Генеральная Ассамблея

Distr.: General
3 August 2018
Russian
Original: English

Совет по правам человека
Тридцать девятая сессия
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

Настоящий доклад представляется во исполнение резолюции 34/7, в которой Совет по правам человека просил Верховного комиссара по правам человека подготовить доклад для выявления и уточнения принципов, стандартов и передовой практики в области поощрения и защиты права на неприкосновенность частной жизни в цифровой век, включая соответствующую ответственность коммерческих предприятий в этой связи, и представить его Совету по правам человека на его тридцать девятой сессии.

GE.18-12799 (R) 220818 230818
1812799

I. Введение

1. Необходимость отвечать на вызовы, которые порождает цифровой мир в контексте права на неприкосновенность частной жизни, становится острее, чем когда-либо. Цифровые технологии, которые развиваются в основном благодаря частному сектору и в которых постоянно используются данные, связанные с жизнью людей, постепенно проникают в социальную, культурную, экономическую и политическую структуру современного общества. Возможности таких технологий, как «большие данные» и искусственный интеллект, и объем используемых в них данных постоянно растут, угрожая породить интрузивную цифровую среду, в которой как государства, так и коммерческие предприятия смогут осуществлять слежение в беспрецедентных масштабах, а также анализировать и прогнозировать поведение людей и даже манипулировать им. Хотя трудно отрицать, что технологиям на основе данных могут быть найдены весьма полезные применения, если не управлять этими технологическими изменениями с большой осторожностью, они могут стать серьезной угрозой для человеческого достоинства, автономии, частной жизни и существования прав человека в целом.

2. Международные и региональные субъекты все больше осознают эти вызовы и начинают действовать соответствующим образом. В июле 2015 года Совет по правам человека назначил Специального докладчика по вопросу о праве на неприкосновенность частной жизни. В многочисленных резолюциях Совет по правам человека и Генеральная Ассамблея выражали обеспокоенность по поводу рисков для неприкосновенности частной жизни, вытекающих из государственных мер слежения и деловой практики[1]. На региональном уровне ряд мер укрепил защиту конфиденциальности данных, например Общий регламент по защите данных Европейского союза, который недавно вступил в силу и имеет глобальные последствия; протокол Совета Европы в целях обновления и модернизации Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера и Руководящие принципы защиты личных данных в Африке Комиссии Африканского союза. В то же время многие правительства приняли законы или внесли законопроекты, предусматривающие расширение их полномочий по слежению, часто в таких формах, которые не соответствуют применимым международным нормам в области прав человека[2].

3. В настоящем докладе приводятся рекомендации по решению некоторых из наиболее острых проблем, связанных с правом на неприкосновенность частной жизни в эпоху цифровых технологий. В нем содержится краткий обзор международных правовых рамок и обсуждение наиболее важных современных тенденций. Затем рассматриваются обязательства государств и ответственность предприятий, в том числе обсуждаются надлежащие гарантии и вопросы надзора. В заключительной главе дается некоторое представление о том, какие средства правовой защиты могут предоставляться в случае нарушений и злоупотреблений, касающихся неприкосновенности частной жизни.

4. Настоящий доклад опирается на доклад Верховного комиссара о праве на неприкосновенность личной жизни в цифровой век (A/HRC/27/37) и на материалы выступлений и обсуждений в ходе рабочего совещания экспертов, которое состоялось

[1] См., например, резолюции 68/167, 69/166 и 71/199 Генеральной Ассамблеи и резолюции 28/16 и 34/7 и решение 25/117 Совета по правам человека.

[2] См., например, Anja Seibert-Fohr, «Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy» (April 2018), доступно по адресу https://ssrn.com/abstract=3168711; https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee and www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SR_right_privacy.pdf.

в феврале 2018 года в Женеве [3]. Авторы также используют материалы 63 письменных представлений, полученных от широкого круга заинтересованных сторон[4].

II. Содержание права на неприкосновенность личной жизни в цифровой век

5. Право на неприкосновенность личной жизни является одним из основных прав человека и закреплено в статье 12 Всеобщей декларации прав человека, статье 17 Международного пакта о гражданских и политических правах, а также во многих других международных и региональных договорах о правах человека[5, 6]. Неприкосновенность личной жизни может быть определена как презумпция того, что частные лица должны иметь определенное поле для самостоятельного развития, взаимодействия и свободы, «частную сферу» во взаимодействии с другими лицами или без него, свободную от вмешательства государства и от чрезмерного инициативного вмешательства со стороны других незваных частных лиц (см., например, A/HRC/13/37, пункт 11, и A/HRC/23/40, пункты 22 и 42). В цифровой среде конфиденциальность информации, включая информацию, которая уже существует или может быть получена о человеке и его или ее жизни, а также решения, основанные на этой информации, имеют особое значение.

6. Защита права на неприкосновенность частной жизни имеет широкий охват и распространяется не только на непосредственное содержание коммуникационных сообщений, но и на метаданные, которые после анализа и обобщения «могут дать даже еще более полное представление о поведении человека, его социальных отношениях, личных предпочтениях и личности, чем то, что можно было бы узнать из самого содержания частного общения» (см. A/HRC/27/37, пункт 19). Защита права на неприкосновенность частной жизни не ограничивается частными, изолированными пространствами, такими как дом того или иного лица, а распространяется на общественное пространство и общедоступную информацию (CCPR/C/COL/CO/7, см. пункт 32). Например, право на частную жизнь вступает в действие тогда, когда государство осуществляет мониторинг общественного пространства, например рынка или железнодорожной станции, и таким образом ведет наблюдение за физическими лицами. Аналогичным образом, когда осуществляется сбор и анализ информации о физическом лице, имеющейся в открытом доступе в социальных сетях, это также затрагивает право на неприкосновенность частной жизни[7]. Публичное распространение информации не лишает ее содержание защиты[8].

7. Право на неприкосновенность частной жизни затрагивается не только в ходе анализа или использования информации о физическом лице человеком или алгоритмом[9]. Даже сам факт подготовки и сбора данных, касающихся личности, семьи и жизни конкретного человека уже затрагивает право на неприкосновенность частной

[3] См. http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgePrivacyWorkhop.aspx и материалы интернет-трансляции по адресу http://webtv.un.org/search/part-1.1-un-expert-workshop-on-the-right-to-privacy-in-the-digital-age/5734527899001/?term=2018-02-19&sort=date&page=2.

[4] Все представления размещены по адресу http://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

[5] См., например, статью 16 Конвенции о правах ребенка; статью 14 Международной конвенции о защите прав всех трудящихся-мигрантов и членов их семей; и статью 22 Конвенции о правах инвалидов.

[6] См., например, статью 10 Африканской хартии прав и благополучия ребенка; статью 11 Американской конвенции о правах человека; и статью 8 Европейской конвенции по правам человека.

[7] См. материалы, представленные для настоящего доклада организацией «Прайваси интернэшнл».

[8] Anja Seibert-Fohr, «Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy».

[9] См. Paul Bernal, «Data gathering, surveillance and human rights: recasting the debate», *Journal of Cyber Policy*, vol. 1, No. 2 (2016).

жизни, поскольку в случае осуществления таких действий лицо утрачивает определенную долю контроля над информацией, что может поставить под угрозу его или ее тайну частной жизни (см. A/HRC/27/37, пункт 20)[10]. Кроме того, само существование тайного слежения представляет собой вмешательство в право на неприкосновенность частной жизни (там же)[11].

8. Право на неприкосновенность частной жизни в равной степени распространяется на всех людей. Любые различия в степени его защиты на основании гражданства или любом другом основании несовместимы с правом на равенство и недискриминацию, закрепленном в статье 26 Международного пакта о гражданских и политических правах.

