Генеральная Ассамблея

Distr.: General
4 August 2022
Russian
Original: English

Совет по правам человека
Пятьдесят первая сессия
12 сентября — 7 октября 2022 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 цифровую эпоху

Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека*

Резюме

В настоящем докладе, представленном в соответствии с резолюцией 48/4 Совета по правам человека, рассматриваются последние тенденции и проблемы, касающиеся права на неприкосновенность частной жизни. В частности, особое внимание в докладе уделяется: a) злоупотреблению хакерскими инструментами, использование которых предполагает вмешательство, b) ключевой роли шифрования в обеспечении осуществления права на неприкосновенность частной жизни и других прав и c) широкомасштабному мониторингу общественных мест. В нем подчеркивается опасность создания систем всепроникающего наблюдения и контроля, которые могут подорвать развитие динамично прогрессирующих обществ, где соблюдаются права человека.

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

I. Введение

1. Настоящий доклад представлен в соответствии с резолюцией 48/4 Совета по правам человека, в которой Совет просил Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) подготовить доклад, в котором были бы проанализированы последние тенденции и проблемы в отношении права человека на неприкосновенность частной жизни, а также выявить и разъяснить соответствующие правозащитные принципы, гарантии и передовой опыт и представить этот доклад Совету на его пятьдесят первой сессии. В докладе отражены ответы, полученные на призыв УВКПЧ о представлении материалов[1].

2. По всему миру люди являются свидетелями впечатляющих научно-технических достижений, а также инноваций, которые улучшают их жизнь и стимулируют экономику. Вместе с тем они также ощущают, как цифровые инструменты могут быть обращены против них, подвергая их новым формам мониторинга, профилирования и контроля. Обеспечение уважения и защиты права на неприкосновенность частной жизни, признанного в статье 12 Всеобщей декларации прав человека, статье 17 Международного пакта о гражданских и политических правах и во многих других международных и региональных договорах о правах человека[2], может играть первостепенную роль в борьбе с новыми цифровыми угрозами правам человека, которые неразрывно связаны с персональными данными, приводящими в действие двигатели цифровых обществ.

3. Основываясь на предыдущих докладах Совету по правам человека, посвященных проблемам права на неприкосновенность частной жизни[3], настоящий доклад посвящен трем ярко выраженным тенденциям, касающимся роли государств в обеспечении осуществления права на неприкосновенность частной жизни и содействии ему: a) повсеместному злоупотреблению связанными с вмешательством хакерскими инструментами, b) ведущей роли шифрования в обеспечении осуществления права на неприкосновенность частной жизни и других прав и c) широкомасштабному мониторингу общественных мест. В докладе подчеркивается весьма реальная и надвигающаяся опасность создания систем всепроникающего наблюдения и контроля, которые в конечном итоге могут подорвать развитие динамично прогрессирующих и процветающих обществ, где соблюдаются права человека, и в заключение приводится ряд рекомендаций, направленных на недопущение такого исхода.

II. Наблюдение за персональными устройствами и сообщениями

A. Взлом

4. В июле 2021 года организация «Запрещенные истории», которая является консорциумом, проводящим журналистские расследования при поддержке организации «Международная амнистия», опубликовала разоблачения, которые касались использования программного обеспечения «Пегасус» и привлекли внимание международного сообщества к кризису в области прав человека, нараставшему в течение многих лет, а именно к распространению во всем мире хакерских инструментов для целенаправленного и скрытого наблюдения за цифровыми устройствами. Несмотря на то, что такие шпионские инструменты, как утверждается,

[1] См. URL: https://www.ohchr.org/en/calls-for-input/2022/call-inputs-report-right-privacy-digital-age-2022.

[2] 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; статью 8 Конвенции о защите прав человека и основных свобод.

[3] См. A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 и A/HRC/48/31.

используются для борьбы с терроризмом и преступностью, они зачастую применяются по незаконным причинам, в том числе для подавления критических или несогласных взглядов и тех, кто их выражает, включая журналистов, оппозиционных политических деятелей и правозащитников.

5. Масштабы использования программы «Пегасус» для осуществления шпионских операций и число жертв ошеломляют. На основе анализа просочившегося списка, в который вошли более 50 000 номеров телефонов потенциальных и реальных объектов слежки, а также криминалистической экспертизы большого количества зараженных телефонов, в 2021 году была представлена информация, согласно которой объектами слежки стали по меньшей мере 189 журналистов, 85 правозащитников, более 600 политиков и государственных чиновников, включая членов кабинета министров, и дипломатов[4]. В ходе расследования были также выявлены факты шпионажа за судьями, адвокатами, врачами, профсоюзными лидерами и учеными[5]. Компания «Эн-эс-оу груп», которая производит и продает «Пегасус», призналась, что объектами ее клиентов ежегодно становятся 12 000–13 000 человек[6].

6. Шпионское программное обеспечение «Пегасус» является наиболее ярким примером в расширяющемся ландшафте шпионского программного обеспечения, продаваемого компаниями государствам по всему миру[7]. По данным исследователей, по меньшей мере 65 государств приобрели коммерческое шпионское программное обеспечение для осуществления слежения[8]. По данным «Эн-эс-оу», в число ее клиентов входят 60 государственных учреждений 45 стран. Всего за несколько дней до разоблачений «Пегасус», «Ситизен лэб» и «Майкрософт» опубликовали доклад, в котором подробно описали, как другое программное обеспечение, «Кандиру», использовалось государствами для преследования правозащитников, диссидентов, журналистов, активистов и политиков[9]. В ноябре 2021 года компания «Мета», специализирующаяся на социальных сетях, объявила о том, что она отключила семь организаций, которые через Интернет преследовали людей в более чем 100 странах. Компания также предупредила около 50 000 человек, которые, по ее мнению, стали объектом такой деятельности[10]. По имеющимся данным, более 500 компаний разрабатывают, продвигают и продают государствам такие средства слежения[11].

7. Возможности инструментов и услуг шпионского программного обеспечения, предлагаемых на мировом рынке, огромны. Например, «Пегасус» после установки предоставляет полный и неограниченный доступ ко всем датчикам и информации на зараженных устройствах, фактически превращая большинство смартфонов в устройства круглосуточного слежения, предоставляя доступ к камере и микрофону, геолокационным данным, электронной почте, сообщениям, фотографиям и

[4] См. URL: https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.

[5] См. URL: https://forbiddenstories.org/about-the-pegasus-project/; URL: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; URL: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[6] В ходе слушаний в Европейском парламенте, комиссия по расследованию использования «Пегасус» и аналогичных шпионских программ для слежения, 21 июня 2022 года, URL: https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

[7] См. URL: https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf, с. 29.

[8] См. URL: https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019.

[9] См. URL: https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[10] См. URL: https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. Другие примеры, см. URL: https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/; URL: https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating; и URL: https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] A/HRC/41/35, п. 6; см. также URL: https://data.mendeley.com/datasets/csvhpkt8tm/2, где представлен международный реестр коммерческого шпионского программного обеспечения.

видеозаписям, а также ко всем приложениям. Это позволяет злоумышленнику увидеть подробную картину жизни своих жертв: их мысли, склонности, профессиональную деятельность, политические взгляды, состояние здоровья, финансовое положение, общественную и личную жизнь. В то время как многие хакерские инструменты требуют определенных действий со стороны жертвы, например нажатия на ссылку или открытия приложения к сообщению, «Пегасус» устанавливается незаметно, с помощью так называемой «атаки с нулевым щелчком»[12]. Это программное обеспечение делает практически невозможным для жертв избежать заражения, если они подверглись взлому.

8. Хакерские операции могут принимать различные формы с разной степенью вмешательства. В то время как получение полного контроля над мобильным телефоном или компьютером позволяет составить подробную картину жизни тех, кто подвергся взлому, множество других хакерских методов могут иметь меньшую степень вмешательства, которое все же является очень серьезным, включая получение доступа к учетным записям электронной почты. Взлом может также позволить получить доступ к другим подключенным устройствам, таким как носимые технологические устройства или транспортные средства, которые могут предоставить дополнительную информацию, в том числе о состоянии здоровья и данных, касающихся местонахождения. Устройства, оснащенные камерами или микрофонами, такие как «умные» динамики или телевизоры, также могут быть превращены в инструменты аудиовизуального слежения. Атака на инфраструктуру поставщиков услуг может открыть доступ к огромному объему информации о тысячах клиентов, включая их сообщения, данные о просмотре сайтов и информацию об их местонахождении[13]. Дальнейшее обсуждение посвящено в первую очередь взлому личных устройств связи.

