Генеральная Ассамблея

Distr.: General
13 September 2021
Russian
Original: English

Совет по правам человека
Сорок восьмая сессия
13 сентября — 1 октября 2021 года
Пункты 2 и 3 повестки дня
Ежегодный доклад Верховного комиссара Организации Объединенных Наций по правам человека и доклады Управления Верховного комиссара и Генерального секретаря

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

Право на неприкосновенность частной жизни в цифровой век*

Доклад Верховного комиссара Организации Объединенных Наций по правам человека

Резюме

В настоящем докладе, подготовленном в соответствии с мандатом, определенным Советом по правам человека в его резолюции 42/15, Верховный комиссар анализирует, как широкое использование государствами и предприятиями искусственного интеллекта, включая технологии профилирования, автоматического принятия решений и машинного обучения, влияет на осуществление права на неприкосновенность частной жизни и смежных прав. После обзора законодательной основы Верховный комиссар выделяет аспекты искусственного интеллекта, способствующие вмешательству в частную жизнь, и приводит примеры воздействия на право на частную жизнь и смежные права в четырех ключевых секторах. Затем Верховный комиссар обсуждает подходы к решению этих проблем, предлагая ряд рекомендаций для государств и предприятий в отношении разработки и внедрения гарантий для предотвращения и минимизации вредных последствий и содействия полному использованию преимуществ, которые может предоставить искусственный интеллект.

* Настоящий доклад был представлен после установленного срока, с тем чтобы отразить в нем самую последнюю информацию.

I. Введение

1. Настоящий доклад представлен в соответствии с резолюцией 42/15 Совета по правам человека, в которой Совет просил Верховного комиссара Организации Объединенных Наций по правам человека организовать семинар экспертов для обсуждения того, как искусственный интеллект, включая технологии профилирования, автоматического принятия решений и машинного обучения, могут, в отсутствие надлежащих гарантий, повлиять на осуществление права на неприкосновенность частной жизни, подготовить тематический доклад по этому вопросу и представить его Совету на его сорок пятой сессии[1].

2. Ни одна другая технологическая разработка последних лет не занимает воображение общественности в большей степени, чем искусственный интеллект (ИИ), в частности технологии машинного обучения[2]. Действительно, эти технологии могут стать огромной позитивной силой, помогая обществу преодолеть некоторые из серьезных проблем современности. Вместе с тем эти технологии могут иметь и негативные, даже катастрофические последствия, если они применяются без достаточного учета их влияния на права человека.

3. Хотя настоящий доклад не посвящен пандемии коронавирусного заболевания (COVID-19), продолжающийся глобальный кризис в области здравоохранения служит мощным и весьма наглядным примером скорости распространения, масштабов использования и воздействия ИИ в различных сферах жизни по всему миру. Для наблюдения за распространением этого заболевания применяются системы отслеживания контактов с использованием различных типов данных (геолокация, кредитные карты, транспортная система, медицинские и демографические данные) и информация о личных сетях. Системы ИИ задействованы для того, чтобы выявлять людей как потенциально инфицированных или заразных, требуя их изоляции или карантина. Системы ИИ, используемые для прогнозируемого выставления оценок, привели к результатам, дискриминирующим учащихся из государственных школ и бедных районов. Эти разработки продемонстрировали широкий спектр воздействия, которое системы ИИ оказывают на повседневную жизнь людей. Во всех этих случаях затрагивается право на неприкосновенность частной жизни, поскольку с помощью ИИ, использующего личную информацию, часто принимаются решения, которые оказывают ощутимое влияние на жизнь людей. Тем не менее с вопросом неприкосновенности частной жизни тесно переплетаются различные воздействия на осуществление других прав, таких как права на здоровье, образование, свободу передвижения, свободу мирных собраний, свободу ассоциации и свободу выражения мнений.

4. В 2019 году в документе «Высокое стремление: призыв к действиям в области прав человека» Генеральный секретарь Организации Объединенных Наций признал, что цифровой век расширил границы человеческого благосостояния, знаний и исследований. Он подчеркнул, что цифровые технологии предоставляют новые средства для отстаивания, защиты и осуществления прав человека. Тем не менее новые технологии слишком часто используются для нарушения прав, особенно прав лиц, которые уже уязвимы или остаются без внимания, например, посредством слежки, репрессий, цензуры и преследования в Интернете, в том числе правозащитников. Цифровизация систем социального обеспечения, несмотря на ее потенциал для повышения эффективности, может привести к исключению наиболее нуждающихся лиц. Генеральный секретарь подчеркнул, что достижения в области новых технологий не должны использоваться для подрыва прав человека, углубления неравенства или усугубления существующей дискриминации. Он подчеркнул, что управление ИИ

[1] Подготовка такого доклада была отложена. См. A/HRC/45/26 и A/HRC/47/61.

[2] Общепринятого определения термина «искусственный интеллект» не существует. В настоящем докладе он используется для обозначения комбинации процессов и технологий, которые позволяют компьютерам, например путем принятия решений и выполнения задач, дополнять или заменять конкретные функции, которые в противном случае должны были бы выполняться людьми (A/73/348, п. 3), что включает в себя машинное обучение и глубокое обучение, но не ограничивается ими.

должно обеспечивать справедливость, подотчетность, объяснимость и прозрачность. В сфере безопасности Генеральный секретарь повторил свой призыв к глобальному запрету на смертоносные автономные системы вооружений.

5. Настоящий доклад основывается на двух предыдущих докладах Верховного комиссара по вопросу о праве на неприкосновенность частной жизни в цифровой век[3]. В нем также учтены выводы, сделанные на виртуальном семинаре экспертов, проведенном в соответствии с резолюцией 42/15 Совета 27 и 28 мая 2020 года, а также ответы на призыв Верховного комиссара представить материалы для настоящего доклада[4].

II. Законодательная основа

6. Статья 12 Всеобщей декларации прав человека, статья 17 Международного пакта о гражданских и политических правах и ряд других международных и региональных документов по правам человека признают право на неприкосновенность частной жизни в качестве одного из основных прав человека[5]. Право на неприкосновенность частной жизни играет ключевую роль в балансе сил между государством и личностью и является основополагающим правом демократического общества[6]. Его значение для осуществления и реализации других прав человека онлайн и офлайн в мире, все более ориентированном на данные, возрастает[7].

7. Право на неприкосновенность частной жизни является выражением человеческого достоинства и связано с защитой автономии и личной идентичности человека[8]. К аспектам частной жизни, имеющим особое значение в контексте использования ИИ, относятся конфиденциальность информации, включая информацию, которая уже существует или может быть получена о лице и ее или его жизни, а также решения, основанные на этой информации[9], и свобода принимать решения относительно своей идентичности.

8. Любое вмешательство в право на неприкосновенность частной жизни не должно быть произвольным или незаконным[10]. Термин «незаконный» означает, что государства могут вмешиваться в осуществление права на неприкосновенность частной жизни только на основании закона и в соответствии с этим законом. Сам закон должен соответствовать положениям, целям и задачам Международного пакта о гражданских и политических правах и должен подробно определять точные обстоятельства, при которых такое вмешательство допустимо[11]. Введение понятия произвольности призвано обеспечить, чтобы даже вмешательство, допускаемое законом, соответствовало положениям, целям и задачам Пакта и в любом случае являлось обоснованным в конкретных обстоятельствах[12]. Соответственно, любое вмешательство в право на частную жизнь должно служить законной цели, быть

[3] A/HRC/27/37 и A/HRC/39/29.

[4] Призыв к участию и полученные материалы см. URL: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx.

[5] См. статью 16 Конвенции о правах ребенка, статью 14 Международной конвенции о защите прав всех трудящихся-мигрантов и членов их семей, статью 22 Конвенции о правах инвалидов, статью 10 Африканской хартии прав и благосостояния ребенка, статью 11 Американской конвенции о правах человека и статью 8 Конвенции о защите прав человека и основных свобод (Европейская конвенция по правам человека).

