными — это глобальное движение, занимающиеся правами коренных народов в том, что касается владения данными, контроля над ними, наличия доступа к ним и обладания данными, получаемыми от них и имеющими отношение к их членам, системам знаний, обычаям или территориям³⁷. Оно подкрепляется правами коренных народов на самоопределение и на управление их землями, ресурсами и культурой, как указано в Декларации Организации Объединенных Наций о правах коренных народов. Из суверенитета коренных народов над данными имплицитно вытекает желание использовать данные так, чтобы поддерживать и улучшать коллективное благосостояние коренных народов.

74. Суверенитету коренных народов над данными принадлежит определенное место в качестве одного из основополагающих принципов механизмов управления, касающихся больших данных и открытых данных. Он реализуется посредством управления данными со стороны коренных народов, которое включает принципы, структуры, механизмы подотчетности, политику, относящуюся к управлению данными, неприкосновенности частной жизни и безопасности, и правовые инструменты. Модели суверенитета коренных народов над данными могут применяться к данным нации/племени, находящимся под их внутренним контролем или в их исключительной собственности, а также данным, которые хранятся или которыми распоряжаются вовне. Сети по вопросам суверенитета коренных народов над данными в Австралии и Новой Зеландии разрабатывают протоколы по вопросам управления данными коренных народов³⁸.

75. Суверенитет коренных народов над данными иллюстрирует, что передовая практика относительно больших данных и открытых данных требует осведомленности о данных, которые отсутствуют, недостаточно представлены или неправильно представлены³⁹, и об интересах, которым отвечает — или не отвечает — такая практика.

D. Гендерные вопросы

76. На консультации прозвучало мнение о том, что неприкосновенность частной жизни может ощущаться по-разному людьми разного пола или разной гендерной идентичности.

77. Неприкосновенность частной жизни представляет собой предмет особой обеспокоенности для лесбиянок, гомосексуалов, бисексуалов, транссексуалов,

from Aotearoa New Zealand and Australia”, *Statistical Journal of the IAOS*, vol. 31, No. 2 (2015).

³⁷ Tahu Kukutai and John Taylor, “Data sovereignty for indigenous peoples: current practice and future needs” and C. Matthew Snipp, “What does data sovereignty imply: what does it look like?”, both in Kukutai and Taylor (eds), *Indigenous Data Sovereignty: Towards an Agenda*, Research Monograph, 2016/38 (Canberra, Australian University Press, 2016). URL: <https://press.anu.edu.au/publications/series/centre-aboriginal-economic-policy-research-caepr/indigenous-data-sovereignty>.

³⁸ Материал, представленный Мэгги Уолтер, Университет Тасмании, Австралия.

³⁹ Материал, представленный Терезой Дирндорфер Андерсон.

интерсексуалов и лиц, сомневающих в своей гендерной идентичности, например, и может также иметь существенное значение для безопасности тех — обычно женщин, — кто спасается от домашнего, семейного или религиозного насилия.

78. В то время как инклюзивные методы сбора данных говорят о признании и уважении, интрузивные методы сбора могут быть существенным барьером на пути получения доступа к услугам, поскольку общины лесбиянок, гомосексуалов, бисексуалов, транссексуалов, интерсексуалов и лиц, сомневающих в своей гендерной идентичности, и другие лица испытывают обоснованную обеспокоенность по поводу неприкосновенности частной жизни, так как они уже столкнулись с опытом дискриминации, стигматизации и целенаправленного насилия.

79. Этот вопрос будет более детально рассмотрен рабочей группой по вопросам неприкосновенности частной жизни и личности. Однако, если смотреть с точки зрения больших данных и открытых данных, то передовая практика требует обзора того, как собираются данные, и осведомленности о возможном воздействии несовершенной практики в отношении неприкосновенности частной жизни и различных результатов на людей разного пола и разной гендерной идентичности.

Е. Права потребителей и сбор и использование персональных данных

80. На опирающихся на данные потребительских рынках использование все большего количества данных для разработки, продажи и рекламирования потребительских товаров означает, что многие вопросы защиты данных становятся также потребительскими вопросами и наоборот. Различие между законами о защите прав потребителей и законами о защите данных сейчас обозначено менее четко⁴⁰.

