Генеральная Ассамблея

Distr.: General
25 January 2021
Russian
Original: English

Совет по правам человека
Сорок шестая сессия
22 февраля — 19 марта 2021 года
Пункт 3 повестки дня
Поощрение и защита всех прав человека, гражданских, политических, экономических, социальных и культурных прав, включая право на развитие

Искусственный интеллект и неприкосновенность частной жизни, а также неприкосновенность частной жизни детей

Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни Джозефа А. Каннатачи* **

Резюме

Настоящий доклад подготовлен во исполнение резолюций 28/16 и 37/2 Совета по правам человека. Никогда еще право человека на неприкосновенность частной жизни не было столь важным и не находилось под большей угрозой. Технологические тенденции, наметившиеся в 2015 году, создают все больше проблем в плане осуществления права на неприкосновенность частной жизни. В настоящем докладе, заключительном докладе первого Специального докладчика по вопросу о праве на неприкосновенность частной жизни, он рассматривает две отдельные проблемы: во-первых, искусственный интеллект и неприкосновенность частной жизни, а затем неприкосновенность частной жизни детей, в частности роль неприкосновенности частной жизни в поддержке самостоятельности и позитивного участия в жизни общества. Для решения этих проблем излагаются руководящие принципы и рекомендации, разработанные на основе консультаций и исследований. Наряду с другими рекомендациями Специального докладчика, содержащимися в его предыдущих докладах, настоящий доклад дополняет план работы, представленный Совету по правам человека в 2016 году (A/HRC/31/64). Обзор деятельности Специального докладчика, осуществленной в рамках его мандата с 2015 года, содержится в приложениях.

* На основании достигнутой договоренности настоящий доклад издается позднее предусмотренного срока его публикации в связи с обстоятельствами, не зависящими от представляющей доклад стороны.

** Приложения к настоящему докладу распространяются в полученном виде только на том языке, на котором они были представлены.

I. Рекомендации по защите неприкосновенности частной жизни при разработке и эксплуатации решений на базе искусственного интеллекта

История вопроса и цель

1. Цель настоящих рекомендаций заключается в том, чтобы сформулировать руководящие принципы, касающиеся использования персональной и неперсональной информации в контексте решений на основе искусственного интеллекта (ИИ)[1], разработанных в рамках прикладных информационно-коммуникационных технологий (ИКТ), и подчеркнуть важность наличия законной основы для обработки данных с использованием ИИ правительствами и корпорациями в рамках общего правозащитного подхода к неприкосновенности частной жизни.

2. Рекомендации основаны на Всеобщей декларации прав человека и отражают дух и понимание этой Декларации. Прежде всего, статьи 7 (недискриминация) и 12 (право на неприкосновенность частной жизни) имеют решающее значение для разработки или применения решений на базе ИИ. Темы и ценности этих статей изложены в статьях 2 и 3 (недискриминация) и 17 (неприкосновенность частной жизни) Международного пакта о гражданских и политических правах и являются обязательствами государств, ратифицировавших этот договор.

3. Права имеют ключевое значение в информационном обществе. Генеральная Ассамблея и Совет по правам человека подтвердили, что права, которыми люди пользуются офлайн, также должны быть защищены онлайн (A/75/62-E/2020/11, п. 9) в качестве условия для сохранения глобального, открытого и интероперабельного характера Интернета (резолюция 26/13 Совета по правам человека), а также в качестве одной из движущих сил ускорения прогресса на базе развития в его различных формах, включая достижение Целей в области устойчивого развития (резолюция 73/179 Генеральной Ассамблеи).

4. В центре рекомендаций — конфиденциальность всех данных[2], используемых в решениях на базе ИИ. Они призваны служить общей международной основой для стандартов защиты данных в отношении решений на базе ИИ, особенно тех, которые будут внедряться на национальном уровне. Признавая многочисленные экономические и социальные выгоды решений на базе ИИ, эти рекомендации призваны служить ориентиром в отношении того, каким образом можно защитить право на неприкосновенность частной жизни в контексте решений на базе ИИ.

5. Осуществление данных рекомендаций требует всестороннего сотрудничества между правительствами, гражданским обществом, частным сектором, техническим сообществом и научными кругами и должно опираться на общие человеческие ценности, такие как инклюзивность, уважение, ориентированность на человека, права человека, международное право, прозрачность и устойчивость.

6. Решения на базе ИИ включают в себя применение систем ИИ, предназначенных для подготовки, прогнозирования или принятия решений, которые влияют на жизнь каждого человека. Решения на базе ИИ несут в себе не только выгоды, но и риски, которые в настоящее время обсуждаются в обществе. Эти дискуссии — по моральным,

[1] Существует несколько определений искусственного интеллекта. Значение, используемое в настоящем докладе, является наиболее распространенным, как оно определено в *Оксфордском справочнике*: «Теория и разработка компьютерных систем, способных выполнять задачи, обычно требующие человеческого интеллекта, такие как зрительное восприятие, распознавание речи, принятие решений и перевод с одного языка на другой». Это далеко не исчерпывающий перечень видов применения технологий ИИ.

[2] Специальный докладчик, находя истоки защиты данных в праве на уважение частной жизни, закрепленном в статье 8 Конвенции о защите прав человека и основных свобод, рассматривает закон о защите данных как элемент подмножества норм, регулирующих защиту неприкосновенности частной жизни. Признавая, что исторические события в Европе привели к прямому включению защиты данных в качестве отдельной статьи в Хартию основных прав Европейского Союза, он, тем не менее, предлагает читателю и другие исторические ссылки.

этическим и общественным вопросам, затрагивающим права человека, таким как неприкосновенность частной жизни, недискриминация и свободное участие, — продолжаются. Все эти вопросы имеют своей исходной посылкой законность обработки данных с точки зрения неприкосновенности частной жизни. Это особенно необходимо, поскольку большинство данных хранится главным образом в частных компаниях, которые используют их коммерческую ценность, объединяя различные наборы данных для максимизации своего аналитического потенциала. Рост озабоченности общественности по поводу интрузивности и потенциального воздействия сбора данных, риска наблюдения и все более широкого использования алгоритмов, использующих такие наборы данных для автоматизации принятия решений, которые влияют на жизнь людей (A/75/62-E/2020/11, п. 10), требует принятия ответных мер.

7. Контекст развертывания ИИ требует эффективно и независимо функционирующего органа регулирования по вопросам неприкосновенности частной жизни и/или защиты данных, осуществляющего надзор за соблюдением специального законодательства.

Сфера охвата

8. Настоящие рекомендации применимы к обработке данных в рамках решений на базе ИИ во всех секторах общества, включая государственный и частный секторы. Обработка данных осуществляется на каждом этапе жизненного цикла решения на базе ИИ, на котором задействуются данные, включая проектирование, разработку, развертывание и вывод из эксплуатации решения на базе ИИ, а также любую итерацию или перестройку на основе предыдущего решения на базе ИИ.

9. Рекомендации применимы ко всем менеджерам решений на базе ИИ. Под ними могут пониматься проектировщики, разработчики или операторы (саморегулирующиеся или главные), каждый в рамках своей конкретной функции. Цель заключается в том, чтобы в рамках той или иной организации по каждому решению на базе ИИ было определено либо юридическое, либо физическое лицо, несущее полную ответственность за решение на базе ИИ.

10. Данные рекомендации не ограничивают и не затрагивают каким-либо иным образом любой закон, который предоставляет субъектам данных большие, более широкие или каким-то образом улучшенные права, защиту и/или средства правовой защиты. Они не ограничивают и не затрагивают каким-либо иным образом любой закон, налагающий обязательства на менеджеров и операторов, осуществляющих обработку данных, в тех случаях, когда этот закон предусматривает более высокие, широкие или строгие обязательства в отношении аспектов конфиденциальности данных.

11. Эти рекомендации не применимы к решениям на базе ИИ, которые могут использоваться частными лицами в контексте чисто частной или бытовой деятельности.

Учет прав человека и этических аспектов

12. Общество несет ответственность за разработку решений на базе ИИ в рамках правозащитного подхода, с соблюдением этических норм и принципа ответственности. В настоящее время решения на базе ИИ затрагивают многие сферы повседневной жизни и будут все больше и больше затрагивать их, оказывая глубокое влияние на личную жизнь и работу людей. В будущем решения на базе ИИ, вероятно, будут охватывать еще более широкий спектр фундаментальных принципов, отражающих право прав человека и этические вопросы. То, как эта технология используется, имеет решающее значение.

13. Недискриминация имеет важнейшее значение для недопущения неравенства, несправедливости и страданий, способных повлиять на осуществление прав человека, включая экономические, социальные и культурные права. Использование решений на базе ИИ нуждается в тщательном мониторинге, а любые случаи дискриминации или

другие проявления, нарушающие права человека, должны устраняться, с тем чтобы избежать таких негативных последствий.

14. Решения на базе ИИ не должны использоваться для принятия окончательных решений, а только в рамках поддержки принятия решений в определенных областях, например в судебной или медицинской сфере. Оценки воздействия на права человека должны неизменно проводиться наряду с оценками защиты данных, с тем чтобы можно было получить целостное представление о необходимых рамочных условиях.

15. Комитеты по всему миру, например Специальный комитет Совета Европы по искусственному интеллекту, в настоящее время работают над созданием нормативной базы и кодексов этики для решений на базе ИИ. Следует использовать их выводы, а также другие соответствующие руководства, такие как Руководящие принципы предпринимательской деятельности в аспекте прав человека.

Искусственный интеллект и конфиденциальность данных

16. Современные системы ИИ включают в себя или представляют собой комбинацию систем анализа, основанных на формализованных экспертных знаниях (хранилище данных, бизнес-аналитика) и машинном обучении, а также на целевом применении полученных результатов. Существует различие между запрограммированными алгоритмическими системами для решения конкретных задач и системами, которые способны обучаться. Последние оснащены алгоритмами обучения и должны обучаться.

17. В алгоритмическом процессе принятия решений, регулярно используемом в качестве основы для ИИ, производится оценка информации, которая ведет к решению, прогнозу или рекомендации к действию. В случае «контролируемого обучения» система ИИ имеет критерии решения конкретной проблемы, в то время как в случае «неконтролируемого обучения» система ИИ сама выбирает или рекомендует соответствующие критерии решения.

18. Следовательно, как обработка данных, так и решение, принятое в результате этой обработки, сопряжены с потенциальными рисками для субъекта данных.

19. Классическая информационная технология, с ее элементами «вход» — «обработка» — «выход», расширяется благодаря способностям воспринимать, понимать, действовать и обучаться. Эти функции, ранее осуществлявшиеся только людьми, во все большей степени выполняются машинами. Термин «понимание» является новой территорией в связи с использованием компьютеров и должен сопровождаться критическим анализом возможностей отслеживания и соблюдения прав человека и этических ценностей.