9. Взлом личных устройств связи представляет собой серьезное посягательство на право на неприкосновенность частной жизни и может быть связан с нарушениями целого ряда других прав. Поскольку проникновение в цифровые устройства связи предоставляет доступ к черновикам, историям поиска и просмотра, оно может также позволить глубоко изучить мыслительные процессы лиц, подвергшихся взлому, а также их политические и религиозные взгляды и убеждения, тем самым нарушая свободу мнений и мысли[14]. Хакерские действия могут оставлять глубокие травмы, влияющие на психическое здоровье жертв и их семей. Взломы, как сообщается, привели к арестам и задержаниям правозащитников и политиков, некоторые из которых, как сообщается, подвергались пыткам[15]. Целенаправленные взломы также связаны с внесудебными казнями[16].

10. Более того, нападение на журналистов и СМИ с помощью хакерских инструментов существенным образом подрывает свободу СМИ, в том числе потому что источники информации могут опасаться обнаружения и последствий. Само существование хакерских программ может оказать сдерживающее воздействие на свободу слова, работу СМИ, общественные дискуссии и участие, что может подорвать демократическое управление. Согласно заключению Верховного суда Индии в его

[12] Следует отметить, что программное обеспечение «Пегасус» является не единственным инструментом с такими возможностями и что количество таких инструментов постоянно растет.

[13] Проведенное полицией Нидерландов и Франции расследование провайдера «ЭнкроЧат», которому удалось проникнуть в серверную инфраструктуру сети зашифрованной связи и собрать информацию о более чем 32 000 телефонов в 121 стране; см. German Federal Court of Justice, decision of 2 March 2022, 5 StR 457/21, para. 18

[14] A/HRC/29/32, п. 20. Всесторонний анализ свободы мысли см. в документе A/76/380.

[15] См. URL: https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/.

[16] A/HRC/41/35, п. 1; см. также документ зала заседаний Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях, озаглавленный «Приложение к докладу Специального докладчика: расследование незаконной смерти г-на Джамаля Хашогги». URL: https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

недавнем постановлении об использовании программного обеспечения «Пегасус», сдерживающее воздействие слежения будет являться «посягательством на жизненно важную роль прессы как общественного наблюдателя»[17].

11. Взлом также может оказать негативное влияние на права на надлежащую правовую процедуру и справедливое судебное разбирательство[18]. Получение доступа к устройству может позволить злоумышленнику не только наблюдать за содержимым этого устройства и его взаимодействием с другими устройствами, но и управлять устройством, в том числе изменять, удалять или добавлять файлы[19]. Таким образом, можно подделать доказательства, чтобы уличить или шантажировать лиц, подвергшихся взлому [20].

12. Более того, шпионское программное обеспечение может воздействовать не только на объекты хакерских операций, но и на всех, кто общается с этими лицами, или, если активирована камера, микрофон или геолокация устройства, на любого человека, имеющего то же физическое местонахождение[21].

13. Наконец, в основе взлома лежат существующие недостатки в безопасности компьютерных систем, которые используются для его осуществления. Сохраняя такие уязвимые места открытыми или даже создавая их, те, кто прибегает к взлому, могут способствовать возникновению угроз безопасности и конфиденциальности для миллионов пользователей и более широкой экосистемы цифровой информации[22].

14. Правозащитные органы и эксперты уже много лет бьют тревогу по поводу шпионского программного обеспечения. Генеральная Ассамблея и Совет по правам человека неоднократно заявляли о том, что государства-члены должны воздерживаться от незаконного или произвольного слежения, в том числе с помощью взлома[23]. Несколько специальных докладчиков выразили резкую критику хакерской практики, которая выходит далеко за рамки того, что необходимо для достижения законных целей, таких как борьба с терроризмом и преступностью[24]. Комитет по правам человека также выразил свою обеспокоенность по поводу финансируемого государством взлома, особенно когда он используется без надлежащего надзора или гарантий[25]. На региональном уровне бывший Специальный докладчик по вопросу о свободе выражения мнений Межамериканской комиссии по правам человека осудил хакерские операции в недопустимых целях и призвал сурово наказывать нарушителей, в том числе за действия, предпринятые по политическим мотивам против журналистов и независимых СМИ[26].

15. В ответ на разоблачения, связанные с использованием программного обеспечения «Пегасус», различные региональные и национальные учреждения, включая Совет Европы, Межамериканскую комиссию по правам человека, Европейский парламент и Верховный суд Индии, выразили обеспокоенность по поводу распространения шпионского программного обеспечения и начали проводить

[17] Supreme Court of India, *Manohar Lal Sharma v. Union of India*, order of 27 October 2021, para. 39.
[18] A/HRC/23/40, п. 62.
[19] A/HRC/39/29, п. 19.
[20] См. URL: https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/, где представлены примеры таких утверждений.
[21] См. URL: https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, с. 8.
[22] A/HRC/39/29, п. 19.
[23] Резолюция Генеральной Ассамблеи 75/176 и резолюции Совета по правам человека 48/4 и 45/18.
[24] A/HRC/17/27; A/HRC/20/17; A/HRC/23/40, п. 62; A/HRC/41/35; A/HRC/41/41; A/73/438; см. также URL: https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.
[25] См. CCPR/C/DEU/CO/7; CCPR/C/NLD/CO/5; CCPR/C/ITA/CO/6.
[26] См. URL: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=87&lID=1.

разбирательства и расследования[27]. Также ведутся уголовные расследования[28] и рассматриваются гражданские иски[29].

16. Руководство по минимальным требованиям и гарантиям, необходимым для любого использования шпионского программного обеспечения на уровне государства, может опираться на имеющийся обширный анализ прав человека с точки зрения слежения[30]. Далеко идущие негативные последствия взлома требуют особенно осторожного подхода к его использованию, ограничивая его самыми исключительными обстоятельствами, в строгом соответствии с требованиями международного права в области прав человека.

17. Однако многие юрисдикции не установили такие важные правовые ограничения и не имеют четких, точных, общедоступных законов, регулирующих хакерские операции. В то время как некоторые государства приняли нормативно-правовую базу, которая соответствует международному праву в области прав человека, другие опираются на слишком широкие или устаревшие законы, принятые до появления современных технологий.

18. Как показали разоблачения программного обеспечения «Пегасус» и соответствующие доклады, взлом данных со стороны различных государственных субъектов часто преследует цели, которые не являются законными с точки зрения международного права в области прав человека. Хотя в определенных обстоятельствах связанные с вмешательством меры слежения могут быть допустимы согласно статьям 17 и 19 Международного пакта о гражданских и политических правах по соображениям защиты государственной безопасности или общественного порядка, взлом никогда не может быть оправдан политическими или коммерческими соображениями, что зачастую происходит, когда объектами взлома становятся правозащитники или журналисты.

19. Даже если преследуются законные цели, такие как цели национальной безопасности или защита прав других лиц, оценка необходимости и соразмерности использования шпионского программного обеспечения существенно ограничивает сценарии, в которых использование шпионского программного обеспечения будет допустимым[31]. Существуют веские аргументы в пользу того, что такие инструменты, как «Пегасус», которые позволяют беспрепятственно вторгаться в жизнь людей и даже, воможно, проникнуть в их мысли, способны извратить суть права на неприкосновенность частной жизни[32] и подорвать абсолютные права на свободу

[27] См. URL: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=87&lID=1; URL: https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/media_center/PReleases/2022/022.asp; URL: https://www.theguardian.com/world/2022/mar/17/pegasus-spyware-ban-el-salvador-iachr-hearing; URL: https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; URL: https://tvn24.pl/tvn24-news-in-english/polands-senate-lunches-special-committee-to-examine-use-of-pegasus-software-5557023; Supreme Court of India, *Manohar Lal Sharma v. Union of India*, order of 27 October 2021.