81. Использование финансовыми службами и другими секторами личных данных потребителей вызывает обеспокоенность на уровне как государственной политики, так и индивидуума⁴¹. Беспристрастная обработка персональных данных все в большей мере становится частью разумных ожиданий потребителей относительно используемых ими услуг и продуктов⁴².

82. В ходе консультации были сравнены подходы на основе законов о защите прав потребителей и законов о неприкосновенности частной жизни/защите данных, и при этом было отмечено, что в некоторых странах предпринимаются инициативы, касающиеся защиты личной информации потребителей.

⁴⁰ Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, "The perfect match? A closer look at the relationship between EU consumer law and data protection law", *Common Market Law Review*, vol. 54 (2017).

⁴¹ Lee Rainie and Maeve Duggan, "Privacy and information sharing", 14 January 2016 (people's comfort level depends on perception of trustworthiness, what happens post collection, and retention length). Phuong Nguyen and Lauren Solomon, *Consumer Data and the Digital Economy – Emerging Issues in Data Collection, Use and Sharing* (Consumer Policy Research Centre, 2018) (found consumers wanted more options over what data is collected, its use, and the Government to participate in improving consumer control over data and protections from data misuse).

⁴² Helberger, Zuiderveen Borgesius and Reyna, "The perfect match?".

83. После скандала, разразившегося с компанией Cambridge Analytica, в июне 2018 года штат Калифорния в Соединенных Штатах принял Закон о защите личной информации потребителей, который должен вступить в силу в январе 2020 года, в целях защиты конфиденциальности данных пользователей технологий и других лиц путем внедрения новых правил в отношении компаний, которые собирают, используют персональные данные и обмениваются ими⁴³. Закон устанавливает четыре основных права для индивидуумов: право знать, какую личную информацию о них имеет то или иное коммерческое предприятие, откуда эта личная информация поступила или куда она была отправлена; право удалять личную информацию, которую то или иное коммерческое предприятие собрало от них; право отказаться от продажи личной информации о них; и право получать от того или иного коммерческого предприятия равные услуги по равным ценам, даже если они осуществляют свои предусмотренные этим Законом права, касающиеся неприкосновенности частной жизни⁴⁴. Закон также предусматривает ограниченное право потребителей предъявлять иски коммерческим предприятиям за нарушения защиты данных от несанкционированного использования на основе существующего в Калифорнии законодательства относительно уведомлений о нарушении правил защиты данных.

84. Вместе с тем, как сообщалось, права, зафиксированные в этом Законе, необходимо усилить по следующим причинам:

- a) термин «коммерческое предприятие» имеет узкое определение⁴⁵. В цифровую эпоху мелкие технологические субъекты и физические лица могут также подрывать неприкосновенность частной жизни бесчисленным множеством путей ввиду отсутствия у них знаний, навыков или ресурсов для обеспечения надлежащей защиты данных⁴⁶;
- b) коммерческие предприятия до сих пор могут взимать более высокие цены с пользователей, осуществляющих свои права на неприкосновенность частной жизни;
- c) пользователи не могут легко привлекать нарушителей к суду ввиду узких исключений;
- d) согласие пользователя требуется только для продажи данных, но не для их сбора, и пользователям нужно отказываться от дачи согласия на продажу данных;
- e) «право знать» не предусматривает конкретные источники или конкретных получателей, а «право на удаление» относится к информации, собранной от них, но не к имеющейся информации о них;
- f) ответственность за обеспечение соблюдения лежит большей частью на калифорнийском Генеральном прокуроре, а не на какой-то независимой организации.

85. В соответствии с законодательством Европейского союза о защите данных аспекты Общего регламента по защите данных предусматривают новые меры по

⁴³ См. https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

⁴⁴ Adam Schwartz, Lee Tien and Corynne McSherry, “How to improve the California Consumer Privacy Act of 2018”, Electronic Frontier Foundation, 8 August 2018.

⁴⁵ Ibid., “the Act defines a “business” as a for-profit legal entity with: (i) annual gross revenue of \$25 million; (ii) annual receipt or disclosure of the personal information of 50,000 consumers, households, or devices; or (iii) receipt of 50 per cent or more of its annual revenue from selling personal information (Section 140(c))”.