20. Машинное обучение относится, в частности, к серии методов оптимизации в искусственных нейронных сетях. Системы ИИ могут иметь очень сложные структуры между входным и выходным слоями. Благодаря определению нескольких иерархических слоев обработки машинное обучение может стать значительно более эффективным (глубокое обучение). Это неизбежно приводит к снижению прослеживаемости решений ИИ. По причине сложности алгоритмов и множества арифметических операций, выполняемых машиной, более глубокие слои обработки (скрытые слои) становятся непрозрачными в критериях принятия решений и их системе взвешивания.

21. Раскрытие алгоритмов, на которых основан ИИ, является основным требованием в текущих дебатах о прозрачности ИИ. Однако на практике конкретная проверка логики принятия решений в высокосложных системах ИИ с использованием раскрытых алгоритмов, скорее всего, будет сопряжена с трудностями. Независимо от того, имеете ли вы дело с ИИ с интерпретируемой способностью, или ИИ с объяснительной способностью, или с другими моделями при наличии сомнений или сбоев в процессе или в результатах, сбор цифровых доказательств необходим для реконструкции того, что произошло, и почему определенный результат был рекомендован или фактически реализован.

22. Внешний мониторинг процессов принятия решений систем ИИ путем анализа самих решений с учетом заданной цели системы и принципа этического управления имеет много преимуществ, в том числе и практических.

23. Решения ИИ, выходящие за рамки ожидаемых результатов или решений, должны выявляться и требовать соответствующего вмешательства. Инструменты, разработанные специально для обнаружения неожиданных результатов и анализа решений ИИ, являются необходимым предварительным условием. Мониторинг машин исключительно машинами увеличивает вероятность непредвиденных рисков или «неизвестных неизвестных». Это обусловливает необходимость соблюдения принципа, согласно которому человеческое суждение должно всегда доминировать в процессах мониторинга ИИ.

24. Помимо эффективности механизмов обучения, успешное машинное обучение зависит от количества и качества доступных данных. Тенденция к использованию больших данных в области информационной технологии и растущая массовая доступность высококачественных данных значительно ускоряют развитие систем ИИ.

25. Очень сложные психологические и эмоциональные процессы, связанные с человеческими знаниями и принятием решений, скорее всего, останутся прерогативой человека, а не машины. Поэтому при оценке и взвешивании плюсов и минусов применимого законодательства в отношении систем ИИ и их процессов принятия решений следует помнить, что машинные решения основаны на иных принципах и механизмах (хотя они в основном разрабатываются людьми), чем те, которые применяются к решениям, принимаемым людьми.

26. Для обеспечения необходимой безопасности систем ИИ необходимо эффективно внедрить инструментарий всеобъемлющего этического и правового управления решениями ИИ в среду управления субъекта, использующего решения ИИ. Кроме того, необходимо расширять цифровое сотрудничество с различными заинтересованными сторонами, с тем чтобы продумать разработку и применение таких стандартов и принципов, в частности стандартов прозрачности и непредвзятости, в автономных интеллектуальных системах в различных социальных контекстах.

A. Принципы конфиденциальности данных при использовании решений на базе искусственного интеллекта

27. Независимо от юрисдикции или правовой среды, применимой к ответственному менеджеру, восемь основных принципов являются обязательными для соблюдения при планировании, разработке и внедрении решений на базе ИИ. Эти принципы и их спецификация не заменяют собой никаких других или более строгих правил защиты данных, применимых к тем, кто работает с решениями на базе ИИ. Эти принципы заключаются в следующем:

a) юрисдикция;

b) этическая и правовая основа;

c) основные требования к данным;

d) ответственность и надзор;

e) контроль;

f) прозрачность и «объясняемость»;

g) права субъекта данных;

h) средства защиты.

Юрисдикция

28. Для обеспечения правовой определенности и прослеживаемости в идеале должна существовать транснациональная рамочная основа, отражающая

международный консенсус и предусматривающая механизмы для выявления и регулирования ответственности в рамках решений на базе ИИ, а также для управления известными рисками.

29. В отсутствие такой транснациональной рамочной основы одним из вариантов являются решения и средства защиты, разработанные на местном уровне, и обеспечение их соблюдения на местном уровне. В этом сценарии, когда решение на базе ИИ использует распределенный механизм принятия решений, этот распределенный механизм также должен находиться в одной юрисдикции.

30. Другими вариантами являются двусторонние или многосторонние соглашения или местное регулирование в пределах одной юрисдикции, осуществляемое при содействии трансграничных соглашений, или вариант, когда ИИ продолжает внедряться в условиях, при которых регулирование определяется влиянием рыночных сил и рисков, будь то с помощью законодательства о защите прав потребителей или других форм правовой защиты.

31. Если и до тех пор, пока не будет разработан конкретный специальный международно-правовой механизм для урегулирования юрисдикционных вопросов в области ИКТ, особенно касающихся решений на базе ИИ, разработанных в одной юрисдикции, но используемых в другой, когда решение на базе ИИ должно работать в нескольких юрисдикциях, он должен создаваться и функционировать в виде многонациональной федерации индивидуальных решений на базе ИИ единой юрисдикции.

Этическая и правовая основа

32. Поскольку обработка персональных данных физических лиц в любом случае нарушает права субъекта данных, обработка данных, лежащая в основе решения на базе, должна иметь под собой прочную этическую и правовую основу. Это становится еще более важным, если сама обработка предназначена для того, чтобы способствовать принятию решений или непосредственно принять решения, влияющие на положение или права субъекта данных. Независимо от юрисдикции или индивидуальной правовой среды менеджера, один или несколько из следующих сценариев могут обеспечить достаточную правовую основу для обработки данных системой ИИ:

a) если закон составлен в соответствии с демократическими принципами и правами человека, он способен обеспечить конкретную правовую основу, если в нем учитывается конфликт интересов между менеджерами и субъектами данных, а также предусмотрены соответствующие средства защиты прав субъектов данных;

b) если использование решения на базе ИИ необходимо для выполнения договора с субъектом данных и имеет его явное согласие, а также если договор не наносит существенного ущерба субъекту данных или не нарушает права человека субъекта данных или других лиц;

c) если субъект данных дал свободное, осознанное согласие, охватывающее цель ИИ, последствия его использования и процедуры отзыва согласия. Согласие должно быть дано в виде четкого утвердительного действия, а ответственный менеджер должен обеспечить систему управления согласием, которая позволяет отозвать согласие в любое время и включает в себя соответствующую документацию;

d) на основе законного преобладающего интереса менеджера и/или значительного общественного интереса, если субъекты данных должным образом проинформированы до начала обработки и имеют возможность возразить против обработки, или имеют право, как минимум, в разумные сроки получить доступ к существующему механизму или процедурам, или исправить свою ситуацию;

e) каждое решение на базе ИИ связано и ограничено целью, для которой оно было изначально разработано, внедрено и надлежащим образом документировано. Хотя это не препятствует другим или дополнительным видам использования (например, дальнейшей обработке) или использованию другим менеджером,

дальнейшее использование должно быть заново оценено с точки зрения правовой основы и средств защиты, включая кажущимися совместимыми цели;

f) были определены специальные условия для защиты и обеспечения правовой основы для применения решений на базе ИИ к субъектам данных, относящимся к особым, чувствительным или уязвимым категориям, таким как дети, заключенные или другие группы.

Основные требования к данным

33. Качество данных включает в себя достоверность, такую как действительность и неизбирательность, а также минимизацию и ограничение цели. Должны быть учтены требования защиты данных, а также любые дополнительные требования к обработке конкретных данных, таких как данные о здоровье или данные о детях.

Ответственность и надзор

34. В рамках организации по каждому решению на базе ИИ следует определить либо юридическое, либо физическое лицо, которое будет нести полную ответственность за обработку данных и ее результаты. Это охватывает все аспекты управления процессом и технологией, включая законность обработки, ее документирование, адаптацию, результаты, надежную проверяемость набора данных алгоритма, обработку, понимание и сотрудничество, а также соблюдение прав субъектов данных. В тех случаях, когда решение на базе ИИ передается за пределы организации, необходимо определить, документировать и согласовать обязанности последующих сторон.

35. Эти обязанности, включая конечного оператора решения на базе ИИ, должны быть прозрачными и адекватно доступными для субъектов данных и государственных надзорных и регулирующих органов.

36. Надлежащий механизм управления, особенно в крупных юридических лицах, может включать в себя сотрудника по вопросам конфиденциальности данных, в обязанности и функции которого входит предоставление консультаций по вопросам соблюдения требований о конфиденциальности данных и мониторинг внедрения решения на базе ИИ. Должность сотрудника по вопросам конфиденциальности данных должна быть обеспечена достаточными ресурсами и полномочиями для выполнения этих функций, а сотрудник, занимающий эту должность, должен пройти полную и надлежащую подготовку или иметь соответствующую квалификацию, будь то сертификацию или опыт, для эффективного и независимого выполнения своих обязанностей и задач. Настоятельно рекомендуется создать эффективные каналы связи между этой должностью и соответствующим надзорным или контролирующим органом. В малых государствах и в начинающих компаниях необходимо инвестировать в управление ИИ, независимо от того, предусматривает ли оно создание такой должности или нет.

37. Информация об этих механизмах подотчетности должна быть предана гласности.

38. Необходимо установить надзор со стороны независимого, компетентного регулирующего органа, равно как и определить судебное средство правовой защиты в случае нарушения соответствующего закона.

Контроль

39. Решения на базе ИИ, в том числе и те, которые закупаются у третьей стороны, должны находиться под полным контролем соответствующего менеджера. На всех этапах, начиная с первой проектной идеи и заканчивая окончательным отключением и выводом из эксплуатации, должно быть неизменно понятно, какие данные обрабатываются в решении на базе ИИ, какие параметры и характеристики качества данных обеспечивают основу для принятия решений и как они будут балансироваться и взвешиваться по отношению друг к другу. Результаты должны постоянно контролироваться и при необходимости корректироваться. В области систем

автоматизированного принятия решений не следует принимать решения, основанные на сознательной или неосознанной предвзятости. Возможные предвзятость и дискриминационные последствия должны отслеживаться и исправляться до внедрения системы и через регулярные промежутки времени в течение всего срока ее службы.

40. В случае использования ИИ для систем поддержки принятия решений, аналогичный набор мер контроля требуется и в отношении лица, принимающего решение.

41. Менеджер, при необходимости, совместно с операторами обработки данных должен иметь возможность в любое время остановить или изменить обработку. Некорректные результаты должны быть задокументированы, как и принятые корректирующие меры, чтобы уменьшить любые риски для субъектов данных. После завершения их использования в целях выявления, исправления или аналитики, некорректные результаты должны удаляться без неоправданной задержки.