[6] A/HRC/39/29, п. 11.

[7] Комитет по правам ребенка, замечание общего порядка № 25 (2021), пп. 67 и 68; и A/HRC/39/29, п. 11.

[8] Комитет по правам ребенка, замечание общего порядка № 25 (2021), п. 67; и Европейский суд по правам человека, *Гудвин против Соединенного Королевства*, заявление № 28957/95, постановление от 11 июля 2002 года, п. 90.

[9] A/HRC/39/29, п. 5.

[10] Подробный анализ терминов «произвольный» и «незаконный» см. в A/HRC/27/37, пп. 21–27.

[11] Комитет по правам человека, замечание общего порядка № 16 (1988), пп. 3 и 8.

[12] Там же, п. 4.

необходимым для достижения этой законной цели и быть соразмерным[13]. Кроме того, любое ограничение должно представлять собой наименее интрузивный вариант действий и не должно нарушать суть права на неприкосновенность частной жизни[14].

9. Право на неприкосновенность частной жизни в равной степени распространяется на всех лиц. Различия в его защите по признаку расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или иного положения несовместимы с принципом недискриминации, закрепленным в пункте 1 статьи 2 и статье 3 Международного пакта о гражданских и политических правах. Дискриминация по этим признакам также нарушает право на равенство перед законом, содержащееся в статье 26 Пакта.

10. Пункт 1 статьи 2 Международного пакта о гражданских и политических правах требует от государств «уважать и обеспечивать» всем находящимся в пределах его территории и под его юрисдикцией лицам права, признаваемые в настоящем Пакте, без какой-либо дискриминации. Другими словами, государства должны не только воздерживаться от нарушения прав, признанных в Пакте[15], но и обязаны предпринимать позитивные шаги для защиты осуществления этих прав. Это подразумевает обязанность принимать адекватные законодательные и другие меры для защиты людей от вмешательства в их частную жизнь, независимо от того, исходит ли оно от государственных органов или от физических или юридических лиц[16]. Эта обязанность также отражена в разделе I Руководящих принципов предпринимательской деятельности в аспекте прав человека, в котором изложена обязанность государств защищать от негативных последствий для прав человека, связанных с компаниями.

11. Предприятия несут ответственность за соблюдение всех международно признанных прав человека. Это означает, что им надлежит избегать нарушений прав человека других людей и устранять те неблагоприятные последствия нарушений прав человека, к которым они причастны. В разделе II Руководящих принципов предпринимательской деятельности в аспекте прав человека представлено авторитетное руководство для всех предприятий по выполнению этой обязанности[17]. Ответственность за соблюдение существует в отношении всех видов деятельности и деловых отношений предприятия.

III. Воздействие искусственного интеллекта на право на неприкосновенность частной жизни и другие права человека

A. Соответствующие особенности систем искусственного интеллекта

12. Работа систем ИИ способна поощрять и углублять вторжения в частную жизнь и другие нарушения прав различными способами и усиливать их. Это включает как работу совершенно новых приложений, так и те особенности систем ИИ, которые расширяют, усиливают или стимулируют вмешательство в право на

[13] *Тунен против Австралии* (CCPR/C/50/D/488/1992), п. 8.3, *Ван Хюлст против Нидерландов* (CCPR/C/82/D/903/1999), пп. 7.3 и 7.6, *Мадхеву против Маврикия* (CCPR/C/131/D/3163/2018), п. 7.5, и CCPR/C/USA/CO/4, п. 22. См. также Комитет по правам ребенка, замечание общего порядка № 25 (2021), п. 69.

[14] Комитет по правам человека, замечание общего порядка № 31 (2004), п. 6; A/HRC/27/37, п. 22, и A/HRC/39/29, п. 10.

[15] Комитет по правам человека, замечание общего порядка № 31 (2004), п. 6.

[16] A/HRC/39/29, п. 23. См. также Комитет по правам человека, замечания общего порядка № 16 (1988), пп. 1 и 9, и № 31 (2004), п. 8; Комитет по правам ребенка, замечание общего порядка № 25 (2021), пп. 36–39.

[17] В своей резолюции 17/4 Совет по правам человека единогласно одобрил Руководящие принципы предпринимательской деятельности в аспекте прав человека.

неприкосновенность частной жизни, в первую очередь за счет расширения сбора и использования персональных данных.

13. Системы ИИ обычно опираются на большие наборы данных, часто включающие персональные данные. Это стимулирует повсеместный сбор, хранение и обработку данных. Многие предприятия оптимизируют свои услуги, с тем чтобы собрать как можно больше данных[18]. Например, онлайновые предприятия, такие как компании социальных сетей, полагаются на сбор и монетизацию огромного количества данных о пользователях Интернета[19]. Так называемый «Интернет вещей» представляет собой быстро растущий источник данных, используемый как предприятиями, так и государствами. Сбор данных происходит в интимных, частных и общественных пространствах[20]. Брокеры данных приобретают, объединяют, анализируют и передают личные данные бесчисленному количеству получателей. Эти операции с данными в значительной степени закрыты от общественного контроля и лишь в незначительной степени сдерживаются существующими правовыми рамками[21]. Полученные в результате наборы данных весьма велики, а собранная информация беспрецедентна по своим масштабам.

14. Помимо раскрытия частной жизни людей, для компаний и государств такие наборы данных делают людей уязвимыми и по ряду других причин. Нарушения конфиденциальности данных неоднократно приводили к раскрытию конфиденциальной информации миллионов людей[22]. Большие массивы данных позволяют бесчисленным образом анализировать данные и обмениваться ими с третьими сторонами, что зачастую приводит к дальнейшему нарушению неприкосновенности частной жизни и другим негативным последствиям для прав человека. Например, договоренности, позволяющие государственным органам иметь прямой доступ к таким наборам данных, хранящимся у предприятий, повышают вероятность произвольного или незаконного вмешательства в право на неприкосновенность частной жизни соответствующих лиц[23]. Особую озабоченность вызывает возможность деанонимизации, которой способствует объединение данных из различных источников[24]. В то же время дизайн наборов данных может иметь последствия для идентичности лиц. Так, набор данных, в котором пол регистрируется в бинарном виде, неправильно определяет тех, кто не идентифицирует себя как мужчина или женщина. Долгосрочное хранение персональных данных также несет в себе особые риски, поскольку данные открыты для будущих форм использования, не предусмотренных на момент их сбора[25]. Со временем данные могут стать неточными, неактуальными или нести исходные ошибки идентификации, что приведет к необъективным или ошибочным результатам обработки данных в будущем[26].

15. Следует отметить, что системы ИИ не полагаются исключительно на обработку персональных данных. Вместе с тем, даже если речь идет не о персональных данных,

[18] Wolflie Christl, *Corporate surveillance in everyday life* (Vienna, Cracked Lab — Institute for Critical Digital Culture, 2017).

[19] Материалы, представленные инициативой «Рейтинг цифровых прав».

[20] Материалы, представленные Центром управления коммуникациями Национального юридического университета Дели, «Деречос дихиталес», «Диджитл райтс уотч», «Глоубл партнерс диджитл», Международным центром некоммерческого права и Федеральным университетом Уберландии.

[21] Aaron Rieke and others, *Data brokers in an open society* (London, Open Society Foundation, 2016).

[22] См., например, https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

[23] Материалы, представленные Глобальной сетевой инициативой.

[24] Материалы, представленные Центром управления коммуникациями Национального юридического университета Дели, «Деречос дихиталес» и международной организацией «Прайвеси».

[25] Материалы, представленные «ОВД-Инфо».

[26] Комитет по ликвидации расовой дискриминации, общая рекомендация № 36 (2020), п. 33.

их использование может негативно сказаться на правах человека, включая право на неприкосновенность частной жизни[27], как показано ниже.