⁴⁶ Материал, представленный Роландом Вэнем, Университет Нового Южного Уэльса, Сидней, Австралия.

защите потребителей в рамках Европейского союза, включая более высокую степень транспарентности и контроля над данными о них, собираемыми компаниями, чем это, возможно, предусмотрено директивами Европейского союза о защите прав потребителей⁴⁷.

86. Австралия внедряет «право на данные о потребителях» — право на переносимость данных⁴⁸, которое не дотягивает до более широких мер защиты, предусмотренных согласно законам о неприкосновенности частной жизни или о защите данных для австралийских потребителей, данные о которых собираются, распространяются и используются на каждодневной основе⁴⁹. В ходе консультации было высказано мнение о том, что это право на переносимость данных, а не защита потребительских данных может потенциально привести к их более широкому использованию третьими сторонами⁵⁰.

87. Есть плюс в установлении тесной связи между законодательством о защите прав потребителей и законодательством о неприкосновенности частной жизни, например, в случае скоординированных правовых действий⁵¹. Закон о защите прав потребителей может быть полезным инструментом для сохранения общего баланса в коммерческих отношениях между потребителями и поставщиками и может использоваться для оценки справедливости ситуаций, в которых компании требуют от потребителей согласия на обработку несоразмерных объемов данных и/или на обмен данными с третьими сторонами.

88. Полученные отклики и комментарии относительно практических мер для оказания юридическим лицам помощи в улучшении их доверительных отношений с пользователями включали передачу условий использования данных посредством стандартных лицензий наподобие шести стандартизованных лицензий Creative Commons. Это усматривалось как одно из потенциальных средств смягчения некоторых из проблем, связанных с комплексной политикой, касающейся неприкосновенности частной жизни, одновременно с упрощением и стандартизацией сообщений пользователям в различных странах⁵². Типы проектов лицензий могут подкрепляться более детальной политикой конфиденциальности по принципу «стандартных условий».

89. Выявление рисков для неприкосновенности частной жизни путем использования маркировочных ярлыков конфиденциальности может сделать варианты защиты личной информации более доступными для потребителей и повысить степень транспарентности и раскрытия рисков для неприкосновенности частной жизни контролерами данных⁵³.

⁴⁷ Helberger, Zuiderveen Borgesius and Reyna, “The perfect match?”.

⁴⁸ Australian Competition and Consumer Commission, “Consumers’ right to their own data is on its way”, press release, 16 July 2018. URL: www.accc.gov.au/media-release/consumers-right-to-their-own-data-is-on-its-way..

⁴⁹ Nguyen and Solomon, *Consumer Data and the Digital Economy*.

⁵⁰ Материал, представленный Катериной Кемп Специальному докладчику во время консультаций по большим данным и открытым данным, 26 и 27 июля 2018 года, Университет Нового Южного Уэльса, Сидней, Австралия.

⁵¹ Группа защиты потребителей в Соединенных Штатах и Европейском союзе совместно просили ведомства по защите потребителей и органы по защите данных проанализировать нарушения законодательства о защите данных и о защите прав потребителей в связи с игрушками, имеющими выход в Интернет. См. Helberger, Zuiderveen Borgesius and Reyna, “The perfect match?”.

⁵² Материал, представленный Центром Алленса по вопросам технологии, права и инноваций, 14 августа 2018 года.

⁵³ См. Lorrie Faith Cranor, “Necessary but not sufficient: standardized mechanisms for privacy notice and choice”, *Journal on Telecommunications and High Technology Law*, vol. 10, iss. 2 (Summer 2012).

Г. Искусственный интеллект

90. Машинное обучение и искусственный интеллект используют огромные количества данных и в свою очередь создают еще больше данных. Сочетание наличия данных, вычислительной мощности и аналитических способностей, использующих алгоритмы высокой сложности, в сочетании с машинным обучением и искусственным интеллектом могут революционизировать общества в позитивном направлении, но одновременно могут и глубоко изменить наш мир и наши шансы выживания, причем не обязательно к лучшему⁵⁴.