42. Должны быть предусмотрены внутренние и внешние обзоры функционирования такого контроля, которые должны быть в состоянии учитывать любые критические выводы в отношении решения на базе ИИ или его результатов.

Транспарентность и «объясняемость»

43. Решения на базе ИИ должны быть прозрачными для общественности и субъектов данных. Информация должна быть содержательной, понятной и охватывать все соответствующие аспекты, касающиеся оценки решения и возможных прав субъектов данных. Это включает в себя «объясняемость» цели, общих функций, вспомогательных процессов, используемых источников данных и диапазона запланированных результатов. Эти аспекты могут включать в себя:

a) источники данных и данные, используемые для ввода в решение на базе ИИ и его обучения, а также выходные данные решения на базе ИИ;

b) цель и правовая основа обработки;

c) параметры, создающие основу для принятия решений на базе ИИ, и система их взвешивания;

d) уточнение того, предназначено ли решение на базе ИИ для подготовки окончательных решений, которые будут приниматься человеком (поддержка принятия решений), или же оно само принимает окончательное решение (автоматизированное принятие решений);

e) как распределяются обязанности между менеджером и оператором обработки данных, если они не идентичны, а также контактная информация и возможные каналы связи;

f) интеграция третьих сторон (например, других менеджеров или операторов обработки данных), передача в другие страны (если таковая производится), а также причина интеграции и передачи. Для этого также требуется заявление о том, что третьи стороны связаны теми же требованиями, такими как требования о защите данных, что и менеджер, и имеют аналогичные функции и обязанности, независимо от того, где они расположены;

g) необходимая информация должна публиковаться, как минимум, в политике конфиденциальности данных, охватывающей решение на базе ИИ, и должна быть доступной, понятной и значимой для субъектов данных.

Права субъекта данных

44. Лица или группы лиц, чья персональная информация или позволяющая идентификацию персональная информация обрабатывается решением на базе ИИ (субъекты данных), имеют право:

a) понимать и обращаться с запросами с целью выяснения в понятной форме, хранятся ли персональные данные в автоматических файлах данных и если да,

то для каких целей, а также какие органы государственной власти или частные лица или органы контролируют или могут контролировать их файлы;

b) отзывать свое согласие без негативных последствий в любой момент времени в ходе обработки, если согласие было дано и используется в качестве правовой основы обработки;

c) возражать против обработки данных по уважительной причине в любой момент времени, если обработка основана на законном интересе;

d) получать информацию о выполнении всех требований по обеспечению конфиденциальности данных, перечисленных в настоящем разделе;

e) получать пропорциональный доступ к своим данным с исчерпывающей письменной информацией о своих персональных данных, о том, как их персональные данные используются и обрабатываются, а также о результатах и о том, как результаты могут повлиять на их положение и их личные права;

f) запрашивать принятие решения человеком, если у их есть обоснованные сомнения в том, что решение, предложенное или принятое решением на базе ИИ, не является точным или корректным;

g) корректировать данные, если они неточны;

h) подавать жалобу и получать средство правовой защиты, если жалоба будет поддержана;

i) стирать и удалять данные, если цель решения на базе ИИ перестает существовать или если данные больше не нужны для других законных целей.

45. Эти права не отменяют других прав и/или не имеют преобладающей силы над правами, предоставленными субъектам данных в соответствии с действующим законодательством в заданной юрисдикции.

Средства защиты

46. Решения на базе ИИ должны функционировать устойчиво и должны быть оснащены средствами защиты от рисков с использованием методов, которые способствуют доверию всех вовлеченных сторон и пониманию ими, включая субъектов данных и общественность. Перед внедрением, пусть даже только на пилотной основе, все решения на базе ИИ должны пройти, как минимум, первоначальную оценку рисков, связанных с правами человека и защитой данных, которая выявляет конкретные риски и критичности, связанные с внедряемым решением. В зависимости от результатов этой первоначальной оценки может потребоваться дополнительная оценка прав и рисков.

47. Технические и организационные средства защиты, опирающиеся на подход «встроенной конфиденциальности», для снижения выявленных рисков должны оцениваться в индивидуальном порядке. Это должно охватывать такие меры, как анонимизация или псевдонимизация, шифрование, разделение клиентов, управление доступом (ограничение), политика удаления данных, а также регистрационный журнал и мониторинг активности.

48. Возникающие новые риски и проблемы, связанные с технологическими, архитектурными и/или структурными разработками, такими как распределенные вычисления, должны быть изучены в ходе оценки рисков.

49. Работа по снижению рисков может быть основана на международных стандартах, таких как стандарты, опубликованные совместно Международной организацией по стандартизации и Международной электротехнической комиссией в серии ISO/IEC 27000 (системы менеджмента информационной безопасности). В частности, стандарт ISO/IEC 27701 содержит расширения для управления конфиденциальностью данных, устанавливающие минимальные меры:

a) защита: меры контроля для защиты от воздействия оцененных рисков;

b) выявление: меры контроля для скорейшего обнаружения аномалий;

c) реагирование: меры контроля для сдерживания и устранения риска аномальных событий, а также для обеспечения того, чтобы основные бизнес-процессы продолжали функционировать до тех пор, пока не будет найдено общее решение и ситуация не вернется в нормальное русло.

B. Оценка критичности решений на базе ИИ

50. Требуемые меры должны быть ориентированы на человека и соразмерны рискам нарушения прав человека, особенно дискриминации, и защиты данных, а также сложности или критичности решения по обработке данных. Могут использоваться следующие подходы.

Оценка прав человека на этапе планирования

51. Все решения на базе ИИ должны уважать принцип верховенства права, права человека, демократические ценности и разнообразие. Поэтому каждое планируемое решение на базе ИИ, включая алгоритмы, должно проходить своевременную оценку с точки зрения прав человека, в том числе оценку с точки зрения этики и равенства. Право на равное обращение не должно быть незаконно нарушено планируемым решением на базе ИИ. Например, решения на базе ИИ с использованием информации, отражающей неосознанную предвзятость, приведут к результатам, которые могут быть дискриминационными по отношению к определенным лицам или группам в обществе. Более того, решение на базе ИИ, загруженное «правильной» информацией, может привести к «неправильным» результатам, поскольку обучение решения на базе ИИ с применением собранной информации может привести к ошибочным предположениям со стороны решения на базе ИИ.

52. Встроенная конфиденциальность и конфиденциальность по умолчанию требуют оценки на этапе планирования того, каким образом внедрение решения на базе ИИ может повлиять на любые права человека, включая право на неприкосновенность частной жизни.

Этап тестирования и корректировки — мониторинг

53. После этапа планирования и первоначальной оценки с точки зрения прав человека выявленные рамочные условия должны быть учтены на этапе дальнейшей разработки. На этапе внедрения и перед запуском в эксплуатацию решения на базе ИИ должны пройти этап интенсивного тестирования с тестированием данных в отдельной, автономной среде для оценки того, насколько основные общие предположения были не только учтены, но и реализованы. Только когда ответственный менеджер будет уверен в том, что решение на базе ИИ работает корректно, оно может запущено в эксплуатацию.

54. На протяжении всего времени эксплуатации решения на базе ИИ, вплоть до его окончательного отключения, результаты, полученные с помощью решения на базе ИИ, должны контролироваться в соответствии с фундаментальными требованиями, определенными на этапе планирования.

55. Сложности контроля всех аспектов работы алгоритмов и постоянное изменение алгоритмов во время эксплуатации решения на базе ИИ требуют постоянной проверки результатов в сравнении с первоначальной запланированной целью решения другим возможным способом, чтобы обеспечить базу сравнения. При подозрении или наблюдении отклонения необходимо соответствующим образом адаптировать ввод данных для решения на базе ИИ или отключить само решение.

56. Чтобы воспользоваться выгодами новых творческих подходов и расширить горизонты разработчика и менеджера, при разработке, тестировании и мониторинге решений на базе ИИ необходимо учитывать рекомендации и отзывы сообщества защиты персональных данных, межсекторальных и межотраслевых организаций, гражданского общества и сообществ пользователей. Для готовых к использованию решений на базе ИИ должен быть создан «испытательный стенд», например путем

размещения в сети Интернет так называемого «черного ящика», где отдельное и автономное решение будет открыто для ввода данных третьими лицами с целью выяснения типа результатов, которые будет выдавать решение на базе ИИ, или может быть рекомендовано создание регуляторами «песочниц» в организациях, занимающихся внедрением решений на базе ИИ.

Оценка критичности на основе использования различных видов данных

57. Помимо надлежащего планирования, тестирования и внедрения, критичность данных и их целевое назначение имеют отношение и к мерам, необходимым для правильной обработки.

58. Это относится к общим данным, таким как общая персональная информация или данные в контексте телекоммуникационных услуг или здоровья. Данные, связанные со здоровьем, и некоторая другая информация, например содержание телекоммуникаций, должны обрабатываться более строго, чем менее конфиденциальная персональная информация. Это означает, что соответствующие технические и организационные меры должны быть усилены по сравнению с другими случаями, например строгое ограничение цели и сведение к минимуму данных, шифрование, псевдонимизация, ограничение доступа и раннее удаление или анонимизация.

59. Планируемая цель использования данных играет ключевую роль в определении необходимого уровня защиты. Если персональная информация обрабатывается исключительно в целях хранения, это может быть менее критично, чем использование для профилирования. Законность цели и мер защиты должна оцениваться чрезвычайно тщательно.

60. Эти меры должны приниматься и документироваться в ходе всех оценок рисков.

Проведение и ведение журнала периодической оценки систем искусственного интеллекта с использованием записей с предоставлением доступа внешним аудиторским и регулирующим органам

61. В ходе оценки проводится проверка системы на:

a) ожидаемые или неожиданные результаты;

b) объективность, предвзятость и дискриминацию в отношении отдельных лиц и групп;

c) компромиссы и уменьшение рисков.

C. Дополнительные соображения

Внешние аудиты и сертификация

62. Системы аудита и сертификации должны иметь доступ ко всей соответствующей внутренней документации, такой как журналы оценки, для контроля за соответствием систем искусственного интеллекта инженерным и этическим нормам, разработанным с использованием коллегиальных и многосторонних подходов.

63. Следует рассмотреть возможность внешней сертификации лицензированным аудитором в области конфиденциальности данных, который также официально признан экспертом в области искусственного интеллекта. Это может быть полезно для снятия озабоченностей общественности и субъектов данных. Это может быть особенно применимо к решениям на базе ИИ, которые могут привести к серьезным неблагоприятным результатам и потере доверия со стороны общественности и/или сообщества регуляторов.