[28] См. URL: https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali; и URL: https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.

[29] URL: https://www.glanlaw.org/nso-spyware-hacking; URL: https://privacyinternational.org/examples/2605/lawsuits-target-nso-group-selling-spyware-governments-targeting-activists-and; URL: https://www.washingtonpost.com/technology/2021/11/23/apple-pegasus-lawsuit-spyware-nso/; и URL: https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf. Обширный обзор предпринятых юридических действий представлен URL: https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

[30] См. A/HRC/27/37; A/HRC/39/29; A/HRC/23/40 и A/HRC/23/40/Corr. 1; CCPR/C/UKR/CO/8; CCPR/C/DEU/CO/7; CCPR/C/ARM/CO/3; CCPR/C/BWA/CO/2; и CCPR/C/FIN/CO/7.

[31] См. Federal Constitutional Court of Germany, judgment of 27 February 2008 (1 BvR 370, 595/07), at 247 (aa).

[32] European Data Protection Supervisor, см. URL: https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, с. 8.

мысли и мнения. Ввиду существенных негативных последствий использования шпионского программного обеспечения и их распространения далеко за пределы любого предполагаемого объекта, его использование должно быть ограничено случаями, когда оно служит для предотвращения или расследования определенного серьезного преступления или деяния, представляющего серьезную угрозу национальной безопасности. Его использование должно быть узконаправленным для проведения расследования в отношении лица или лиц, подозреваемых в совершении таких деяний или совершивших их. К этому можно прибегать лишь в крайнем случае, иными словами, все меры, связанные с меньшей степенью вмешательства, должны быть исчерпаны или показана их бесперспективность, и должны быть установлены жесткие ограничения по объему и продолжительности. Следует получать доступ только к относящимся к делу данным и собирать только их[33]. Эти меры также должны подлежать строгому независимому надзору; необходимо предварительное одобрение судебного органа[34]. Кроме того, надежный и прозрачный экспортный контроль, прямо учитывающий риски, связанные с правами человека, может стать мощным инструментом предотвращения нарушений прав и злоупотреблений[35]. УВКПЧ повторяет свой недавний призыв, а также призыв экспертов и групп по правам человека ввести мораторий на продажу, передачу и использование инструментов взлома до тех пор, пока не будет создан режим гарантий, основанный на правах человека[36].

B. Ограничения на шифрование

20. В последние годы правительства разных стран предприняли действия, которые, преднамеренно или нет, могут подорвать безопасность и конфиденциальность зашифрованных сообщений. Это имеет серьезные последствия для осуществления права на неприкосновенность частной жизни и других прав человека.

21. Шифрование является одним из основных факторов обеспечения конфиденциальности и безопасности в Интернете и необходимо для защиты прав, включая права на свободу мнений и их свободное выражение, свободу ассоциации и мирных собраний, безопасность, здоровье и недискриминацию. Шифрование гарантирует, что люди могут свободно обмениваться информацией, не опасаясь, что их данные могут стать известны другим, будь то государственные органы или киберпреступники. Шифрование необходимо для того, чтобы люди чувствовали себя в безопасности, свободно обмениваясь с другими людьми информацией о различных переживаниях, мыслях и самоопределении, включая конфиденциальную медицинскую или финансовую информацию, сведения о гендерной идентичности и сексуальной ориентации, художественное самовыражение и информацию, связанную с принадлежностью к меньшинствам. В условиях преобладания цензуры шифрование позволяет людям сохранять пространство, чтобы придерживаться мнений, выражать их и обмениваться мнениями с другими людьми. В определенных случаях журналисты и правозащитники не могут выполнять свою работу без защиты надежного шифрования, укрывающего их источники и ограждающего их от влиятельных лиц, в отношении которых ведется расследование. Шифрование предоставляет женщинам, которые сталкиваются с особыми угрозами слежения, преследования и насилия в Интернете, высокий уровень защиты от недобровольного раскрытия информации[37].

[33] См. URL: https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf.

[34] См. A/HRC/39/29 о минимальных гарантиях в отношении мер скрытого слежения.

[35] A/HRC/39/29, п. 25; См. A/HRC/20/24, п. 40; A/HRC/48/31, п. 46; и A/HRC/41/35, пп. 34 и 66. Европейский союз недавно принял меры, направленные на более строгий учет прав человека, приняв новый регламент об экспортном контроле.

[36] См. URL: https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; URL: https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; URL: https://www.amnesty.org/en/documents/doc10/4516/2021/en/; и URL: https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/.

[37] A/HRC/35/9, п. 18.

В вооруженных конфликтах обмен зашифрованными сообщениями незаменим для обеспечения безопасной связи между гражданскими лицами. Примечательно, что за два месяца после начала вооруженного конфликта на Украине 24 февраля 2022 года количество скачиваний приложения для обмена зашифрованными сообщениями «Сигнал» на Украине выросло более чем на 1000 % по сравнению с предыдущими месяцами[38].

22. Жизненно важная роль шифрования как инструмента обеспечения неприкосновенности частной жизни и прав человека широко признана, в том числе государствами, органами Организации Объединенных Наций, Верховным комиссаром Организации Объединенных Наций по правам человека и экспертами по правам человека[39]. Генеральная Ассамблея и Совет по правам человека также подчеркнули важность шифрования для защиты прав человека в нескольких резолюциях, призывая государства воздерживаться от вмешательства в технологии шифрования[40] и поощряя компании работать над созданием решений, обеспечивающих и защищающих конфиденциальность цифровых сообщений и операций, включая меры по шифрованию, использованию псевдонимов и обеспечению анонимности[41]. Специальные докладчики и региональные эксперты выразили поддержку надежному шифрованию как средству обеспечения прав, рекомендовав поощрять и защищать надежное шифрование и предостерегая от мер, которые произвольно или незаконно ограничивают использование этой основополагающей технологии[42]. Комитет по правам ребенка подчеркнул, что любые меры по обнаружению материалов о сексуальной эксплуатации детей и надругательстве над ними в зашифрованных сообщениях должны быть строго ограничены в соответствии с принципами законности, необходимости и соразмерности[43]. Совет по правам человека, Организация Объединенных Наций и региональные эксперты по правам человека подчеркивают, что шифрование является жизненно важным для журналистской работы и защиты источников[44]. В системе показателей универсальности Интернета, опубликованных Организацией Объединенных Наций по вопросам образования, науки и культуры, подчеркивается важность шифрования для обеспечения доверия и безопасности в Интернете[45].

23. Несмотря на преимущества шифрования, государства иногда ограничивают его использование, например, для защиты национальной безопасности и борьбы с преступностью, в частности для обнаружения материалов о сексуальном насилии над детьми. Ограничения включают запрет на зашифрованные сообщения и уголовную ответственность за предложение или использование средств шифрования[46] или обязательную регистрацию и лицензирование средств шифрования[47]. Аналогичным образом, в некоторых случаях были выдвинуты требования к разработчикам систем

[38] См. https://sensortower.com/blog/signal-telegram-ukraine-russia-2022.

[39] См. URL: https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid.

[40] Резолюция Генеральной Ассамблеи 75/176 и резолюции Совета по правам человека 39/6, 44/12, 45/18 и 48/4.

[41] Резолюция Генеральной Ассамблеи 75/176 и резолюция Совета по правам человека 48/4.

[42] См. A/HRC/29/32;
URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf; A/HRC/41/41;
URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf; URL: https://www.osce.org/representative-on-freedom-of-media/379351; и
URL: https://www.oas.org/en/iachr/expression/reports/ENGIA2020.pdf.

[43] Комитет по правам ребенка, замечание общего порядка № 25 (2021) о правах детей в связи с цифровой средой, п. 70.

[44] Резолюция 45/18 Совета по правам человека; A/HRC/29/32; и
URL: https://www.osce.org/representative-on-freedom-of-media/379351.

[45] См. URL: https://en.unesco.org/internet-universality-indicators, индикатор D.5.