91. Последний из указанных результатов может произойти в результате потенциально негативного воздействия искусственного интеллекта на права человека, включая право на неприкосновенность частной жизни. Методы искусственного интеллекта могут использоваться и используются для идентификации людей, которые хотят остаться анонимными; для микроадресации рассылаемых сообщений; для получения конфиденциальной информации о людях из неконфиденциальных данных; для профилирования людей на основе данных в масштабах всего населения; и для вынесения решений с использованием этих данных, тем самым оказывая глубокое воздействие на жизнь людей⁵⁵.

92. Поскольку все больше действий и решений поручаются машинам, настоятельно необходимо обеспечить прозрачность машинного обучения и алгоритмов с точки зрения их логики и их допущений. Алгоритмы, используемые в машинном обучении и искусственном интеллекте, становятся все более сложными, и обеспечить прозрачность будет трудно. Но эта сложность не должна препятствовать проверке на предмет подтверждения законности⁵⁶. В настоящее время использование технологий больших данных не влечет достаточной степени ответственности в том, что касается соблюдения норм международного права прав человека, положений о защите данных, секторальных положений о неприкосновенности частной жизни, этических кодексов или промышленных стандартов⁵⁷. Утверждается, что машины должны соблюдать более высокие этические стандарты, чем люди, и что, при наличии правильного выбора, неприкосновенность частной жизни будет не исторической аномалией, а вместо этого технологией данным правом⁵⁸.

93. Общий регламент по защите данных ограничивает использование автоматизированного принятия решений в определенных обстоятельствах и требует предоставления лицам информации относительно существования механизма автоматизированного принятия решений, используемой логики, а также значения и предполагаемых последствий обработки таких данных для соответствующего лица⁵⁹. Существует общий запрет — с небольшими исключениями — в отношении решений, выносимых исключительно за счет автоматизированных процессов, когда такие решения влекут за собой правовые или иные существенные последствия.

⁵⁴ Toby Walsh, 2062: *The World that AI Made*, (Carlton, Victoria, Australia, La Trobe University Press, 2018).

⁵⁵ Privacy International and Article19, "Privacy and freedom of expression in the age of artificial intelligence", April 2018.

⁵⁶ European Union Agency for Fundamental Rights, #BigData: *Discrimination in Data Supported Decision Making* (Luxembourg, European Union Publications Office, 2018).

⁵⁷ Lee Rainie and Janna Anderson, *Code-Dependant: Pros and Cons of the Algorithm Age* (Pew Research Center, 2017).

⁵⁸ Walsh, 2062: *The World that AI Made*.

⁵⁹ European Union General Data Protection Regulation 2016/679 of 27 April 2016, articles 13, 14 and 22.

94. Регламент определяет профилирование как автоматизированную обработку данных в целях анализа или составления прогнозов об отдельных людях и устанавливает обязательство относительно включения защиты данных сознательно и автоматически. Оценки воздействия на конфиденциальность данных станут обязательными для многих инвазивных с точки зрения неприкосновенности частной жизни режимов использования искусственного интеллекта и машинного обучения, которые подпадают под действие законодательства о защите данных и которые связаны с существенными предполагаемыми рисками, такими как обработка конфиденциальных сведений. В случае искусственного интеллекта оценка воздействия на конфиденциальность данных может — возможно, должна — позволять юридическим лицам моделировать воздействие их алгоритмов примерно так же, как ученые-климатологи моделируют изменение климата или погодные условия⁶⁰.

95. Агентство Европейского союза по основным правам высказало мысль о том, что один из методов обеспечения эффективной подотчетности может предусматривать создание специальных органов с исключительным мандатом на обеспечение надзора над технологиями, связанными с большими данными, аналогично роли органов по защите данных⁶¹.

96. Хотя средства еще предстоит определить, важно то, что новые технологии потребовали укрепления международного гуманитарного права на протяжении XX века⁶².

