КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
Контртеррористический центр ООН (КТЦ ООН)

INTERPOL

При финансовой поддержке Европейского союза

Кибербезопасность и новые технологии

Создание законодательной базы, механизмов обеспечения прозрачности и надзора в отношении сбора данных в Интернете

Выражение признательности

Настоящий доклад является результатом совместной инициативы Контртеррористического центра Организации Объединенных Наций (КТЦ ООН) при Контртеррористическом управлении Организации Объединенных Наций (КТУ ООН) и Интерпола, направленной на укрепление потенциала правоохранительных органов и органов уголовного правосудия в области противодействия использованию новых технологий в террористических целях. Реализация этой совместной инициативы стала возможной благодаря щедрой финансовой поддержке Европейского союза.

Содержание

Совместное предисловие

Достижения в области информационно-коммуникационных технологий и их доступность сделали привлекательным для террористических и насильственных экстремистских групп их использование для совершения широкого спектра противоправных действий, включая подстрекательство, радикализацию, вербовку, обучение, планирование, сбор информации, коммуникацию, подготовку, пропаганду и финансирование. Террористы постоянно осваивают новые технологические рубежи, и государства-члены выражают все большую озабоченность относительно использования новых технологий в террористических целях.

В ходе седьмого обзора Глобальной контртеррористической стратегии Организации Объединенных Наций государства-члены попросили Контртеррористическое управление Организации Объединенных Наций и другие соответствующие структуры в рамках Глобального договора по координации контртеррористической деятельности «совместно поддерживать инновационные меры и подходы в том, что касается наращивания у государств-членов (по их запросу) способности учитывать в деле предупреждения терроризма и борьбы с ним те вызовы и возможности, которые порождаются новыми технологиями, включая аспекты, относящиеся к правам человека».

В своем докладе Генеральной Ассамблее о деятельности системы Организации Объединенных Наций по осуществлению Глобальной контртеррористической стратегии Организации Объединенных Наций (A/77/718) Генеральный секретарь подчеркивает, что «[...] новые и новейшие технологии открывают беспрецедентные возможности для улучшения благополучия человека и предлагают новые инструменты для борьбы с терроризмом. [...] Несмотря на активизацию усилий и усиление координации, ответные меры международного сообщества часто запаздывают. Иногда такие ответные меры неоправданно ограничивают права человека, в частности право на неприкосновенность частной жизни и свободу выражения мнений, включая право на поиск и получение информации».

Подготовив семь докладов, представленных в этом сборнике, который выпускается при сотрудничестве Контртеррористического центра Организации Объединенных Наций с Международной организацией уголовной полиции в рамках совместной инициативы CT TECH, финансируемой Европейским союзом, мы стремимся поддержать правоохранительные органы и органы уголовного правосудия государств-членов в их противодействии использованию новых и новейших технологий в террористических целях и задействовать такие технологии для борьбы с терроризмом в рамках проводимой работы при полном соблюдении прав человека и верховенства права.

Наши ведомства готовы и впредь оказывать поддержку государствам-членам и другим нашим партнерам в области предотвращения терроризма и борьбы с ним во всех его формах и проявлениях, а также в использовании положительного влияния технологий в борьбе с терроризмом.

Владимир Воронков
Заместитель Генерального секретаря,
Контртеррористическое управление
Организации Объединенных Наций,
Исполнительный директор,
Контртеррористический центр
Организации Объединенных Наций

Стивен Кавана
Исполнительный директор,
Полицейская служба Интерпола

Выражение признательности

Настоящий документ был разработан и подготовлен при участии широкого круга заинтересованных сторон. В частности, Контртеррористическое управление Организации Объединенных Наций (КТУ ООН) хотело бы выразить признательность:

- **Камелю Эль-Хилали – доктору философии в области права**
  Парижский Университет Пантеон-Асса

Термины и определения

Беспристрастные механизмы надзора	принимают решения на основе фактов и в соответствии с законом, без каких-либо ограничений, неправомерного влияния, стимулов, давления, угроз или вмешательства, как прямого, так и косвенного, любых лиц по любой причине[1].
Даркнет/дарквеб	Зашифрованная часть сети Интернет, доступ к которой осуществляется с помощью специального программного обеспечения, которое само по себе не является криминальным, например браузера Tor. Однако общепризнанным является тот факт, что даркнет содержит в себе множество криминальных веб-сайтов и сервисов, размещенных в этих сетях[2].
Действия правоохранительных органов	Этот термин, как правило, описывает действия правоохранительных органов, предпринимаемые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Доказательства	Официальный термин для обозначения информации, являющейся частью судебного процесса, которая используется для подтверждения или опровержения совершения предполагаемого преступления. Все доказательства являются информацией, но не вся информация является доказательством. Таким образом, информация – это первоначальная, исходная форма доказательств[3].
Зеттабайт	Один зеттабайт равен одному миллиарду терабайтов.
Искусственный интеллект	Под этим термином обычно понимают дисциплину, занимающуюся разработкой технологических инструментов, позволяющих имитировать когнитивные функции человеческого мозга, такие как планирование, обучение, рассуждение и анализ.
Метаданные	определяются как «свод данных, описывающих другие данные и сообщающих информацию о них».
Наблюдение	Систематическое наблюдение или мониторинг отдельных лиц, групп или деятельности уполномоченным государственным органом, в том числе сбор, запись, анализ или распространение информации, с целью предотвращения, расследования и/или преследования преступной деятельности. Сюда относится физическое, электронное (прослушка, устройства слежения и т. д.) или цифровое (просмотр интернет-страниц, переписка по электронной почте, взаимодействие в социальных сетях) наблюдение.
Правовая основа для доступа правительства к персональным данным	включает национальные законы, постановления исполнительной или судебной власти, административные регламенты, прецедентное право и другие юридически обязательные документы или требования, включая правовые обязательства, вытекающие из международного и наднационального права, применимого в данной стране.

1 Управление Верховного комиссара ООН по правам человека, «Основные принципы независимости судебной власти», URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-independence-judiciary

2 Европейский центр киберпреступности (EC3),«Оценка угроз организованной преступности в Интернете за 2019 год» (Европол, 2019 год), URL: https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

3 Руководство ИДКТК по содействию использованию и признанию приемлемости в качестве доказательств в национальных уголовных судах информации, собранной, обработанной, сохраняемой и передаваемой военными для целей судебного преследования за террористические преступления (2019 г.), URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

Независимые механизмы надзора	независимы от политических, экономических, военных или иных целей. Они обладают: 1) формальной (де-юре) независимостью, требующей, чтобы они оставались вне бюрократической, иерархической системы подчинения в министерстве или других государственных учреждениях; и 2) фактической (де-факто) независимостью, связанной с самоопределением органа при применении надлежащих мер[4].
Новые технологии	Термин «Новые технологии» охватывает широкий спектр различных технологий[5], однако для целей данного документа под новыми технологиями понимается использование и злоупотребление такими новыми технологиями, как Интернет, социальные сети, криптовалюты, системы распознавания лиц и даркнет[6].
Оперативная информация	Информация, являющаяся результатом сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, которая используется лицами, принимающими решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование оперативной информации и обмен ею должны осуществляться в соответствии с обязательствами государств-членов по соблюдению международных договоров в области прав человека.
Персональные данные в Интернете	означает любую информацию в Интернете, относящуюся к идентифицированному или поддающемуся идентификации лицу.
Правовая основа для доступа правительства к персональным данным	включает национальные законы, постановления исполнительной или судебной власти, административные регламенты, прецедентное право и другие юридически обязательные документы или требования, включая правовые обязательства, вытекающие из международного и наднационального права, применимого в данной стране.
Реабилитация	В контексте уголовного правосудия термин «реабилитация» используется для обозначения мероприятий, проводимых исправительной системой с целью изменения взглядов или поведения правонарушителей, для того чтобы снизить вероятность повторного совершения ими преступления, а также подготовить и обеспечить их реинтеграцию в общество.
Терроризм	Преступные деяния, в том числе против гражданского населения, совершаемые с намерением причинить смерть или серьезные телесные повреждения, или акты захвата заложников, которые призваны вызвать состояние ужаса у широких слоев населения, группы лиц или отдельных лиц, запугать население или заставить правительство или международную организацию совершить или воздержаться от совершения какого-либо действия и которые являются преступлениями в рамках и в соответствии с определениями международных конвенций и протоколов в области противодействия терроризму[7].
Уголовное правосудие	Юридический процесс, который предусматривает предъявление обвинений в совершении уголовно наказуемого деяния физическому или юридическому лицу, проведение судебных слушаний, разрешение дела, назначение наказания, а также исправление и реабилитацию осужденных.
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств в поддержку обвинения в судебном процессе.
Эффективные механизмы надзора	независимы, обладают соответствующим опытом, компетенцией и ресурсами, имеют полный беспрепятственный доступ к информации, инфраструктуре и должностным лицам и наделены достаточными мандатами и полномочиями, определенными законом, для проверки соблюдения действующего законодательства, в том числе соответствия требованиям в области прав человека, инициирования и надлежащего проведения расследований в отношении неправомерных действий должностных лиц.