9. Государство-участник обязано уважать и обеспечивать любому лицу, находящемуся в пределах компетенции или эффективного контроля этого государства-участника, права, признаваемые в Пакте, даже если лицо не находится на его территории[12]. Право прав человека применяется там, где государство осуществляет свою власть или эффективный контроль в отношении инфраструктуры цифровой связи, где бы она ни находилась, например посредством прямого прослушивания или проникновения в коммуникационную инфраструктуру, расположенную за пределами территории этого государства. Аналогичным образом, если государство осуществляет нормативную юрисдикцию в отношении третьей стороны, которая контролирует информацию о том или ином лице (например, в отношении поставщика облачных услуг), данное государство также обязано распространять меры защиты прав человека на тех лиц, чьи права на неприкосновенность частной жизни могут пострадать в результате получения или использования этой информации (см. A/HRC/27/37, пункт 34).

10. В соответствии со статьей 17 Пакта любое вмешательство допускается только в том случае, если оно не является ни произвольным, ни противоправным. Правозащитные механизмы неизменно толкуют эти слова как указывающие на всеобъемлющие принципы законности, необходимости и соразмерности (см. A/HRC/27/37, пункты 21–27)[13]. В соответствии с этими принципами государства могут нарушать право на частную жизнь лишь в той степени, в какой это предусмотрено законом, и в соответствующем законодательстве должны подробно определяться конкретные обстоятельства, в которых такое вмешательство может допускаться[14]. Вмешательство является незаконным и произвольным не только в том случае, если оно не допускается законом, но и тогда, когда тот или иной закон или конкретное вмешательство противоречит положениям, целям и задачам Пакта[15]. Ограничение может быть законным и не произвольным, если оно преследует законную цель (см. A/HRC/29/32, пункт 33). Ограничение должно быть необходимым для достижения этой законной цели и пропорционально ей и представлять собой наименее интрузивный вариант действий. Кроме того, любое ограничение права на неприкосновенность частной жизни не должно нарушать существо признанного в Пакте права (см. A/69/397, пункт 51).

11. Право на неприкосновенность частной жизни имеет решающее значение для соблюдения и осуществления прав человека в сети Интернет и вне ее. Оно является одной из основ демократического общества и играет ключевую роль в осуществлении широкого спектра прав человека, начиная от свободы выражения мнений (см. A/HRC/23/40 и A/HRC/29/32, пункт 15) и свободы ассоциации и собраний

[10] См. также Европейский суд по правам человека, *Ротару против Румынии*, жалоба № 28341/95, постановление от 4 мая 2000 года, и *Копп против Швейцарии*, жалоба № 23224/94, постановление от 25 марта 1998 года.

[11] См. также Европейский суд по правам человека, *Роман Захаров против России,* жалоба № 47143/06, постановление от 4 декабря 2015 года.

[12] См. замечание общего порядка № 31 (2004 год) Комитета по правам человека о характере общего юридического обязательства, налагаемого на государства – участники Пакта, пункт 10.

[13] См. также резолюцию Совета по правам человека 34/7, пункт 2.

[14] См. замечание общего порядка № 16 (1988 год) Комитета по правам человека о праве на личную жизнь, пункты 3 и 8.

[15] Там же, пункт 4.

(см. A/HRC/31/66, пункты 73–78 и A/72/135, пункты 47–50) и заканчивая запрещением дискриминации и др.[16]. Посягательство на право на неприкосновенность частной жизни может иметь несоразмерные последствия для определенных лиц и/или групп, что усугубляет неравенство и дискриминацию[17]. Чрезмерно широкие нормы регулирования в области конфиденциальности могут представлять собой неоправданные ограничения других прав, в частности права на свободу выражения мнений, когда, например, несоразмерные ограничения мешают законной новостной журналистской деятельности, художественному самовыражению или научным исследованиям. Из-за ограничений по объему документа в настоящем докладе не могут быть рассмотрены вопросы взаимосвязи между правом на неприкосновенность частной жизни и другими правами человека, связанные с ним дискриминационные последствия для конкретных лиц и групп и подходы к их защите.

III. Посягательства на неприкосновенность частной жизни: тенденции и проблемы

A. Расширение использования личных данных правительствами и компаниями

Усиление цифрового следа

12. Государства и компании собирают и используют все больше данных, относящихся к частной жизни физических лиц. Огромные потоки данных, касающихся миллиардов людей, собираются персональными компьютерами, смартфонами, «умными часами», фитнес-браслетами и другими личными аксессуарами. Стремительно растущее число других взаимосвязанных устройств и датчиков, установленных в так называемых «умных домах» и «умных городах», добавляют дополнительные данные. Масштабы и глубина собираемой и используемой информации огромны: начиная от идентификаторов устройств, адресов электронной почты и телефонных номеров и заканчивая биометрическими, медицинскими и финансовыми данными и моделями поведения. Многие подобные вещи происходят без ведома затронутых лиц и без осознанного согласия.

Обмен и сведение данных

13. Компании и государства постоянно обмениваются личными данными из различных источников и баз данных и занимаются их сведением, причем ключевую роль здесь играют коммерческие поставщики данных. Как следствие, люди оказываются бессильны, поскольку практически невозможно отследить, кто и какой информацией о них обладает, не говоря уже о том, чтобы контролировать множество ситуаций, в которых такая информация может использоваться.

Биометрические данные

14. Государства и предприятия все чаще внедряют системы, предусматривающие сбор и использование биометрических данных, таких как ДНК, лицевая геометрия, голос, узор сетчатки и радужной оболочки глаза и отпечатки пальцев. Некоторые страны создали огромные централизованные базы данных для хранения такой информации в разных целях – от целей национальной безопасности и уголовных расследований до поиска лиц при необходимости получения основных услуг, таких как социальные и финансовые услуги и образование. Государственные субъекты во всем мире устанавливают камеры видеонаблюдения с замкнутой системой в городах, на железнодорожных вокзалах и в аэропортах, где используется автоматическое распознавание лиц для поиска и маркировки отдельных людей. Биометрические

[16] См. Paul Bernal, «Data gathering, surveillance and human rights: recasting the debate».

[17] См. резолюцию 71/199 Генеральной Ассамблеи, пункт 5 g); резолюцию 34/7 Совета по правам человека, пункт 5 g); и материалы, представленные для настоящего доклада Международной сетью организаций за гражданские свободы.

технологии все чаще используются для контроля за миграцией как на границах, так и внутри стран. Создание массовых баз биометрических данных вызывает серьезную озабоченность в области прав человека. Такие данные носят особенно конфиденциальный характер, поскольку они по определению неразрывно связаны с конкретным лицом и его жизнью и могут подвергаться серьезным злоупотреблениям. Например, крайне трудно компенсировать последствия кражи персональных биометрических данных, которая может серьезно затронуть права физического лица. Кроме того, биометрические данные могут быть использованы не для тех целей, для которых они собирались, включая незаконное отслеживание и мониторинг отдельных лиц. С учетом этих рисков при сборе биометрических данных необходимо уделять особое внимание вопросам необходимости и соразмерности. В этой связи вызывает тревогу тот факт, что некоторые государства приступили к осуществлению масштабных проектов с использованием биометрических данных, не внедрив адекватных правовых и процессуальных гарантий.

Укрепление аналитического потенциала

15. Аналитический потенциал технологий, основанных на использовании данных, продолжает расти в геометрической прогрессии. Методы анализа больших данных и искусственный интеллект расширяют возможности государств и компаний получать точную информацию о жизни людей, делать выводы об их физических и психических характеристиках и создавать подробные личные досье. Многие системы, используемые правительствами и компаниями, создаются именно для этой цели – сбор максимального объема информации о физических лицах в целях анализа, профилирования, оценки, классификации и в конечном итоге принятия решений о них, причем зачастую автоматических.