Изменения в законодательстве и нормативных актах

64. Возможные изменения в законодательстве и нормативных актах рассматриваются во всем мире и затронут большинство решений на базе ИИ. Соблюдение требований в значительной степени будет зависеть от:

a) соответствия существующим и разрабатываемым национальным и международным стандартам;

b) сертификации соответствующим сертификационным органом, действующим на основании национального или международного соглашения.

Участие в обсуждениях

65. Лица, ответственные за стратегии и/или оперативные решения в области ИИ, а также те, кто следит за их использованием, должны участвовать в дискуссиях по вопросам ИИ и возникающим этическим и техническим вопросам.

Образование и информационно-просветительская деятельность

66. ИИ — это сложная тема, и развертывание данных в системах ИИ и их использование в решениях на базе ИИ требуют ясного, всестороннего объяснения пользователям и поставщикам данных, а также руководителям, менеджерам и другим лицам, участвующим в принятии решений по системам ИИ и их работе. Одной лишь публикации алгоритмов недостаточно.

II. Принципы и рекомендации в отношении права детей на неприкосновенность частной жизни

67. Дети, как и все люди, обладают правами и свободами человека. В международных и региональных правовых документах сформулировано право на неприкосновенность частной жизни и право детей на неприкосновенность частной жизни[3].

68. Основными документами, закрепляющими права детей, являются Всеобщая декларация прав человека и Конвенция о правах ребенка, которая получила практически всеобщее признание благодаря ее ратификации 193 сторонами.

69. Статья 4 Конвенции гласит:

1) Ни один ребенок не может быть объектом произвольного или незаконного вмешательства в осуществление его права на личную жизнь, семейную жизнь, неприкосновенность жилища или тайну корреспонденции или незаконного посягательства на его честь и репутацию.

2) Ребенок имеет право на защиту закона от такого вмешательства или посягательства.

70. Эта статья должна толковаться широко, с тем чтобы в полной мере учитывать опыт детей, связанный с неприкосновенностью частной жизни[4].

71. Права ребенка являются универсальными, неделимыми, взаимозависимыми и взаимосвязанными[5]. Их право на неприкосновенность частной жизни обеспечивает им доступ к другим правам, имеющим важнейшее значение для развития личности и

[3] Они включают в себя региональные документы, такие как Африканская хартия прав и благополучия ребенка (1990 год) и Европейская конвенция об осуществлении прав детей (1996 год), а также региональные системы, такие как Межамериканская система прав человека.

[4] John Tobin and Sarah M. Field, “Article 16: The right to protection of privacy, family, home, correspondence, honour, and reputation”, in *The UN Convention on the Rights of the Child: a commentary*, John Tobin, ed. (Oxford, Oxford University Press, 2019).

[5] Комитет по правам ребенка, замечание общего порядка № 16 (2013), п. 12.

правосубъектности[6], таким как право на свободу выражения мнений и право на ассоциацию, а также право на здоровье[7]. Неприкосновенность частной жизни детей связана с их физической и психической неприкосновенностью, самостоятельностью при принятии решений, личной идентичностью, конфиденциальностью информации и физической/пространственной неприкосновенностью.

72. Основы будущей интеллектуальной, эмоциональной и сексуальной жизни закладываются в детском и подростковом возрасте, чему способствуют условия частной жизни[8]. Во всем мире опыт детства и право на неприкосновенность частной жизни являются различными[9]. Межсекторальные факторы, такие как раса, влияют на формирование детства[10].

73. Как правило, областями, важными для формирования личности детей, являются семья и домашняя жизнь, школа и социальные сети. Как и права детей, эти области взаимосвязаны и отражают основополагающие структурные факторы.

74. Дети, не имеющие дома и семьи, такие как несопровождаемые дети, беспризорные дети, дети в учреждениях интернатного типа, дети, находящиеся в зонах конфликтов и в других уязвимых ситуациях, сталкиваются с гораздо большими проблемами в плане доступа к своим правам человека[11].

75. Хотя неприкосновенность частной жизни для разных людей означает разные вещи, Специальный докладчик подчеркивает позитивный, стимулирующий аспект права на неприкосновенность частной жизни, который касается врожденного достоинства человека и способствует осуществлению других прав человека[12].

76. «Самоопределение» характеризуется как способность человека решать, раскрывать ли и в какой степени аспекты своей личной жизни[13]. Под самостоятельностью понимается способность к саморегуляции в мыслях, чувствах и действиях. Под термином «ребенок» понимается лицо, не достигшее 18 лет.

Определение проблем

Интересы, создающие напряженность

77. Рассмотрение вопроса о том, каким образом право детей на неприкосновенность частной жизни и личную неприкосновенность предполагает их самостоятельность, заключается в изучении факторов напряженности и различных точек зрения, в рамках которых эти права действуют.

78. Конвенция о правах ребенка наделяет государства-участники и родителей способностью и обязанностью, когда это необходимо, принимать решения по осуществлению детьми своих прав, предусмотренных в статье 16, в соответствии с их

[6] Представление Регионального отделения для региона Ближнего Востока и Северной Африки Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) (разрешение на размещение представления не было предоставлено).

[7] Submission from International Federation of Library Associations and Institutions, p. 2. В тех случаях, когда такое разрешение дано, материалы, полученные Специальным докладчиком в ответ на его консультации, будут размещаться по адресу URL: www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx.

[8] Submission from Belgian Disability Forum, p. 2.

[9] Submissions from InternetLab and Alana Institute; Office of the Victorian Information Commissioner, Australia.

[10] Rebecca Epstein, Jamila Blake and Thalia González, “Girlhood interrupted: the erasure of black girls’ childhood”, Georgetown Law Center on Poverty and Inequality, 2017.

[11] Submission from Maat for Peace, Development and Human Rights, p. 7.

[12] См. резолюцию 68/167 Генеральной Ассамблеи, резолюцию 20/8 Совета по правам человека и A/HRC/13/37.

[13] Abstract of the German Federal Constitutional Court’s judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES].

развивающимися способностями (ст. 5), в целях обеспечения наилучших интересов ребенка (ст. 3)[14].

79. Традиционно права детей на неприкосновенность частной жизни рассматривались в качестве вопроса, который должен регулироваться взрослыми. Однако потребности детей в личной жизни отличаются от потребностей взрослых и могут вступать в противоречие с ними[15]. Например, «шерентинг» (размещение родителями в соцсетях информации о ребенке (фотографии, истории о жизни...)) может привести к тому, что право родителей на свободу выражения мнений вступит в конфликт с правом их ребенка на неприкосновенность частной жизни[16].

80. Толкование взрослыми потребностей детей в личной жизни может препятствовать здоровому развитию самостоятельности и независимости, а также ограничивать неприкосновенность частной жизни детей во имя их защиты[17]. Ярким примером служит то, что взрослые полагаются на надзор в целях защиты детей. Это ограничивает права детей на неприкосновенность частной жизни и самостоятельность, однако дети все чаще подвергаются технологическому надзору со стороны правительств, частного сектора, родителей, семьи и сверстников[18]. Родительский надзор усиливается, а не уменьшается с возрастом ребенка, т. е. по мере того как молодые люди становятся (или должны становиться) более независимыми[19]. Родители и лица, ухаживающие за детьми с дополнительными потребностями, предпочитают еще более защитный подход, включающий в себя высокие настройки конфиденциальности по умолчанию и возможность определять конфиденциальность своих детей в сети[20].

81. Поведение родителей может противоречить озвучиваемым опасениям родителей. По имеющимся данным, 57 % родителей подростков в возрасте 13–17 лет беспокоит то, что их ребенок может получать или рассылать откровенные изображения, а 85 % испытывают беспокойство по поводу неприкосновенности частной жизни своих детей в цифровой сфере[21]. Однако менее одного из трех родителей используют настройки родительского контроля на устройствах своих детей, а 81 % сознательно разрешают своим детям использовать настройку «без возрастных ограничений» в YouTube без надзора[22].

82. О необходимости оценки, политики ограничения и регулирования рисков, ориентированных на ребенка, на основе фактических данных свидетельствует недавнее исследование, показавшее, что взрослые, не имевшие личного негативного опыта в сети, такого как угрозы насилия или «троллинг», с большей вероятностью захотят ограничить доступ к информации и анонимность в сети[23].

---

[14] Tobin and Field, “Article 16”.

[15] Submissions from Parental Rights Foundation; Action Canada for Sexual Health and Rights, p. 4; Commission Nationale de l’Informatique et des Libertés (CNIL), p. 11.

[16] Представление Южно-австралийского комиссара по делам детей и молодежи (в котором термин «шерентинг» объясняется в качестве растущей тенденции родителей и будущих родителей использовать Интернет для размещения информации о своих детях онлайн, что формирует личность ребенка онлайн задолго до того, как ребенок сможет дать согласие или начнет создавать свой собственный цифровой след), стр. 3.

[17] Submission from International Child Rights Center and MINBYUN.

[18] Там же; Jane Bailey and Valerie Steeves, *Defamation Law in the Age of the Internet: young people’s perspectives* (Law Commission of Ontario, Canada, 2017); submission from Ariel Foundation International.

[19] Submission from South Australia Commissioner for Children and Young People.

[20] URL: www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf.

[21] Monica Anderson “A majority of teens have experienced some form of cyberbullying”, Pew Research Center, 27 September 2018.

[22] Submission from ACT/The App Association.

[23] BT/DEMOS, “Online harms: a snapshot of public opinion” (2020). URL: https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf.

83. По мере взросления дети желают и требуют уважения своей частной жизни не только от школ, предприятий и правительств, но и от своих родителей[24]. Эта потребность растет со взрослением детей. В то время как дети в возрасте от 5 до 7 лет обычно не рассматривают родительский контроль за их деятельностью онлайн как нарушение неприкосновенности частной жизни, подростки в возрасте от 15 до 17 лет часто обеспокоены контролем со стороны родителей и школы[25]. Подростки считают, что частная жизнь и частное пространство без оценочных суждений и контроля позволяют им исследовать идеи и возможности творческого самовыражения и развивать независимое мнение[26]. Родительский контроль должен быть соразмерен развивающим способностям и взглядам ребенка[27].

Личная идентичность

84. Современные дети — это первое поколение, родившееся в цифровую эпоху[28], в то время как их родители являются первыми, кто воспитывает «цифровых детей»[29].

85. Все чаще идентичность ребенка начинает формироваться до его рождения с изображений в утробе, которые родители и семьи размещают в Интернете. Многие из этих изображений содержат встроенную личную информацию.

86. Формирование цифровой идентичности детей продолжается в основном в результате действий семьи на протяжении всего детства, при этом 80 % детей, живущих в развитых западных странах, приобретают цифровой след до достижения ими двухлетнего возраста[30]. Изображения детей также используются без их согласия для сбора пожертвований на цели благотворительности[31].