16. Инструменты ИИ широко используются для понимания закономерностей человеческого поведения. При наличии доступа к нужным массивам данных, можно сделать выводы о том, сколько людей в определенном районе, скорее всего, посещают то или иное культовое сооружение, какие телепередачи они предпочитают и даже примерно в какое время они обычно просыпаются и ложатся спать. Инструменты ИИ позволяют делать далеко идущие выводы о людях, в том числе об их психическом и физическом состоянии[28], и идентифицировать группы, например, людей с определенными политическими или личными пристрастиями. ИИ также используется для оценки вероятности будущего поведения или событий. Выводы и прогнозы, сделанные ИИ, несмотря на их вероятностный характер, могут стать основой для принятия решений, затрагивающих права людей, иногда полностью автоматизированным способом.

17. Многие выводы и прогнозы глубоко затрагивают осуществление права на частную жизнь, включая самостоятельность людей и их право на определение сведений о своей идентичности. С ними также связано множество вопросов, касающихся других прав, таких как право на свободу мысли и убеждений, право на свободу выражения мнения, право на справедливое судебное разбирательство и смежные права.

18. Решения на основе ИИ не свободны от ошибок. Фактически, масштабируемость решений ИИ может резко усилить негативные последствия при наличии, казалось бы, небольших ошибок[29]. Ошибочные результаты работы систем ИИ имеют различные причины, начиная с того, что результаты работы алгоритмов ИИ имеют вероятностные элементы, что означает, что в их результатах присутствует неопределенность[30]. Кроме того, актуальность и точность используемых данных часто вызывают сомнения. Далее, нереалистичные ожидания могут привести к внедрению инструментов ИИ, которые не приспособлены для достижения желаемых целей. Например, анализ сотен относящихся к медицине инструментов ИИ, применяемых для диагностики и прогнозирования рисков COVID-19, с разработкой которых связывали большие надежды, показал, что ни один из них не был пригоден для клинического использования[31].

19. Результаты работы систем ИИ, основанные на ошибочных данных, могут способствовать нарушениям прав человека множеством способов, например, ошибочно указывая на человека как на вероятного террориста или как на лицо, совершившее мошенничество в сфере социального обеспечения. Особую озабоченность вызывают предвзятые наборы данных, которые приводят к дискриминационным решениям на основе систем ИИ[32].

20. Процессы принятия решений в рамках многих систем ИИ непрозрачны. Сложность среды данных, алгоритмов и моделей, лежащих в основе разработки и функционирования систем ИИ, а также намеренная секретность государственных и частных структур являются теми факторами, которые подрывают значимые способы

[27] Совет Европы, «Руководящие принципы по решению проблемы воздействия алгоритмических систем на права человека» (приложение к Рекомендации CM/Rec(2020)1 Комитета министров государствам-членам, касающейся воздействия алгоритмических систем на права человека), разд. A, п. 6.

[28] Материалы, представленные «Деречос дихиталес» и международной организацией «Прайвеси».

[29] Материалы, представленные Германией.

[30] Агентство Европейского союза по основным правам, «#BigData: Дискриминация в процессе принятия решений на основе данных» (Вена, 2018 год), с. 4 оригинала.

[31] См. URL: https://www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/.

[32] Комитет по ликвидации расовой дискриминации, общая рекомендация № 36 (2020), пп. 31–36; и Группа высокого уровня по цифровому сотрудничеству, «Век цифровой взаимозависимости» (июнь 2019 года), сс. 17 и 18 оригинала.

понимания общественностью влияния систем ИИ на права человека и общество. Непрозрачности в значительной степени способствуют системы машинного обучения; они могут выявлять закономерности и разрабатывать предписания, которые трудно или невозможно объяснить[33]. Это часто называют проблемой «черного ящика»[34]. Непрозрачность затрудняет значимую проверку системы ИИ и может стать препятствием для эффективного определения ответственности в случаях, когда системы ИИ причиняют вред[35]. Тем не менее стоит отметить, что эти системы не обязательно должны быть полностью непонятными[36].

B. Опасения по поводу воздействия систем искусственного интеллекта в ключевых отраслях

21. В настоящем разделе показано, как такие опасения проявляются на практике путем рассмотрения четырех ключевых областей, в которых применение инструментов ИИ вызывает озабоченность.

Искусственный интеллект в сферах правоохранительной деятельности, национальной безопасности, уголовного правосудия и пограничного контроля

22. Государства все активнее внедряют системы ИИ в сферы правоохранительной деятельности, национальной безопасности, уголовного правосудия и пограничного контроля[37]. Хотя многие из этих приложений действительно могут вызывать беспокойство, в настоящем разделе основное внимание будет уделено нескольким отдельным примерам некоторых возникающих проблем в области прав человека, которые отличаются большим разнообразием.

23. Системы ИИ часто используются в качестве инструментов прогнозирования. В них применяются алгоритмы для анализа больших объемов данных, включая данные за прошлые периоды, для оценки рисков и прогнозирования будущих тенденций. В зависимости от цели данные об обучении и анализируемые данные могут включать, например, сведения о судимостях, об арестах, статистику преступлений, сведения о вмешательстве полиции в конкретных районах, сообщения в социальных сетях, данные о сообщениях и сведения о поездках[38]. Эти технологии могут быть использованы для создания профилей людей, определения мест, которые могут стать местами повышенной криминальной или террористической активности, и даже для выявления людей как вероятных подозреваемых и будущих рецидивистов[39].

24. Последствия этой деятельности для частной жизни и прав человека в целом являются весьма разнообразными. Во-первых, используемые наборы данных включают информацию о большом количестве людей, что затрагивает их право на неприкосновенность частной жизни. Во-вторых, они могут вызвать вмешательство государственных органов, например в виде обыска, допроса, ареста и судебного преследования, хотя сами по себе оценки ИИ не должны рассматриваться как

[33] Материалы, представленные Германией.

[34] См. URL: https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/.

[35] См. URL: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6; и https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/abs/ai-for-humanitarian-action-human-rights-and-ethics/C91D044210CADF7A0E023862CF4EE758.

[36] См., например, Inioluwa Deborah Raji and others, «Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing», 3 January 2020 (Иниолува Дебора Раджи и другие, «Ликвидация пробелов в подотчетности ИИ: определение сквозной структуры для внутреннего алгоритмического аудита», 3 января 2020 года).

[37] Углубленный анализ последствий использования ИИ и других цифровых технологий в сфере пограничного контроля для прав человека см. в документе A/75/590.

[38] Материалы, представленные международной организацией «Прайвеси». См. также A/HRC/44/57, п. 35.

[39] См. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

основание для обоснованных подозрений из-за вероятностного характера прогнозов. Затронутые права включают право на частную жизнь, право на справедливое судебное разбирательство, свободу от произвольного ареста и задержания, а также право на жизнь. В-третьих, в связи с присущей решениям на основе ИИ непрозрачностью возникают особенно острые вопросы, касающиеся подотчетности государства, когда ИИ используется для принятия принудительных мер, тем более в областях, которые обычно страдают от общего отсутствия прозрачности, таких как деятельность контртеррористических сил[40]. В-четвертых, инструменты прогнозирования несут в себе риск увековечивания или даже усиления дискриминации, отражая встроенные исторические расовые и этнические предрассудки в используемых наборах данных, например в виде непропорционально пристального внимания, уделяемого полицией определенным меньшинствам[41].

25. Развитие технологии биометрического распознавания привело к тому, что она все чаще используется правоохранительными органами и органами национальной безопасности. Биометрическое распознавание основано на сравнении цифрового представления определенных черт лица, таких как лицо, отпечаток пальца, радужная оболочка глаза, голос или походка, с другими такими представлениями в базе данных[42]. На основе их сопоставления делается вывод о степени вероятности того, что данное лицо действительно является тем лицом, которое должно быть идентифицировано. Эти процессы все чаще осуществляются в режиме реального времени и на расстоянии. В частности, удаленное распознавание лиц в режиме реального времени все чаще используется властями по всему миру[43].