16. В результате создается среда, порождающая угрозы для людей и обществ, которые трудно переоценить. Например, в последние годы мы стали свидетелями утечки данных огромных масштабов, в результате чего затронутые лица стали жертвами кражи персональных данных и раскрытия глубоко личной информации. Незаконный сбор и анализ данных происходит в контексте избирательных кампаний. Профили, «оценка» и «ранжирование» лиц могут использоваться для оценки права на медицинское обслуживание, иного страхового покрытия, финансовых услуг и др. Непрозрачные решения на основе использования данных в делах, имеющих серьезные последствия, например при вынесении приговоров и проведении оценки рецидива, могут угрожать обеспечению надлежащей правовой процедуры. Попытки выявить лиц, представляющих потенциальную угрозу безопасности, в контексте прогнозирования преступности вызывают озабоченность, учитывая проблемы, связанные с транспарентностью, нарушением конституционных прав, подотчетностью и возможной дискриминацией[18].

B. Государственное слежение и перехват сообщений

Массовое слежение

17. Многие государства продолжают осуществлять тайное массовое слежение и перехват коммуникаций, сбор, хранение и анализ данных о всех пользователях в рамках широкого круга средств коммуникации (например, электронная почта, телефонные и видеозвонки, текстовые сообщения и посещаемые веб-сайты). Хотя некоторые государства утверждают, что такое неизбирательное массовое слежение необходимо для защиты национальной безопасности, эта практика «не допускается международным правом прав человека, поскольку при таких мерах невозможно проводить анализ каждого конкретного случая на предмет необходимости и соразмерности применяемых мер» (см. A/HRC/33/29, пункт 58)[19]. Как отметил Европейский суд по правам человека «система тайного слежения, созданная для

[18] См. Ajay Sandhu, «Data driven policing: highlighting some risks associated with predicting crime», Human Rights Centre, Essex University.

[19] См. также A/HRC/27/37, пункт 25.

защиты национальной безопасности, может подорвать или даже уничтожить демократию под предлогом ее защиты»[20].

Доступ к данным пользователей, имеющимся у коммерческих предприятий

18. Государства часто полагаются на компании в деле сбора и перехвата личных данных. Например, некоторые государства обязывают поставщиков телекоммуникационных услуг и услуг доступа в Интернет предоставлять им прямой доступ к потокам данных, проходящих 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[21]. Кроме того, некоторые государства требуют доступа к информации, которая собирается и хранится поставщиками телекоммуникационных и интернет-услуг. Государства продолжают вводить императивные требования к телекоммуникационным компаниям и поставщикам интернет-услуг, обязывающие их хранить данные о коммуникациях в течение длительного периода времени[22]. Многие такие законы требуют от компаний неизбирательно собирать и хранить информацию о трафике всех подписчиков и пользователей в рамках всех средств электронной коммуникации. Они ограничивают способность людей общаться анонимно, создают опасность злоупотреблений и могут облегчить раскрытие информации третьим сторонам, включая преступников, политических противников или коммерческих конкурентов, путем взлома или иной кражи данных. Такие законы выходят за пределы того, что может считаться необходимым и соразмерным[23].

Взлом

19. По всей видимости, правительства все чаще полагаются на агрессивное проникающее программное обеспечение, которые «внедряется» в цифровые устройства физических лиц. Такого рода хакерская деятельность дает возможность осуществлять неизбирательный перехват и сбор всех видов коммуникаций и данных (зашифрованных и незашифрованных), а также получать дистанционный и тайный доступ к личным устройствам и хранящимся на них данным, позволяя проводить слежение в режиме реального времени и манипулировать данными на таких устройствах[24]. Это угрожает не только праву на неприкосновенность личной жизни, но и правам, относящимся к процессуальной законности, применительно к использованию таких доказательств в ходе судопроизводства (см. A/HRC/23/40, пункт 62). Хакерская деятельность также ставит серьезные проблемы, связанные с экстерриториальностью, поскольку она может затрагивать физических лиц во многих юрисдикциях[25]. Кроме того, взлом опирается на использование уязвимых мест в системах информационно-коммуникационных технологий (ИКТ) и, таким образом, усугубляет угрозы безопасности для миллионов пользователей.

Попытки ослабления шифрования и анонимности

20. Неоднократные попытки государств ослабить технологии шифрования и ограничить доступ к инструментам анонимизации также угрожают безопасности и конфиденциальности общения и другой деятельности в Интернете. Некоторые государства требуют встраивания в системы шифрования сообщений утвержденных «потайных ходов», обязывают поставщиков услуг шифрования сообщений передать ключи шифрования (см. A/HRC/29/32, пункты 38–45) или даже запрещают или

[20] См. *Роман Захаров против России*, пункт 232.

[21] См. *Роман Захаров против России*, пункт 270.

[22] См. CCPR/C/ZAF/CO/1, пункты 42–43, и CCPR/C/PAK/CO/1, пункты 35–36.

[23] См., например, объединенные дела Европейского суда C-203/15 и C-698/15, *«Теле2 Свериге АБ» против Шведского почтового и телекоммуникационного агентства и Министр внутренних дел против Уотсона*, постановление от 21 декабря 2016 года, пункт 107; CCPR/C/ZAF/CO/1, пункты 42–43; и CCPR/C/CMR/CO/5, пункты 39–40.

[24] См. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, «Encryption and anonymity follow-up report» (June 2018).

[25] См. материалы, представленные «Прайваси интернэшнл».

блокируют некоторые приложения для безопасной связи, включая приложения для использования зашифрованных текстовых сообщений и виртуальные частные сети и сети по анонимизации. Шифрование и анонимность обеспечивают отдельным лицам и группам пространство неприкосновенности частной жизни в Интернете, где они могут иметь собственное мнение и осуществлять свободу выражения мнений без произвольного и незаконного вмешательства или посягательств (A/HRC/29/32)[26]. Инструменты шифрования и анонимизации широко используются во всем мире, в том числе правозащитниками, гражданским обществом, журналистами, лицами, сообщающими о нарушениях, и политическими диссидентами, которым угрожает преследование и притеснение. Их ослабление ставит под угрозу конфиденциальность всех пользователей и подвергает их опасности незаконного вмешательства не только государств, но и негосударственных субъектов, включая преступные сети[27]. Такое широкомасштабное и неизбирательное воздействие несовместимо с принципом соразмерности (см. A/HRC/29/32, пункт 36).

Обмен разведывательными данными

21. Правительства по всему миру регулярно обмениваются разведывательными данными о физических лицах вне каких-либо правовых рамок и без надлежащего надзора[28]. Обмен разведданными создает серьезный риск того, что государства могут использовать этот канал для обхода внутренних правовых ограничений, полагаясь на другие стороны для получения информации и последующего обмена ею. Такая практика несовместима с принципом законности и может поставить под угрозу сам принцип права на неприкосновенность частной жизни (см. A/HRC/27/37, пункт 30). Угроза для защиты прав человека является особенно серьезной в тех случаях, когда разведданные предоставляются государствам со слабой правоохранительной системой и/или государствам, известным своими продолжительными и систематическими нарушениями прав человека. Разведывательные данные, полученные одним государством от другого, могли быть получены в нарушение международного права, в том числе в результате применения пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения. Риски в области прав человека, связанные с обменом разведданными, усугубляются отсутствием на сегодняшний день транспарентности, подотчетности и надзора за функционированием механизмов обмена разведданными (см. A/69/397, пункт 44, CCPR/C/GBR/CO/7, пункт 24, CCPR/C/SWE/CO/7, пункт 36). За очень немногими исключениями, законодательство не смогло поставить обмен разведывательной информацией в надлежащие правовые рамки в соответствии с принципом законности согласно международному праву прав человека[29].