G. Принципы, касающиеся больших данных и открытых данных

97. В своем докладе от октября 2017 года Специальный докладчик поднял вопрос о разработке принципов для регулирования больших данных и открытых данных. Консультация показала, что любая такая разработка должна, насколько это возможно, опираться на международные соглашения о защите данных, рассматриваемые в качестве «передовой практики». В настоящее время ими являются Общий регламент по защите данных и Модернизированная конвенция 108, причем Конвенция берет начало в Совете Европы, но открыта на глобальном уровне для присоединения государств, принявших согласованные принципы⁶³.

98. Влияние Общего регламента по защите данных ощущается не только посредством принятия местных законодательных актов или его экстерриториального применения. Компании за пределами Европы — самым ярким примером является «Майкрософт» — добровольно идут на соблюдение Регламента во всех своих коммерческих операциях, независимо от юридического обязательства делать это. Такой добровольный выбор, возможно, является столь же значимым, что и предусмотренный законом вариант действий⁶⁴.

⁶⁰ Andrew Smith, “Franken-algorithms: the deadly consequences of unpredictable code”, The Guardian, 30 August 2018. URL: <https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger>, quoting Neil F. Johnson and others, “Population polarization dynamics and next-generation social media algorithms”, 16 December 2017. URL: <https://arxiv.org/pdf/1712.06009.pdf>.

⁶¹ European Union Agency for Fundamental Rights.

⁶² Walsh, 2062: *The World that AI Made*.

⁶³ Материал, представленный Грэмом Гринлифом, Университет Нового Южного Уэльса, Сидней, август 2018 года.

⁶⁴ Graham Greenleaf, “Global convergence of data privacy standards and laws: speaking notes for the European Commission events on the launch of the General Data Protection Regulation in Brussels and New Delhi”, University of New South Wales Law Research Series, No. 56, 25 May 2018. URL: www.austlii.edu.au/au/journals/UNSWLRS/2018/56.html.

99. Если взглянуть с иной точки зрения, то страны с широкими законами о локализации данных создают новые стандарты конфиденциальности для данных, собираемых в пределах их юрисдикции. В Китае Закон о кибербезопасности ввел ограничения на трансграничную передачу данных, которые отличаются от международных режимов конфиденциальности, таких как Общий регламент по защите данных и добровольные трансграничные правила о конфиденциальности личной информации, принятые Азиатско-Тихоокеанским экономическим сотрудничеством⁶⁵. Хотя и Регламент, и Закон, как представляется, имеют схожие критерии трансграничной передачи, Закон не предусматривает отступления, существующие в Регламенте⁶⁶. Кроме того, Закон не содержит определенных механизмов, предусмотренных Регламентом, таких как обязательные корпоративные правила или стандартные положения о защите данных, помогающие компаниям добиться одобрения.

100. Предварительные рекомендации Специального докладчика, содержащиеся в его докладе Генеральной Ассамблее от октября 2017 года, были выработаны независимо от Общего регламента по защите данных и Модернизированной конвенции 108, но они согласованы с этими документами (см. таблицу)⁶⁷. Достигнутое согласование важно при рассмотрении более широкого международного контекста: Модернизированная конвенция 108 неуклонно приобретает глобальный характер и включает многие, хотя и не все, из новых элементов Регламента⁶⁸. Вполне возможно, что в ближайшие 5–10 лет экстерриториальное действие Регламента наряду с все более широким клубом государств-участников Конвенции будет оказывать значительное воздействие на углубляющуюся общемировую культуру неприкосновенности частной жизни. Точный характер этой эволюции еще формируется, так же как и ее значение для будущих нововведений, таких как самостоятельные принципы, касающиеся больших данных и открытых данных.

101. Хотя нужна согласованная международная основа для регулирования больших данных и открытых данных, было бы преждевременно начинать работу над самостоятельными принципами, конкретно касающимися больших данных и/или открытых данных, до того, как пройдет достаточно времени для подтверждения надежности и международного воздействия Общего регламента по защите данных и Модернизированной конвенции 108.

102. Поэтому рекомендации, касающиеся больших данных и открытых данных, следует толковать в духе существующих принципов неприкосновенности частной жизни и защиты данных, а не как какие-то новые уникальные правила.

⁶⁵ Samm Sacks, Paul Triolo and Graham Webster, “Beyond the worst-case assumptions on China’s cybersecurity law”, blog post, New America, 13 October 2017; и материал, представленный Центром Алленса по вопросам технологии, права и инноваций, 14 августа 2018 года.