26. Удаленное биометрическое распознавание в режиме реального времени вызывает серьезные опасения в рамках международного права прав человека, на что Верховный комиссар уже обращала внимание ранее[44]. Некоторые из этих опасений отражают проблемы, связанные с инструментами прогнозирования, включая возможность ошибочной идентификации лиц и непропорционального воздействия на представителей определенных групп[45]. Кроме того, технология распознавания лиц может быть использована для составления профиля человека на основе его этнической, расовой, национальной принадлежности, пола и других характеристик[46].

27. Удаленное биометрическое распознавание связано с глубоким вмешательством в право на частную жизнь. Биометрическая информация о человеке является одним из ключевых атрибутов его личности, поскольку оно раскрывает уникальные особенности, отличающие ее или его от других лиц[47]. Кроме того, дистанционное биометрическое распознавание резко повышает способность государственных органов систематически идентифицировать личность и отслеживать людей в общественных местах, не позволяя людям жить своей жизнью без наблюдения со стороны и оказывая прямое негативное воздействие на осуществление прав на свободу выражения мнений, мирных собраний и ассоциации, а также на свободу передвижения[48]. В таких условиях Верховный комиссар приветствует недавние усилия

[40] A/74/335 и A/HRC/43/46, пп. 37 и 38.

[41] Материалы, представленные компанией «Тек хайв эдвайзори лимитед». См. также Комитет по ликвидации расовой дискриминации, общая рекомендация № 36 (2020), п. 33; документ зала заседаний Верховного комиссара Организации Объединенных Наций по правам человека о поощрении и защите прав человека и основных свобод африканцев и лиц африканского происхождения от чрезмерного применения силы и других нарушений прав человека со стороны сотрудников правоохранительных органов (A/HRC/47/CRP.1), URL: https://www.ohchr.org/Documents/Issues/Racism/A_HRC_47_CRP_1.pdf, пп. 15 и 19.

[42] A/HRC/31/64, п. 14.

[43] Материалы, представленные Международным центром некоммерческого права.

[44] A/HRC/44/24.

[45] Материалы, представленные международной организацией «Прайвеси».

[46] A/HRC/44/57, пп. 39 и 40.

[47] A/HRC/44/24, п. 33. См. также Европейский суд по правам человека, дело *Реклос и Давурлис против Греции*, заявление № 1234/05, решение от 15 апреля 2009 года, п. 40.

[48] См. Европейский совет по защите данных и Европейский надзорный орган по защите данных, совместное мнение 5/2021, п. 30; и материалы, представленные Международным центром

по ограничению или запрещению использования технологий биометрического распознавания в режиме реального времени[49].

28. Помимо этого, были разработаны инструменты ИИ, которые якобы позволяют определять эмоциональное и психическое состояние людей по их мимике и другой «предсказывающей биометрии», с тем чтобы решить, представляют ли они угрозу безопасности или нет[50]. Системы распознавания эмоций по лицу основываются на той предпосылке, что можно автоматически и систематически определять эмоциональное состояние человека по его выражению лица, что не имеет под собой прочной научной основы[51]. Исследователи обнаружили лишь слабую связь эмоций с выражением лица[52] и подчеркнули, что выражения лица различаются в разных культурах и контекстах[53], что подвергает распознавание эмоций предвзятости и неправильному толкованию. С учетом этих опасений использование систем распознавания эмоций государственными органами, например с целью выявления отдельных лиц для остановки или ареста полицией или с целью оценки достоверности заявлений во время допросов, способно подорвать такие права человека, как право на частную жизнь, свободу и справедливое судебное разбирательство.

Системы искусственного интеллекта и государственные услуги

29. Системы ИИ все чаще используются для содействия предоставлению государственных услуг, часто с заявленной целью разработки более эффективных систем для своевременного и точного оказания услуг. Это также все больше проявляется в гуманитарном контексте, когда предоставление гуманитарных товаров и услуг может быть связано с системами ИИ. И хотя такие цели являются законными и даже похвальными, внедрение инструментов ИИ при оказании государственных и гуманитарных услуг может оказать негативное воздействие на права человека, если не будут приняты надлежащие меры предосторожности.

30. ИИ используется при оказании различных государственных услуг, начиная от принятия решений о выплате пособий по социальному обеспечению и заканчивая выявлением семей для посещения их службами по уходу за детьми[54]. Эти решения принимаются с использованием больших массивов данных, которые включают не только государственные данные, но потенциально также информацию, полученную от частных организаций, таких как компании социальных сетей или брокеры данных, часто собранную без учета обеспечивающей защиту законодательной основы[55]. Более того, поскольку вычислительные алгоритмы и контроль над системами ИИ, как правило, принадлежат частным компаниям, такие договоренности часто означают, что частные компании получают доступ к массивам данных, содержащим информацию о значительной части населения. Это вызывает озабоченность в отношении конфиденциальности, а также опасения по поводу того, как историческая предвзятость, заложенная в данных, повлияет на принятие решений государственными органами.

некоммерческого права и международной организацией «Прайвеси». См. также A/HRC/44/24, п. 34, и A/HRC/41/35.

[49] Материалы, представленные Европейским союзом. См. также URL: https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html; и Европейская комиссия, Предложение по регламенту Европейского парламента и Совета, устанавливающему согласованные правила по искусственному интеллекту (Закон об искусственном интеллекте) и вносящему изменения в некоторые законодательные акты Союза, COM(2021) 206 final, 21 апреля 2021 года, ст. 5 1) d).

[50] См. URL: https://www.ohchr.org/Documents/Issues/Terrorism/biometricsreport.pdf.

[51] См. URL: https://www.nature.com/articles/d41586-020-00507-5.

[52] См. URL: https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780190613501.001.0001/acprof-9780190613501-chapter-7.

[53] См. URL: https://journals.sagepub.com/doi/10.1177/1529100619832930; и https://pubmed.ncbi.nlm.nih.gov/22509011/.

[54] См. A/74/493.

[55] Материалы, представленные международной организацией «Прайвеси».

31. Основная проблема, связанная с использованием ИИ для оказания государственных услуг, заключается в том, что оно может носить дискриминационный характер, особенно в отношении маргинализированных групп[56]. Специальный докладчик по вопросу о крайней нищете и правах человека предупредил о «цифровой антиутопии в сфере социального обеспечения», в которой беспрепятственное сопоставление данных используется для разоблачения, обследования и наказания получателей социального обеспечения, а на получателей налагаются условия, подрывающие индивидуальную автономию и выбор[57]. Эти опасения недавно нашли свое подтверждение в Нидерландах, где широко освещавшееся решение суда запретило цифровую систему выявления мошенничества в сфере социального обеспечения, поскольку было установлено, что она нарушает право на неприкосновенность частной жизни. Данная система предоставила центральным и местным органам власти широкие полномочия по обмену и анализу данных, которые ранее хранились отдельно, включая данные о занятости, жилье, образовании, пособиях и медицинском страховании, а также другие виды идентифицируемых данных. Более того, этот инструмент был направлен на районы с низким уровнем дохода и меньшинства, что привело к фактической дискриминации по социально-экономическому признаку[58].

Использование искусственного интеллекта в контексте занятости

32. Ряд работодателей из предприятий всех видов и размеров демонстрируют растущий спрос на средства мониторинга работников с помощью технологий, основанных на данных, включая системы ИИ, и управления ими. Так называемый «анализ людских ресурсов» претендует на предоставление более эффективной и объективной информации о сотрудниках. Это может включать автоматизированное принятие решений о приеме на работу, порядке продвижения по службе или увольнении.