4 См., например, ОЭСР, «Руководство по обеспечению публичной добропорядочности», раздел 12.2.3, URL: https://www.oecd-ilibrary.org/sites/7715f0e0-en/index.html?itemId=/content/component/7715f0e0-en

5 Искусственный интеллект, интернет вещей, блокчейн-технологии, криптоактивы, дроны и беспилотные летательные системы, ДНК, отпечатки пальцев, кибертехнологии, системы распознавания лиц, 3D-печать.

6 Проектный документ CT TECH – Приложение I. Описание действий.

7 Резолюция 1566 (2004) Совета Безопасности, пункт постановляющей части 3.

Краткое содержание

Наиболее эффективными мерами борьбы с терроризмом являются мероприятия, соответствующие международным обязательствам в области прав человека. Интрузивная национальная политика в области безопасности может оказывать отрицательное воздействие на соблюдение и защиту прав человека, в частности прав на неприкосновенность частной жизни, свободу выражения мнений и объединений, а также недискриминацию. Вне зависимости от способа реализации политики в области безопасности — в режиме онлайн или офлайн — обеспечение соответствия такой политики обязательствам в области международного права требует принятия адекватной правовой базы, отвечающей требованиям в области прав человека, и создания эффективных и независимых механизмов обеспечения прозрачности и надзорной деятельности.

В настоящем руководстве основное внимание уделяется обязательствам государств-членов, а не ИКТ-компаний. Обязательства этих компаний в области прав человека рассматриваются в «Руководящих принципах предпринимательской деятельности в аспекте прав человека» Организации Объединенных Наций[8].

8 «Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты» | Управление Верховного комиссара ООН по правам человека.

[I]

Базовая информация

1.1 Обзор

Государства — члены Организации Объединенных Наций придают большое значение вопросу влияния новых технологий в борьбе с терроризмом. В ходе седьмого обзора Глобальной контртеррористической стратегии Организации Объединенных Наций (A/RES/75/291)[9] в июле 2021 года государства-члены выразили глубокую озабоченность по поводу «использования Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, включая непрекращающееся распространение террористического контента», попросили Контртеррористическое управление Организации Объединенных Наций и другие соответствующие структуры в рамках Глобального договора по координации контртеррористической деятельности «совместно поддерживать инновационные меры и подходы в том, что касается наращивания у государств-членов (по их запросу) способности учитывать в деле предупреждения терроризма и борьбы с ним те вызовы и возможности, которые порождаются новыми технологиями, включая аспекты, относящиеся к правам человека». Резолюции 2178 (2014)[10] и 2396 (2017)[11] Совета Безопасности призывают государства-члены сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий и средств связи для совершения террористических актов. Резолюция (2017) 2396 Совета Безопасности также призывает государства-члены **расширять сотрудничество с частным сектором, особенно с компаниями, работающими в секторе информационно-коммуникационных технологий (ИКТ)**, в деле сбора цифровых данных и доказательств по делам, связанным с терроризмом.

В своем 30-м докладе Совету безопасности Организации Объединенных Наций[12] Группа по аналитической поддержке и наблюдению за санкциями отметила, что «Многие государства-члены подчеркнули растущую роль социальных сетей и других онлайн-технологий в финансировании терроризма и распространении пропаганды», указав, что платформы, на которые ссылаются государства-члены, включают, среди прочих, Telegram, Rocket.Chat, Hoop и TamTam. В докладе также говорится о том, что **сторонники ИГИЛ используют платформы в дарквебе** для хранения учебных материалов, размещать которые другие сайты отказываются, и доступа к ним, а также **для приобретения новых технологий**.

Противодействие использованию новых и новейших технологий в террористических целях обсуждалось на специальном заседании Контртеррористического комитета (КТК) Совета Безопасности ООН, которое состоялось 28–29 октября 2022 года в Нью-Дели и завершилось принятием документа, не имеющего обязательной силы и известного как Делийская декларация[13].

9 Глобальная контртеррористическая стратегия Организации Объединенных Наций: седьмой обзор (A/RES/75/291), N2117570.pdf (un.org)

10 Резолюция 2178 (2014) Совета Безопасности, URL: http://undocs.org/S/RES/2178(2014)

11 Резолюция 2396 (2017) Совета Безопасности, URL: http://undocs.org/S/RES/2396(2017)

12 Тридцатый доклад Группы аналитической поддержки и наблюдения за санкциями, представленный во исполнение резолюции 2610 (2021) по ИГИЛ, «Аль-Каиде» и связанным с ними лицам, группам, предприятиям и организациям S/2022/547 (undocs.org)

13 Делийская декларация, URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf

КТК отметил **«с озабоченностью расширение использования в глобализованном обществе террористами и их сторонниками Интернета и других информационно-коммуникационных технологий**, включая платформы социальных сетей, в террористических целях» и признал **«необходимость обеспечения баланса между стимулированием инноваций и предотвращением использования новых и новейших технологий — по мере расширения их применения — в террористических целях и противодействием такому их использованию»**, одновременно с этим особо отмечая **«необходимость сохранения глобальной цифровой связности и свободного и надежного потока информации**, что способствовало бы экономическому развитию, коммуникации, участию и доступу к информации».

1.2 Инициатива CT TECH

CT TECH — это совместная инициатива КТУ ООН/КТЦ ООН и Интерпола, реализуемая в рамках Глобальной контртеррористической программы КТУ ООН/КТЦ ООН по кибербезопасности и новым технологиям. Она направлена на укрепление потенциала правоохранительных органов и органов уголовного правосудия в отдельных государствах-партнерах для противодействия использованию новых и новейших технологий в террористических целях, а также на оказание поддержки правоохранительным органам государств-партнеров в использовании новых и новейших технологий в борьбе с терроризмом.

Для достижения общей цели предусмотрена реализация инициативы CT TECH по двум направлениям, состоящим из шести компонентов.

РИСУНОК 1

ТАБЛИЦА 1. **Направления и компоненты CT TECH**

Направление 1: принятие эффективных мер реагирования в рамках контртеррористической политики в ответ на вызовы и возможности новых технологий в борьбе с терроризмом при полном соблюдении прав человека и принципа верховенства права.	
 **Компонент 1.1**	Подготовка информационных материалов для разработки мер реагирования в рамках национальной контртеррористической политики в ответ на вызовы и возможности новых технологий в борьбе с терроризмом при полном соблюдении прав человека и принципа верховенства права.
 **Компонент1.2**	Повышение уровня осведомленности и знаний о передовой практике в области идентификации рисков и преимуществ, связанных с новыми технологиями в контексте борьбы с терроризмом, при полном соблюдении прав человека и принципа верховенства права.
 **Компонент 1.3**	Укрепление потенциала отдельных государств-партнеров в сфере разработки мер реагирования в рамках национальной контртеррористической политики для противодействия использованию террористами новых технологий и применения новых технологий в деле борьбы с терроризмом при полном соблюдении прав человека и принципа верховенства права.
Направление 2: укрепление оперативного потенциала правоохранительных органов и органов уголовного правосудия для противодействия использованию новых технологий в террористических целях и применения новых технологий в деле предотвращения терроризма и борьбы с ним при полном соблюдении прав человека и принципа верховенства права.	
 **Компонент 2.1**	Предоставление практических инструментов и руководства для правоохранительных органов в целях противодействия использованию новых технологий в террористических целях и применения новых технологий в деле предотвращения терроризма и борьбы с ним при полном соблюдении прав человека и принципа верховенства права.
 **Компонент 2.2**	Развитие у специалистов правоохранительных органов и органов уголовного правосудия государств-партнеров навыков, направленных на противодействие использованию новых технологий в террористических целях и применение новых технологий в деле предотвращения терроризма и борьбы с ним при полном соблюдении прав человека и принципа верховенства права.
 **Компонент 2.3**	Расширение международного сотрудничества и обмена информацией между органами полиции государств-партнеров по вопросам противодействия использованию террористами новых технологий и применения новых технологий в борьбе с терроризмом.

1.3 Цель и назначение документа

Целью настоящего документа является предоставление руководства по созданию независимых эффективных механизмов обеспечения прозрачности и ведения надзорной деятельности за наблюдением в Интернете и сбором данных в Интернете, связанных с борьбой с терроризмом.

1.3.1 Сфера охвата

Настоящий документ призван повысить осведомленность о правах человека и проблемах неприкосновенности частной жизни в связи с практикой сбора данных в Интернете в рамках контртеррористической деятельности правоохранительных органов, а также предложить ряд рекомендаций в отношении надзора для обеспечения надлежащих гарантий в отношении практики сбора данных в Интернете в соответствии с международными нормами и практикой в области прав человека.

1.3.2 Целевая аудитория

Настоящее руководство предназначено в первую очередь для разработчиков политики. Кроме того, с его основными принципами и соответствующими механизмами следует ознакомиться представителям правоохранительных органов.