Трансграничный доступ к данным, находящимся в распоряжении компаний

22. Недавно были предприняты усилия по созданию правовых механизмов, направленных на облегчение доступа государств к личной информации, хранящейся на серверах коммерческих предприятий за рубежом. Получение доказательств в ходе уголовного расследования, несомненно, является важной и законной целью. Однако такой доступ может привести к ослаблению или обходу процессуальных гарантий, таких как требование о получении разрешения со стороны независимого органа и создание надлежащих механизмов надзора. Трансграничные запросы также могут негативно влиять на доступ отдельных лиц к механизмам апелляции и судебной защиты. Особую озабоченность вызывает опасность того, что государства со слабой

[26] См. также UCI Law International Justice Clinic, «Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression»; Amnesty International, «Encryption. A matter of human rights» (March 2016); и Wolfgang Schulz and Joris van Hoboken, «Human rights and encryption», United Nations Educational, Scientific and Cultural Organization (2016).

[27] См. http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138.

[28] См. Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards* (April 2018) и http://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf.

[29] См. материалы, представленные «Прайваси интернэшнл».

правоохранительной системой и/или проблемами в области прав человека могут получить доступ к конфиденциальной информации о физических лицах без надлежащей защиты от нарушений прав человека.

IV. Обязанности государств

A. Обязанность государства соблюдать и защищать право на неприкосновенность частной жизни в цифровой век

23. 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. Государства-участники обязаны воздерживаться от нарушения прав, признаваемых в Пакте, и любое ограничение любого из этих прав должно быть допустимым соответствующими положениями Пакта[30]. Однако обязательства государств выходят за рамки обязательства «уважать» и включают также «позитивные» меры защиты осуществления прав. В контексте права на неприкосновенность частной жизни это предполагает обязанность принимать законодательные и другие меры для введения в действие запрета и защиты от незаконного или произвольного вмешательства и вторжений как со стороны государственных органов, так и со стороны физических и юридических лиц[31].

24. Обязанность по защите отражена в разделе I Руководящих принципов предпринимательской деятельности в аспекте прав человека, озаглавленном «Обязанность государства защищать права человека и подробно раскрывающем обязанность государств защищать от негативных последствий для прав человека, связанных с компаниями. Принцип 1 Руководящих принципов требует принятия необходимых мер, направленных на предупреждение и расследование нарушений прав человека, наказание за них и компенсацию ущерба посредством эффективной политики, законодательства, нормативного регулирования и судопроизводства. В последующих принципах определяются различные правовые и политические области, в которых государствам следует принять «рациональный комплекс мер» − национальных и международных, обязательных и добровольных − способствующих соблюдению предприятиями прав человека[32]. Примеры применения подхода, предусмотренного в Руководящих принципах в отношении сектора ИКТ, включают в себя разработанные на уровне Европейского союза отраслевые руководящие принципы, где основное внимание сосредоточено на рекомендуемых способах борьбы компаний в сфере ИКТ с любыми негативными последствиями своей деятельности.

25. Обязанность государств защищать от нарушений права на неприкосновенность частной жизни со стороны компаний и других третьих сторон, образованных или домицилированных в пределах их юрисдикции, имеет экстерриториальные последствия. Например, государства должны вводить применимые к технологиям слежения режимы экспортного контроля, которые служат для оценки правовых рамок, регулирующих использование технологий в стране назначения, правозащитной репутации предлагаемого конечного пользователя и гарантий и процедур надзора в отношении использования полномочий по ведению слежения. В экспортно-лицензионные соглашения необходимо включать гарантии защиты прав человека. Кроме того, государства обязаны защищать лиц, находящихся под их юрисдикцией, от экстерриториального нарушения их права на неприкосновенность частной жизни, например с помощью средств перехвата коммуникаций или взлома.

[30] См. Комитет по правам человека, замечание общего порядка № 31, пункт 6.

[31] См. Комитет по правам человека, замечания общего порядка № 16, пункты 1 и 9, и № 31, пункт 8.

[32] См. Принцип 2, комментарий.

B. Ответственность государства за обеспечение надлежащих гарантий и эффективного надзора

26. Осуществление права на неприкосновенность частной жизни в значительной степени зависит от правовых, нормативных и институциональных рамок, предусматривающих надлежащие правовые гарантии, включая эффективные механизмы надзора. В эпоху, когда государствам и компаниям доступен огромный объем личных данных, а физические лица имеют ограниченное представление и контроль за тем, как используется информация о них и их жизни, крайне важно сосредоточить внимание на мерах по смягчению последствий такого властного и информационного дисбаланса для прав человека.

1. Общие рамки защиты от ненадлежащего вмешательства

27. Одним из главных элементов государственной системы защиты неприкосновенности частной жизни должны быть законы, устанавливающие стандарты обработки личной информации как государствами, так и частными субъектами[33]. Хотя государства располагают свободой в определении рационального комплекса мер, регулирующих использование корпорациями личной информации, пункт 2 статьи 17 Международного пакта о гражданских и политических правах устанавливает необходимость защиты физических лиц посредством закона. Растущая взаимосвязь между обработкой общественных и личных данных и накопленный опыт, свидетельствующий о массовых и неоднократных злоупотреблениях личными данными некоторыми компаниями, подтверждают, что для обеспечения надлежащего уровня защиты частной жизни необходимы законодательные меры[34].

28. На глобальном уровне растет консенсус в отношении минимальных стандартов, которые должны регулировать обработку личных данных государствами, предприятиями и другими частными субъектами. Международные документы и руководящие принципы, отражающие эти изменения, включают, среди прочего, Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера, 1990 года; Конвенцию о защите частных лиц в отношении автоматизированной обработки данных личного характера и ее обновленные версии, в которых устанавливается высокий уровень защиты на глобальном уровне[35]; Принципы неприкосновенности частной жизни 1980 года Организации экономического сотрудничества и развития, обновленные в 2013 году; Конвенция о кибербезопасности и защите личных данных Африканского союза (Конвенция Малабо); Мадридская резолюция Международной конференции уполномоченных по защите данных и права на неприкосновенность частной жизни; Рамки защиты частной жизни форума Азиатско-тихоокеанского экономического сотрудничества. Эти стандарты, в частности Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, легли в основу рамок защиты конфиденциальности данных многих государств и могут использоваться как ориентиры при разработке надлежащих инструментов политики[36].

[33] См. Комитет по правам человека, замечание общего порядка № 16, пункт 9, A/HRC/13/37, пункт 61, и A/HRC/17/27, пункт 56. Глобальный обзор законодательства о конфиденциальности данных см. в представлении для настоящего доклада Грэхэма Гринлифа, Университет Нового Южного Уэльса. В настоящем докладе термин «обработка» охватывает любые операции с использованием личных данных, включая сбор, хранение, использование, изменение, уничтожение, раскрытие, передачу и сведение.

[34] См. резолюции Совета по правам человека 34/7, пункт 5 f), и 38/7, пункт 17.

[35] Помимо 47 государств – членов Совета Европы, эту конвенцию ратифицировали Маврикий, Сенегал, Тунис и Уругвай, а несколько других государств находятся в процессе присоединения.

[36] Подробные руководящие указания см. в https://privacyinternational.org/advocacy-briefing/2165/guide-policy-engagement-data-protection и Access Now, «Creating a data protection framework: a do’s and don’ts guide for lawmakers. Lessons from the EU general data protection regulation» (2018).

29. Вышеупомянутые документы и рекомендации содержат ряд ключевых принципов, прав и обязанностей, обеспечивающих минимальный уровень защиты личных данных. Во-первых, обработка личных данных должна быть справедливой, законной и транспарентной. Лица, чьи персональные данные проходят обработку, должны информироваться об обработке данных, ее обстоятельствах, характере и масштабах, в том числе с помощью транспарентных правил конфиденциальности данных. В целях предупреждения произвольного использования личной информации обработка личных данных должна осуществляться на основании свободного, конкретного, осознанного и недвусмысленного согласия затронутых лиц или ином законном основании, предусмотренном в законе[37]. Обработка личных данных должна быть необходимой и соразмерной законной цели, которая должна быть указана субъектом, осуществляющим эту обработку. Следовательно, объем и тип данных и срок их хранения должны быть ограничены, данные должны быть точными, и по мере возможности должны использоваться технологии анонимизации и псевдонимизации данных. Следует избегать изменения цели без согласия затронутого лица, а в случае такого изменения оно должно ограничиваться целями, совместимыми с первоначально указанной целью. Учитывая уязвимость личных данных для несанкционированного разглашения, изменения или удаления, важно принимать надлежащие меры безопасности. Кроме того, субъекты, занимающиеся обработкой личных данных, должны нести ответственность за соблюдение применимых правовых и политических рамок в сфере обработки данных. Наконец, данные, носящие секретный характер, должны иметь более высокий уровень защиты[38].