33. Хотя в основном такие технологии направлены на мониторинг поведения и производительности, связанных с работой, ряд приложений систем ИИ также распространяется на поведение и данные, не относящиеся к работе[59]. Пандемия COVID-19 усилила эту тенденцию в отношениях. Во-первых, некоторые компании, предоставляющие работникам профилактические медицинские программы, все чаще собирают данные о состоянии здоровья. Во-вторых, поскольку все больше процессов выполняется в цифровом формате, а люди работают из дома, мониторинг рабочих мест системами ИИ переносится в дома людей. Оба проявления такой тенденции повышают риск объединения данных, полученных в результате мониторинга на рабочем месте, с данными, не связанными с работой. Такие методы мониторинга на основе ИИ создают огромные риски для права на неприкосновенность частной жизни на протяжении всего жизненного цикла данных. Кроме того, данные могут быть использованы в иных целях, чем те, о которых изначально сообщалось сотрудникам, что может привести к так называемому «расползанию функций»[60]. В то же время количественная социологическая основа многих систем ИИ, используемых для управления людьми, не является прочной и подвержена предвзятости. Например, если компания использует алгоритм приема на работу с использованием ИИ, разработанный с использованием прошлых наборов данных, в которых предпочтение отдается белым мужчинам среднего возраста, полученный алгоритм будет дискриминировать женщин, «людей цвета», молодых или пожилых людей, которые были бы в равной степени

[56] Материалы, представленные «Диджитл райтс уотч». Углубленный анализ неравномерного воздействия автоматизации в системах социального обеспечения см. в статье Virginia Eubanks, *Automating Inequality* (New York, St. Martin's Press, 2018).

[57] См. A/74/493. См. также письмо Специального докладчика IRL 1/2020, в котором он отметил аналогичные опасения в отношении карты цифровых услуг, и ответ на него. В настоящем докладе содержится несколько ссылок на сообщения, направленные мандатариями специальных процедур Совета по правам человека. Все эти сообщения и ответы на них см. URL: https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[58] См. URL: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25522.

[59] См. URL: https://journals.sagepub.com/doi/10.1177/20539517211013051.

[60] Christl, *Corporate surveillance in everyday life*.

квалифицированы для заполнения данной вакансии[61]. В то же время структуры подотчетности и прозрачности для защиты работников нередко отсутствуют, и работники все чаще сталкиваются с тем, что они практически не получают никаких объяснений относительно практики мониторинга с использованием ИИ[62]. Хотя в некоторых ситуациях компании действительно заинтересованы в предотвращении неправомерного поведения на рабочем месте, меры по осуществлению такого намерения часто не оправдывают широко распространенную связанную с вмешательством практику количественной оценки социальных способов взаимодействия и обусловленных ими целей в отношении показателей производительности на рабочем месте. В рабочей обстановке и в свете властных отношений между работодателем и работником можно также предвидеть возможные сценарии, когда работники будут вынуждены отказываться от своих прав на частную жизнь в обмен на работу[63].

Искусственный интеллект для управления информацией в Интернете

34. Платформы социальных сетей используют системы ИИ для поддержки принятия решений по управлению контентом[64]. Компании используют эти системы для ранжирования контента и принятия решений о том, чему уделять повышенное внимание, а что отодвинуть на второй план, в том числе путем персонализации этих решений для разных пользователей на с учетом их профилей. Автоматизация также используется при введении ограничений на контент, в том числе в ответ на различные правовые требования в пределах юрисдикций и между ними[65]. Принятие обязательств по его фильтрации для посредников, связанных с предполагаемым вредом в Интернете, создает риски в плане расширения широкого использования ИИ без учета серьезного воздействия этих систем на права на неприкосновенность частной жизни и свободу выражения мнений на местном и глобальном уровнях.

35. Огромные массивы данных, на которые опираются системы курирования, усиления и модерации, создаются и постоянно расширяются благодаря обширному онлайн-мониторингу и профилированию пользователей платформы и их личных сетей[66]. Этот нескончаемый процесс сбора информации и формирования на ее основе выводов в сочетании с чрезвычайной концентрацией рынка привел к тому, что горстка компаний по всему миру владеет профилями миллиардов людей и сетевой общественной сферой в целом и контролирует их.

36. Курирование контента с помощью ИИ, осуществляемое компаниями, обладающими огромной рыночной властью, вызывает опасения по поводу воздействия на способность человека формировать и развивать свое мнение, как отмечали два последовательных обладателя мандата Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение[67]. Более того, рекомендательные системы платформ, как правило, сосредоточены на максимизации вовлеченности пользователей, опираясь на данные о предпочтениях, демографических и поведенческих моделях людей, что, как было показано, часто способствует распространению сенсационного контента, потенциально усиливая тенденции к поляризации[68]. Более того, целевое использование информации может быть нежелательным и даже привести к опасному вторжению в частную жизнь. Например, работа рекомендательных систем приводит к тому, что платформы

[61] Материалы, представленные Польшей. См. также URL: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

[62] См. URL: https://journals.sagepub.com/doi/full/10.1177/2053951720938093.

[63] См. URL: https://www.californialawreview.org/print/3-limitless-worker-surveillance/.

[64] См. URL: https://www.theverge.com/2020/11/13/21562596/facebook-ai-moderation; и https://journals.sagepub.com/doi/full/10.1177/2053951720943234.

[65] См. OTH 71/2018 и OTH 73/2020. Углубленный анализ автоматизированной фильтрации контента см. также URL: https://journals.sagepub.com/doi/full/10.1177/2053951720920686.

[66] A/73/348, п. 17.

[67] Там же, п. 25, и A/HRC/47/25, п. 36.

[68] См. URL: https://www.brookings.edu/techstream/how-youtube-helps-form-homogeneous-online-communities/.

социальных сетей предлагают жертвам насилия лицо, совершившее преступление, для целей возможных дружеских отношений и наоборот, подвергая такие жертвы риску. Кроме того, было доказано, что предвзятость групп большинства или доминирующих групп, отраженная в данных результатов поиска, влияет на информацию, которой делятся представители меньшинств или уязвимых групп или которая их касается. Например, исследования показали тревожную степень гендерной[69] и расовой предвзятости в результатах поиска «Гугл»[70].

IV. Решение проблем

37. Необходимость правозащитного подхода к новым технологиям в целом и искусственному интеллекту в частности признается все большим числом экспертов, заинтересованных сторон и международным сообществом[71]. Подход, основанный на правах человека, предлагает инструментарий, который поможет обществу определить способы предотвращения и ограничения вреда при максимальном использовании преимуществ технического прогресса.

A. Основные принципы

38. Основанный на правах человека подход к ИИ требует применения ряда базовых принципов, включая равенство и недискриминацию, участие и подотчетность — принципов, которые также лежат в основе Целей в области устойчивого развития и Руководящих принципов предпринимательской деятельности в аспекте прав человека. Кроме того, к технологиям ИИ должны последовательно применяться требования законности, легитимности, необходимости и пропорциональности[72]. Помимо этого, ИИ должен применяться таким образом, чтобы способствовать осуществлению экономических, социальных и культурных прав, обеспечивая реализацию таких ключевых аспектов этих технологий, как наличие, ценовая приемлемость, доступность и качество[73]. Лица, страдающие от нарушений прав человека и злоупотреблений, связанных с использованием ИИ, должны иметь доступ к эффективным судебным и внесудебным средствам правовой защиты[74].

39. Как было указано выше, ограничения права на неприкосновенность частной жизни должны быть предусмотрены законом, быть необходимыми для достижения законной цели и быть соразмерными этой цели. На практике это означает, что от государств требуется тщательно определить, способна ли соответствующая мера достичь поставленной цели, насколько важна эта цель и каково будет воздействие данной меры. Государства также должны определить, могут ли связанные с меньшим вмешательством подходы привести к тем же результатам с той же эффективностью. В случае положительного ответа такие меры должны быть приняты. Верховный комиссар уже обозначил такие необходимые ограничения и гарантии в контексте наблюдения со стороны спецслужб и правоохранительных органов[75]. Следует отметить, что тесты на необходимость и соразмерность также могут привести к тому выводу, что определенные меры не следует принимать. Например, требования о

[69] Материалы, представленные Австрией и Германией.

[70] Safiya Umoja Noble, *Algorithms of Oppression* (New York, New York University Press, 2018).