1.3.3 Преимущества

История изобилует примерами реагирования на террористические угрозы, которые порождали или усиливали существующее недовольство, что, в свою очередь, может стать питательной средой для терроризма и насильственного экстремизма, способствующего терроризму. Эффективные механизмы независимого надзора способствуют повышению подотчетности и прозрачности.

1.3.4 Ограничения

В настоящем руководстве не рассматриваются многочисленные проблемы, связанные с приобретением государственными учреждениями персональных данных, агрегированных в коммерческих целях, хотя эта практика вызывает серьезные вопросы, касающиеся неприкосновенности частной жизни. В нем также не рассматриваются вопросы надзора за частным сектором.

[II]

Подход

2.1 Обзор

Цель настоящего доклада заключается в том, чтобы предоставить государствам-членам поддержку и возможности для более полного соответствия международным нормам и стандартам в области прав человека при использовании новых технологий для предотвращения терроризма и борьбы с ним, уделяя особое внимание созданию эффективных и независимых механизмов обеспечения прозрачности и ведения надзорной деятельности за наблюдением в Интернете и сбором данных в Интернете в связи с борьбой с терроризмом. Доклад направлен на поддержку разработки эффективных ответных мер антитеррористической политики, которые соответствуют Глобальной контртеррористической стратегии Организации Объединенных Наций и реализуются при полном соблюдении принципа верховенства права и международных норм и стандартов в области прав человека.

2.2 Руководящая основа

РИСУНОК 2

Руководящей основой является концептуальная модель, которая выступает в качестве направляющего, синхронизирующего и информационного ориентира при подготовке доклада. Она призвана обеспечить согласованность Глобальной контртеррористической стратегии (ГКТС) Организации Объединенных Наций с национальной контртеррористической политикой и стратегией государства-члена на всех этапах — от разработки до реализации — на уровне целей и результатов, механизмов и потенциала правоохранительных органов и органов уголовного правосудия в отношении новых технологий.

ГКТС Организации Объединенных Наций, принятая Генеральной Ассамблеей, определяет широкий спектр действий государств-членов по борьбе с террористическими угрозами в рамках четырех основных направлений:

Направление I:	Меры по устранению условий, способствующих распространению терроризма
Направление II:	Меры по предотвращению терроризма и борьба с ним
Направление III:	Меры по укреплению потенциала государств по предотвращению терроризма и борьбе с ним и укреплению роли системы Организации Объединенных Наций в этой области
Направление IV:	Меры по обеспечению всеобщего уважения прав человека и принципа верховенства права в качестве фундаментальной основы для борьбы с терроризмом

Государствам-членам рекомендуется выработать собственные политико-правовые основы борьбы с терроризмом в соответствии с ГКТС Организации Объединенных Наций. Они должны обеспечить, чтобы принятые ими контртеррористические законы, политика, стратегии и меры отвечали их обязательствам по международному праву, включая международное право прав человека, международное беженское право и международное гуманитарное право. Политико-правовые основы борьбы с терроризмом государств-членов должны быть направлены на предотвращение и устранение насильственного экстремизма, который способствует терроризму, предотвращение террористической деятельности или ограничение возможностей для ее осуществления, принятие соответствующих мер по защите граждан, находящихся под юрисдикцией государства, а также служб и инфраструктуры от обоснованно предсказуемых угроз совершения террористических атак и привлечение террористов к ответственности за их деяния.

Для достижения намеченных результатов и целей в борьбе с терроризмом в распоряжении национальных правоохранительных органов и органов уголовного правосудия государств-членов имеется целый ряд инструментов. К ним относятся, среди прочего, следующие:

ТАБЛИЦА 2. **Механизмы национальных правоохранительных органов и органов уголовного правосудия высокого порядка в борьбе с терроризмом**

Механизм	Описание
Уголовное правосудие	Юридический процесс, который предусматривает предъявление обвинений в совершении уголовно наказуемого деяния физическому или юридическому лицу, проведение судебных слушаний, разрешение дела и назначение наказания, а также исправление и реабилитацию осужденных.
Оперативная информация	Информация, являющаяся результатом сбора, разработки, распространения, анализа и интерпретации данных, полученных из широкого круга источников, которая используется лицами, принимающими решения, в целях планирования последующих решений или действий на стратегическом, оперативном или тактическом уровнях. Сбор, хранение, использование и обмен оперативной информацией должны осуществляться в соответствии с обязательствами государств-членов по международному праву прав человека.
Уголовное расследование	Процесс сбора информации (или доказательств) для установления факта совершения преступления, выявления преступника и представления доказательств для уголовного преследования.
Действия правоохранительных органов	Этот термин, как правило, описывает действия правоохранительных органов, предпринятые для противодействия угрозе, которые могут включать задержание отдельных лиц, пресечение деятельности злоумышленников (например, удаление контента, арест активов) и т. д.
Реабилитация	В контексте уголовного правосудия термин «реабилитация» используется для обозначения мероприятий, проводимых исправительной системой с целью изменения взглядов или поведения правонарушителей, для того чтобы снизить вероятность повторного совершения ими преступления, а также подготовить и обеспечить их реинтеграцию в общество.
Реинтеграция	Комплексный процесс возвращения человека в социальную и (или) функциональную среду.

Эффективное использование и развертывание указанных механизмов и инструментов зависит от имеющихся возможностей. Нередко возможности, требуемые для обеспечения реализации механизмов, определяют и представляют с помощью модели возможностей. Модель возможностей состоит в распределении ключевых функций по логическим детализированным группам в процессе осуществления механизмов и мер. Модель возможностей определяет требования к персоналу (структуре и навыкам), процессам, технологиям, инфраструктуре и финансам.

Руководящая основа служит для обеспечения максимальной согласованности между стратегией и ее реализацией в обоих направлениях — «сверху вниз» и «снизу вверх».

2.3 Методология

РИСУНОК 3

Методология разработки настоящего документа «Создание законодательных рамок и механизмов обеспечения прозрачности для сбора данных в Интернете» предусматривает использование результатов исследований и аналитических материалов, а также проведение консультаций с соответствующими заинтересованными сторонами и экспертами, в том числе использование документов проекта CT TECH, проведение консультаций с заинтересованными сторонами, использование данных внутреннего анализа, проведение кабинетных исследований, совещаний экспертных групп, организация сотрудничества с различными структурами в рамках Глобального договора по координации контртеррористической деятельности, а также применение руководящей основы, описанной выше в разделе 2.2. К ключевым результатам этой деятельности относятся определение основных вопросов и проблем в области прав человека и неприкосновенности частной жизни, связанных со сбором данных в Интернете, а также ключевых аспектов для осуществления надзора с помощью законодательных механизмов и механизмов обеспечения прозрачности.

2.3.1 Совещания экспертных групп и консультации

Данное руководство было разработано при участии экспертов в рамках совещаний экспертных групп (СЭГ), а также по результатам индивидуальных консультаций и обзоров. СЭГ объединили экспертов и практиков из контртеррористических служб и правоохранительных органов, правозащитных организаций, частного сектора, научных кругов и гражданского общества для обсуждения вопросов, связанных с противодействием использованию новых технологий в террористических целях, применением новых технологий в рамках проводимой работы, определением передового опыта в этой области, а также для обсуждения рисков, проблем и неудачного опыта, требующих внимания и осторожности. Руководство было доработано в ходе взаимодействия со структурами Глобального договора по координации контртеррористической деятельности Организации Объединенных Наций и его Рабочей группой по новым угрозам и защите критически важной инфраструктуры, которая содействует координации и согласованности усилий, прилагаемых государствами-членами для предотвращения возникающих террористических угроз и реагирования на них с соблюдением прав человека и принципа верховенства права в качестве фундаментальной основы в соответствии с международным правом, включая международное право прав человека, международное гуманитарное право и международное беженское право.

2.3.2 Обзор справочных материалов

При разработке настоящего руководства были задействованы, приняты во внимание, дополнены и использованы в качестве основы данные имеющихся исследований, руководств и публикаций, среди которых:

ТАБЛИЦА 3. **Справочные материалы**

1	Глобальная контртеррористическая стратегия Организации Объединенных Наций.
2	Доклады Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век».
3	Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина, «Сборник примеров передовой практики по правовым и институциональным основам и мерам, обеспечивающим соблюдение прав человека спецслужбами в условиях борьбы с терроризмом, в том числе по вопросам надзора за ними».
4	«Состояние международного сотрудничества в области законного доступа к цифровым доказательствам», доклад о тенденциях ИДКТК, январь 2022 г.
5	Тшванские принципы национальной безопасности и права на информацию.
6	УНП ООН, «Руководство по подотчетности деятельности полиции, надзору за ней и обеспечению неподкупности».
7	ОЭСР, «Руководство по обеспечению публичной добропорядочности».
8	Совет Европы, «Практическое руководство по использованию персональных данных в полицейском секторе».
9	Доклад Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю, A/ HRC/23/40.