[46] См. PSE 2/2017 и LBY 3/2022. Все сообщения, упомянутые в настоящем докладе, см. URL: https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[47] См. URL: https://hrsly.com/wp-content/uploads/2022/06/OL-LBY-3.2022-DownLoadPublicCommunicationFile.pdf (LBY 3/2022).

шифрования предоставить правоохранительным или другим государственным органам доступ ко всем сообщениям по запросу, что фактически может быть равносильно полному ограничению шифрования, которое может привести к созданию своего рода «лазеек» (встроенного пути обхода шифрования, позволяющего получить скрытый доступ к данным в текстовой форме) или, по крайней мере, содействовать ему[48]. Еще одной формой вмешательства в шифрование является требование о создании и поддержании систем депонирования ключей, при этом все закрытые ключи, необходимые для расшифровки данных, должны быть переданы государству или назначенной третьей стороне[49]. Введение требований прослеживаемости, согласно которым поставщики должны иметь возможность отследить любое сообщение в обратном направлении до его предполагаемого отправителя, также может потребовать ослабления стандартов шифрования[50]. В последнее время различные государства начали вводить общие обязательства по мониторингу для поставщиков услуг в области цифровой связи, в том числе предлагающих услуги зашифрованной связи, или рассматривать возможность их введения[51]. Такие обязанности могут фактически заставить этих поставщиков отказаться от надежного сквозного шифрования или найти весьма проблематичные обходные пути (см. пункты 27–28 ниже).

24. Несомненно, широко используемые возможности шифрования, возможности, которые общественность потребовала в качестве ответа на массовое слежение и киберпреступность, создают дилемму для государств, стремящихся защитить население, в особенности его наиболее уязвимые группы, от серьезных преступлений и угроз безопасности. Однако, как отметил Специальный докладчик по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, существует опасность того, что регулирование шифрования может подорвать права человека[52]. Государства, стремящиеся ограничить шифрование, зачастую не могли доказать, что вводимые ограничения необходимы для достижения определенной законной цели, учитывая наличие различных других инструментов и способов, которые позволяют получить информацию, необходимую для конкретных правоохранительных или других законных целей[53]. Такие альтернативные меры включают совершенствование обычной деятельности полиции и повышение уровня ее обеспеченности ресурсами, проведение секретных операций, анализ метаданных и укрепление международного сотрудничества полиции.

25. Более того, воздействие большинства ограничений шифрования на право на неприкосновенность частной жизни и связанные с ним права чрезвычайно велико и зачастую затрагивает не только лиц, на которых направлены данные ограничения, но и все население в целом. Прямые запреты со стороны государства или, в частности, установление уголовной ответственности за шифрование не могут быть оправданы, поскольку они не позволят всем пользователям в пределах их юрисдикции иметь безопасный способ общения. Системы депонирования ключей имеют серьезные уязвимые стороны, поскольку они зависят от защищенности хранилища, а хранящиеся ключи могут подвергаться кибератакам. Более того, обязательные «лазейки» в средствах шифрования создают обязательства, которые выходят далеко за рамки их необходимости в отношении конкретных пользователей, идентифицированных как подозреваемые в совершении преступлений или создании угрозы безопасности. Они ставят под угрозу конфиденциальность и безопасность всех пользователей и подвергают их незаконному вмешательству не только со стороны государств, но и негосударственных субъектов, включая преступные сети[54]. Требования

[48] См. GBR 4/2015, MYS 2/2018, AUS 5/2018 и AUS 6/2018.

[49] См. RUS 7/2016 и RUS 7/2018.

[50] См. IND 31/2018, IND 3/2019, BRA 6/2020 и BRA 7/2020.

[51] Например, the “EARN IT” Act adopted in the United States of America in 2020 (см. USA 4/2020); the draft Online Safety Bill in the United Kingdom (см. GBR 5/2022); the European Commission proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 11 May 2022 (COM(2022) 209); и Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (см. IND 8/2021).

[52] См. A/HRC/29/32.

[53] Там же, п. 39.

[54] A/HRC/39/29, п. 20.

лицензирования и регистрации оказывают аналогичное несоразмерное воздействие, поскольку в них устанавливается, что программное обеспечение для шифрования должно иметь уязвимые стороны, которые можно использовать[55]. Такие негативные последствия не обязательно сводятся к пределам юрисдикции, вводящей ограничение; скорее всего, «лазейки», установленные в юрисдикции одного государства, станут частью программного обеспечения, используемого в других регионах мира.

26. Недавно была предложена концепция так называемого сканирования на устройстве пользователя для обнаружения определенных форм нежелательного содержания, чтобы избежать многих проблем, описанных выше. Сканирование на устройстве пользователя переносит этап обнаружения содержимого с серверов, через которые передаются сообщения, на сами персональные устройства. Таким образом, содержание, которое подлежит проверке, проверяется перед шифрованием, используемым для передачи. В августе 2021 года компания «Эпл» объявила о планах, касающихся введения такой системы для своих сервисов «айМеседж» и «айКлауд», но приостановила реализацию предложенного изменения после резкой критики со стороны широкого круга экспертов по безопасности информационных технологий, криптографов и правозащитных групп[56]. Однако различные законодательные инициативы[57] могут хотя бы косвенно способствовать тому, чтобы службы интернет-связи внедряли такие системы, налагая широкие обязательства по мониторингу всех сообщений, включая зашифрованные. Поскольку содержание сообщений после их шифрования не может быть доступно никому, кроме отправителя и получателя, любое общее обязательство по мониторингу заставит поставщиков услуг либо отказаться от шифрования во время передачи, либо искать доступ к сообщениям до их шифрования.

27. Введение общего сканирования на устройстве пользователя будет представлять собой смену парадигмы, которая вызовет множество серьезных проблем с возможными тяжелыми последствиями для осуществления права на неприкосновенность частной жизни и других прав. В отличие от других мер вмешательства, введение обязательного общего сканирования на устройстве пользователя неизбежно затронет всех, кто пользуется современными средствами связи, а не только людей, причастных к преступлениям и серьезным угрозам безопасности. Обязательное сканирование на устройстве пользователя изменяет способность людей полностью контролировать устройства связи, которые неразрывно сопряжены со всеми аспектами их жизни, и ограничивать информацию, которой эти устройства обмениваются[58]. Более того, при общем сканировании сообщений невозможно избежать частых ложноположительных срабатываний, даже при высокой точности, что может привести к привлечению к ответственности большого числа невиновных лиц[59]. Учитывая возможность такого воздействия, неизбирательное слежение, скорее всего, окажет сдерживающее воздействие на свободу выражения мнений и ассоциации, при этом люди ограничат способы общения и взаимодействия с другими людьми и будут заниматься самоцензурой[60].

28. Сканирование на устройстве пользователя также создает новые проблемы в сфере безопасности, повышая вероятность нарушения безопасности[61]. Процессом

[55] A/HRC/29/32, п. 41.

[56] См. URL: https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf.

[57] European Commission, proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 11 May 2022 (COM (2022) 209); см. также draft Online Safety Bill in the United Kingdom of Great Britain and Northern Ireland, URL: https://www.gov.uk/government/publications/draft-online-safety-bill.

[58] Материалы, представленные Руководящим комитетом Глобальной коалиции по шифрованию и организацией «Прайвеси интернэшнл».

[59] См. URL: https://doi.org/10.48550/arXiv.2110.07450.

[60] Более подробную информацию о сдерживающем воздействии наблюдения см. п. 47 ниже.

[61] По сравнению с атаками на корпоративные серверы атаки на персональные устройства могут осуществляться большим количеством участников и на менее защищенной инфраструктуре. Недоброжелатели могут использовать свой доступ к устройству для перепроектирования механизма сканирования, см. URL: https://doi.org/10.48550/arXiv.2110.07450.