[71] Резолюция 75/176 Генеральной Ассамблеи, п. 6; резолюции 47/16 Совета по правам человека, п. 8 d), и 47/23, шестнадцатый пункт преамбулы; A/73/348, пп. 47–60, A/75/590, п. 57, и A/HRC/43/29; материалы, представленные Австрией, Комиссаром по вопросам охраны частной жизни Канады, «Диджитл райтс уот», Глобальной сетевой инициативой и международной организацией «Прайвеси».

[72] A/HRC/43/29, п. 41.

[73] Подробный анализ роли новых технологий для реализации экономических, социальных и культурных прав см. в документе A/HRC/43/29.

[74] Международный пакт о гражданских и политических правах, п. 3 ст. 2, и Руководящие принципы предпринимательской деятельности в аспекте прав человека, принцип 15 c) и компонент III.

[75] A/HRC/39/29, пп. 34–41.

тотальном, неизбирательном удержании коммуникационных данных, налагаемые на телекоммуникационные и другие компании, не пройдут проверку на соразмерность[76]. Аналогичным образом введение требований биометрической идентификации для получателей социальных пособий является непропорциональным, если не предусмотрено никакой альтернативы. Более того, крайне важно, чтобы меры оценивались не изолированно, а при этом учитывалось совокупное воздействие отдельных, но взаимодействующих мер. Так, прежде чем принять решение о развертывании новых средств наблюдения на основе ИИ, государство должно оценить существующие возможности и их влияние на осуществление права на неприкосновенность частной жизни и других прав.

B. Законы и нормативные акты

40. Эффективная защита права на неприкосновенность частной жизни и взаимосвязанных прав зависит от правовых, нормативных и институциональных рамок, созданных государствами[77].

41. С появлением систем ИИ, основанных на данных, возросла важность эффективной правовой защиты в рамках законов о конфиденциальности данных. Эти меры защиты должны соответствовать минимальным стандартам, определенным в предыдущем докладе Верховного комиссара о праве на неприкосновенность частной жизни[78].

42. Рамки конфиденциальности данных должны учитывать новые угрозы, связанные с использованием ИИ[79]. Так, законы могут накладывать ограничения на тип данных, которые могут быть на законных основаниях выведены и/или в дальнейшем использованы и переданы. Законодатели также должны рассмотреть вопрос об укреплении прав отдельных лиц, в том числе путем предоставления им права на значимое объяснение и на возражение против полностью автоматизированных решений, которые затрагивают их права[80]. По мере развития технологий ИИ необходимо будет продолжать разрабатывать дополнительные гарантии в рамках защиты конфиденциальности данных.

43. Одним из ключевых элементов противодействия растущей сложности и непрозрачности глобальной среды данных, включая ее обширную информационную асимметрию, являются независимые органы надзора за конфиденциальностью данных. Эти органы должны обладать эффективными правоприменительными полномочиями и быть обеспечены достаточными ресурсами. Организации гражданского общества должны быть наделены полномочиями для поддержки исполнения законов о конфиденциальности данных, в том числе путем создания надежных механизмов рассмотрения жалоб.

[76] Там же, п. 18; и Суд Европейского союза, «Цифровые права Ирландии и другие», C-293/12 и C-594/12, п. 69. См. также Суд Европейского союза, дело *Максимилан Шремс против Комиссара по защите данных*, C-362/14, п. 94, в котором говорится, что «законодательство, разрешающее государственным органам иметь доступ на обобщенной основе к содержанию электронных сообщений, должно рассматриваться как компрометирующее суть фундаментального права на уважение частной жизни».

[77] A/HRC/39/29, п. 26.

[78] Там же, пп. 28–33.

[79] Например, принятый в 2018 году протокол Совета Европы о внесении изменений в Конвенцию о защите частных лиц в отношении автоматизированной обработки данных личного характера является ответом на появление новой практики обработки данных.

[80] См. Общее положение о защите данных Европейского союза, которое включает такие права, и Закон о правах на частную жизнь Калифорнии, который уполномочивает регулирующий орган принимать соответствующие правила.

44. Помимо законодательства о конфиденциальности данных, необходимо пересмотреть и потенциально принять более широкий спектр законов для решения проблем ИИ с соблюдением прав человека[81].

45. Принимая во внимание разнообразие приложений, систем и способов использования ИИ, регулирование должно быть достаточно конкретным, с тем чтобы решать отраслевые проблемы и адаптировать ответные меры к соответствующим рискам[82]. Чем выше риск для прав человека, тем строже должны быть законодательные требования к использованию технологии ИИ. Соответственно, приоритет должны иметь те сектора, где ставки для отдельных лиц особенно высоки, такие как правоохранительная деятельность, национальная безопасность[83], уголовное правосудие, социальная защита, занятость, здравоохранение, образование и финансовый сектор. Соразмерный с риском подход к законодательству и регулированию потребует запрета определенных технологий, приложений или вариантов использования ИИ, если они будут оказывать потенциальное или фактическое воздействие, которое не оправдано в соответствии с международным правом прав человека, включая те из них, которые не проходят проверку на необходимость и соразмерность. Более того, нельзя допускать те виды использования ИИ, которые по своей сути противоречат запрету на дискриминацию. Например, в соответствии с этими принципами следует запретить социальное ранжирование людей правительствами[84] или системами ИИ, которые распределяют людей по кластерам по запрещенным дискриминационным основаниям[85]. Для систем, использование которых представляет риск для прав человека при развертывании в определенных условиях, государствам необходимо будет регулировать их использование и продажу для предотвращения и смягчения неблагоприятного воздействия на права человека[86] как на территории государства, так и за ее пределами. В тех случаях, когда возможно неблагоприятное воздействие на права человека, необходимо в обязательном порядке привлекать людей для выполнения надзорных функций и принятия решений[87]. С учетом того, что может пройти время, прежде чем риски будут оценены и устранены, государства также должны наложить мораторий на использование потенциально высокорискованных технологий, таких как дистанционное распознавание лиц в режиме реального времени, пока не будет гарантировано, что их применение не способно нарушить права человека.

46. Кроме того, государства должны принять надежные режимы экспортного контроля для трансграничной торговли технологиями наблюдения, с тем чтобы предотвратить продажу таких технологий, когда существует риск, что они могут быть

[81] См. Совет Европы, Рекомендация CM/Rec(2020)1 Комитета министров государствам-членам, касающаяся воздействия алгоритмических систем на права человека.

[82] В предложенном Европейским союзом Законе об ИИ используется такой подход, основанный на оценке рисков. В материалах, представленных Коалицией за свободу Интернета, Глобальной сетевой инициативой и «Глоубл партнерс диджитл», говорится о поддержке регулирования на основе оценки рисков.

[83] В документах A/HRC/27/37 и A/HRC/39/29 Верховный комиссар разъяснила требования к мерам наблюдения, принимаемым в контексте уголовных расследований и в целях защиты национальной безопасности, на которых должно строиться законодательство в этой области.

[84] Материалы, представленные Европейским союзом; Catelijne Muller, «The impact of artificial intelligence on human rights, democracy and the rule of law» (Кателин Мюллер, «Влияние искусственного интеллекта на права человека, демократию и верховенство права»), доклад Совету Европы, Специальный комитет по искусственному интеллекту (CAHAI(2020)06-fin), 24 июня 2020 года, п. 75; и Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), «Проект текста рекомендации по этике искусственного интеллекта» (SHS/IGM-AIETHICS/2021/JUN/3 Rev.2), 25 июня 2021 года, п. 26.

[85] См. Европейский совет по защите данных и Европейский надзорный орган по защите данных, совместное мнение 5/2021, п. 33.

[86] Материалы, представленные «Деречос дихиталес».

[87] См. URL: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6.

использованы для нарушения прав человека, включая нападения на правозащитников или журналистов[88].