⁶⁶ Xiaoyan Zhang, “Cross-border data transfers: CSL vs. GDPR”, The Recorder, 2 January 2018; и материал, представленный Центром Алленса по вопросам технологии, права и инноваций, 14 августа 2018 года.

⁶⁷ Материал, представленный Грэмом Гринлифом, август 2018 года.

⁶⁸ С 2011 года Конвенция 108 увеличила состав своих участников сверх 47, являющихся членами Совета Европы, получив просьбы о присоединении от Аргентины, Буркина-Фасо, Кабо-Верде, Маврикия, Марокко, Мексики, Сенегала, Туниса и Уругвая. Одиннадцать других стран, или их органы по защите данных, являются наблюдателями в ее Консультативном комитете.

**Рекомендации Специального докладчика, содержащиеся в его докладе
от октября 2017 года, и их согласование с Общим регламентом по защите
данных и Модернизированной конвенцией 108**

<i>Пункт доклада Специального докладчика от октября 2017 года (A/72/540)</i>	<i>Раздел Общего регламента по защите данных Европейского союза</i>	<i>Статья Модернизированной конвенции 108</i>
131 a), об ответственности	5 (2) «Подотчетность»	10 (1)
131 b), о транспарентности	12 «Транспарентность»; 22 (3) «Автоматизированное принятие решений» и транспарентность	5 (4), 8(1)
131 c), о качестве	5 (1) (c) «минимизация данных», (d) «точность»	5(1)
131 d), о предсказуемости машинного обучения	22 «Автоматизированное принятие решений»	8 (1), (2)
131 e), о безопасности	32–34 «безопасность» (включая уведомление о нарушении)	7 (1)
131 f), о выявлении рисков и инструментах их снижения	35 «Оценка воздействия на защиту данных»; 36 «Предварительные консультации»	10 (2);
131 g), об обучении персонала	37–39 «Сотрудник по защите данных»	–
131 h), об определении четких приоритетов для регулирования защиты частной жизни	52 «Независимость» органа по защите данных	15 (5)
131 i), о достаточных полномочиях регулирующих органов в связи с «большими данными»	57 «Задачи», 58 «Полномочия»	12, 15
131 j), о законах относительно конфиденциальности личных данных на предмет их соответствия техническому прогрессу	4 (1) «персональные данные»; 4 (4) «профилирование»; 4 (5) «псевдонимизация»; 22 «Автоматизированное принятие решений»; 25 «защита данных сознательно и автоматически»;	8 (1) и (2); 10 (3)
131 k), о формальных консультационных механизмах	36 «Предварительные консультации»; 57 (b), (c), (d) и (g) «Задачи» органа по защите данных	–
131 l), о консультациях по опасным практическим методам	36 «Предварительные консультации»;	–
131 m), о новых технических методах	57 (i) «Задачи органа по защите данных – отслеживать новые технологии»; 25 «Защита данных сознательно и автоматически»	10 (3)
131 n), об осведомленности граждан	12 «Транспарентность»; 13–15 «Уведомление субъектам данных»; 57 (b), (c), (e) «Задачи» органа по защите данных	15 (2) (e)
126, об обязательных требованиях и эффективных правоприменительных механизмах для открытых данных в отношении деидентификации	25 «Защита данных сознательно и автоматически»; 4 (1) «персональные данные»; 4 (5) «псевдонимизация»	10 (3)

Пункт доклада Специального докладчика от октября 2017 года (A/72/540)	Раздел Общего регламента по защите данных Европейского союза	Статья Модернизированной конвенции 108
127, о тщательных оценках влияния на принцип неприкосновенности частной жизни, если в открытых данных используются данные на уровне единичной записи	35 «Оценка воздействия на защиту данных»	10 (2)
128, никаких открытых данных и никакого обмена данными на уровне единичной записи без надежной деидентификации	4 (1) «персональные данные»; 4 (5) «псевдонимизация»	2 (d)
129, обеспечение дополнительной защиты конфиденциальных данных	9 «Специальные категории»	6

Источник: Грэм Гринлиф, материал, представленный после консультации, 7 августа 2018 года.