[III]

Введение

3.1 Обзор

По мере ускорения технологического прогресса террористы все чаще злоупотребляют инновациями в этой сфере для реализации своих разрушительных планов. Эксплуатация террористами быстрого распространения коммуникационных платформ, социальных сетей, шифровальных методов и новейших технологий создает серьезные проблемы для правоохранительных органов. Внедрение технологий в арсенал террористических групп создает беспрецедентные угрозы, требуя от правительств пересмотра стратегий и адаптации подходов.

При разработке контртеррористической политики государства-члены должны признать острую необходимость понимания, предвидения и эффективного реагирования на использование террористами новых технологий. Такая политика сосредоточена на ряде аспектов, включая осведомленность, меры по предотвращению угроз, национальные возможности по борьбе с терроризмом, сотрудничество и инициативы по наращиванию потенциала. Принимая комплексную, гибкую и отвечающую требованиям прав человека национальную контртеррористическую политику, правительства стремятся оставаться на шаг впереди, инициативно снижая риски, связанные со злоупотреблением террористами новыми технологиями, и одновременно обеспечивая безопасность и защиту прав лиц, находящихся под их юрисдикцией, включая право на неприкосновенность частной жизни.

3.2 Новые технологии и борьба с терроризмом

Развитие цифровых технологий, инноваций в области обработки и передачи данных и Интернета привело к созданию гиперсвязанного мира, в котором доступ к информации, обмен ею и ее получение происходят практически мгновенно. По состоянию на 2022 год почти 70 процентов населения мира пользуется Интернетом[14], из которых более 93 процентов — это пользователи социальных сетей[15]. По оценкам, в 2022 году в мире будет создано более 97 зеттабайт[16] информации[17]. В то время как подобные технологические достижения способствуют преобразованию общества во имя всеобщего блага, террористы используют эти технологии в злонамеренных целях. Применение новых технологий в террористических целях ставит перед государствами-членами серьезные задачи по борьбе с терроризмом, в частности, по противодействию использованию технологий, которые обеспечивают анонимность и позволяют координировать действия и действовать удаленно.

С другой стороны, новые технологии открывают широкие возможности для укрепления потенциала контртеррористических и правоохранительных органов. Например, с их помощью правоохранительные органы смогут выполнять большие объемы работы с меньшими затратами, принимать своевременные решения

14 Отчет МСЭ о глобальной возможности установления соединений за 2022 год, URL: https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index

15 Инфографика Data Never Sleeps от компании Domo, DataNeverSleeps 10.0 | Domo

16 Один зеттабайт равен одному миллиарду терабайтов.

17 Statista,Totaldatavolumeworldwide 2010-2025 (доклад «Общий объем данных по всему миру за 2010–2025 годы») | Statista

в ускоренном порядке, генерировать новые идеи и осуществлять противодействие удаленно. В то же время возникает обеспокоенность по поводу рисков для неприкосновенности частной жизни и осуществления прав человека в целом, обусловленных соответствующим законодательством, разрешающим использование таких технологий, которое зачастую не соответствует действующим международным стандартам в области прав человека, а также их применение правоохранительными органами.

Противодействие использованию новых технологий в террористических целях зависит от понимания механизмов такого использования, разработки эффективной правовой базы и мер реагирования на уровне политики, отвечающих требованиям в области прав человека, а также наращивания оперативного потенциала для противодействия применению таких технологий в террористических целях, включая освоение и использование новых технологий.

3.2.1 Вызовы: использование новых технологий в террористических целях

Достижения в области информационно-коммуникационных технологий (ИКТ) и их доступность сделали привлекательным для террористических и насильственных экстремистских групп использование Интернета и социальных сетей для совершения широкого спектра противоправных действий, включая подстрекательство к терроризму, радикализацию насилия, вербовку, обучение, планирование, сбор информации, коммуникацию, подготовку, пропаганду и финансирование. Террористы также используют зашифрованные коммуникации и дарквеб для обмена террористическим контентом и опытом, например, разработками самодельных взрывных устройств и стратегиями нападений, а также для координации нападений и содействия их совершению, приобретения оружия и поддельных документов. Между тем развитие технологий в области искусственного интеллекта, машинного обучения, телекоммуникаций 5G, робототехники, больших данных, алгоритмической фильтрации, биотехнологий, беспилотных автомобилей и летательных аппаратов может привести к тому, что, как только эти технологии станут коммерчески доступными, недорогими и удобными в использовании, их также смогут применять террористы для расширения диапазона и повышения уровня смертоносности своих атак.

3.2.2 Возможности: контртеррористическая деятельность правоохранительных органов

Новые технологии открывают перед правоохранительными органами ценные возможности для эффективного противодействия терроризму при условии применения в соответствии с международным правом прав человека. Правоохранительные органы могут использовать новые технологии для выявления, расследования, судебного преследования и разрешения дел о преступлениях, связанных с терроризмом, новыми и более эффективными способами.

Использование оперативной информации из открытых источников обеспечивает быстрый сбор данных об интересующих объектах, что может повысить эффективность правоохранительной деятельности. Передовые технологии анализа данных и искусственного интеллекта (ИИ) позволяют обрабатывать и анализировать огромные объемы информации, благодаря чему правоохранительные органы имеют возможность выявлять закономерности, обнаруживать потенциальные угрозы и принимать превентивные меры реагирования на террористическую деятельность. Новейшие системы наблюдения, включая распознавание лиц и биометрические технологии, помогают идентифицировать и отслеживать перемещения подозреваемых, повышая эффективность расследований, предотвращая потенциальные атаки и привлекая предполагаемых террористов к ответственности. Кроме того, с помощью инструментов цифровой криминалистики можно получать важные доказательства путем извлечения данных из электронных устройств, что позволяет правоохранительным органам выявлять скрытые связи, разрушать террористические сети и привлекать предполагаемых террористов к ответственности.

Использование новых технологий может способствовать более эффективному распределению ограниченных ресурсов правоохранительных органов. При этом крайне важно, чтобы эти технологии использовались с учетом этических норм и при строгом соблюдении принципа верховенства права и международных норм и стандартов в области прав человека, в том числе права на неприкосновенность частной жизни. Необходимо внедрить меры и механизмы для обеспечения прозрачности и подотчетности, чтобы гарантировать ответственное использование и предотвратить потенциальное злоупотребление этими мощными инструментами. Кроме того, рекомендуется внедрить комплексные программы обучения, для того чтобы сотрудники правоохранительных органов могли овладеть необходимыми навыками с целью эффективного применения новых технологий с уче-

том международных норм и стандартов в области прав человека, а также в рамках правовых и этических норм. Ответственно подходя к использованию новых технологий, правоохранительные органы могут значительно расширить свои усилия по борьбе с терроризмом и обеспечить безопасность и защиту населения.

3.2.3 Права человека и новые технологии

Терроризм бросает серьезный вызов самим принципам верховенства права, защиты прав человека и их эффективного осуществления. Он может дестабилизировать законно сформированные правительства, подорвать плюралистическое гражданское общество, поставить под угрозу мир и безопасность и иметь отрицательные последствия для социально-экономического развития. Государства обязаны принимать надлежащие меры для защиты граждан, находящихся под их юрисдикцией, от обоснованно предсказуемых угроз совершения террористических атак. Обязанность государств защищать права человека предполагает принятие необходимых и адекватных мер для предотвращения, пресечения и привлечения к ответственности за совершение действий, ставящих под угрозу эти права, таких как угроза национальной безопасности или насильственные преступления, включая терроризм. Все подобные меры должны отвечать стандартам международного права прав человека и принципа верховенства права.

В контексте использования новых и новейших технологий в контртеррористической деятельности государства должны обеспечить, чтобы соответствующие законы, политика и практика гарантировали соблюдение таких прав, как право на неприкосновенность частной жизни, право на свободу выражения мнений, свободу ассоциации, свободу мысли, совести, убеждений и религии, право на свободу и личную неприкосновенность, право на справедливое судебное разбирательство, включая презумпцию невиновности, а также принцип недискриминации. Кроме того, государства должны строго соблюдать принцип абсолютного запрета пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания.

ООН, Интерпол и ЕС неоднократно подчеркивали взаимосвязь между новыми технологиями, борьбой с терроризмом и правами человека, включая гендерное равенство. В Глобальной контртеррористической стратегии ООН и различных резолюциях Генеральной Ассамблеи и Совета Безопасности подчеркиваются обязательства государств-членов по соблюдению международного права прав человека, международного беженского права и международного гуманитарного права в деле противодействия терроризму. В частности, согласно Глобальной контртеррористической стратегии ООН «действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга», в связи с чем необходимо принять меры по обеспечению всеобщего уважения прав человека и принципа верховенства права в качестве фундаментальной основы борьбы с терроризмом. В связи с этим в Стратегии государствам-членам предлагается бороться с использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе с непрекращающимся распространением террористического контента, при соблюдении международного права, включая международное право прав человека, а также право на свободу выражения мнений.