проверки также можно управлять, что позволяет искусственно создавать ложноположительные или ложноотрицательные профили[62]. Даже если для нынешних целей проверка на устройстве пользователя является узкоспециальной, открытие устройств для проверки по требованию государства, скорее всего, в будущем приведет к попыткам расширить объем содержания, которое является объектом таких мер[63]. В частности, там, где верховенство права является ослабленным, а права человека находятся под угрозой, последствия проверки на устройстве пользователя могут быть гораздо шире, например она может быть использована для подавления политических дискуссий или для преследования оппозиционных деятелей, журналистов и правозащитников[64]. В свете широкого спектра значительных рисков для защиты прав человека в результате введения обязательной общей проверки на устройстве пользователя, такие требования не должны вводиться без дальнейшего существенного рассмотрения их потенциального воздействия на права человека и мер, смягчающих последствия данного вреда. Без глубокого исследования и анализа представляется маловероятным, что такие ограничения можно считать соразмерными в соответствии с международным правом в области прав человека, даже если они введены для достижения законных целей, учитывая серьезность их возможных последствий[65].

III. Слежение за населением

29. Верховным комиссаром неоднократно выражалась обеспокоенность по поводу массового слежения, в частности в отношении массового перехвата сообщений[66]. Несмотря на то что некоторые государства усовершенствовали меры защиты от слежения, вызывающая серьезную обеспокоенность практика наблюдения за деятельностью в Интернете значительной части населения или даже целых групп населения не прекратилась. В то время как предыдущие доклады были посвящены в основном слежению за личными сообщениями, они в меньшей степени касались последствий для неприкосновенности частной жизни, связанных со слежением за общественными местами, что обсуждается ниже.

A. Наблюдение за общественными местами

30. Камеры наблюдения, установленные для слежения за улицами, парковками, транспортными узлами общественного пользования и другими общественными местами, стали обычным явлением во многих странах. Ожидается, что в 2021 году количество используемых в мире камер наблюдения превысит один миллиард[67].

[62] URL: https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; и URL: https://openreview.net/forum?id=CQbqeGAM_Ki.

[63] URL: https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/; URL: https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; и URL: https://doi.org/10.48550/arXiv.2110.07450.

[64] Там же.

[65] A/HRC/39/29, п. 20, и A/HRC/29/32, п. 43. Мнение Суда Европейского союза подтверждает этот вывод. Недавно суд постановил, что автоматизированный анализ данных о трафике и местоположении в общем и неизбирательном порядке должен применяться только в случае крайней необходимости в ответ на серьезную, подлинную, настоящую или прогнозируемую угрозу национальной безопасности. Суд отклонил любые другие обоснования. См. *La Quadrature du Net and Others v. Premier ministre and Others*, judgment of 6 October 2020 (joined cases C-511/18, C-512/18 and C-520/18), para. 177. Более того, его прецедентное право указывает на еще более сильное скептическое отношение к проверке данных о содержании, Court of Justice of the European Union, *Maximillan Schrems v. Data Protection Commissioner*, judgment of 6 October 2015 (C-362/14), para. 94.

[66] См. A/HRC/27/37; A/HRC/39/29; и URL: https://www.ohchr.org/en/press-releases/2013/07/mass-surveillance-pillay-urges-respect-right-privacy-and-protection.

[67] См. URL: https://venturebeat.com/2022/06/18/how-ml-powered-video-surveillance-could-improve-security/.

В 10 городах мира с самой высокой плотностью видеонаблюдения на 1000 жителей приходится от 39 до 115 камер видеонаблюдения[68].

31. В дополнение к государственным системам слежения некоторые компании интегрировали средства наблюдения для частного использования, со специальными функциями для сообщения органам власти о происшествиях или даже предоставления им прямого доступа к потокам данных[69]. Это значительно расширяет общественное пространство под наблюдением, одновременно подрывая прозрачность, надзор и подотчетность.

32. В последние годы возможности камер наблюдения резко возросли благодаря добавлению сложных средств видеоанализа. По оценкам, в 2010 году менее 2 % продаваемых сетевых камер были оснащены встроенной системой видеоанализа, но к 2016 году эта доля выросла до более чем 40 % и, скорее всего, продолжит расти[70]. Аналитические функции все больше опираются на искусственный интеллект. Дополнительные возможности распознавания лиц и выявления подозрительного поведения являются одними из наиболее проблемных функций сложных систем видеонаблюдения[71]. Кроме того, использование беспилотных летательных аппаратов в целях слежения стало нормой во многих странах, где они используются для наблюдения за протестами и другими собраниями[72].

33. Под общим термином «умные города» осуществляется все большее количество инициатив, основанных на данных и направленных на изменение городских районов. Проекты «умных городов» направлены на сбор и обработку данных для информационного обеспечения управления городскими объектами с помощью все более совершенных сенсорных технологий. Хотя большая часть данных, собранных и обработанных в этих условиях, относится к таким вопросам, как данные о транспортных потоках, загрязнении или шуме, не относящимся к сфере персональных данных, другие собранные данные могут быть легко связаны с отдельными лицами, например номерные знаки автомобилей и данные «умных» счетчиков. Более того, якобы анонимные данные зачастую могут быть лишены анонимности[73], а инфраструктура, например камеры, установленные для мониторинга транспортных потоков, могут быть использованы для отслеживания отдельных лиц[74].

34. Эти изменения зачастую происходят на фоне новых систем установления личности и расширения баз биометрических данных. В целом ряде стран системы установления личности связаны с обширным централизованным хранением персональных данных, включая биометрическую информацию, такую как отпечатки пальцев, геометрия лица, сканирование радужной оболочки глаза и ДНК. Более того, базы данных часто взаимосвязаны и доступны для поиска другим службам. Вследствие этого устанавливать личности людей, где бы они ни находились, становится все проще и проще.

B. Мониторинг в режиме онлайн

35. Наряду с этим широкое распространение получил мониторинг общественного интернет-дискурса. Во всем мире многие органы власти собирают и анализируют сообщения в социальных сетях, а также частные и профессиональные сети, созданные на общедоступных коммуникационных платформах. Такое наблюдение за

[68] См. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; и URL: https://surfshark.com/surveillance-cities.

[69] См. URL: https://www.accessnow.org/amazon-ring-privacy-review/.

[70] См. URL: https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf.

[71] См. материалы, представленные «Деречос Дихиталес» и Международной сетью организаций за гражданские свободы.

[72] См. материалы, представленные организацией «Международная амнистия» и «СИВИКУС».

[73] См. URL: https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

[74] Подробнее о влиянии «умных городов» на права человека см. URL: https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/; и URL: https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

социальными сетями варьируется от изучения конкретных пользователей до сбора, хранения и анализа огромных объемов данных. Полученные данные могут включать: имена; возраст; фотографии и соответствующие цифровые шаблоны; адреса; сообщения и реакции на сообщения других людей; социальные и профессиональные контакты и связанные сети; данные о местонахождении; интересы; сексуальную ориентацию; гендерную идентификацию; политическую принадлежность и деятельность; религиозные убеждения; и информацию о состоянии здоровья.

36. Зачастую различные виды прогнозного анализа являются частью наблюдения за социальными сетями, включая попытки выявить возможные очаги преступности. Однако такой анализ также может быть использован для оценки поведения людей в прошлом, настоящем и будущем и присвоения баллов риска, связанных с вероятностью того, что они могут стать правонарушителями или угрозой безопасности[75]. Наблюдение за социальными сетями также используется для прогнозирования возможности массовых беспорядков[76].

37. Подобная деятельность может служить различным законным и незаконным целям, от расследования и предотвращения преступлений до проверки лиц, претендующих на получение социальных льгот, мониторинга протестов, измерения общественных настроений и составления моделей поведения людей в обществе[77].

C. Воздействие на права человека

38. Современные технологии, основанные на данных, резко меняют расстановку сил между организацией, осуществляющей слежение, и теми, за кем ведется наблюдение. До появления крупномасштабного автоматизированного слежения и средств анализа данных существовали практические ограничения наблюдения, которые обеспечивали определенный уровень защиты людей даже в общественных местах[78]. Сложные цифровые инструменты ставят под сомнение эти «естественные» меры защиты, которые существовали в прошлом. Сегодня один сотрудник может следить за аккаунтами десятков людей в социальных сетях, а с помощью современного программного обеспечения и анализа больших объемов данных небольшие команды могут наблюдать и составлять профили тысяч аккаунтов[79].