87. Дети сегодня участвуют в онлайн-активности различными способами и в более раннем возрасте, чем раньше[32]. Частота использования ими социальных сетей претерпевает кардинальное изменение в возрасте с 9 до 10 лет и с 11 до 12 лет, удваиваясь с 34 % до 69 %[33]. С седьмого по одиннадцатый классы число детей, общающихся онлайн, увеличивается вдвое[34]. Многие дети в возрасте до 13 лет имеют профили в социальных сетях (38 % детей в возрасте 9–12 лет, согласно европейским исследованиям)[35], а большинство из них — от двух до пяти профилей[36]. Пандемия коронавирусного заболевания (COVID-19) усилила эту тенденцию: с марта по сентябрь 2020 года число ежедневно активных пользователей «Facebook's Messenger Kids» выросло на 350 %[37].

88. Все чаще самоуважение и самооценка, необходимые для формирования личности и идентичности, развиваются в цифровом виде[38]. Дети используют Интернет для непрерывного освещения своей жизни, а смайлики-эмоджи «сердечки» и

[24] Submissions from Future of Privacy Forum; Ariel Foundation International.
[25] Submission from Global Privacy Assembly, Digital Education Working Group, p. 25.
[26] Submission from Office of the Victorian Information Commissioner, Australia.
[27] Submission from CNIL, p. 11.
[28] Submission from Canadian Human Rights Commission, p. 2.
[29] Danah Boyd, "Social network sites as networked publics: affordances, dynamics, and implications", in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Zizi Papacharissi ed. (Routledge, 2011).
[30] Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 42.
[31] Submissions from International Child Rights Center and MINBYUN; Ombudsman for Children, Croatia, p. 3.
[32] Submissions from Information Commissioner's Office, United Kingdom; CNIL; Information and Data Protection Commissioner, Albania.
[33] Submission from Economic Commission for Latin America and the Caribbean (ECLAC).
[34] Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 29.
[35] Там же, стр. 53.
[36] Submission from Information and Data Protection Commissioner, Albania, p. 14.
[37] Submission from Facebook.
[38] Submissions from Anna Bunn, p. 11; Office of the Victorian Information Commissioner, Australia, p. 2.

«большой палец вверх» в социальных сетях становятся дополнениями к их мыслям[39], но при этом они обеспокоены потерей контроля над своей информацией в сети[40].

89. Насилие, сексуальные домогательства и киберзапугивание присутствуют в цифровой жизни, особенно в отношении молодежи из числа ЛГБТКИ (см. A/HRC/43/52). Около 25 % подростков в возрасте от 13 до 17 лет сообщили о том, что им присылались откровенные изображения без их согласия[41]. Около 29 % девочек и 20 % мальчиков сообщили о том, что они являются получателями невостребованных откровенных изображений. Нежелательное получение и распространение изображений, даже если они не являются объективно вредными, оскорбительными или непристойными, может препятствовать развитию у ребенка чувства собственного достоинства, самостоятельности, выстраиванию отношений с другими и психосоциальному развитию[42].

90. Растление и совращение детей, как онлайн, так и офлайн, являются нарушением физической неприкосновенности и самостоятельности в принятии решений. Это имеет долгосрочные последствия для личности и способностей, и продолжающееся существование в сети материалов, содержащих информацию о сексуальном насилии по отношению к детям, усугубляет эти последствия. Формы и последствия сексуальных злоупотреблений обусловлены тем, как общество воспринимает детей и их тело[43]. Противодействие таким злоупотреблениям требует стратегий, основанных на правах человека[44]. Погружение молодых людей в постоянно расширяющийся спектр цифровых технологий создает непрерывный поток данных, собираемых и улучшаемых с помощью искусственного интеллекта, приложений машинного обучения, а также технологий распознавания лиц и речи. Дети и их данные служат своего рода топливом для бизнеса цифрового мира[45]. Рынок онлайн-рекламы для детей может составить 1,7 млрд долл. США к 2021 году, при этом компании, занимающиеся онлайн-рекламой, соберут более 72 млн единиц данных на каждого ребенка до достижения им 13-летнего возраста[46].

91. Маркетологи ведут «обработку» молодых людей, оказывают на них влияние и налаживают с ними постоянные отношения. Дети младшего возраста особенно уязвимы для целенаправленного маркетинга, поскольку они не проводят различия между рекламой и контентом, между вымыслом и реальностью, а также не понимают убеждающей природы рекламы[47]. Технология, включающая поведенческие методы (убеждающий дизайн/«темные схемы»), максимизирует заинтересованность, вызывает импульсивное поведение, влияет на принятие решений, порождает опасения отчуждения и оттесняет на второй план проблемы, связанные с неприкосновенностью частной жизни[48].

92. Профилирование детей ограничивает их потенциальное саморазвитие в детстве, подростковом возрасте и, возможно, во взрослой жизни, поскольку поведенческие прогнозы и методы подталкивания могут предопределять варианты и выбор.

[39] Submission from Ariel Foundation International.
[40] Submissions from C. Mahieu; Office of the Victorian Information Commissioner, Australia; CNIL.
[41] Monica Anderson, “A majority of teens have experienced some form of cyberbullying”.
[42] Submissions from Bunn; Mahieu.
[43] Submission from InternetLab and Alana Institute.
[44] Комитет по ликвидации дискриминации в отношении женщин, общая рекомендация № 38 (2020 год); Submission from Maat for Peace, Development and Human Rights, p. 7.
[45] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019); submission from InternetLab and Alana Institute.
[46] Submission from CNIL, p. 3.
[47] Submissions from Campaign for Commercial-Free Childhood and Center for Digital Democracy; InternetLab and Alana institute; CNIL.
[48] Submissions from Information Commissioner’s Office, United Kingdom; Office of the Victorian Information Commissioner, Australia; Mahieu; Jonathan Crock and others, American University; CNIL; ECLAC.

Предлагаемые технологические решения должны оцениваться с точки зрения прав и интересов ребенка, так как обработка персональных данных ребенка может[49]:

a) нарушать неприкосновенность частной жизни и защиту данных, включая потерю самостоятельности и нанесение ущерба личной репутации;

b) наносить вред психическому и эмоциональному здоровью и физическому благополучию детей;

c) приводить к экономическому ущербу или коммерческой эксплуатации[50].

93. Дети и подростки нуждаются в мерах реагирования, которые сведут к минимуму корпоративный доступ к их данным и их использование[51]; установлении пределов для коммерческой деятельности и механизмах для обеспечения их наилучших интересов, включая возможность удаления размещенных материалов[52]. Дети считают, что они должны иметь возможность реализовать свои права на обращение в любую компанию с запросом о предоставлении копии их персональных данных, и около 40 % считают, что они должны иметь возможность делать запросы о доступе к данным или об их удалении в любом возрасте, а 21 % считают, что должны иметь такую возможность в 13 лет и младше. Лишь 13,5 % считают, что для подачи запроса о доступе к данным или их удалении необходимо быть старше 18 лет[53].

94. Цифровая эра благоприятствует развитию детей. Однако дети должны иметь возможность пользоваться без ограничений, налагаемых коммерческой практикой, своими правами на беспрепятственное развитие личности.

95. Из Южной Америки поступают сообщения о том, что технологии биометрического наблюдения и отслеживания используются для выявления и отслеживания детей, подозреваемых в неправомерных действиях, а также о том, что в ходе судебных процессов не обеспечивается защита частной жизни детей[54]. Выявление детей, представляющих интерес для правоохранительных органов, или детей родителей, находящихся в заключении, или родителей, связанных с терроризмом, противоречит неприкосновенности частной жизни, ведет к стигматизации и дискриминации и препятствует развитию личности[55]. Препятствия для развития могут возникать также в тех случаях, когда эти дети не идентифицируются соответствующими службами поддержки[56], хотя обмен данными может быть проблематичным, особенно с сотрудниками служб безопасности[57].

Сексуальность, гендер, физическая неприкосновенность и физическая самостоятельность

96. Дети очень сильно отличаются друг от друга по своим физическим, интеллектуальным, социальным и эмоциональным способностям. Эти различия особенно заметны в подростковом возрасте — периоде, характеризующемся

[49] Submission from Canadian Human Rights Commission, p. 2. Office of the Victorian Information Commissioner, Australia; Campaign for Commercial-Free Childhood and Center for Digital Democracy.

[50] Submissions from Information Commissioner’s Office, United Kingdom.

[51] Valerie Steeves, “Young Canadians in a wired world, phase III: trends and recommendations”, MediaSmarts, 2014.

[52] Submission from The eQuality Project.

[53] Submission from Global Privacy Assembly, p. 24.

[54] Submission from InternetLab and Alana Institute.

[55] Комитет по правам ребенка, замечание общего порядка № 24 (2019).

[56] Submissions from Children of Prisoners Europe; Families Outside; International Coalition for the Children of Incarcerated Parents; Quaker United Nations Office.

[57] United Nations Office on Drugs and Crime (UNODC), *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* (Vienna, 2017) pp. 138–139; United Nations, Office of Counter-Terrorism, *Children affected by the foreign-fighter phenomenon: ensuring a child rights-based approach* (2019), p. 103.

быстрыми физическими, когнитивными и социальными изменениями, в том числе половым и репродуктивным созреванием[58].

97. Сексуальное самовыражение, физическая неприкосновенность и физическая самостоятельность являются частью сложной ткани частной жизни детей, а также их свободы выражения мнений[59]. Подростки должны иметь возможность принимать решения, касающиеся их благополучия и тела, а также безопасно и в частном порядке познавать свою сексуальность по мере взросления[60], будь то офлайн или онлайн[61].