Н. Выводы

103. Данные являются и будут оставаться одним из главных экономических активов, таким как капитал или рабочая сила. Их нераздельная зависимость от личной информации требует примирения с законами о неприкосновенности частной жизни и о защите данных.

104. Международное право прав человека требует, чтобы любое вмешательство в право на неприкосновенность частной жизни было законным, необходимым и пропорциональным. Порой возражения против неприкосновенности частной жизни могут быть законными, но являются ли они этическими — это другой вопрос. Можно сомневаться в том, что некоторые из приведенных здесь примеров являются этическими, законными, необходимыми и пропорциональными. Недавние случаи неправильного управления данными частными и государственными структурами требуют твердых ответных мер для недопущения их повторения.

105. Международное право прав человека также требует, чтобы те, кто сталкивается с нарушением их права на неприкосновенность частной жизни, имели доступ к средствам правовой защиты. Это приобретает еще большее значение в эпоху больших данных и открытых данных.

106. Одной из ключевых проблем в плане публичной огласки данных в качестве открытых данных является отсутствие какого-либо метода, позволяющего однозначно определить, имеется ли личная информация в предположительно деидентифицированных наборах данных или агрегированных данных.

107. В основе политики и практики, окружающих открытые данные, лежат экономические и политические факторы. Бизнес-модели, присущие капиталистической экономике, не имеют большого стимула защищать персональные данные, когда это не вызывает никакого экономического вреда в противовес прибылям, которые будут получены.

108. Международная система с последовательными мерами по защите данных и четкими правилами транснационального доступа поможет оценивать меры по защите неприкосновенности частной жизни и конкурирующие интересы, которые могут иметься у стран в смысле получения доступа к данным, например в контексте правоохранительной деятельности, или которые могут иметься у многонациональных корпораций в плане управления потоками данных собственными силами.

109. Инициативы, способствующие неограниченному обмену данными, и инициативы, ликвидирующие существующие правовые гарантии неприкосновенности частной жизни, идут вразрез с защитой права на неприкосновенность частной жизни и должны прекратиться.

110. Установление уголовной ответственности за реидентификацию (в общественных интересах) деидентифицированных наборов данных не пользуется поддержкой как гарантия в отношении личных данных.

111. Детальные данные на уровне единичной записи (идентифицируемые данные) не должны разглашаться или публиковаться в Интернете без согласия субъекта данных. Использование физических и технических методов, таких как безопасная исследовательская среда, для ограничения доступа к конфиденциальным данным на уровне единичной записи является вполне уместным.

112. Законодательство о защите прав потребителей и законодательство о защите данных могут с пользой для дела дополнять друг друга. Законодательство о неприкосновенности частной жизни с его правозащитными и социальными аспектами служит опорой для законодательства о защите прав потребителей. Опора только на законодательство о защите прав потребителей лишит людей возможности пользоваться более широкими благоприятствующими аспектами взаимозависимости между основными правами человека и соответствующими механизмами правовой защиты.

113. Нынешние и потенциальные проявления искусственного интеллекта требуют независимого надзора со стороны экспертов в различных тематических областях. Эволюция этой технологии требует прочной правовой и политической основы, зиждущейся на правах человека. Это — срочная и кардинально важная задача.

114. Применение статьи 22 Общего регламента по защите данных требует пристального контроля на предмет его способности решать вопросы автоматизированной обработки, возникающие в связи с использованием искусственного интеллекта.

115. Необходимо заняться отсутствием технологических возможностей, требующихся для разработки соответствующих систем, методов и процессов и для обеспечения надежных систем, методов и процессов, в интересах крепкой защиты персональных данных. В этом должны участвовать мелкие технологические компании и новые компании.

116. Когда государства-члены обдумывают законодательство для поощрения открытых данных⁶⁹, рекомендуются следующие параметры:

- g) все законодательство должно быть прочно увязано с международными правозащитными обязательствами каждого государства;
- h) передовую практику в области законодательства о защите данных следует анализировать в качестве примеров для подражания;
- i) этические принципы и механизмы подотчетности в области данных, основанные на принципах справедливости и законности, необходимы

⁶⁹ Например, см. предложения Австралии в документе “New Australian Government data sharing and release legislation: issues paper for consultation”, URL: www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation, в материале, представленном М. Патерсоном.