30. Во всех документах и рекомендациях, упомянутых выше, признается, что лицам, чьи данные проходят обработку, должны предоставляться определенные права. Как минимум, затрагиваемые лица имеют право знать, что личные данные были удержаны и обработаны, иметь доступ к хранимым данным, исправлять неточные или устаревшие данные и уничтожать или исправлять данные, которые хранятся незаконно или необоснованно. В новых договорах были добавлены существенные дополнительные права, в частности право возражать против обработки личных данных, по крайней мере в тех случаях, когда осуществляющая обработку организация не смогла доказать наличия законных и веских оснований для такой обработки[39]. Государствам следует уделять особое внимание предоставлению надежной защиты от нарушений права на неприкосновенность частной жизни, связанных с профилированием и автоматизированным принятием решений. Описанные выше права должны также применяться к информации, получаемой, определяемой и прогнозируемой автоматическими методами, в той мере, в которой эта информация квалифицируется в качестве личных данных. Важно, чтобы правовая база не допускала, чтобы эти права неоправданно ограничивали право на свободу выражения мнений, включая обработку личных данных для журналистских, художественных и научных целей.

31. Правовые рамки защиты конфиденциальности данных должны также устанавливать определенные обязанности субъектов, осуществляющих обработку личных данных. Эти требования охватывают не только организационные аспекты, такие как создание внутреннего механизма надзора, но и обязательные меры, такие как уведомления о нарушении конфиденциальности данных и оценки воздействия на неприкосновенность частной жизни. В условиях усложняющейся технологической среды такие оценки играют ключевую роль в предотвращении и смягчении ущерба для неприкосновенности частной жизни[40]. Кроме того, важными инструментами защиты

[37] См. пункт 2 статьи 5 обновленной Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера; пункт 1 статьи 13 Конвенции Малабо; и принцип 12 Мадридской резолюции.

[38] См. статью 6 обновленной Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера.

[39] Там же, статья 9 1) d). См. также статью 21 Общего регламента по защите данных и пункт 1 статьи 18 Конвенции Малабо.

[40] Углубленный анализ методов оценки воздействия на неприкосновенность частной жизни см. в David Wright and Paul de Hert, eds., *Privacy Impact Assessment* (New York, Springer, 2012).

права на неприкосновенность частной жизни являются требования, касающиеся разработки продуктов и услуг, такие как обеспечение встроенной конфиденциальности[41] и конфиденциальности по умолчанию[42].

32. В глобализированном мире передача данных, в том числе большого объема личных данных, стала обычным явлением и необходима для реализации многих услуг. Государства должны принимать меры к тому, чтобы такая передача данных не представляла собой или не облегчала неправомерное вмешательство в право на неприкосновенность частной жизни. В то же время следует избегать жестких требований о локализации данных, которые обязывают всех субъектов, занимающихся обработкой данных, хранить все личные данные внутри страны (A/HRC/32/38, пункт 61). Вместо этого государствам следует сосредоточить внимание на способах защиты личных данных, передаваемых другому государству, по меньшей мере на уровне, требуемом международным правом прав человека.

33. Государствам следует создать независимые надзорные органы в сфере обработки личных данных. Такие органы имеют существенно важное значение для защиты прав человека от злоупотреблений, связанных с обработкой личных данных. Контрольный орган нуждается в законодательной базе с целью четкого определения его мандата, полномочий и независимого статуса. Такие надзорные органы должны получить технические, финансовые и людские ресурсы, необходимые для эффективного мониторинга деятельности по обработке данных государств и коммерческих предприятий, а также для обеспечения соблюдения юридических требований в этой области. Кроме того, эти органы должны иметь достаточные правовые полномочия для выполнения своих функций, в том числе возможность вводить санкции, соразмерные совершенным нарушениям и злоупотреблениям[43].

2. Процессуальные гарантии и надзор в сфере слежения и перехвата коммуникаций

Гарантии

34. Хотя все виды государственных мероприятий, связанных со слежением, должны осуществляться на основании закона (см. A/HRC/27/37, пункт 28), Специальный докладчик по вопросу о праве на неприкосновенность частной жизни обращал внимание на повсеместное отсутствие такого законодательства. Следует отметить, что во многих юрисдикциях разведывательные и правоохранительные органы исключены из положений законодательства о конфиденциальности данных. Такие исключения должны быть ограничены исходя из принципов необходимости и соразмерности, с тем чтобы обеспечить надлежащий уровень конфиденциальности данных в рамках всех ветвей власти. При разработке законодательства, непосредственно затрагивающего вопросы слежения, следует руководствоваться следующими минимальными стандартами.

35. Закон должен быть общедоступным. Тайные правила и тайные толкования законодательства не обладают необходимыми качествами «закона» (там же, пункт 29). Законы должны быть достаточно четкими. Степень свободы принятия решений, предоставленная исполнительной власти или суду, и способы реализации этой свободы должны быть обозначены достаточно четко (см. A/69/397, пункт 35)[44]. С этой целью должны быть описаны характер правонарушения и категории лиц, которые могут подвергаться слежению. Размытые и чересчур широкие обоснования, например общие ссылки на «национальную безопасность», не могут считаться достаточно четкими законодательными положениями. Слежение должно основываться на

[41] Т. е. защита конфиденциальности данных должна быть элементом, встроенным на этапе разработки той или иной системы.

[42] Требование о том, чтобы система применяла настройки соблюдения конфиденциальности по умолчанию.

[43] См., например, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

[44] См. также *Роман Захаров против России*, пункт 230.

обоснованных подозрениях, и соответствующее разрешающее решение должно быть достаточно избирательным[45]. Закон должен строго распределять среди конкретных органов полномочия по ведению слежения и получению доступа к результатам слежения.

36. С точки зрения охвата нормативно-правовая база слежения должна охватывать запросы государства к коммерческим предприятиям. Она должна охватывать доступ к информации, хранящейся за пределами государства, и обмен информацией с другими государствами. В законе необходимо обеспечить ясность структуры подотчетности и прозрачность деятельности государственных учреждений, отвечающих за ведение слежения.

37. Полномочия тайного слежения могут быть оправданы лишь в той мере, в какой они являются абсолютно необходимыми для достижения законной цели и удовлетворяют требованию о соразмерности (см. A/HRC/23/40, пункт 83 b))[46]. Применение мер тайного слежения должно ограничиваться предупреждением или расследованием наиболее серьезных преступлений и угроз. Продолжительность слежения должна ограничиваться строгим минимальным сроком, необходимым для достижения указанной цели. Должны быть введены жесткие правила использования и хранения полученных данных и четко определены обстоятельства, при которых собранные и сохраненные данные должны быть уничтожены, исходя из принципов строгой необходимости и соразмерности[47]. Обмен разведывательными данными должен производиться в соответствии с теми же принципами законности, строгой необходимости и соразмерности.