3.2.4 Гендер, технологии и меры реагирования на уровне политики

Понятие «гендер» охватывает роли, поведение, занятия и качества, которые в конкретном обществе в определенный период времени считаются подходящими для мужчин и женщин, девочек и мальчиков. Помимо социальных атрибутов и возможностей, ассоциируемых с принадлежностью к мужскому или женскому полу, гендер связан с отношениями между женщинами и мужчинами, девочками и мальчиками. Гендер является частью более широкого социокультурного контекста и пересекается с другими факторами идентичности, включая пол, социальный класс, расовую принадлежность, уровень бедности, этническую принадлежность, сексуальную ориентацию, возраст и т. д. Мужчины, женщины, девочки и мальчики, а также лица с другими гендерными идентичностями и моделями самовыражения чувствуют себя в безопасности по-разному и в соответствии со своими особыми потребностями, уязвимостями и возможностями[18]. В частности, несмотря на отсутствие иерархических структур в Интернете, которое позволяет устранить гендерные ограничения и создает возможности для расширения прав и возможностей женщин, использование новых технологий так-

18 ДКВС, БДИПЧ ОБСЕ, Структура «ООН-женщины», «Гендер и реформирование сектора безопасности: комплект учебных материалов» (Женева: ДКВС, 2008 г.), URL: https://www.dcaf.ch/gender-and-security-toolkit

же повышает вероятность их вербовки или активного участия в деятельности насильственных экстремистских и террористических групп в Интернете[19]. Имеющиеся данные свидетельствуют о том, что в своих целях террористические группировки умело используют гендерный фактор — неравенство, нормы и роли, включая маскулинность, — и манипулируют им. Так, ИГИЛ мастерски вербует женщин через социальные сети, адаптируя свои послания для обращения к лицам женского пола, говорящим на разных языках и живущим в разных социальных, экономических и культурных условиях в Западной Европе, Центральной Азии, на Ближнем Востоке и в Северной Африке, и нередко эксплуатируя опыт женщин в области гендерного неравенства. Еще один важный аспект, касающийся гендера и новых технологий, связан с цифровым гендерным разрывом, согласно которому во всем мире доступ женщин к Интернету оценивается в 85 процентов по сравнению с мужчинами, при этом около 1,7 млрд женщин из стран Глобального Юга вообще не имеют доступа к нему. Такое неравенство создает проблемы в области прав человека, лежащие в основе всех аспектов кибербезопасности, включая потенциальную подверженность риску, отсутствие безопасности или участие в структуре управления[20].

19 ИДКТК, «Гендерные аспекты мер реагирования, принимаемых в связи с возвращением иностранных боевиков-террористов: перспективы исследований», февраль 2019 г.

20 ДКВС, «Гендерное равенство, кибербезопасность и управление сектором безопасности: понимание роли гендера в управлении кибербезопасностью», январь 2023 г.

[IV] Сбор данных в Интернете правоохранительными органами

4.1 Обзор

По мере ускорения технического прогресса террористы все чаще используют коммуникационные платформы, социальные сети, методы шифрования и другие новые и перспективные технологии для вербовки и организации членов группировок, приобретения оружия, финансирования операций, а также для планирования, поддержки, совершения и сокрытия террористических актов. В то же время эти же технологии предоставляют правоохранительным органам новые инструменты для выявления потенциальных подозреваемых в терроризме, наблюдения за членами террористических организаций, отслеживания их деятельности и пресечения их операций. Однако по мере того как новые технологии облегчают выявление, наблюдение и управление, возрастает угроза основным правам, включая право на неприкосновенность частной жизни, свободу выражения мнений и объединений, а также недискриминацию, а в качестве предлога для оправдания навязчивого сбора данных в Интернете зачастую неправомерно используются соображения национальной безопасности. Если соответствующие технологии могут быть новыми, то опасности, связанные с нерегулируемым наблюдением, таковыми не являются. Еще в 1978 году Европейский суд по правам человека отметил, что «[о]сознавая опасность, что [нерегулируемое наблюдение] может подорвать и даже уничтожить демократию под предлогом ее защиты, Суд утверждает, что [...] Государства не могут во имя борьбы против шпионажа и терроризма предпринимать любые действия, которые они считают подходящими»[21]. Аналогичным образом, согласно Глобальной контртеррористической стратегии ООН «действенные меры по борьбе с терроризмом и защита прав человека являются целями, которые не противоречат, а дополняют и взаимно подкрепляют друг друга»[22]. Тем не менее государства-члены регулярно осуществляют электронное и цифровое наблюдение за представителями гражданского общества, журналистами и лицами, которые просто не согласны со своими правительствами, и используют собранную информацию для преследования, репрессий и принуждения к молчанию под предлогом национальной безопасности.

В ответ на растущую обеспокоенность по поводу стремительного роста наблюдения со стороны государства с помощью новых технологий Генеральная Ассамблея приняла резолюцию 73/179, подтверждающую право на неприкосновенность частной жизни и призывающую государства «создавать новые или продолжать использовать уже имеющиеся независимые, эффективные, обеспеченные надлежащими ресурсами и беспристрастные внутренние механизмы судебного, административного и/или парламентского надзора, позволяющие обеспечивать прозрачность, сообразно обстоятельствам, и подотчетность в связи с осуществлением государствами слежения за сообщениями, их перехвата и сбора персональных данных»[23]. Действенный надзор и надлежащее возмещение ущерба, в том числе с использованием судебного надзора или других правовых средств, являются принципами, подтвержденными в седьмом и восьмом обзорах Глобальной контртеррористической стратегии Организации Объединенных Наций[24].

К передовой практике и механизмам должны относиться: четкие и точные внутренние инструкции по доступу правоохранительных органов к данным в Интернете, которые должны предоставляться соответствующим сотрудникам до получения доступа к персональным данным; внутренний контроль за сбором данных

21 Европейский суд по правам человека, *Класс и другие* против *Германии*, № 5029/71, 6 сентября 1978 г., п. 49.

22 A/RES/60/288, Преамбула к направлению IV.

23 A/RES/73/179, пункт постановляющей части 6 *d*).

24 A/RES/75/291, п. 106 (седьмой обзор), A/RES/77/298, п. 110 (восьмой обзор).

во время операций; получение предварительного независимого разрешения на сбор определенных видов информации; независимый надзор за правоохранительными операциями во время и после операций; а также доступ к механизмам возмещения ущерба и предоставление эффективных средств правовой защиты жертвам нарушений прав человека.

4.2 Терминология: сбор данных в Интернете и наблюдение в Интернете

Несмотря на то что термины «сбор данных в Интернете» и «наблюдение в Интернете» (или «цифровое наблюдение)» часто используются как взаимозаменяемые, между ними есть разница. Под сбором данных в Интернете понимается процесс сбора, хранения и обработки информации о лицах и их действиях в Интернете. Сбор информации может осуществляться с помощью файлов cookie на сайте, регистрации пользователей, онлайн-опросов и т. д. В Европе, в частности, такой сбор требует ознакомления и согласия пользователя. Что касается всех видов государственной деятельности, сбор персональных данных в Интернете должен регулироваться, служить законной цели, установленной законодателем, быть соразмерным и необходимым для достижения этой законной цели и использоваться для этой цели[25], однако сбор и обработка этих данных не обязательно требуют предварительного независимого разрешения и строгого надзора.

Например, полицейскому, остановившему автомобиль за нарушение правил дорожного движения, может не потребоваться предварительное разрешение суда для проверки водительских прав по базе данных водителей, лишенных права на управление транспортным средством, или номерного знака по базе данных угнанных автомобилей. Кроме того, водители, имеющие права на управление транспортным средством, знают, что их персональные данные собираются, хранятся и обрабатываются государственными органами в целях обеспечения безопасности дорожного движения.

При этом доступ к некоторым категориям данных, таким как генетические данные, персональные данные, связанные с правонарушениями, уголовными делами и приговорами, и связанные с ними меры безопасности, биометрические данные, однозначно идентифицирующие человека, персональные данные, содержащие информацию о расовом или этническом происхождении, политических взглядах, членстве в профсоюзах, религиозных или иных убеждениях, состоянии здоровья или сексуальной жизни, может обрабатываться только в том случае, если это предусмотрено законом и приняты соответствующие меры защиты для устранения потенциального риска дискриминации или неблагоприятных правовых последствий, существенно влияющих на субъектов данных. Такие меры могут носить технический характер, например, дополнительные мероприятия в области безопасности, а также организационный характер. Защитные меры должны быть адаптированы к каждой операции по обработке данных с учетом их специфики. Настоятельно рекомендуется использовать несколько уровней защиты для этих категорий данных (например, хранение на отдельных серверах, более короткие периоды хранения данных и т. д.). Кроме того, крайне важно принять специальные меры безопасности для предотвращения несанкционированного или нежелательного доступа к этим категориям данных[26].

В отличие от обычного сбора и обработки данных, наблюдение в Интернете предполагает мониторинг онлайн-активности конкретных физических и юридических лиц силами безопасности, как правило, без их ведома или согласия. Отсутствие осведомленности и согласия требует более строгого надзора, вплоть до полной прозрачности в любое время.

Поскольку все формы наблюдения — физического, электронного и цифрового — в целом поднимают более важные вопросы конфиденциальности, они требуют более строгого надзора, нежели иные формы сбора персональных данных. В настоящем руководстве основное внимание уделяется сбору персональных данных в контексте операций по наблюдению.