для практической деятельности государственного и частного секторов в сфере данных;

j) адекватные модели регулирования в отношении неприкосновенности частной жизни и защиты данных требуют структурной независимости, достаточных ресурсов и регулирующего органа, способного быть независимым;

k) ликвидация законов о неприкосновенности частной жизни и защиты данных с целью создать благоприятную среду для открытых данных противоречит глобальным тенденциям, здравому смыслу и международным правозащитным обязательствам государств касательно права на неприкосновенность частной жизни;

l) определения и концепции должны проводить различие между обменом данными, их использованием, разглашением и публикацией;

m) необходимо, чтобы системы совместной разработки использовали модели и механизмы широкого участия с достаточно разнообразным представительством в целях решения таких вопросов, как суверенитет коренных народов над данными.

I. Рекомендации

117. Первоначальные рекомендации, которые Специальный докладчик вынес в своем докладе Генеральной Ассамблее от 19 октября 2017 года (A/72/540), были расширены на основе итогов консультации следующим образом:

a) внутренние усилия правительств по обмену персональными данными должны быть отличимыми в сферах законодательства, политики и практики от предоставления данных общественности в качестве открытых данных;

b) если только есть возможность — и до тех пор, пока не появится возможность — однозначно определять, имеется ли личная информация среди агрегированных данных, или определять, что дезагрегированные данные не могут быть реагрегированы, открытые данные не должны содержать записей на уровне единичной записи;

c) работа по выработке международных стандартов в отношении неприкосновенности частной жизни, обеспечивающих сохранение обмена данными и международной деятельности по стандартизации, должна продолжаться без промедления и должна поддерживаться государствами-членами;

d) изучение дифференцированных режимов конфиденциальности является необходимым и должно использоваться для агрегированных статистических данных и сложных видов данных, а также для других технологий, сохраняющих конфиденциальность, таких как гомоморфное шифрование и безопасное многостороннее вычисление;

e) в качестве промежуточного минимального ответа на согласие с детальными нормами неприкосновенности частной жизни, унифицированными на глобальном уровне, государствам-членам рекомендуется ратифицировать Модернизированную конвенцию 108 через посредство соответствующего подзаконного правового акта (Протокол CETS 223) и осуществить без необоснованных задержек содержащиеся в нем принципы через

посредство внутригосударственного законодательства, уделяя особое внимание незамедлительному осуществлению тех положений, которые требуют гарантий в отношении персональных данных, собранных для целей слежки и для других целей, имеющих отношение к национальной безопасности;

f) в целях согласования с передовой практикой при проведении обзора и обновлении своего внутригосударственного законодательства в рамках осуществления Модернизированной конвенции 108 государствам-членам за пределами Европейского союза рекомендуется, по мере возможности, учитывать также те гарантии и средства правовой защиты, которые содержатся в Общем регламенте по защите данных, но которые не считаются обязательными согласно Конвенции;

g) правительствам и корпорациям следует признать суверенитет коренных народов над данными, которые касаются их или собраны от них и которые имеют отношение к коренным народам, их системам знаний, обычаям или территориям, всегда включая официально закрепленные, разработанные коренными народами принципы, акцент на руководящую роль коренных народов и механизмы подотчетности;

h) государствам-членам следует провести обзор адекватности всех правовых и политических основ, касающихся искусственного интеллекта, для защиты свободы выражения мнения и права на неприкосновенность частной жизни; развивать активное междисциплинарное сотрудничество между специалистами по статистике, юристами, специалистами в области общественных наук, специалистами в области компьютеров, математиками и экспертами в тематических областях; и разрабатывать стратегии для предотвращения или устранения любого негативного воздействия на осуществление прав человека в результате использования алгоритмов, автоматизированной обработки, машинного обучения и искусственного интеллекта.

118. Специальный докладчик повторяет также рекомендации, которые он вынес в своем предыдущем докладе (см. [A/72/540](#), пункты 126–131).