39. Подобные разработки повышают результативность и расширяют сферу применения других мер слежения за общественными местами. Например, развитие технологии распознавания лиц наряду с другими технологиями биометрического распознавания коренным образом изменило традиционную практику аудиовизуального мониторинга, поскольку данная технология существенным образом расширила возможности установления личности людей в общественных местах, включая участников собраний. Технология распознавания лиц в режиме реального времени позволяет устанавливать личности людей в режиме реального времени, а также осуществлять за ними целенаправленное наблюдение и слежение. Ретроспективное установление личности людей может, по-видимому, расширить круг источников данных, что приведет к воздействию, которое может быть сопряжено с такой же степенью вмешательства[80], если его не применять крайне осторожно.

40. Влияние наблюдения в общественных местах на права человека еще больше усугубляется тем, что источники данных все чаще объединяются, например путем объединения записей видеонаблюдения, оснащенного системой распознавания лиц, с данными социальных сетей и государственных баз данных[81], включая информацию о

[75] См. URL: https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, с. 152.
[76] См. URL: https://dx.doi.org/10.2139/ssrn.2702426, с. 1.
[77] См. URL: https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[78] A/HRC/44/24, п. 34.
[79] См. URL: https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[80] См. материалы организации «Международная амнистия».
[81] См. материалы, представленные Международной сетью организаций за гражданские свободы.

социальном обеспечении, миграции, подозреваемых в терроризме, арестах или даже списки лиц, отмеченных по политическим причинам.

41. Кроме того, государства используют обширные подборки данных, собранные различными частными компаниями. В предыдущих докладах Верховный комиссар и специальные докладчики обращали особое внимание на проблему, связанную с обращением государств с требованием о предоставлении доступа к данным, собираемым поставщиками телекоммуникационных и интернет-услуг, зачастую на фоне принятия законов об обязательном хранении данных[82]. Круг компаний, получающих такие требования, постоянно растет. Некоторые государства заставляют компании предоставлять им прямой доступ к потокам данных, проходящим через их сети. Такие системы прямого доступа вызывают серьезную озабоченность, поскольку они особенно уязвимы для злоупотреблений и, как правило, идут в обход основных процессуальных гарантий[83].

42. Более того, государства все в большей степени полагаются на услуги по наблюдению, предлагаемые коммерческими предприятиями, например, приобретая данные у брокеров данных и других компаний, собирающих и продающих персональные данные[84]. Такая практика может обойти важнейшие процедурные ограничения и гарантии, позволяя государствам косвенно получить доступ к инструментам, которые они не могли бы применить сами, не нарушая своих обязательств в области прав человека. Например, инструмент распознавания лиц, разработанный компанией «Клиавью ЭйАй», используется тысячами правоохранительных органов, несмотря на то что он был создан путем сбора фотографий миллиардов людей из Интернета, что является массовым нарушением прав, связанных с неприкосновенностью частной жизни[85].

43. Систематическое наблюдение за людьми в общественном пространстве в режиме онлайн и офлайн, особенно в сочетании с дополнительными способами анализа и соединения полученной информации с другими источниками данных, представляет собой вмешательство в право на неприкосновенность частной жизни и может иметь крайне пагубные последствия для осуществления других прав человека[86]. Оно может представлять угрозу свободе выражения мнений и мирных собраний, участию и демократии, поэтому к нему следует подходить с максимальной осторожностью и только в строгом соответствии с требованиями в отношении прав человека. Это происходит, даже если отслеживаемые действия осуществляются в обществе или на открытых платформах социальных сетей, поскольку у людей должно быть пространство, свободное от систематического наблюдения и вторжения, в частности, со стороны государственных структур. Как ранее отмечал Верховный комиссар, защита права на неприкосновенность частной жизни распространяется на

[82] A/HRC/27/37, п. 26; A/HRC/39/29, п. 18; A/HRC/23/40 и A/HRC/23/40/Corr.1, пп. 65–67; и A/69/397, пп. 53–55.

[83] A/HRC/39/29, п. 19.

[84] См., например, URL: https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances; и URL: https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, с. 25.

[85] Различные органы по защите данных, установив, что компания «Клиавью ЭйАй» нарушила закон о защите данных, наложили крупные штрафы и/или распорядились стереть полученные персональные данные, см. URL: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; см. также URL: https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy; URL: https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en; и URL: https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. Органы по защите данных постановили, что полиция, используя данный инструмент, нарушила закон о защите данных, см. URL: https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en; и URL: https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

[86] См. CCPR/C/NGA/CO/2, в котором Комитет по правам человека выразил обеспокоенность по поводу мониторинга социальных сетей, п. 40.

общественные места и информацию, которая находится в открытом доступе[87]. Комитет по правам человека отверг идею о том, что данные, собранные в общественных местах, автоматически становятся общественным достоянием и могут быть свободно доступны[88]. Европейский суд по правам человека признал, что общедоступная или заметная информация вполне может подпадать под действие права на неприкосновенность частной жизни, в частности когда персональные данные систематически или постоянно регистрируются[89].

44. Одна из особых проблем в сфере общественного наблюдения связана с сохранением фотографий. Изображения людей являются одним из основных атрибутов их личности, поскольку они раскрывают уникальные особенности, отличающие их от других людей. Запись, анализ и хранение изображений лица человека без его согласия представляют собой посягательство на его право на неприкосновенность частной жизни. Благодаря внедрению технологии распознавания лиц в общественных местах, которая требует сбора и обработки изображений лиц всех людей, снятых на камеру, такое вмешательство происходит в массовом и неизбирательном масштабе[90].

45. Более того, меры наблюдения в общественном пространстве могут привести к принятию мер, непосредственно влияющих на отдельных лиц и сообщества, включая меры принуждения, и часто являются основой для них. Такие меры включают усиленный мониторинг и полицейский надзор за определенными районами, группами или отдельными лицами, что иногда приводит к допросам, арестам и задержанию отдельных лиц. Некоторые группы и отдельные лица также могут быть помечены как связанные с потенциальной угрозой или риском, например как потенциальные террористы или преступники, часто по сути без веских доказательств. Правительства некоторых стран используют результаты различных мер наблюдения в общественном пространстве для выявления своих критиков или людей, не соответствующих социальным ожиданиям, что может привести к преследованию, задержанию или отказу в предоставлении основных услуг[91].

46. Операции слежения, как правило, чаще направлены на меньшинства и маргинализированные общины[92]. Существует опасность того, что использование искусственного интеллекта может закрепить подобные модели дискриминации[93], включая использование технологий распознавания лиц для расового и этнического профилирования[94]. Было доказано, что использование систем прогнозирования для охраны правопорядка и отправления правосудия чаще затрагивает меньшинства[95].

---

[87] A/HRC/39/29, п. 6.

[88] CCPR/C/COL/CO/7, п. 32.

[89] См. European Court of Human Rights, *Rotaru v. Romania*, para. 43, judgment of 4 May 2000; *Peck v. the United Kingdom*, judgment of 28 January 2003, para. 59; *Perry v. the United Kingdom*, judgment of 17 July 2003, para. 38; *Vukota-Bojić v. Switzerland*, judgment of 18 January 2017, para. 55.

[90] A/HRC/44/24, п. 33.

[91] См. URL: https://privacyinternational.org/explainer/55/social-media-intelligence.

[92] См. CERD/C/CHN/CO/14–17; и URL: https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

[93] См. документ зала заседаний Верховного комиссара о поощрении и защите прав человека и основных свобод африканцев и лиц африканского происхождения от чрезмерного применения силы и других нарушений прав человека сотрудниками правоохранительных органов, пп. 93 и 94. URL: https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session47/list-reports.

[94] A/HRC/41/35, п. 12, и A/HRC/44/57, п. 39.