25 См. например, Совет Европы, «Практическое руководство по использованию персональных данных в полицейском секторе», разделы 2 и 3, URL: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

26 Совет Европы, «Практическое руководство по использованию персональных данных в полицейском секторе», раздел 4, URL: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

4.3 Метаданные

Метаданные обычно определяются как «свод данных, описывающих другие данные и сообщающих информацию о них». Изначально считалось, что сбор метаданных, относящихся к сообщениям, представляет меньшую опасность, чем сбор содержания сообщений. Например, Европейский суд по правам человека постановил, что коммуникационные данные являются «неотъемлемой частью» частного сообщения и, соответственно, к ним применяется степень защиты в соответствии со статьей 8, хотя и в меньшей степени по сравнению с защитой, которая предоставляется содержанию сообщения[27]. Однако благодаря развитию технологий метаданные, включая идентификацию владельца IP-адреса, абонентские данные, идентификатор мобильного устройства или IP-адрес электронного письма, идентификатор мобильного абонента (IMSE) и адреса электронной почты, могут оказаться весьма информативными в экосистеме, где люди оставляют свои «электронные следы» в своем цифровом контенте. Таким образом, метаданные могут выступать в роли аналога защищенного содержания сообщений, и, как следствие, сбор таких данных может быть весьма навязчивым[28]. Суд Европейского союза, например, пришел к выводу, что «данные, взятые в целом, могут позволить сделать очень точные выводы относительно частной жизни лиц, чьи данные были сохранены, например, их повседневных привычек, постоянного или временного места жительства, ежедневных или иных передвижений, деятельности, социальных отношений этих лиц и социальной среды, частью которой они являются. В частности, эти данные позволяют составить профиль соответствующих лиц — информацию, которая, с учетом права на неприкосновенность частной жизни, является не менее чувствительной, чем фактическое содержание сообщений»[29]. Таким образом, различия между идентифицирующими персональными данными и кажущимися анонимизированными метаданными становятся все более искусственными и с трудом обоснуемыми.

4.4 Руководящие принципы

Согласно международному праву прав человека, государства могут отступать[30] от определенных прав и налагать ограничения на их осуществление. Тем не менее существуют абсолютные права, и никакие ограничения таких прав и отступления от них не допускаются[31]. Для целей настоящего руководства ниже описаны условия, применяемые к ограничениям и отступлениям от прав, которые это допускают. Любое вмешательство в такие права человека, как право на неприкосновенность частной жизни, свободу выражения мнений и объединений, должно быть предусмотрено законом и необходимо для достижения законной цели (включая охрану государственной безопасности, общественного порядка, безопасности граждан, прав и свобод других лиц). Любые меры также должны основываться на принципах необходимости и соразмерности. В связи с этим ограничения прав человека всегда должны осуществляться с учетом запрета на дискриминацию[32].

---

27 См. Европейский суд по правам человека, *Big Brother Watch and other* против *Соединенного Королевства* и *Мейлоун* против *Соединенного Королевства*, (1985), п. 84.

28 Экспертное заключение Amici Curiae Article 19, Electronic Frontier Foundation, Fundación Karisma и Privacy International для Межамериканского суда по правам человека по делу *Члены коллегии адвокатов «Хосе Альвеар Рестрепо* против *Колумбии*, с. 10, URL: https://www.law.berkeley.edu/wp-content/uploads/2022/05/Amicus-Brief-CCAJAR-v.-Colombia.pdf

29 Решения по делу C-623/17, Privacy International и по объединенным делам C-511/18, La Quadrature du Net и другие, C-512/18, French Data Network и другие, C-520/18, Ordre des barreaux francophones et germanophone и другие, п. 117.

30 В чрезвычайных ситуациях, при которых «жизнь нации находится под угрозой», государства имеют право временно корректировать некоторые обязательства в области прав человека при соблюдении ряда условий. Об отступлениях см. Замечание общего порядка № 29 Комитета по правам человека о чрезвычайном положении (Статья 4), CCPR/C/21/Rev.1/Add.11.

31 К ним относятся запрет на применение пыток и жестоких, бесчеловечных или унижающих достоинство видов обращения или наказания, на рабство и подневольное состояние, а также принцип законности, согласно которому никто не может быть наказан за поступок, не запрещенный законом. Абсолютный характер этих прав означает, что их нельзя ограничивать, увязывая их осуществление с преследованием законной цели, в том числе в случае вооруженного конфликта или любого чрезвычайного положения.

32 См., например, Сиракузские принципы о положениях, касающихся ограничения и умаления прав в Международном пакте о гражданских и политических правах (E/ CN.4/1985/4, приложение); Замечание общего порядка № 37 Комитета по правам человека о праве на мирные собрания (статья 21), CCPR/C/GC/37, пп. 36 и 46; Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 32.

4.4.1 Закрепление в законе

Любые контртеррористические меры, ограничивающие права человека, должны быть основаны на национальном законодательстве. Национальная правовая база должна быть достаточно предсказуемой, доступной и обеспечивать адекватные гарантии от злоупотреблений, в том числе проведение независимых проверок и надзора, а также содержать эффективные средства правовой защиты на случай нарушения прав человека. Предсказуемость означает, что закон должен быть сформулирован достаточно четко, чтобы дать возможность частному лицу соответствующим образом корректировать свои действия[33], а компетентным органам — определить, когда права могут быть ограничены, а также установить объем и порядок осуществления любых предоставленных им дискреционных полномочий[34]. Закон должен быть в достаточной степени доступен, чтобы частные лица имели возможность ознакомиться с его содержанием[35]. Решение о санкционировании вмешательства в право на неприкосновенность частной жизни, например, посредством выдачи ордера, должно приниматься только конкретным независимым органом, предусмотренным законом, и строго индивидуально[36]. Секретные правила, руководства и толкования правил не обладают необходимыми качествами «закона»[37]. Наконец, законы должны быть приняты демократическим путем[38].

4.4.2 Законная цель

Ограничения прав человека должны быть необходимы для достижения законных целей охраны государственной безопасности, общественного порядка/безопасности граждан, здоровья и морали, равно как и основных прав и свобод других лиц[39]. «Интересы государственной безопасности» могут служить основанием для введения ограничений, «если такие ограничения необходимы для сохранения способности государства защищать существование нации, свою территориальную целостность или политическую независимость от реальной угрозы или применения силы»[40].

При этом известны случаи, когда государства неправомерно ссылались на императивы государственной безопасности, в частности на борьбу с терроризмом, в качестве предлога для оправдания не имеющего четкого определения произвольного вмешательства в права человека. «Использование аморфной концепции национальной безопасности для обоснования интрузивных ограничений пользования правами человека является предметом серьезной обеспокоенности. Данная концепция имеет широкое определение и в этой связи явля-

---

33 См., например, Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 25ff; Европейский суд по правам человека, *«Санди Таймс»* против *Соединенного Королевства* (№ 1), жалоба № 6538/74, 26 апреля 1979 г., § 49.

34 См., например, Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 25; Европейский суд по правам человека, *Мейлоун* против *Великобритании*, жалоба № 8691/79, 2 августа 1984 г., §§ 66–68.

35 См., например, Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 25; Европейский суд по правам человека, *«ГроппераРадиоАГ» и другие* против *Швейцарии*, жалоба № 10890/173, Серия A № 173, 28 марта 1990 г., §§ 65–68.

36 Замечание общего порядка № 16 Комитета по правам человека, п. 8, URL: https://www.refworld.org/docid/453883f922.htmlml

37 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/27/37, п. 29. См. также Европейский суд по правам человека, *Мейлоун* против *Соединенного Королевства*, (1985 г.), 7 ЕСПЧ 14, пп. 67 и 68, URL: https://www.stradalex.com/nl/sl_src_publ_jur_int/document/echr_8691-79; Африканская комиссия по правам человека и народов, «Принципы и руководящие положения по правам человека и народов в условиях борьбы с терроризмом в Африке», Часть 11, A: Правовая база, касающаяся любого вмешательства в частную жизнь, а также порядок такого вмешательства, должны быть доступны широкой общественности. URL: https://achpr.au.int/sites/default/files/files/2021-05/principlesandguidelinesonhumanandpeoplesrightswhilecounteringterrorisminafrica.pdf

38 См. Африканский суд по правам человека и народов, *XYZ* против *Республики Бенин*, Решение 27 ноябрь 2022 г., пп. 101 и 102, заключающее, что оспариваемый закон был незаконно принят в упрощенном порядке и что нераспространение информации о законе дополнительно представляло собой нарушение права на информацию, пп. 118–121. URL: https://africanlii.org/afu/judgment/african-court/2020/3

39 См., например, ЕСПЧ, Статья 8 (2); МКПЧ, Статьи 13 (2) (b) и 30; АСПЧН, Статья 11. См. также Африканская комиссия по правам человека и народов, Принципы и руководящие положения по правам человека и народов в условиях борьбы с терроризмом в Африке, Общий принцип M.