38. В тех случаях, когда государства рассматривают вопрос о принятии целенаправленных мер по взлому данных, они должны избирать крайне осторожный подход, прибегая к таким мерам лишь в исключительных случаях для расследования или предотвращения наиболее серьезных преступлений или угроз и действуя с привлечением судебных органов (см. CCPR/C/ITA/CO/6, пункт 37)[48]. Операции по взлому данных должны иметь узкий охват, ограничивающий доступ к информации конкретными целями и типами информации. Государства должны воздерживаться от принуждения частных компаний к содействию проведению операций по взлому, подрывая тем самым безопасность их собственных продуктов и услуг. Принуждение к расшифровке данных может быть допустимо лишь на адресной, индивидуальной основе и при наличии судебного ордера и защиты прав на надлежащую правовую процедуру (см. A/HRC/29/32, пункт 60).

Санкционирование и надзор независимого органа[49]

39. Меры надзора, включая запросы к коммерческим предприятиям о предоставлении коммуникационных данных и обмен разведывательными данными, должны на всех этапах санкционироваться, пересматриваться и контролироваться независимыми органами, в том числе, когда впервые отдается приказ об их применении, в процессе их осуществления и после его окончания (см. CCPR/C/FRA/CO/5, пункт 5)[50]. Независимый и предпочтительно судебный орган, санкционирующий конкретные меры слежения, должен убедиться в том, что имеются явные доказательства наличия достаточной угрозы и что предлагаемые меры слежения являются целенаправленными, строго необходимыми и соразмерными, и должен санкционировать (или запретить) ex ante применение мер наблюдения.

[45] Там же, пункты 248 и 260.

[46] См. также *Сабо и Виши против Венгрии*, пункт 73.

[47] См. *Роман Захаров против России*, пункт 231.

[48] См. также Access Now, «A human rights response to government hacking» (September 2016) и Privacy International, «Government hacking and surveillance: 10 necessary safeguards».

[49] См. A/HRC/34/60 и European Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update*, (Luxembourg, Publications Office of the European Union, 2017).

[50] См. также *Роман Захаров против России*, пункт 233.

40. Рамки надзора могут включать сочетание административного, судебного и/или парламентского надзора[51]. Надзорные органы должны быть независимыми от компетентных органов, осуществляющих слежение, и обладать надлежащим и необходимым опытом, навыками и ресурсами. Санкционирование и надзор должны быть организационно отделены друг от друга. Независимые надзорные органы должны превентивно расследовать и контролировать деятельность тех органов, которые осуществляют слежение и имеют доступ к информации, полученной в результате слежения, и проводить периодические обзоры возможностей и технологических изменений в сфере слежения. Учреждения, осуществляющие слежение, должны по запросу предоставлять всю необходимую информацию для эффективного надзора и регулярно отчитываться перед надзорными органами и должны быть обязаны вести учет всех принятых мер слежения[52]. Необходимо также обеспечить транспарентность процессов надзора и их контроль со стороны общественности, а решения надзорных органов должны быть предметом апелляции или независимого обзора. Учет в работе надзорных органов различных точек зрения, например с помощью экспертных консультаций и консультаций с участием многих заинтересованных сторон (см., например, A/HRC/34/60, пункт 36), имеет особенно важное значение в отсутствие состязательного процесса: важно создавать «точки трения» – постоянно ставить под сомнение имеющиеся подходы и представления[53].

Принцип транспарентности

41. Государственные органы власти и надзорные органы должны также участвовать в распространении общественной информации о существующих законах, мерах политики и практике в области слежения и перехвата коммуникаций и других видов обработки личных данных, так как открытые обсуждения и пристальный анализ являются крайне важными для понимания преимуществ и недостатков методов слежения (см. A/HRC/13/37, пункт 55). Лица, ставшие объектом слежения, должны быть поставлены об этом в известность, и им необходимо разъяснить ex post facto причины нарушения их права на неприкосновенность частной жизни. Они должны также иметь возможность изменить и/или удалить неактуальную личную информацию, при условии, что такая информация больше не требуется для целей текущего или запланированного расследования (см. A/HRC/34/60, пункт 38).

V. Обязанности компаний

42. В разделе II Руководящих принципов предпринимательской деятельности в аспекте прав человека представлено авторитетное руководство для всех предприятий, независимо от их размера, сектора, условий деятельности, форм собственности и структуры, с целью предупреждения и преодоления всех негативных последствий для прав человека, включая право на неприкосновенность частной жизни[54]. В нем излагается обязанность компаний соблюдать все признанные на международном уровне права человека, т. е. им следует избегать нарушения прав человека других и устранять неблагоприятные последствия для прав человека оказанного ими воздействия[55]. Ответственность за соблюдение существует в отношении всех видов деятельности и деловых отношений компании. В цифровом пространстве особенно важно, что ответственность за соблюдение применяется независимо от того, где находятся пострадавшие лица. Ответственность за соблюдение прав существует

[51] См. резолюцию 71/199 Генеральной Ассамблеи, пункт 5 d).

[52] См. Европейский суд по правам человека, *Кеннеди против Соединенного Королевства*, жалоба № 26839/05, постановление от 18 мая 2010 года, пункт 165, и Роман Захаров против России, пункт 272.

[53] См. материалы, представленные для настоящего доклада специалистами проекта «Права человека, большие данные и технологии», Центр по правам человека, Эссекский университет.

[54] Руководящие принципы были единогласно одобрены Советом по правам человека в его резолюции 17/4.

[55] Руководящий принцип 11.

независимо от того, выполняет ли государство свои собственные обязательства в области прав человека.

43. Выполнение обязанности соблюдать права человека требует от предприятий: a) избегать неблагоприятного воздействия в рамках своей деятельности; b) избегать содействия оказанию неблагоприятного воздействия в рамках своей деятельности как напрямую, так и через какие-либо внешние структуры (правительство, бизнес или другие); и c) стремиться предотвращать или смягчать неблагоприятное воздействие на права человека, которое непосредственно связано с их деятельностью, продукцией или услугами вследствие их деловых отношений, даже если они непосредственно не способствовали оказанию такого воздействия[56]. Например, компания, которая передает данные о пользователях какому-либо государству, которое затем использует эти данные для выявления и преследования политических диссидентов, будет содействовать таким нарушениям прав человека, включая право на неприкосновенность частной жизни. Компании, которые производят и продают технологии, используемые для незаконного или произвольного вмешательства, также содействуют оказанию неблагоприятного воздействия на права человека.

44. Если между требованием соблюдения международного права прав человека и обязательств в рамках национального законодательства имеются противоречия, компании должны стремиться соблюдать нормы международного права прав человека в максимально возможной степени и по мере возможности смягчать любое негативное воздействие, например путем как можно более узкого толкования требований государства[57].

45. Для выполнения своей обязанности соблюдать права человека предприятиям с учетом своих размеров и условий деятельности следует определить свою политику и процедуры, включая:

a) широко обнародовать программное обязательство на самом высоком уровне и включить ответственность за соблюдение прав человека во все элементы оперативной политики и процедур[58];

b) проводить процессы должной осмотрительности в вопросах прав человека, что предполагает:

i) проведение оценок воздействия на права человека для выявления и оценки любого фактического или потенциального неблагоприятного воздействия на права человека;

ii) интеграцию этих оценок и принятие надлежащих мер для предупреждения и смягчения выявленного неблагоприятного воздействия на права человека;

iii) отслеживание эффективности принятых мер;

iv) представление официальной информации о том, какие меры приняты предприятием в связи с его воздействием на права человека[59];

c) предоставление возмещения ущерба или сотрудничество в деле возмещения ущерба в тех случаях, когда компания выявляет отрицательное воздействие, которое она причинила или которому она содействовала[60].

46. Согласно Руководящим принципам, все компании несут ответственность за применение должной осмотрительности в вопросах прав человека для выявления и устранения любого воздействия своей деятельности на права человека. Если приводить конкретный пример, то компании, торгующие технологиями слежения, должны проводить в рамках должной осмотрительности тщательную оценку

[56] Руководящий принцип 13. См. также УВКПЧ, «Ответственность корпораций за соблюдение прав человека: пособие по толкованию» (2012 год).
[57] Руководящий принцип 23.
[58] Руководящий принцип 16.
[59] Руководящие принципы 17–21.
[60] Руководящий принцип 22 и раздел VI настоящего доклада.