[95] Комитет по ликвидации расовой дискриминации, общая рекомендация № 36 (2020) о предупреждении и борьбе с расовым профилированием со стороны сотрудников правоохранительных органов, пп. 33–34; A/HRC/44/57, п. 43; документ зала заседаний Верховного комиссара 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, п. 93; A/HRC/48/31, п. 24; URL: https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/; URL: https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf; и

47. Кроме того, слежение оказывает значительное сдерживающее воздействие на осуществление людьми своих прав, в частности права на свободу выражения мнений и мирных собраний[96]. В различных исследованиях показаны масштабы такого воздействия. Опрос 2015 года показал, что 25 % участников, которые знали о деле Эдварда Сноудена, изменили свое отношение к использованию различных технологических платформ[97]. Другое исследование показало, что от 34 % до 61 % писателей (в зависимости от страны) избегали или по крайней мере рассматривали возможность избегать определенных тем в своих работах из-за страха слежки со стороны государства[98]. В ходе опроса, проведенного Советом по технологиям Норвегии, 39 % респондентов заявили, что будут избегать употребления слов и фраз, за которыми следит полиция[99]. Как ранее отмечал Верховный комиссар, такое сдерживающее воздействие распространяется на собрания, включая мирные протесты[100].

D. Требования к соблюдению прав человека

48. Наблюдение в общественном пространстве, несомненно, влечет за собой серьезные риски для прав человека и может существенно подорвать право на неприкосновенность частной жизни. Таким образом, важно, чтобы государства, прибегающие к использованию общественного наблюдения, оценивали потенциальные последствия своих действий для прав человека и строго следили за соблюдением международного права в области прав человека, которое требует, чтобы любое такое вмешательство или ограничение было основано на законе, было необходимым для достижения законной цели и соразмерным. Существующие меры общественного наблюдения зачастую не отвечают данным требованиям.

49. Законность: несмотря на далеко идущие последствия различных форм наблюдения в общественном пространстве, во многих странах отсутствует надлежащая применимая нормативно-правовая база. Законы о защите данных часто отсутствуют, являются ненадлежащими или делают широкие исключения для правоохранительных и разведывательных служб[101]. Более того, зачастую общие законы о конфиденциальности данных не содержат подробных указаний и не обеспечивают надлежащих ограничений на использование определенных инструментов слежения. В связи с этим необходимы специальные правовые акты, в частности, для слежения, осуществляемого в контексте правоохранительной деятельности и национальной безопасности[102]. Законы и подзаконные акты должны иметь четко определенные и строгие ограничения на доступ к государственным базам данных и их объединение. К сожалению, имеется мало признаков того, что государства идут в сторону регулирования использования методов, технологий и инструментов слежения в социальных сетях. Несмотря на то что регулирующие органы и законодатели на местном, национальном и региональном уровнях предпринимают все больше усилий по регулированию распознавания лиц и других

URL: https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[96] A/HRC/27/37, п. 20; см. в отношении протестов: A/HRC/44/24, пп. 29, 35 и 52; Европейский суд по правам человека, *Big Brother Watch and Others v. the United Kingdom*, judgment of 25 May 2021 (58170/13, 62322/14 and 24960/15), п. 495; URL: http://dx.doi.org/10.15779/Z38SS13; URL: https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; и URL: https://pen.org/research-resources/global-chilling/.

[97] См. URL: https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

[98] См. URL: https://pen.org/research-resources/global-chilling/.

[99] См. URL: https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Online-with-the-public.pdf.

[100] A/HRC/44/24, пп. 35 и 53.

[101] A/HRC/39/29, п. 34.

[102] Минимальные требования к законам о слежении были ранее изложены Верховным комиссаром, см. A/HRC/27/37 и A/HRC/39/29.

биометрических средств наблюдения[103], большинство органов власти продолжают использовать системы биометрического наблюдения, несмотря на отсутствие нормативно-правовой базы для такой деятельности.

50. Законные цели: несомненно, общественное наблюдение может служить широкому спектру законных целей, например защите жизни или физической неприкосновенности людей и безопасности важнейших объектов инфраструктуры. К сожалению, общественное наблюдение регулярно проводится с целями, которые недопустимы в соответствии с международным правом в области прав человека. Общественное наблюдение неоправданно используется, в частности, для выявления и отслеживания лиц, придерживающихся оппозиционных политических взглядов, для расового и этнического профилирования, в отношении сообществ лесбиянок, геев, бисексуалов, трансгендеров и интерсексуалов, а также для оценки соответствия людей общественным нормам.

51. Необходимость и соразмерность: хотя наблюдение в общественном пространстве может быть допустимым, государства должны продемонстрировать, что меры являются необходимыми и соразмерными. Однако результативность мер наблюдения зачастую является сомнительной, что вызывает серьезные вопросы относительно их необходимости или соразмерности. Данные о влиянии видеонаблюдения на безопасность и предотвращение преступлений неоднозначны. Большинство исследований указывают на незначительное снижение некоторых видов преступлений (например, преступлений, связанных с транспортными средствами и имуществом) в районах, контролируемых камерами наблюдения, в то время как на насильственные преступления присутствие камер наблюдения, как правило, не влияет[104]. Более того, сравнение между многочисленными муниципальными образованиями в различных юрисдикциях показывает практически полное отсутствие взаимосвязи между количеством камер общественного наблюдения и уровнем преступности или безопасности в масштабах всего муниципального образования[105]. Что касается автоматизированной системы обнаружения угроз, широко используемой полицией для обнаружения выстрелов с целью выявления возможных мест преступления, то, как было показано, в 89 % случаев она ошибочно определяет звуки как выстрелы[106]. Наконец, многие полицейские управления, подписавшиеся на услуги прогностической охраны правопорядка, впоследствии прекратили это сотрудничество, ссылаясь на ограниченную полезность[107].

52. Общее наблюдение за людьми в общественных местах почти всегда является несоразмерным. Меры по наблюдению в общественных местах должны быть адресными и преследовать конкретную законную цель, например предотвращение определенной угрозы общественной безопасности, достаточно значимой для того, чтобы перевесить их негативное воздействие на права человека. Такие меры должны быть ограниченными, направленными на определенные места и время, например когда есть подтверждения того, что существует вероятность совершения преступления или могут возникнуть угрозы общественной безопасности. Должна отсутствовать альтернатива с меньшим вмешательством в частную жизнь. Необходимо ввести

[103] См. the proposed European Union Artificial Intelligence Act; the European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, URL: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en; см. также law in Washington State, United States of America, relating to the use of facial recognition, URL: https://www.securityindustry.org/report/washington-facial-recognition-law-faq/; а также запреты и моратории, принятые местными и региональными законодательными органами.

[104] См. URL: https://academicworks.cuny.edu/jj_pubs/256/; и URL: https://doi.org/10.1080/01924036.2021.1879885.

[105] См. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

[106] См. URL: https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/; и URL: https://igchicago.org/2021/08/24/oig-finds-that-shotspotter-alerts-rarely-lead-to-evidence-of-a-gun-related-crime-and-that-presence-of-the-technology-changes-police-behavior/.

[107] См. URL: https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

строгие ограничения на продолжительность хранения полученных данных и связанные с этим цели, для которых такие данные будут использоваться. Системы дистанционного биометрического наблюдения, в частности, вызывают серьезные опасения в отношении их соразмерности, учитывая их крайне высокую степень вмешательства и широкое воздействие на большое число людей[108]. В таких условиях Верховный комиссар приветствовала недавние усилия по ограничению или запрету использования технологий дистанционного биометрического распознавания и призвала ввести мораторий на их использование в общественных местах, по крайней мере до тех пор, пока не будут созданы основные гарантии[109]. Если такие технологии вообще используются, они должны применяться только для реагирования на такие ситуации, как серьезные преступления и серьезные угрозы общественной безопасности, если дискриминационные последствия могут быть исключены и подвергнуты надлежащему и действенному надзору, включая независимое разрешение и регулярные независимые проверки соблюдения прав человека.