47. Спектр рисков, возникающих в связи с системами ИИ, предполагает необходимость адекватного независимого, беспристрастного надзора за разработкой, внедрением и использованием систем ИИ. Надзор может осуществляться комбинацией административных, судебных, квазисудебных и/или парламентских надзорных органов[89]. Например, помимо органов по защите конфиденциальности данных, в систему надзора должны входить агентства по защите прав потребителей, отраслевые регуляторы, антидискриминационные органы и национальные институты по правам человека. Более того, межотраслевые регуляторы, занимающиеся надзором за использованием ИИ, могут помочь установить фундаментальные стандарты и обеспечить согласованность политики и правоприменения.

C. Проявление должной осмотрительности в вопросах прав человека

48. Государства и предприятия должны всеобъемлющим образом обеспечить проявление должной осмотрительности в вопросах прав человека при приобретении, разработке, развертывании и эксплуатации систем ИИ, а также перед передачей или использованием больших данных о лицах[90]. Помимо обеспечения ресурсами и руководства такими процессами, государства могут также требовать от компаний всеобъемлющего проявления должной осмотрительности в вопросах прав человека или иным образом стимулировать их к этому.

49. Целью процессов проявления должной осмотрительности в вопросах прав человека является выявление, оценка, предотвращение и смягчение неблагоприятного воздействия на права человека, которое может оказать то или иное образование, которому оно может способствовать или с которым оно будет непосредственно связано[91]. Если в рамках процессов обеспечения должной осмотрительности выясняется, что использование ИИ несовместимо с правами человека из-за отсутствия значимых способов смягчения ущерба, применение такой формы использования должно быть прекращено. Оценка воздействия на права человека является важным элементом процессов обеспечения должной осмотрительности в плане прав человека[92]. Должную осмотрительность необходимо обеспечивать на протяжении всего жизненного цикла системы ИИ[93]. Особое внимание следует уделять непропорциональному воздействию на женщин и девочек, лесбиянок, геев, бисексуалов, трансгендеров и квиров, инвалидов, лиц, принадлежащих к меньшинствам, пожилых людей, лиц, живущих в условиях нищеты, и других лиц, находящихся в уязвимом положении.

50. Необходимо проводить значимые консультации с потенциально затронутыми правообладателями и представителями гражданского общества, при этом к оценке

[88] A/HRC/41/35, п. 49, и A/HRC/44/24, п. 40. В этих докладах Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение и Верховный комиссар также призвали ввести мораторий на выдачу экспортных лицензий на технологии наблюдения.

[89] См. URL: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.

[90] В рамках проекта «Би-тех» Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) разрабатываются руководящие указания по применению Руководящих принципов предпринимательской деятельности в аспекте прав человека в технологической отрасли, включая меры реагирования на воздействие на права человека использования технологий ИИ.
См. URL: https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

[91] Обзор должной осмотрительности в области прав человека в контексте ИИ см. URL: https://international-review.icrc.org/articles/ai-humanitarian-action-human-rights-ethics-913, сс. 174–178 оригинала.

[92] Краткое изложение методологий оценки воздействия на права человека см. URL: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.

[93] A/HRC/43/29, п. 62 g), и A/HRC/44/24, пп. 38, 53 j) i) и 54 c).

воздействия, в том числе к разработке и оценке мер по смягчению последствий, следует привлекать экспертов с междисциплинарными навыками. Государства и предприятия должны постоянно контролировать воздействие используемых ими систем ИИ, с тем чтобы проверить, не оказывают ли они негативного воздействия на права человека. Результаты оценки воздействия на права человека, действия, предпринятые для устранения рисков в области прав человека, и консультации с общественностью должны быть обнародованы[94].

D. Связь между государством и предпринимательством

51. Ситуации, когда между государством и технологической компанией существует тесная связь, требуют особого внимания[95]. Государство является важным экономическим субъектом, который в состоянии определять то, как разрабатывается и используется ИИ, помимо выполнения своей роли в плане принятия правовых и политических мер. В тех случаях, когда государства сотрудничают с разработчиками ИИ и поставщиками услуг из частного сектора, они должны предпринимать дополнительные шаги для обеспечения того, чтобы ИИ не использовался в целях, несовместимых с правами человека. Такие меры должны применяться в отношении управления государственными компаниями, финансирования исследований и разработок, оказания финансовой и иной поддержки государствами технологическим компаниям ИИ, осуществления усилий по приватизации и практики государственных закупок.

52. В тех случаях, когда государства действуют как экономические субъекты, они продолжают нести основную ответственность по международному праву прав человека и должны активно выполнять свои обязательства. В то же время предприятия по-прежнему отвечают за соблюдение прав человека в рамках сотрудничества с государствами, и им надлежит изыскивать способы соблюдения прав человека, когда они сталкиваются с требованиями государства, противоречащими законодательству о правах человека[96]. Так, при наличии требований о предоставлении доступа к персональным данным, которые не соответствуют стандартам в области прав человека, они должны использовать свои рычаги для противодействия тому вреду, который может быть нанесен, или для его смягчения[97].

53. Государства способны усилить защиту прав человека, последовательно требуя ответственного ведения предпринимательской деятельности. Например, когда агентства по экспортным кредитам предлагают поддержку технологическим компаниям ИИ, они должны убедиться в том, что эти компании имеют солидный послужной список в области соблюдения прав человека и могут продемонстрировать это на основе действенных процессов должной осмотрительности.

54. В тех случаях, когда государства полагаются на предприятия ИИ в плане предоставления общественных товаров или услуг, они должны убедиться в том, что способны осуществлять надзор за разработкой и внедрением систем ИИ. Они могут добиться этого, запрашивая и оценивая информацию о точности и рисках приложения ИИ. Если соответствующие риски не могут быть эффективно снижены, государства не должны использовать ИИ для предоставления общественных товаров или услуг.

[94] A/73/348, п. 68.

[95] См. URL: https://www.ohchr.org/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf.

[96] Руководящие принципы предпринимательской деятельности в аспекте прав человека, принцип 23 b).

[97] A/HRC/32/38, п. 58. См. также URL: https://www.ohchr.org/Documents/Issues/Terrorism/biometricsreport.pdf, сс. 39 и 40 оригинала.

E. Прозрачность

55. Разработчики, маркетологи, операторы и пользователи систем ИИ должны в значительной степени активизировать свои усилия в отношении прозрачности использования ИИ. В качестве первого шага государства, предприятия и другие пользователи ИИ должны сделать доступной информацию о том, какие системы и для каких целей они используют, а также сведения о личности разработчика и оператора таких систем[98]. Затрагиваемые лица должны систематически получать информацию о тех случаях, когда решения принимаются или были приняты автоматически или с помощью средств автоматизации[99]. Физические лица также должны быть уведомлены о том, что предоставленные ими персональные данные станут частью набора данных, используемого системой ИИ[100]. Кроме того, в отношении приложений, серьезно затрагивающих права человека, государства должны ввести реестры, содержащие ключевую информацию об инструментах ИИ и их использовании[101]. Необходимо обеспечить эффективное исполнение обязательств по обеспечению прозрачности и прав на доступ к данным, на их уничтожение и исправление, содержащихся в рамочных документах о конфиденциальности данных. Особое внимание следует уделить тому, чтобы люди могли лучше понимать и контролировать профили, которые были для них составлены[102].

56. Следует все более повышать прозрачность, включая постоянные усилия по преодолению описанной выше проблемы «черного ящика». Разработка и систематическое внедрение методологии, позволяющей сделать системы ИИ более объяснимыми, которые часто называют алгоритмической прозрачностью, имеют огромное значение для обеспечения адекватной защиты прав[103]. Это особенно важно, когда ИИ используется для определения критических моментов в рамках судебных процессов или в случае предоставления социальных услуг, которые необходимы для реализации экономических, социальных и культурных прав. Исследователи уже разработали ряд подходов, которые способствуют достижению этой цели[104], и важно обеспечить увеличение инвестиций в эту область. Государства также должны предпринять шаги для обеспечения того, чтобы защита интеллектуальной собственности не препятствовала значимой проверке систем ИИ, оказывающих воздействие на права человека[105]. Правила закупок должны быть обновлены с учетом необходимости обеспечения прозрачности, включая возможность аудита систем ИИ[106]. В частности, государствам следует избегать использования тех систем ИИ, которые могут оказывать существенное негативное воздействие на права человека, но не могут быть подвергнуты значимому аудиту[107].