40 Сиракузские принципы о положениях, касающихся ограничения и умаления прав в Международном пакте о гражданских и политических правах (E/ CN.4/1985/4, приложение), п. 29; Замечание общего порядка № 37 Комитета по правам человека о праве на мирные собрания (Статья 21), CCPR/C/ GC/37, п. 42.

ется уязвимой для манипуляций со стороны государства, которое рассматривает ее в качестве средства для оправдания действий, которые направлены против таких уязвимых групп, как правозащитники, журналисты или мирные активисты. Она также используется для обоснования зачастую ненужной секретности вокруг расследований или действий правоохранительных органов, подрывая принципы прозрачности и подотчетности[41].

4.4.3 Необходимость и соразмерность

Сами по себе ограничения должны применяться не только для достижения законной цели, но также быть необходимыми для защиты этой цели. Требование необходимости превышает/устанавливает более высокий порог, нежели просто «обоснованность или целесообразность». По сути, мера нарушает критерий необходимости, если защита может быть обеспечена другими способами, не ограничивающими рассматриваемое право.

Меры по ограничению допускающего ограничения права должны быть соразмерны преследуемой законной цели; кроме того, они должны соответствовать своей функции защиты и должны представлять собой наименее интрузивное среди тех средств, которые могут способствовать достижению желаемого результата, а также быть соразмерны интересу, который необходимо защитить[42]. Например, в одном из рассматриваемых дел Европейский суд по правам человека постановил, что «всеобъемлющая без каких-либо оговорок» природа права хранения ДНК представляла собой «несоразмерное вмешательство» в частную жизнь лиц, у которых были взяты данные. Суд придал особое значение тому факту, что для хранения материала «не был установлен предел времени» вне зависимости от характера или тяжести преступления, а также возраста подозреваемого, что особенно уместно в данном деле, поскольку один из обвиняемых был оправдан, а дело в отношении второго было прекращено[43].

4.4.4 Отсутствие дискриминации

Запрет на дискриминацию в международном праве в области прав человека является абсолютным, и никакие ограничения и отступления от данного права не допускаются вне зависимости от наличия чрезвычайной ситуации[44]. Основаниями, по которым запрещена дискриминация, являются, помимо прочих, пол, расовая принадлежность, цвет кожи, этническое происхождение, язык, религия, политические или иные убеждения, национальное или социальное происхождение или иное положение.

---

41 Доклад Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю, A/ HRC/23/40, п. 58, URL: http://www.ohchr.org/Documents/HRBodies /HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

42 См., например, Замечание общего порядка № 31 Комитета по правам человека, п. 6. Африканская комиссия по правам человека и народов, «Принципы и руководящие положения по правам человека и народов в условиях борьбы с терроризмом в Африке», Общий принцип M, URL: https://achpr.au.int/sites/default/files/files/2021-05/principlesandguidelinesonhumanandpeoplesrightswhilecounteringterrorisminafrica.pdf

43 Европейский суд по правам человека, *S. и Марпер* против *Соединенного Королевства* (2009 г.) 48 ЕСПЧ 50, п. 118. По данному делу один из обвиняемых был оправдан, а дело против второго было прекращено. Правительство Соединенного Королевства само признало, что хранение данных ДНК «не было ни оправдано какими-либо подозрениями в причастности заявителей к преступлению или склонности к преступлению, ни направлено на сохранение сведений в отношении расследованных предполагаемых преступлений в прошлом». Также о принципе соразмерности см. Межамериканский суд по правам человека, *Роше Азанья* против *Никарагуа*. Обстоятельства и возмещение ущерба. Решение от 3 июня 2020 г., Серия C № 403, п. 53.

44 См., например, Всеобщую декларацию прав человека (Статьи 1 и 2) и Международный пакт о гражданских и политических правах (Статья 26), а также Конвенцию о ликвидации всех форм расовой дискриминации (CERD). Межамериканский суд по правам человека, например, постановил, что «принцип равенства перед законом, равной защиты перед законом и недопущения дискриминации относится к jus cogens, поскольку на нем основывается вся правовая структура национального и международного общественного порядка и этот принцип проходит через все право». Межамериканский суд по правам человека, консультативное заключение OC-18/03 о правовом положении и правах мигрантов без документов, 17 сентября 2003 г., п. 101. Африканская комиссия по правам человека и народов, «Принципы и руководящие положения по правам человека и народов в условиях борьбы с терроризмом в Африке», Общий принцип G. Комитет по ликвидации расовой дискриминации призвал государства обеспечить, чтобы любые меры, принимаемые в рамках борьбы с терроризмом, не являлись по своей цели или последствиям дискриминационными по признаку расы, цвета кожи, сословного, национального или этнического происхождения и чтобы иностранные граждане и лица без гражданства не подвергались расовому или этническому профилированию или стереотипированию.

4.5 Права субъектов данных

Международное право, касающееся прав субъектов данных, разработано в недостаточной степени. Соответствующие правовые нормы Европейского союза запрещают произвольное вмешательство, помимо прочего, в право на неприкосновенность частной жизни, свободу выражения мнений, включая право на поиск информации[45], право на свободу объединений и запрет на дискриминацию.

По своей сути право Европейского союза требует как минимум, чтобы лица, которых затрагивает сбор и обработка данных в Интернете, имели право быть осведомленными об осуществлении сбора и обработки их персональных данных, иметь доступ к хранящимся данным, обеспечивать исправление неточных или устаревших данных, а также удалять или исправлять данные, хранящиеся незаконно или без необходимости. Кроме того, они имеют право возражать против обработки своих персональных данных, если государство или организация, осуществляющая обработку данных, не приведет законных оснований для сбора и обработки этих данных, и имеют право на средства правовой защиты в случае нарушения их прав[46].

Тем не менее в контексте правоохранительной деятельности и операций могут вводиться ограничения данных общих правил, если такие ограничения предусмотрены законом, соответствуют сути основных прав и свобод и представляют собой необходимую и соразмерную меру в демократическом обществе, в том числе для защиты национальной безопасности или предотвращения, расследования и преследования уголовных преступлений[47]. Например, при проведении расследования и ведении наблюдения за подозреваемым, представляющим высокий уровень риска, обработка данных и долгосрочное хранение данных могут быть оправданы без уведомления лица, за которым ведется наблюдение при условии, что оповещение объекта наблюдения может нанести ущерб текущему или запланированному расследованию. Однако при достижении цели скрытого наблюдения и отсутствии иных ограничений объект должен быть проинформирован о том, что в отношении него была применена такая мера. К другим обстоятельствам, при которых ограничение права на доступ к информации, связанной с обработанными данными, может быть оправданно, относится, например, случай, при котором предоставление информации субъекту данных может поставить под угрозу безопасность свидетеля или информатора. Кроме того, если конкретные оперативные данные указывают на то, что операции по отмыванию денег проводились с целью финансирования террористических операций, данные, собранные о частных лицах, могут храниться с разрешения внешнего надзорного органа в течение более длительного периода, чем это может быть строго необходимо для целей индивидуального расследования. В то же время сокрытие информации об обработке данных полицией должно применяться лишь в редких случаях и при наличии четкого обоснования[48].

45 Свобода получения и передачи информации является неотъемлемой частью основного права на свободу выражения мнений. См., например, URL: https://www.un.org/ruleoflaw/thematic-areas/governance/freedom-of-information/#:~:text=Freedom%20of%20information%20is%20an,right%20of%20freedom%20of%20expression

46 Совет Европы, Модернизированная конвенция 108 о защите физических лиц при автоматизированной обработке персональных данных. См. также Статью 21 Общего регламента Европейского союза по защите данных и Статью 18 (1) Конвенции Африканского союза о кибербезопасности и защите персональных данных (Конвенция Малабо).

47 Там же, Статья 11.

48 Совет Европы, «Практическое руководство по использованию персональных данных в полицейском секторе», разделы 5, 7. URL: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

[V] Механизмы обеспечения прозрачности и ведения надзорной деятельности

5.1 Обзор

Несмотря на весьма незначительное количество международных или региональных документов, определяющих тип надзорных механизмов, требуемых от государств-членов, из материальных обязательств вытекают обязательства процессуального характера. Европейский суд по правам человека постановил, что для обеспечения прав и свобод Конвенция обязывает высшие органы власти договаривающихся государств не только соблюдать соответствующие права, но также предотвращать или устранять любые нарушения на нижестоящих уровнях[49].

Передовая практика требует как минимум наличия внутренних правил, касающихся сбора и обработки данных; санкционирования независимым органом, как правило, судебным, сбора данных с высокой степенью интрузивности, например, операций по наблюдению; наличия эффективных гражданских надзорных органов во время и после проведения правоохранительных операций; доступности и распространения информации о сборе и обработке персональных данных правительством; существования эффективных независимых органов, способных обеспечить средства правовой защиты в случае нарушения прав субъектов, включая судебные органы.