воздействия на права человека перед любой потенциальной сделкой. Смягчение рисков должно включать четкие гарантии конечного использования, внесенные в договорные соглашения и предусматривающие серьезные правозащитные гарантии, предотвращающие произвольное или незаконное использование данной технологии, и периодические обзоры применения технологии государствами[61]. Компании, осуществляющие сбор и хранение данных пользователей, должны провести оценку рисков в области конфиденциальности, связанных с потенциальными запросами государств о предоставлении таких данных, включая оценку правовой и институциональной среды соответствующих государств. Они должны обеспечить надлежащие процедуры и гарантии в целях предотвращения и смягчения потенциального вреда для неприкосновенности частной жизни и других прав человека. Кроме того, должна проводится оценка воздействия на права человека в рамках утверждения условий службы и проектных и инженерных решений, имеющих последствия для безопасности и неприкосновенности частной жизни, и решений, принимаемых в целях предоставления или прекращения обслуживания в конкретном контексте (см. A/HRC/32/38, пункт 11).

47. В рамках процесса обеспечения должной осмотрительности в вопросах прав человека руководящие принципы предусматривают подотчетность предприятий за то, каким образом они устраняют свое воздействие на права человека и предполагают их готовность распространять такую информацию за пределами предприятия, особенно в тех случаях, когда озабоченности высказываются затрагиваемыми сторонами или от их имени[62]. В цифровой среде это означает раскрытие информации о том, какие личные данные полежат сбору, как долго они хранятся, в каких целях и как они используются и кому и при каких обстоятельствах они передаются. Это относится в том числе к запросам государств о доступе к пользовательским данным. В тех случаях, когда национальные законы и правила препятствуют такой отчетности, компаниям следует в максимально возможной степени использовать любые имеющиеся рычаги и рекомендуется выступать за предоставление возможности обнародовать такую информацию.

48. В рамках реализации своих обязательств в соответствии с Руководящими принципами компании сектора ИКТ разработали рекомендации по вопросам осуществления политики в области прав человека. Такие инициативы включают в себя Принципы свободы выражения мнений и неприкосновенности частной жизни Глобальной сетевой инициативы (принципы ГСИ)[63] и Руководящие принципы проекта «Диалог телекоммуникационной индустрии»[64]. Например, в принципах ГСИ конкретно указывается, что участвующие компании «будут использовать средства защиты в отношении личной информации» и «будут уважать и добиваться защиты прав пользователей на неприкосновенность частной жизни при наличии требований со стороны государства, закона или правила, которые ставят конфиденциальность под угрозу в нарушение межународно признанных норм и стандартов».

49. Индекс корпоративной отчетности проекта «Рейтинг цифровых прав» предназначен для целенаправленной оценки ряда сетевых, мобильных и телекоммуникационных компаний по их обнародованным обязательствам и мерам, затрагивающим свободу выражения мнений и неприкосновенность частной жизни[65]. Он может стать полезным инструментом для привлечения компаний к ответственности за их воздействие на права пользователей.

[61] См. материалы, представленные «Прайваси интернэшнл» Специальному докладчику по вопросу о поощрении и защите права на свободу мнений и их свободное выражение (январь 2016 года), доступно по адресу http://www.ohchr.org/Documents/Issues/Expression/PrivateSector/PrivacyInternational.pdf.

[62] Руководящий принцип 21.

[63] Доступно по адресу https://globalnetworkinitiative.org/gni-principles/. См. также материалы, представленные для настоящего доклада Глобальной сетевой инициативой.

[64] Доступно по адресу https://globalnetworkinitiative.org/gni-principles/.

[65] См. https://rankingdigitalrights.org/index2018/.

VI. Средства правовой защиты

50. Жертвы нарушения неприкосновенности частной жизни или злоупотреблений со стороны государства и/или компаний должны иметь доступ к эффективным средствам правовой защиты. Государства не только обязаны обеспечивать подотчетность и средства правовой защиты в случае нарушений прав человека, совершенных государственными субъектами, но и должны также принимать надлежащие меры для обеспечения доступа пострадавших от связанных с предпринимательской деятельностью нарушений прав человека к эффективным средствам правовой защиты (см. раздел III Руководящих принципов предпринимательской деятельности в аспекте прав человека). В зависимости от характера конкретного случая или ситуации жертвы должны иметь возможность получить средства правовой защиты через эффективные судебные и внесудебные государственные механизмы рассмотрения жалоб (A/HRC/32/19, Corr.1 и Add.1 и A/HRC/38/20 и Add.1). Соответствующие государственные внесудебные механизмы в области ИКТ включают независимые органы с полномочиями по мониторингу практики государственного и частного сектора в области конфиденциальности данных, такие как органы по защите неприкосновенности частной жизни и защите данных.

51. В тех случаях, когда предприятия устанавливают, что они оказали неблагоприятное воздействие на права человека или способствовали ему, им следует в рамках законных процессов возмещать причиненный ущерб в связи с тем неблагоприятным воздействием на права человека, которое они оказали или которому они способствовали, или сотрудничать с целью его возмещения[66]. С целью обеспечения эффективности любого внесудебного механизма следует гарантировать его легитимность, доступность, предсказуемость, справедливость, транспарентность, источник непрерывного обучения, а механизмы жалоб на оперативном уровне должны быть основаны на взаимодействии и диалоге[67].

52. В случае, когда предприятие не способствовало оказанию неблагоприятного воздействия на права человека, но такое воздействие тем не менее непосредственно связано с его деятельностью, продукцией или услугами через его деловые отношения, надлежащие шаги прописаны в руководящем принципе 19. Они могут включать в себя использование любых имеющихся у компании рычагов для оказания воздействия на ее деловых партнеров или клиентов с целью возмещения ущерба[68].

53. В Руководящих принципах также подчеркивается роль, которую механизмы рассмотрения жалоб на оперативном уровне могут играть при непосредственном рассмотрении жалоб. Такие механизмы могут принимать различные формы, которые будут зависеть от типа компании, потребностей заинтересованных сторон и профиля компании с точки зрения рисков в области прав человека. Для определения того, каким образом эти механизмы могут быть разработаны и функционировать в секторе ИКТ на практике, необходимы дальнейшие обсуждения с заинтересованными сторонами в рамках этого сектора.

54. На практике существуют значительные пробелы и препятствия в том, что касается обеспечения доступа к средствам правовой защиты в случае нарушения неприкосновенности частной жизни. Транснациональный характер и последствия слежения, перехвата коммуникаций и различных форм обработки личных данных создают правовые и практические трудности (см. A/HRC/34/60, пункт 34). Кроме того, препятствием для доступа к средствам правовой защиты часто является отсутствие у жертв информации или доказательств относительно ненадлежащего вмешательства (см. A/HRC/27/37, пункт 40). Например, запросы государства о доступе к хранимым компаниями данным часто сопровождаются запретом на разглашение информации, который не позволяет компаниям уведомлять затронутых лиц. Кроме того,

[66] Руководящий принцип 22.

[67] Руководящий принцип 31.

[68] См. руководящий принцип 19 и комментарий к нему. См. также УВКПЧ, «Ответственность корпораций за соблюдение прав человека: пособие по толкованию», стр. 48–52.

государства часто не уведомляют лиц, затронутых другими мерами слежения, в частности в случаях массового слежения. Учитывая, что заблаговременное или совпадающее по времени уведомление может поставить под угрозу эффективность слежения, частные лица должны, тем не менее, уведомляться сразу же после окончания слежения (см. A/HRC/23/40, пункт 82). Если это не представляется возможным, то в законодательстве следует предоставлять значительную процессуальную правоспособность тем, кто мог теоретически быть затронут этими мерами (см. A/HRC/13/37, пункт 38). Кроме того, предприятиям следует уведомлять своих клиентов, как только им становится известно о взломе личных данных, который мог сказаться на их правах.