98. Однако права детей на физическую неприкосновенность и самостоятельность ущемляются действиями правительств, коммерческих структур, медицинских и других специалистов, родителей и сверстников. Выявленные нарушения включают в себя следующее[62]:

a) в случае девочек: проведение калечащих операций на половых органах;браки по принуждению; принуждение к сексу; принудительная беременность и материнство; принудительное тестирование на беременность; принудительная стерилизация; отказ в предоставлении информации и услуг в области репродуктивного и сексуального здоровья; обязательное уведомление и/или согласие родителей на применение предписанных противозачаточных средств и аборт; «конверсионная» терапия; уголовное наказание за половые сношения по обоюдному согласию со сверстниками, включая отправление сообщений сексуального содержания; развратные действия онлайн и офлайн; убийства, совершаемые в защиту чести; и «осуждение за бесстыдство»;

b) в случае мальчиков: проведение калечащих операций на половых органах; браки по принуждению; принуждение к сексу; принудительная стерилизация; отказ в предоставлении информации и услуг в области репродуктивного и сексуального здоровья; «конверсионная» терапия; уголовное наказание за половые сношения по обоюдному согласию со сверстниками, включая отправление сообщений сексуального содержания; развратные действия онлайн и офлайн; домогательства; и телесные наказания;

c) дети с различной гендерной идентичностью, сексуальной ориентацией и самовыражением, а также с различными сексуальными характеристиками: насилие; дискриминация и домогательства; патологизация их гендерной идентичности или тела; ненужное медицинское лечение; публикация подробностей о гениталиях; стигматизация; «показательное» изнасилование; «конверсионная» терапия; отказ в предоставлении конкретных медицинских услуг, включая предоставлении информации и услуг в области репродуктивного и сексуального здоровья для трансгендеров; отказ в доступе к записям в медицинской карте; уголовное наказание за половые сношения по обоюдному согласию со сверстниками, включая отправление сообщений сексуального содержания; развратные действия онлайн и офлайн; и отсутствие юридического признания гендерной идентичности.

99. Нарушения неприкосновенности частной жизни затрагивают другие права, такие как права, закрепленные в статьях 3, 6, 8, 12, 16, 19 и 29 (пункт 1) Конвенции о правах ребенка. Так, например[63]:

a) обязательное тестирование на беременность ущемляет права девочек на достоинство, равенство и самостоятельность;

[58] Комитет по правам ребенка, замечание общего порядка № 4 (2003).

[59] Submissions from Matimba; Council of Europe; Australian Human Rights Commission.

[60] Submission from Center for International Human Rights.

[61] Submission from ParentsTogether.

[62] Submissions from Crock and others; Human Rights Watch; ILGA-Europe, Transgender Europe and The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation; NNID, Netherlands organisation for sex diversity; CHOICE for Youth and Sexuality; OutRight Action International; Australian Human Rights Commission; Center for International Human Rights; Council of Europe.

[63] Submission from Organisation Intersex International Europe.

b) опросы с целью выявления учащихся различной половой/гендерной идентичности нарушают право на недискриминацию, а при использовании для отчисления учащихся — их право на образование;

c) «добровольное» тестирование на девственность, часто навязываемое родителями, ущемляет права девочек на достоинство, равенство и самостоятельность;

d) процессы с интенсивным использованием медикаментозных средств, влекущие за собой хирургическое вмешательство в целях юридического признания гендерной идентичности, затрагивают право на здоровье[64];

e) обязательное согласие или уведомление родителей о предоставлении услуг в области сексуального или репродуктивного здоровья затрагивают право на здоровье, идентичность, жизнь, защиту от причинения вреда и наилучшее обеспечение интересов ребенка.

100. Дети нуждаются в праве и имеют право на консультационную помощь по вопросам здоровых сексуальных отношений, согласия на них и их безопасной практики[65]. Всестороннее половое просвещение может помочь детям защищать и развивать их личную жизнь, независимость и самостоятельность[66], а также способствовать благополучию, особенно молодых людей из числа ЛГБТКИ-сообщества[67]. Из различных регионов мира, в том числе из Бразилии, Ганы, Доминиканской Республики, Кении и Польши, поступали сообщения о противодействии всестороннему половому просвещению детей и подростков[68].

Признание личности

101. Все люди обладают правами именно в силу присущей им и равной идентичности в качестве человеческих существ[69]. Системы записи и учета актов гражданского состояния официально устанавливают личность, но редко обращаются к учреждениям по делам детей с вопросами по поводу их записей[70].

102. Официальное установление личности начинается с регистрации рождения. Однако многие дети во всем мире и в непропорционально большой степени в общинах аборигенов и коренных народов не регистрируются[71]. Отсутствие юридического признания отрицательно сказывается на доступе ко многим правам, необходимым для обеспечения самостоятельности, таким как право на образование.

103. Свидетельства о рождении могут создавать проблемы с точки зрения уважения достоинства, идентификации, конфиденциальности и развития детей-транссексуалов и детей-интерсексов, детей, рожденных в рамках международных соглашений о суррогатном материнстве, пропавших без вести детей, несопровождаемых детей-беженцев и детей в учреждениях интернатного типа, в частности[72].

[64] Submissions from Matimba; A. McCarthy.

[65] Комитет по правам ребенка, замечание общего порядка № 15 (2013); Комитет по экономическим, социальным и культурным правам, замечание общего порядка № 22 (2016); submissions from Australian Human Rights Commission; Mahieu; Center for Reproductive Rights, p. 1.

[66] Submissions from Action Canada for Sexual Health and Rights; ILGA Europe, Transgender Europe and The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation.

[67] Submission from McCarthy.

[68] Submission from Human Rights Watch, para. 18.

[69] Dinah Shelton, “On identity”, *The George Washington International Law Review*, vol. 39 (1999).

[70] Submission from Rights in Records by Design, Monash University and Federation University; *D.Z. v. Netherlands* (CCPR/C/130/D/2918/2016).

[71] Submission from Australian Human Rights Commission.

[72] Submissions from Australian Human Rights Commission; Submission from Rights in Records by Design, Monash University and Federation University; Kathryn Allan and David Lacey, “Identity management in disaster response environments: a child exploitation mitigation perspective”, *Australian Journal of Emergency Management*, vol. 33, No. 3 (July 2018).

Образование и школьное обучение

104. Целью образования является развитие личности, талантов, умственных и физических способностей детей в их самом полном объеме. Образование является одним из прав человека и основным средством, позволяющим детям жить достойной жизнью[73]. Оно расширяет права и возможности детей, индивидуально и коллективно, защищая их от эксплуатации. Право на образование требует, чтобы государства уважали, защищали и осуществляли его, устраняя такие препятствия на пути к образованию, как гендерные запреты и насилие[74].

105. Школы играют значительную роль в повседневном опыте детей в плане неприкосновенности их частной жизни. После объявления пандемии COVID-19 к 1 апреля 2020 года 193 страны закрыли школы, что затронуло примерно 90 % общемирового числа учащихся[75].

106. Что касается онлайн-образования, то количество загрузок учебных приложений увеличилось на 90 % по сравнению со средним еженедельным показателем в конце 2019 года[76]. Переход к онлайн-образованию усилил существующий дисбаланс сил между компаниями, занимающимися образовательными технологиями, и детьми, а также между правительствами и детьми и родителями, при этом несколько правительств отошли от соблюдения действующих законов о конфиденциальности данных о детях. В Уэльсе, например, правительство отменило требование о согласии родителей и учащихся[77]. В других местах защита права детей на неприкосновенность частной жизни в государственных школах отсутствует[78]. Тем не менее негосударственные субъекты регулярно контролируют цифровые образовательные записи детей[79].

107. Оцифровывание и хранение данных об обучении детей охватывает характеристики мышления, траекторию обучения, степень вовлеченности, быстроту реакции, прочитанные страницы и просмотренные видеоматериалы[80]. Большинство детей и родителей не имеют возможности оспаривать правила конфиденциальности компаний, занимающихся образовательными технологиями, или отказаться от предоставления данных, поскольку образование является обязательным[81].

108. При отборе школами учебных приложений и веб-инструментов основное внимание уделяется соображениям, касающимся учебной программы и стоимости, а не конфиденциальности[82]. В сентябре 2020 года в результате анализа 496 приложений в области образовательных технологий в 22 странах было установлено, что многие из них занимаются сбором идентификаторов устройств, 27 прикладных программ собирают данные о местонахождении и 79 из 123 протестированных вручную прикладных программ обмениваются данными о пользователях с третьими сторонами, такими как партнеры по рекламной деятельности[83]. Безопасность данных вызывает озабоченность. Например, компания Microsoft сообщила о 5,7 млн инцидентов с вредоносным ПО, затронувших пользователей ее образовательного программного обеспечения в период с 24 августа по 24 сентября 2020 года[84].

109. Сами школы хранят значительный объем информации о детях и все чаще отслеживают детей, наблюдая за деятельностью учеников онлайн, и с помощью камер

[73] Конвенция о правах ребенка, ст. 29 1) a).
[74] Резолюция 75/166 Генеральной Ассамблеи.
[75] Submission from ParentsTogether.
[76] Submission from Human Rights Watch, para. 44.
[77] Там же, п. 48.
[78] Submission from South Australia Commissioner for Children and Young People.
[79] URL: https://rm.coe.int/educational-settings/16809f3ba3.
[80] Submission from Global Privacy Assembly, p. 4.
[81] Представления от DefendDigitalMe; Council of Europe.
[82] Submission from Office of the Victorian Information Commissioner, Australia.
[83] Alfred Ng, “Education apps are sending your location data and personal info to advertisers”, CNET, 1 September 2020.
[84] Submission from Human Rights Watch, para. 49.

видеонаблюдения[85]. Как и применение образовательных технологий, использование этой технологии требует подотчетности, осмысленного согласия, ограничения целей, сведения к минимуму данных, прозрачности и гарантий безопасности[86].

110. Образовательные процессы не имеют надобности и не должны подрывать осуществление права на неприкосновенность частной жизни и других прав независимо от того, где и каким образом ведется образовательный процесс[87], а также усиливать существующее неравенство[88].

Соответствие возрасту и развивающиеся способности

111. Термин «соответствие возрасту», как правило, принимается в качестве соответствия между хронологическим возрастом и поведением, а также соответствия между хронологическим возрастом и услугами, доступными детям, такими как онлайновый контент. Соответствие возрасту в нормативном смысле является стандартом, который провайдеры онлайн-услуг должны соблюдать при оказании услуг, подходящих для детей. Одним из недавних примеров является Кодекс разработки информационной продукции, соответствующей возрастным ограничениям, в Соединенном Королевстве Великобритании и Северной Ирландии[89]. В Соединенных Штатах Америки Закон о защите частной жизни детей в Интернете 1998 года налагает требования на операторов веб-сайтов и онлайн-услуг, предназначенных для детей до 13 лет, а также на операторов других веб-сайтов или онлайн-услуг, которые знают, что они собирают персональную информацию онлайн от детей в возрасте до 13 лет.

112. Тем не менее механизм соответствия возрасту не является панацеей, поскольку:

a) материал может быть соответствующим возрасту, но по-прежнему являться вредным для детей и их прав. Этот механизм может защищать и расширять права и возможности ребенка, когда он индивидуализирован, но может не удовлетворять потребности определенной возрастной группы детей, учитывая значительные различия в интеллектуальном и эмоциональном развитии детей одного и того же возраста[90];

b) в качестве общего порогового уровня соответствие возрасту создает неравенство для детей с различными способностями и является весьма примерным показателем их развивающихся способностей, потенциально ограничивая развитие их личности и самостоятельное осуществление ими своих прав и, возможно, является дискриминационным;

c) когда критерием для доступа к услугам является возраст, требуются поддающиеся проверке документы, удостоверяющие личность, что вызывает озабоченность по поводу безопасности, регламентирующих подходов и отсутствия стандартов и инструментов подтверждения достоверности возраста и отраслевых схем сертификации[91]. Другие указывают, что процессы проверки возраста могут осуществляться таким образом, чтобы отвечать требованиям конфиденциальности[92].