IV. Выводы и рекомендации

53. **В настоящем докладе представлен обзор нескольких основных областей, в которых право на неприкосновенность частной жизни в цифровой сфере в настоящее время находится под угрозой. Стремительное внедрение цифровых технологий порождает целый ряд дополнительных проблем, которые не рассматриваются в данном докладе, но заслуживают внимания в дальнейшем. Например, одной из серьезных проблем остается скрытое массовое слежение, о котором говорилось в предыдущих докладах Верховного комиссара[110]. Кроме того, несмотря на повсеместное распространение систем цифрового установления личности и различных вариантов использования биометрических данных, последствия для прав человека мало изучены. Повсеместное слежение за пользователями Интернета со стороны бесчисленных компаний, таких как рекламодатели, финансовые учреждения и брокеры данных, требует гораздо большего внимания на международных форумах по правам человека. Пандемия коронавирусной инфекции (COVID-19) и ошеломляющее количество цифровых мер реагирования на нее могли бы стать темой отдельного доклада. Необходимо более глубоко изучить и понять, каким образом нарушения и злоупотребления в сфере неприкосновенности частной жизни влияют на маргинализированных людей и людей, находящихся в уязвимом положении. Необходимо очень внимательно следить за новыми явлениями, такими как стремление к широкому внедрению технологий блокчейна, расширенная и виртуальная реальность и разработка все более мощных нейротехнологий.**

54. **Однако, даже если сосредоточиться лишь на нескольких основных разработках, в настоящем докладе представлена тревожная картина того, как право на неприкосновенность частной жизни неуклонно подрывается в цифровую эпоху. Настоящий анализ не следует понимать как отрицание огромных преимуществ, которые приносят обществу цифровые технологии — напротив, общество должно полностью принять технологический прогресс, который расширяет возможности людей, улучшает жизнь, укрепляет правосудие и повышает производительность. Однако многочисленные способы, которыми повсеместное слежение угрожает правам человека и верховенству права и может разрушить динамичную плюралистическую демократию, вызывают глубокую обеспокоенность. Особенности современных сетевых цифровых технологий могут сделать их опасными инструментами контроля и угнетения: каждое действие в цифровом пространстве оставляет след в виде данных; технологии облачных вычислений облегчают объединение и анализ разрозненных источников данных; автоматизация увеличивает возможный масштаб и результативность слежения; а цифровое слежение трудно заметить тем, кто ему**

[108] A/HRC/48/31, пп. 26–27; A/HRC/44/24, пп. 33–38.
[109] A/HRC/48/31, пп. 27 и 59 d).
[110] См. A/HRC/27/37 и A/HRC/39/29.

подвергается. Более того, цифровое слежение тесно связано с отсутствием прозрачности в целом. Население зачастую очень мало знает о различных методах наблюдения, вплетенных во многие аспекты жизни. Государства слишком часто отказываются публиковать достоверную информацию о том, какие системы наблюдения они используют и для каких целей, и зачастую не хотят представлять подтверждения результативности этих систем.

55. **Меры слежения, несовместимые с международным правом в области прав человека, уже получили широкое распространение. Даже если слежение используется в законных целях, базовая инфраструктура может быть легко перепрофилирована и зачастую служит целям, для которых она изначально не предназначалась (так называемое «размывание функций»), или после изменения политического ландшафта. Лицам, принимающим решения, следует помнить об этом при рассмотрении новых проектов, расширяющих полномочия по сбору и анализу персональных данных. Крайне необходимы общественные дискуссии о границах, в которых допустимо слежение. Без активного общественного обсуждения общество рискует скатиться к системам слежения, позволяющим власть имущим осуществлять беспрецедентный контроль над повседневной жизнью.**

56. **Учитывая это, УВКПЧ рекомендует государствам:**

a) обеспечить, чтобы любое вмешательство в право на неприкосновенность частной жизни, включая взлом, ограничение доступа и использование технологий шифрования и слежение за населением, соответствовало международному праву в области прав человека, включая принципы законности, необходимости и соразмерности, а также недискриминации, и не нарушало сущность этого права;

b) систематически проявлять должную заботу о правах человека, включая регулярные комплексные оценки воздействия на права человека, при проектировании, разработке, приобретении, размещении и использовании систем наблюдения;

c) принимать во внимание, при проявлении должной заботы о правах человека и оценке необходимости и соразмерности новых систем и полномочий, связанных со слежением, всю правовую и технологическую среду, в которую эти системы или полномочия внедрены или будут внедрены; кроме того, государствам следует учитывать риски злоупотреблений, размывания функций и перепрофилирования, включая риски в результате будущих политических изменений;

d) принять и эффективно применять через независимые, беспристрастные и обеспеченные ресурсами органы власти законодательство о конфиденциальности данных для государственного и частного секторов, соответствующее международному праву в области прав человека, включая гарантии, надзор и средства правовой защиты для действенной защиты права на неприкосновенность частной жизни;

e) принять незамедлительные меры для успешного повышения прозрачности использования технологий наблюдения, в том числе путем надлежащего информирования населения и затронутых лиц и сообществ и регулярного предоставления данных, необходимых населению для оценки их результативности и воздействия на права человека;

f) содействовать общественному обсуждению использования технологий наблюдения и обеспечить конструктивное участие всех заинтересованных сторон в принятии решений о приобретении, передаче, продаже, разработке, размещении и использовании технологий наблюдения, включая разработку государственной политики и ее реализацию;

g) ввести мораторий на внутреннюю и транснациональную продажу и использование систем наблюдения, таких как хакерские инструменты и биометрические системы, которые могут быть использованы для установления

личности или классификации людей в общественных местах, до тех пор, пока не будут созданы надлежащие гарантии защиты прав человека; такие гарантии должны включать меры внутреннего и экспортного контроля в соответствии с рекомендациями, вынесенными в настоящем документе и в предыдущих докладах Совету по правам человека[111];

h) обеспечить, чтобы жертвы нарушений прав человека и злоупотреблений, связанных с использованием систем наблюдения, имели доступ к действенным средствам правовой защиты.

57. **В связи с конкретными вопросами, поднятыми в настоящем докладе, УВКПЧ рекомендует государствам:**

Взлом

a) обеспечить, чтобы взлом персональных устройств применялся властями только в качестве крайней меры, использовался только для предотвращения или расследования конкретного деяния, представляющего серьезную угрозу национальной безопасности или конкретного серьезного преступления, и был направлен исключительно на лицо, подозреваемое в совершении этих деяний; такие меры должны подлежать строгому независимому надзору и требовать предварительного одобрения со стороны судебного органа;

Шифрование

b) поощрять и защищать надежное шифрование и избегать любых прямых или косвенных, общих и неизбирательных ограничений на использование шифрования, таких как запреты, установление уголовной ответственности, введение стандартов слабого шифрования или требований обязательного общего сканирования на устройстве пользователя; вмешательство в шифрование частных сообщений отдельных лиц должно осуществляться только с разрешения независимого судебного органа и на индивидуальной основе и быть направленным на отдельных лиц при условии, что это требуется для расследования серьезных преступлений или предотвращения серьезных преступлений или серьезных угроз общественной безопасности или национальной безопасности;

Слежение за общественными местами и контроль за экспортом технологий наблюдения

c) принять надлежащую нормативно-правовую базу для регулирования сбора, анализа и обмена собранной информации из социальных сетей, в которой были бы четко определены допустимые основания, предварительные условия, процедуры выдачи разрешений и надлежащие механизмы надзора;

d) не прибегать к использованию общего мониторинга общественных мест, нарушающего неприкосновенность частной жизни, и обеспечить, чтобы все меры общественного наблюдения были строго необходимы и соразмерны для достижения важных законных целей, в том числе путем строгого ограничения их места и времени, а также продолжительности хранения данных, цели использования данных и доступа к ним; биометрические системы распознавания должны использоваться в общественных местах только для предотвращения или расследования серьезных преступлений или серьезных угроз общественной безопасности и при условии выполнения всех требований международного права в области прав человека в отношении общественных мест[112];

e) установить надежные и хорошо продуманные режимы экспортного контроля, применимые к технологиям слежения, использование которых

[111] См. A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 и A/HRC/48/31.

[112] Включая требования, изложенные в A/HRC/44/24, п. 53 j) i–v), и A/HRC/48/31, п. 59 d).

сопряжено с высоким риском для осуществления прав человека; государства должны требовать проведения прозрачных оценок воздействия на права человека с учетом возможностей подлежащих использованию технологий, а также ситуацию в государстве-получателе, включая соблюдение прав человека, верховенство права, наличие и действенное применение применимых законов, регулирующих деятельность по наблюдению, и существование независимых надзорных механизмов;

f) обеспечить, чтобы при предоставлении и использовании технологий слежения государственно-частные партнерства поддерживали и прямо включали нормы в области прав человека и не способствовали отказу от ответственности государства за соблюдение прав человека.