55. Жертвы сталкиваются также с новыми и все более серьезными вызовами в контексте алгоритмического принятия решений, когда физические лица могут не иметь доступа к вводимых данных или оспорить выводы, сделанные алгоритмом, или то, каким образом полученные выводы были использованы при принятии решения[69]. Государствам и компаниям в сотрудничестве с другими заинтересованными сторонами следует рассмотреть возможные механизмы для решения этой проблемы, например создание обеспеченных ресурсами экспертных органов аудита.

56. Дополнительные проблемы вызваны характером ущерба, причиняемого в результате нарушения неприкосновенности частной жизни. Воздействие нарушений неприкосновенности частной жизни трудно исправить, и они могут привести к длительным последствиям и затронуть также другие права человека. Простота хранения, обмена, перенаправления и объединения данных и досье влияет на постоянство цифровых данных, т. е. физическое лицо может столкнуться с новыми и сохраняющимися рисками для своих прав в будущем[70].

57. Ущерб, нанесенный неприкосновенности частной жизни, существенно влияет на жизнь человека, даже в случае отсутствия количественной оценки экономических и иных последствий; характер ущерба не должен мешать жертвам обращаться за возмещением. Например, организации по защите прав потребителей могут наделяться полномочиями добиваться возмещения от имени жертв корпоративных нарушений неприкосновенности частной жизни.

VII. Выводы и рекомендации

58. **Международные правозащитные рамки создают прочную основу для разработки мер реагирования на многочисленные вызовы, возникающие в эпоху цифровых технологий. Существует настоятельная необходимость полного выполнения государствами своих обязательств по соблюдению права на неприкосновенность частной жизни, а также своих обязанностей по защите этого права, в том числе от корпоративных злоупотреблений. Для достижения этой цели государствам необходимо создать надлежащие правовые и политические рамки, в том числе принять надлежащие законодательные и нормативные акты с целью защиты неприкосновенности частной жизни, основанные на принципах законности, соразмерности и необходимости, и обеспечить гарантии, надзор и средства правовой защиты.**

59. **Дальнейшего углубленного изучения требуют многие вопросы, которые не могли быть рассмотрены в настоящем докладе, например взаимосвязь права на неприкосновенность частной жизни и других прав человека, включая экономические, социальные и культурные права; несоразмерные и дискриминационные последствия вторжения в частную жизнь отдельных лиц и/или групп, находящихся в зоне риска; воздействие больших данных и машинного обучения, в том числе в целях прогнозирования и превентивных**

[69] См. пункт 33 материала, представленного для настоящего доклада специалистами проекта «Права человека, большие данные и технологии», Эссекский университет.

[70] Там же, пункт 7.

целях, на осуществление права на неприкосновенность частной жизни и других прав человека; и регулирование рынков технологий слежения.

60. **Еще одна область, заслуживающая дополнительного внимания – это характер и виды средств правовой защиты, которые являются эффективными в ситуациях нарушения права на неприкосновенность частной жизни. В качестве первого шага следует на систематической основе определить виды корректив ных мер, которые могут быть уместными в разных ситуациях. Результаты могут быть использованы при разработке дальнейших руководящих указаний. В процессе проведении такого анализа следует уделять должное внимание руководящим указаниям и рекомендациям, разработанным в рамках проекта в области ответственности и правовой защиты Управления Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ). В более общем плане, следует предпринять усилия с целью разработки руководств для конкретных секторов, касающихся обязанностей предприятий по соблюдению права на неприкосновенность частной жизни.**

61. **Верховный комиссар рекомендует государствам:**

a) признать все последствия новых технологий, в частности технологий на основе данных, не только для права на неприкосновенность частной жизни, но и для всех других прав человека;

b) принять эффективное, продуманное и всеобъемлющее законодательство о защите частной жизни, включая защиту конфиденциальности данных, которое соответствует международным нормам в области прав человека в плане гарантий, надзора и средств правовой защиты, с целью действенной защиты права на неприкосновенность частной жизни;

c) обеспечить, чтобы системы, использующие большие объемы данных, включая системы, предусматривающие сбор и хранение биометрических данных, внедрялись только тогда, когда государства могут доказать, что они являются необходимыми и соразмерными для достижения законной цели;

d) создать независимые органы, наделенные полномочиями по мониторингу практики государственного и частного сектора в области конфиденциальности данных, расследованию нарушений, получению жалоб от физических лиц и организаций и применению штрафов и других эффективных санкций за незаконную обработку личных данных частными компаниями и государственными органами;

e) обеспечить с помощью соответствующего законодательства и других средств соответствие любого ограничения права на неприкосновенность частной жизни, включая отслеживание коммуникаций и обмен разведывательной информацией, международным нормам в области прав человека, включая принципы законности, необходимости и соразмерности, независимо от гражданства или местонахождения затронутых лиц, и разъяснить, что санкционирование мер слежения требует разумных оснований подозревать, что какое-либо лицо совершило или совершает уголовное преступление или осуществляет деяния, связанные с конкретной угрозой для национальной безопасности;

f) укрепить механизмы независимого санкционирования государственного слежения и надзора за ним и обеспечить, чтобы эти механизмы были компетентными и обладали необходимыми ресурсами для осуществления контроля и обеспечения законности, необходимости и соразмерности мер слежения;

g) пересмотреть законы с целью исключения требования к телекоммуникационным и иным компаниям о тотальном и неизбирательном удержании коммуникационных данных;

h) принять меры в целях повышения уровня прозрачности и подотчетности в процессе приобретения технологий слежения государствами;

i) в полной мере выполнять свою обязанность по обеспечению защиты от нарушений права на неприкосновенность частной жизни в результате действий коммерческих предприятий во всех соответствующих секторах, в том числе в секторе ИКТ, путем принятия надлежащих мер, направленных на предупреждение и расследование таких нарушений, наказание за них и компенсацию ущерба посредством эффективных мер политики, законодательства, нормативного регулирования и судебного разрешения споров;

j) обеспечить, чтобы все жертвы нарушений и ущемлений права на неприкосновенность частной жизни имели доступ к эффективным средствам правовой защиты, в том числе в рамках трансграничных дел.

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

a) прилагать все усилия с целью выполнения своих обязанностей по соблюдению права на неприкосновенность частной жизни и других прав человека. Как минимум, предприятиям следует полностью внедрить в свою работу Руководящие принципы предпринимательской деятельности в аспекте прав человека, что предполагает проведение эффективной должной осмотрительности в вопросах прав человека в рамках всей их деятельности и в отношении всех прав человека, включая право на неприкосновенность частной жизни, и принятие соответствующих мер для предотвращения, смягчения и устранения фактического и потенциального воздействия;

b) прилагать усилия с целью обеспечения высокого уровня безопасности и конфиденциальности любых сообщений, которые они передают, и любых персональных данных, которые они собирают, хранят и каким-либо иным образом обрабатывают. Проводить на постоянной основе оценку оптимальных методов обеспечения и укрепления безопасности продуктов и услуг;

c) соблюдать основные принципы конфиденциальности, указанные в пунктах 29–31 настоящего доклада, и обеспечивать максимально возможную транспарентность в тех элементах своей внутренней политики и практики, которые затрагивают право на неприкосновенность частной жизни их пользователей и клиентов;

d) в тех случаях, когда они оказали неблагоприятное воздействие 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;

e) вносить вклад в работу проекта в области ответственности и правовой защиты УВКПЧ с целью разработки руководящих указаний и рекомендаций для повышения эффективности негосударственных механизмов рассмотрения жалоб в связи с нарушениями права на неприкосновенность частной жизни в цифровом пространстве.