---

98 A/HRC/43/29, п. 52, и A/73/348, п. 49.

99 Совет Европы, «Руководящие принципы по решению проблемы воздействия алгоритмических систем на права человека», (приложение к Рекомендации CM/Rec(2020)1 Комитета министров государствам-членам, касающейся воздействия алгоритмических систем на права человека), разд. B, п. 4.2.

100 A/73/348, п. 49.

101 A/HRC/43/29, п. 52. Предложение Европейского союза в отношении закона об ИИ содержит положения о реестре систем ИИ с высоким риском.

102 См. URL: https://link.springer.com/article/10.1007/s12394-008-0003-1, с. 67.

103 Обзор элементов алгоритмической прозрачности см. URL: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6, сс. 320–323 оригинала.

104 См. URL: https://arxiv.org/abs/2001.00973 и https://arxiv.org/ftp/arxiv/papers/1711/1711.01134.pdf.

105 Совет Европы, «Руководящие принципы по решению проблемы воздействия алгоритмических систем на права человека» (приложение к Рекомендации CM/Rec(2020)1 Комитета министров государствам-членам, касающейся воздействия алгоритмических систем на права человека), разд. B, п. 4.1.

106 См. материалы, представленные Германией, «Деречос дихиталес», Коалицией за свободу Интернета и «Глоубл партнерс диджитл».

107 A/73/348, п. 55, и A/HRC/43/29, п. 54.

V. Выводы и рекомендации

A. Выводы

57. **В настоящем докладе подчеркивается неоспоримое и неуклонно растущее воздействие технологий ИИ на осуществление права на неприкосновенность частной жизни и других прав человека, как положительное, так и отрицательное. В нем говорится о тревожных изменениях, включая разросшуюся экосистему сбора персональных данных и обмена ими, в значительной степени отличающихся непрозрачностью, которая лежит в основе широко используемых систем ИИ. Такие системы влияют на подходы правительства в области охраны правопорядка и отправления правосудия, определяют доступность государственных услуг, решают, кто имеет шанс быть принятым на работу, и влияют на то, какую информацию люди видят и какой информацией они могут делиться в Интернете. Более того, риск дискриминации в случае решений, принимаемых на основе ИИ, слишком реален. В настоящем докладе описывается ряд путей преодоления фундаментальных проблем, связанных с ИИ, при этом подчеркивается, что только комплексный подход, основанный на правах человека, может обеспечить устойчивые решения на благо всех.**

58. **Вместе с тем с учетом разнообразия новых вопросов, возникающих в контексте ИИ, настоящий доклад представляет собой моментальное отображение постоянно развивающегося пространства ИИ. Области, заслуживающие дальнейшего анализа, включают здравоохранение, образование, жилье и финансовые услуги. Биометрические технологии, которые становятся все более популярным решением для государств, международных организаций и технологических компаний, являются той областью, в которой в срочном порядке необходимо вынести дополнительные рекомендации по правам человека. Кроме того, одним из направлений будущей работы с точки зрения прав человека должен стать поиск путей заполнения огромного пробела в подотчетности в глобальной среде данных. Наконец, необходимо срочно изыскать и внедрить решения для преодоления дискриминации, обусловленной использованием ИИ.**

B. Рекомендации

59. **Верховный комиссар рекомендует государствам:**

a) полностью признать необходимость защиты и укрепления всех прав человека при разработке, использовании и контроле ИИ в качестве основной цели и обеспечить равное уважение и соблюдение всех прав человека как в Интернете, так и за его пределами;

b) обеспечить, чтобы использование ИИ соответствовало всем правам человека и чтобы любое вмешательство в право на частную жизнь и другие права человека посредством использования ИИ было предусмотрено законом, преследовало законную цель, соответствовало принципам необходимости и пропорциональности и не нарушало сущности соответствующих прав;

c) прямо запретить те приложения ИИ, которые не могут работать в соответствии с международным правом прав человека, и наложить мораторий на продажу и использование тех систем ИИ, для которых характерен высокий риск в плане осуществления прав человека, до тех пор, пока не будут приняты адекватные гарантии защиты прав человека;

d) ввести мораторий на использование технологий дистанционного биометрического распознавания в общественных местах по крайней мере до тех пор, пока ответственные органы не смогут продемонстрировать соблюдение стандартов конфиденциальности и защиты данных и отсутствие серьезных проблем в плане точности и последствий дискриминационного характера, а также до тех пор, пока не будут выполнены все рекомендации, изложенные в пункте 53 j) (i)–v)) документа A/HRC/44/24;

e) принять и эффективно применять через независимые, беспристрастные органы законодательство о конфиденциальности данных в государственном и частном секторах в качестве важнейшей предпосылки для защиты права на неприкосновенность частной жизни в контексте ИИ;

f) принять законодательную и нормативную базу, которая адекватно предотвращает и смягчает многогранное негативное воздействие на права человека, связанное с использованием ИИ в государственном и частном секторах;

g) обеспечить, чтобы жертвы нарушений прав человека и злоупотреблений, связанных с использованием систем ИИ, имели доступ к эффективным средствам правовой защиты;

h) требовать адекватного объяснения всех поддерживаемых ИИ решений, которые могут существенно повлиять на права человека, особенно в государственном секторе;

i) активизировать усилия по борьбе с дискриминацией, связанной с использованием систем ИИ государствами и коммерческими предприятиями, в том числе путем проведения систематических оценок и мониторинга результатов использования систем ИИ и последствий их внедрения, введения соответствующих требований и оказания им поддержки;

j) обеспечить, чтобы деятельность государственно-частных партнерств в сфере предоставления и использования технологий ИИ была прозрачной и подлежала независимому надзору на предмет соблюдения прав человека, а также не приводила к отказу правительства от своей ответственности за соблюдение прав человека.

60. **Верховный комиссар рекомендует государствам и коммерческим предприятиям:**

a) систематически проводить комплексную проверку соблюдения прав человека на протяжении всего жизненного цикла систем ИИ, которые они проектируют, разрабатывают, внедряют, продают, получают или эксплуатируют. Необходимо, чтобы ключевым элементом их должной осмотрительности в отношении прав человека стали регулярные и всесторонние оценки воздействия на права человека;

b) значительно повысить прозрачность использования ИИ, в том числе путем адекватного информирования общественности и затронутых лиц и создания условий для независимого внешнего аудита автоматизированных систем. Чем вероятнее и серьезнее потенциальное или фактическое воздействие на права человека, связанное с использованием ИИ, тем в большей степени испытывается потребность в прозрачности;

c) обеспечить участие всех соответствующих заинтересованных сторон в принятии решений по разработке, внедрению и использованию ИИ, в частности, затронутых лиц и групп;

d) повышать объяснимость решений на основе ИИ, в том числе путем финансирования и проведения исследований для достижения этой цели.

61. **Верховный комиссар рекомендует коммерческим предприятиям:**

a) прилагать все усилия для выполнения своей обязанности уважать все права человека, в том числе путем всестороннего введения в действие Руководящих принципов предпринимательской деятельности в аспекте прав человека;

b) активизировать свои усилия по борьбе с дискриминацией, связанной с разработкой, продажей или эксплуатацией систем ИИ, в том числе путем проведения систематических оценок и мониторинга результатов работы систем ИИ и последствий их внедрения;

c) решительно действовать в интересах того, чтобы к созданию ИИ привлекались работники, представляющие различные группы людей;

d) в тех случаях, когда они оказали неблагоприятное воздействие на права человека или содействовали ему, обеспечивать предоставление или сотрудничать с целью предоставления возмещения в рамках законных процессов, в том числе посредством эффективных механизмов рассмотрения жалоб на оперативном уровне.