[85] Submission from South Australia Commissioner for Children and Young People.

[86] Submissions from InternetLab and Alana Institute; Research Group on Technology, Information and Society, University of Fortaleza, Brazil; Ombudsman of the Autonomous City of Buenos Aires; Council of Europe.

[87] Конвенция о правах ребенка, замечание общего порядка № 1 (2001 год); Резолюция 75/166 Генеральной Ассамблеи; submissions from DefendDigitalMe; Ombudsman of the Autonomous City of Buenos Aires; Research Group on Technology, Information and Society, University of Fortaleza, Brazil; Hungarian National Authority for Data Protection and Freedom of Information, case number NAIH/2020/7127/.

[88] Резолюция 75/166 Генеральной Ассамблеи; submissions from Ombudsman of the Autonomous City of Buenos Aires; ECLAC; Council of Europe.

[89] URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/.

[90] Конвенция о правах ребенка, замечание общего порядка № 7 (2005).

[91] Submission from CNIL, p. 10. Facebook.

[92] Submission from Yoti.

113. Считается, что один лишь возраст является несовершенным критерием оценки способностей детей. Некоторые страны признают способность не на основе хронологического возраста[93]. В начале 2020 года власти Онтарио (Канада) ввели в действие законодательство, позволяющее молодым людям получать доступ к своей персональной информации и требовать ее исправления непосредственно на основе способностей, а не возраста[94]. В случае конфликта права ребенка могут превалировать над решениями родителей или опекунов[95].

114. Готовность детей к принятию решений и их самостоятельность наиболее эффективно определяются не только хронологическим возрастом, но и контекстом, включая существующие риски и поддержку, индивидуальный опыт, затрагиваемые права и способность понимать последствия своих действий (или бездействия). При определении того, в каких случаях дети способны, например, дать согласие на обработку их персональных данных, необходимо принимать во внимание их реальное понимание процесса обработки данных, их наилучшие интересы, права и взгляды[96].

115. По сути, понятие соответствия возрасту с трудом согласуется с принципом развивающихся способностей. Вопрос маркировки услуг с учетом развивающихся способностей детей требует более тщательного изучения.

Варианты решений

116. Максимальное уважение частной жизни детей является важнейшим средством обеспечения их интересов[97]. Подход, ориентированный на обеспечение наилучших интересов, требует, чтобы взрослые активно выясняли мнения детей и относились к ним со всей серьезностью. Об этом не всегда свидетельствуют действия государств, компаний, родителей и других лиц[98], однако дети признаются по международному праву в качестве человеческих существ, а не только как молодая поросль, и поэтому имеют право на права человека в соответствии с международным правом[99].

117. Все стороны — правительства, компании, общины, частные лица и родители — должны признавать детей в качестве носителей прав. Эффективная и всеобъемлющая борьба со злоупотреблениями в отношении детей, например с использованием ИКТ, требует основанного на правах человека многостороннего подхода с активным привлечением детей, семей, общин, правительств, гражданского общества и частного сектора[100].

118. Хотя зависимость детей, а следовательно, и их уязвимость, могут приводить к возникновению рисков, риск не равнозначен нанесению вреда, и столкновение с некоторыми рисками является необходимым условием для того, чтобы дети могли развить устойчивость к ним и навыки справляться с ними[101]. Определение детей только по фактору уязвимости без учета их способностей или потенциала может привести к чрезмерно протекционистским действиям, потенциально вредным для личности детей.

Защита данных детей

119. Хотя концепция неприкосновенности частной жизни является более широкой и сложной, защита данных тесно связана с ней. Свободное развитие личности происходит в благоприятных условиях тогда, когда люди защищены от неограниченного сбора, хранения, использования и обмена персональными данными.

[93] URL: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf.
[94] Submission from Global Privacy Assembly, p. 20.
[95] Ibid., p. 25
[96] Submission from Council of Europe.
[97] Submission from UNODC.
[98] Submission from Promsex.
[99] John Tobin, “Understanding children’s rights: a vision beyond vulnerability”, *Nordic Journal of International Law*, vol. 84, No. 2 (June 2015).
[100] Submission from UNODC; Facebook.
[101] Submission from South Australia Commissioner for Children and Young People.

120. Многие считают согласие основополагающим принципом. Согласие, однако, не обязательно отражает или защищает самостоятельность ребенка, особенно в тех случаях, когда существует дисбаланс сил. Кроме того, согласие родителей не всегда может отвечать наилучшим интересам ребенка или согласовываться с его взглядами[102].

121. Европейский общий регламент по защите данных способен улучшить защиту персональных данных детей, поскольку он предусматривает специальную защиту несовершеннолетних путем запроса информации, учитывающей особенности несовершеннолетних, относительно обработки их данных (ст. 12)[103]; особую бдительность по отношению к профилированию детей (пункт 71 декларативной части); и усиленное право на забвение (пункт 65 декларативной части), а статья 8 признает способность ребенка давать согласие на обработку данных в возрасте от 13 до 16 лет[104]. Кроме того, общие элементы встроенной защиты данных, неприкосновенность частной жизни по умолчанию, право не подвергаться автоматизированному индивидуальному принятию решений (ст. 22) и оценка воздействия защиты данных заслуживают более широкого применения для защиты персональных данных детей[105].

122. Конвенция 108+[106] также защищает от решений, принимаемых исключительно на основе автоматизированной обработки данных (ст. 1) a)), а недавно принятые Советом Европы руководящие принципы защиты данных детей в образовательной среде расширяют определение обработки персональных данных, охватывая прогнозы о группах или лицах с общими характеристиками, и определение обработки биометрических данных, с целью охвата этих видов обработки[107].

Инженерия защиты конфиденциальности и цифровая грамотность

123. Технологический дизайн может помочь противостоять «убеждающему дизайну» и «темным схемам»[108], а также продвигать цели законов и нормативных актов[109].

124. Наряду с инженерией защиты конфиденциальности цифровых технологий, дети и подростки нуждаются в приобретении оперативных навыков и определенных когнитивных и социальных способностей для использования технологий вдумчивым, этичным и безопасным образом. Обучение навыкам цифровой грамотности может предотвратить вредное поведение онлайн в источнике[110]. Существует широкое согласие, в том числе среди детей, в отношении того, что цифровая грамотность может повысить их онлайновую безопасность и самостоятельность[111], особенно учитывая все

[102] Submission from Ombudsman for Children, Croatia, p. 4.

[103] Simone van der Hof and Eva Lievens, “The importance of privacy by design and data protection impact assessments in strengthening protection of children’s personal data under the GDPR”, *Communications Law*, vol. 23, No. 1 (2018).

[104] До достижения этого возраста для обработки данных требуется согласие родителя или опекуна от имени ребенка.

[105] Van der Hof and Lievens, “The importance of privacy”.

[106] Конвенция о защите физических лиц при обработке персональных данных, пересмотренная в соответствии с Протоколом о внесении изменений в Конвенцию, Совет Европы, серия международных договоров 223. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[107] Submission from Council of Europe.

[108] Submissions from Campaign for Commercial-Free Childhood and Center for Digital Democracy; CNIL.

[109] Submission from ACT/The App Association.

[110] Jane Bailey and Valerie Steeves, *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls’ and Young Women’s Voices* (University of Ottawa Press, 2015); Jane Bailey and Jacquelyn Burkell, “Legal remedies for online attacks: young people’s perspectives”, *The Annual Review of Interdisciplinary Justice Research*, vol. 9 (2020).

[111] Submission from International Federation of Library Associations and Institutions; Office of the Victorian Information Commissioner, Australia; Future of Privacy Forum; Council of Europe; Australian Human Rights Commission; and Crock and others, p. 5.

более ранний возраст выхода детей в сеть, а также трудности, с которыми сталкиваются родители при оказании действенной поддержки[112].

125. Однако одни лишь технические решения и цифровая грамотность будут недостаточными без решительных и последовательных действий со стороны государств по устранению структурного неравенства и обеспечению неприкосновенности частной жизни, защиты данных и безопасности детей. У государств имеются значительные возможности для инвестиций в улучшение партнерских отношений с гражданским обществом, промышленностью, научными кругами и детьми в целях совместного создания решений в виде прототипов[113].

III. Выводы

126. **Поощрение неприкосновенности частной жизни детей и воспитание их самостоятельности требуют:**

a) разработки политики, законов и регламентов, которые:

i) признают детей в качестве носителей прав человека, благодаря чему их права на неприкосновенность частной жизни, самостоятельность и равенство становятся неотъемлемыми[114];

ii) используют широкое определение неприкосновенности частной жизни, охватывающее не только защиту данных, чтобы обеспечить полное развитие потенциала детей[115];

iii) учитывают мнения детей, подходы детей к неприкосновенности частной жизни, результаты исследований, ориентированных на детей, и/или оценки воздействия на неприкосновенность частной жизни детей в рамках государственной политики[116];

iv) предусматривают независимые механизмы примирения, арбитража и исправления индивидуальных или системных нарушений прав человека детей[117] и обеспечивают принятие правоприменительных мер в случае нарушений[118];

b) устраняют структурные подходы, которые позиционируют детей в качестве уязвимых и неправоспособных;

c) поощряют технологические инновации, направленные на совершенствование услуг по передаче информации при одновременной защите неприкосновенности частной жизни детей[119].

[112] Submissions from Information and Data Protection Commissioner, Albania;. InternetLab and Alana.

[113] Резолюция 75/166 Генеральной Ассамблеи.

[114] Bailey and Steeves, *eGirls, eCitizens*.

[115] Submissions from South Australia Commissioner for Children and Young People; Submission from International Child Rights Center and MINBYUN. Submission from Hungarian National Authority for Data Protection and Freedom of Information, p. 58.

[116] Submission from South Australia Commissioner for Children and Young People; Bailey and Steeves, *eGirls, eCitizens.*

[117] Submission from Canadian Human Rights Commission.

[118] Submission from 5Rights Foundation.

[119] Submission from ACT/The App Association.

IV. Рекомендации

127. **Специальный докладчик рекомендует государствам:**

a) обеспечивать, чтобы права и ценности Конвенции о правах ребенка, касающиеся неприкосновенности частной жизни, личности и самостоятельности, служили основой для законодательства, политики, решений, систем учета и услуг правительства;

b) поддерживать всесторонний анализ способности детей к самостоятельному принятию решений в отношении доступа к онлайновым и другим услугам, чтобы сделать возможным применение конкретно ориентированных на детей законов, политики и регламентов по защите неприкосновенности частной жизни на основе фактических данных;

c) принимать стандарты соответствия возрасту в качестве нормативного инструмента только с крайней осмотрительностью, когда нет более эффективных средств;

d) поощрять и требовать реализации принципов встроенной безопасности, встроенной защиты конфиденциальности и конфиденциальности по умолчанию в отношения продуктов и услуг для детей и обеспечить, чтобы дети имели эффективные средства правовой защиты от нарушений конфиденциальности;

e) поощрять партнерство с гражданским обществом и промышленностью для совместного создания технологических решений в наилучших интересах детей и молодежи;

f) принять к использованию рекомендации Специального докладчика по защите от нарушений неприкосновенности частной жизни по гендерному признаку (A/HRC/43/52, пп. 33–34);

g) разработать комплексные планы действий в области онлайнового образования на основе статьи 29 (пункт 1) Конвенции о правах ребенка и Руководящих принципов Совета Европы по защите данных детей в образовательной среде[120];

h) обеспечить создание и обновление соответствующих правовых основ для онлайнового образования;

i) создать государственную инфраструктуру для некоммерческих образовательных и социальных пространств;

j) устранить все законодательные пробелы и процедурные исключения для обеспечения того, чтобы все дети, вступающие в контакт с системами правосудия, сохраняли неприкосновенность частной жизни на протяжении всего судебного процесса, путем издания действующих на протяжении всей жизни приказов о неразглашении любых данных о привлечении к уголовной ответственности;

k) провести обзор правовых норм, позволяющих добровольные действия компаний по законному и соразмерному выявлению в сети материалов, содержащих информацию о сексуальном насилии по отношению к детям;

l) обеспечить, чтобы персональные данные детей, связанных с террористическими или агрессивными экстремистскими группами, были засекречены и передавались только в тех случаях, когда это строго необходимо для координации индивидуальной реабилитации и реинтеграции;

m) перед увязкой баз данных о личности граждан и баз данных о личности преступников проводить оценки воздействия на права человека с точки зрения последствий для детей и их частной жизни, а также проводить

[120] URL: www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting.

консультации для оценки необходимости, соразмерности и законности биометрического наблюдения;

n) разработать практику и законы для обеспечения того, чтобы информация, предоставляемая средствам массовой информации, не нарушала права детей на неприкосновенность частной жизни и чтобы информация, сообщаемая средствами массовой информации и другими органами, не нарушала неприкосновенность частной жизни детей, родители которых находятся в конфликте с законом;

o) обеспечить защиту частной жизни детей при всех контактах с родителями, находящимися в заключении, включая письменные, электронные и телефонные разговоры, а также посещения мест заключения;

p) обеспечить, чтобы биометрические данные не собирались от детей, за исключением случаев, когда это является исключительной мерой, только когда это законно, необходимо, соразмерно и полностью соответствует правам ребенка;

q) обеспечить беспристрастную, точную, безопасную обработку персональных данных детей для конкретной цели в соответствии с законной правовой основой с использованием мер защиты данных, представляющих собой передовую практику, таких как Общий регламент по защите данных и Конвенция 108+;

r) обеспечить, чтобы лица, осуществляющие обработку персональных данных, в том числе родители или опекуны и педагоги, были осведомлены о праве детей на неприкосновенность частной жизни и защиту данных;

s) обеспечить доступность для детей информации об осуществлении их прав, например на веб-сайтах органов по защите данных, и обеспечить предоставление консультаций, механизмов подачи жалоб и средств правовой защиты специально для детей, в том числе в связи с киберзапугиванием;

t) обеспечить, чтобы анонимность, псевдонимность или использование детьми технологий шифрования не были запрещены законом или на практике;

u) обеспечить детям и молодым людям любого происхождения возможности для участия в процессе принятия решений и разработки ориентированных на них рамок, политики и программ;

v) запретить автоматизированную обработку персональных данных, которые содержат личные характеристики детей, для принятия решений, касающихся ребенка, или для анализа или прогнозирования личных предпочтений, поведения и установок, за исключением случаев, когда это делается только в исключительных обстоятельствах в наилучших интересах ребенка или в преобладающих общественных интересах, при наличии соответствующих правовых гарантий;

w) обеспечить, чтобы права и ценности Конвенции о правах ребенка, касающиеся неприкосновенности частной жизни, личности и самостоятельности, служили основой для политики, управленческих решений и услуг предприятий;

x) соблюдать Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок в отношении «защиты, соблюдения и средств правовой защиты» и соответствующие руководящие указания по гендерным вопросам (A/HRC/41/43, приложение)[121];

y) создать механизмы правовой защиты и рассмотрения жалоб, обеспечивая при этом, чтобы они не препятствовали доступу к государственным механизмам;

[121] URL: www.ohchr.org/Documents/Issues/Business/Gender_Booklet_Final.pdf.

z) предоставлять понятную информацию о возможностях сообщения о проблемах, включая жалобы, а также о механизмах исправления положения и рассмотрения жалоб;

aa) принимать разумные, соразмерные, своевременные и эффективные меры для обеспечения того, чтобы их сети и онлайн-сервисы не использовались в преступных или иных незаконных целях, наносящих вред детям;

bb) взаимодействовать с правоохранительными органами в целях содействия правовой идентификации и судебному преследованию лиц, совершивших преступления в отношении детей.

Будущая работа

128. **К насущным приоритетам будущей работы по вопросам неприкосновенности частной жизни и детей относятся:**

a) развертывание международных усилий по разработке рамок для руководства по проектированию в целях защиты неприкосновенности частной жизни детей в Интернете;

b) задействование детей во время посещения стран и в подготовке тематических докладов по вызывающим озабоченность вопросам, касающимся неприкосновенности их частной жизни;

c) изучение норм родительского контроля и их влияния на развитие ребенка.

Annex I

Overview of activities

The key achievements of the mandate since 2015 include:

A. Detailed thematic reports and recommendations on:

Big data and open data, A/72/540 (2017) and A/73/438 (2018)

Health-related data, A/74/277 (2019)

Privacy and gender, A/HRC/40/63 (2019)

Artificial intelligence and privacy, and children's privacy, A/HRC/46/37 (2021)

B. Security and surveillance

The establishment of the International Intelligence Oversight Forum, which met in Bucharest (2016), Brussels (2017), Valletta (2018) and London (2019).

The draft legal instrument on government-led surveillance, while not progressed, has increasingly been demonstrated as needed and a useful reference for future work.

Networks have been established through the use of working parties, consultations and involvement of regional human rights bodies/entities, particularly in Europe.

Discussions with and specific recommendations to intelligence agencies, police forces and/or Governments of Member States concerning reinforcement of safeguards and remedies, including legislation regarding surveillance, encryption and independent oversight authorities.

Intensive work on complaints of infringement of privacy by Julian Assange and President Lenin Moreno, including preparation of interim reports.

The Special Rapporteur presented a report to the Human Rights Council on governmental surveillance activities from a national and international perspective, A/HRC/34/60 (2017).

The Special Rapporteur presented a report to the General Assembly on the implications of the COVID-19 pandemic for the right to privacy, A/75/147 (2020).

Communications to Member States

Since 2015, 101 communications have been issued to Member States concerning practices that appeared inconsistent with the right to privacy. Thirty were issued in 2020 (see annex II).

Visits and events

The COVID-19 pandemic prevented any official country visits during 2020.

Country visits were undertaken in: the United States of America in 2017 (A/HRC/46/37/Add.4); France in 2018 (A/HRC/46/37/Add.2); the United Kingdom of Great Britain and Northern Ireland in 2018 (A/HRC/46/37/Add.1); Germany in 2018 (A/HRC/46/37/Add.3); Argentina in 2019 (A/HRC/46/37/Add.5) and the Republic of Korea in 2019 (A/HRC/46/37/Add.6).

During 2020, the Special Rapporteur continued to promote privacy via online events, including the forty-second International Conference of Data Protection and Privacy Commissioners and multiple civil society organization and non-governmental organization events.

Taskforces

Security and surveillance

The annual International Intelligence Oversight Forum 2020 was postponed due to the COVID-19 pandemic. However, collaborative networks were maintained. The Special Rapporteur continued to work with various countries and their intelligence agencies on the upgrading of laws regulating surveillance and encryption. More detailed laws are needed to protect encryption and thereby, the privacy of communications.

Taskforce on corporations' use of personal data

The Special Rapporteur held five taskforce meetings attended by civil society organizations and leading corporations. The dialogue was highly productive, addressing issues including identity verification, European Court judgments concerning cross border movement of data, artificial intelligence, and privacy and children.

The taskforce's recommendation on artificial intelligence is provided in the main text of the present report. The draft was provided for international consultation, to which 28 submissions were received.

Taskforce on privacy and personality: children

The Special Rapporteur worked independently yet collaboratively with the Committee on the Rights of the Child on new guidelines to protect children's privacy. He also provided feedback to the Committee on its draft general comment No. 25.

The Special Rapporteur released a call for contributions on how privacy affects the development of personality, particularly the evolving capacity of the child and the growth of autonomy. Contributions were sought from interested parties on research, consultations with children and good practice mechanisms. Nearly 60 submissions were received. The principles and recommendations are included in the main body of the present report.

Annex II

Communications on the right to privacy

Communications (joint and from the Special Rapporteur on the right to privacy alone) on the right to privacy sent, and replies received, between 1 June 2015 and 1 January 2021

TIME PERIOD: Sent and Responses Received	*TYPE of COMMUNICATION*						
	Joint Urgent Appeals	*Joint Allegation Letters*	*Joint Other Letters*	*SRP Urgent Appeals*	*SRP Allegation Letters*	*SRP Other Letters*	*Total*[a]
2015–2020 Sent	6	60	19	0	5	11	101
2015–2020 Responses	4[b]	51[c]	10[d]	0	7[d]	5	77[a]
2020 Sent	1	22	5	0	0	2	30
2020 Responses	0	16[e]	4[f]	0	0	2	22[a]

Source: OHCHR communication database, https://spcommreports.ohchr.org/TmSearch/Results.

Abbreviation: SRP, Special Rapporteur on privacy.

[a] The number of replies received is not equal to the number of matters raised, as some replies included more than one response.

[b] Two Joint Urgent Appeals received two responses each.

[c] 44 responses to Joint Allegation Letters included six matters which received two responses, and one matter received a total of three responses, making a total of 51 responses from Member States.

[d] Two replies consisted of two responses.

[e] One reply included three responses.

[f] One reply consisted of two responses.