Для того чтобы система надзора была эффективной, рекомендуется иметь как минимум шесть взаимозависимых компонентов надзора и контроля, включая:

- внутренний надзор в правоохранительных органах;
- исполнительный контроль (контроль над политикой, финансовый контроль и горизонтальный надзор со стороны государственных органов);
- парламентский надзор (члены парламента, парламентские комиссии по расследованию);
- судебный контроль;
- надзор со стороны независимых органов, таких как национальные институты по правам человека, омбудсмены и т. д.;
- надзор со стороны гражданского общества[50].

49 *Ассанидзе* против *Грузии* (71503/01) — решение от 8 апреля 2004 г.

50 Совет Европы, Механизмы полицейского надзора в государствах — членах Совета Европы, раздел 3, с. 67, URL: https://rm.coe.int/police-oversight-mechanisms-in-the-coe-member-states/16807175dd

5.2 Эффективные надзорные органы

Для обеспечения эффективности надзорные органы должны иметь возможность инициировать и проводить независимые расследования, обладать достаточными ресурсами — бюджетом, знаниями и опытом, материалами, — а также иметь полный беспрепятственный доступ к информации, инфраструктуре и должностным лицам[51]. Например, надзорные органы должны иметь доступ ко всей соответствующей информации вне зависимости от уровня ее секретности, если они считают, что она необходима для выполнения их функций. Доступ надзорных органов к информации должен быть закреплен в законе, определяющем их функции и полномочия. На любые попытки ограничить доступ надзорных органов к секретной информации должен налагаться запрет, и в случае необходимости такие попытки должны подвергаться санкциям. Тем не менее может возникнуть необходимость исключить из публичных отчетов информацию, указывающую на потенциальные цели, свидетелей и отдельные методы.

Правоохранительные органы получают все более широкие возможности для сбора, обмена и получения информации, используя для этих целей все более сложные комплексные системы. Соответственно, надзорным органам может потребоваться независимая техническая экспертиза для понимания функционирования различных систем.

5.2.1 Независимые надзорные органы

«Независимые надзорные механизмы» независимы от политических, экономических, военных или иных целей. Они обладают: 1) формальной (де-юре) независимостью, требующей, чтобы они оставались вне бюрократической, иерархической системы подчинения в министерстве или других государственных учреждениях; и 2) фактической (де-факто) независимостью, связанной с самоопределением органа при проведении расследований и обеспечении или рекомендации возмещения ущерба[52].

5.3 Предварительное независимое разрешение на проведение операций по наблюдению и специальных расследований

Комитет по правам человека отмечает, что решение о выдаче разрешения на любое вмешательство в право на неприкосновенность частной жизни должно приниматься только конкретным органом, предусмотренным законом, и строго индивидуально[53]. Европейский суд по правам человека указывает на то, что санкционирующий наблюдение орган необязательно должен являться судебным органом, однако такой несудебный орган должен быть достаточно независим от исполнительной власти. В то же время Суд отметил, что вмешательство властей в права частного лица должно быть предметом эффективного контроля, который обычно должен обеспечиваться судебной властью, по крайней мере в последней инстанции, причем судебный контроль дает наилучшие гарантии независимости, беспристрастности и надлежащего порядка. Суд также счел, что несмотря на то что выдача разрешения до вмешательства не является абсолютным требованием как таковым, в некоторых обстоятельствах судебный контроль после вмешательства может быть недостаточным, чтобы компенсировать его отрицательное воздействие, и поэтому судебное санкционирование

51 Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина. Подборка оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью, A/HRC/14/46, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

52 См., например, ОЭСР, «Руководство по обеспечению публичной добропорядочности», раздел 12.2.3, URL: https://www.oecd-ilibrary.org/sites/7715f0e0-en/index.html?itemId=/content/component/7715f0e0-en

53 Замечание общего порядка № 16, п. 8.

до факта вмешательства представляется необходимым[54]. Этот принцип применим как к целевому, так и к нецелевому наблюдению. Кроме того, выдача разрешения должна быть основана на конкретных фактах. Например, Межамериканский суд по правам человека выразил обеспокоенность по поводу того, что национальный суд выдал разрешение на наблюдение, несмотря на то, что в запросе на него не были указаны какие-либо причины или основания. Он также отметил, что органы, запросившие разрешение, не указали, что менее интрузивные средства получения информации были недоступны[55].

На проведение особо интрузивных правоохранительных операций, прежде чем приступить к осуществлению любых из следующих видов деятельности непосредственно или во взаимодействии/в сотрудничестве с организациями частного сектора, необходимо получить предварительное разрешение независимого органа:

- осуществление целевого наблюдения, включая сбор и доступ в отношении коммуникационных данных (в том числе если они находятся в частном секторе);
- осуществление нецелевого массового наблюдения, независимо от используемых методов или технологий или типа коммуникаций, являющихся объектом наблюдения;
- использование селекторов или ключевых слов для извлечения данных из информации, собранной в рамках массового наблюдения, особенно когда эти селекторы относятся к лицам, поддающимся идентификации;
- сбор коммуникаций/метаданных напрямую или доступ к ним посредством запросов, направленных третьим лицам, включая частные компании;
- эксплуатация компьютерных сетей, являющаяся формой взлома[56].

Европейский суд по правам человека рассматривал операции по наблюдению в ряде случаев; установленные принципы применимы ко всем формам наблюдения. Независимые разрешения на наблюдение должны включать:

- данные о лицах, за коммуникациями которых будет вестись наблюдение;
- состав преступлений для обоснования вмешательства;
- продолжительность наблюдения;
- процедуру составления кратких отчетов о содержании перехваченных сообщений;
- меры предосторожности для обеспечения безопасности и целостности перехваченного материала;
- обстоятельства, в том числе предельные сроки, при которых перехваченная информация должна быть стерта или уничтожена, например, после снятия обвинения или оправдания обвиняемого[57].

Независимый и эффективный орган, санкционирующий меры наблюдения, также должен убедиться в наличии четких доказательств достаточной угрозы и в том, что предлагаемое наблюдение является целевым, строго необходимым и соразмерным, и заранее разрешить (или отклонить) наблюдение[58].

---

54 *Сабо и Виши* против *Венгрии*, п. 77.

55 Европейский суд по правам человека также постановил, что «случаи, когда судья просто одобряет действия служб безопасности без реальной проверки фактов или адекватного надзора» представляют собой нарушение статьи 8 Конвенции. См. *Золтан Варга* против *Словакии*, пп. 155–160.

56 Совет Европы, Демократический и эффективный надзор за деятельностью национальных служб безопасности, с. 12, URL: https://book.coe.int/en/commissioner-for-human-rights/6682-pdf-democratic-and-effective-oversight-of-national-security-services.html

57 OSCE/ODIHR, Human Rights in Counter-Terrorism Investigations: Практическое руководство для сотрудников правоохранительных органов, сноска 48, цитата из публикации «Борьба с терроризмом и защита прав человека: Руководство», с. 205, сноска 687, цитата ЕСПЧ, *Хювик* против *Франции*, дело № 4/1989/164/220, 27 марта 1990 г., пп. 32 и 33; ЕСПЧ, *Крюслен* против *Франции*, жалоба № 11801/85, 24 апреля 1990 г., п. 35; ЕСПЧ, *Гройтер* против *Нидерландов*, жалоба № 40045/98, 19 марта 2002 г.

58 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/39/29, п. 39, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement

Те же принципы применяются, когда правоохранительные органы запрашивают персональные данные у представителей частного сектора.

5.3.1 Надзор в ходе операций и последующий анализ деятельности и операций

Комитет по правам человека отмечает, что программы наблюдения, перехвата и взлома могут отвечать требованиям прав человека только при наличии надежных и независимых механизмов надзора[59].

Первая степень контроля в любой системе подотчетности полиции — это механизмы внутреннего контроля внутри полицейской службы. Эффективные средства контроля помогают предотвращать неправомерные действия и бороться с ними. Указанные механизмы имеют три основных компонента:

- профессиональные и этические стандарты;
- непрерывный надзор и мониторинг;
- внутренняя отчетность и дисциплинарные меры.

В этой связи крайне важно, чтобы полицейские службы разработали всеобъемлющие профессиональные стандарты (кодексы поведения, этические кодексы), обеспечивающие четкое руководство по выполнению полицейских обязанностей и полномочий на практике.

Судебная власть является неотъемлемым элементом системы подотчетности полицейских органов. Деятельность по наблюдению или скрытому сбору данных должна быть санкционирована судебным представителем или органом либо аналогичным независимым механизмом, до начала такой деятельности, насколько это возможно. В системах континентальной правовой традиции за надзор за текущей деятельностью правоохранительных органов отвечает судья-следователь. И во всех системах судебная власть должна рассматривать обвинения в неправомерных действиях правоохранительных органов и применять санкции и средства правовой защиты.

Одной из основополагающих функций парламентов во всем мире является разработка, изменение и принятие законов. Поэтому на них лежит ответственность за создание ясной, четкой, доступной, всеобъемлющей и недискриминационной правовой базы для программ наблюдения, осуществляемых правоохранительными органами, которая соответствовала бы международному праву, в том числе международным нормам и стандартам в области прав человека. Кроме того, поскольку законодательные органы отвечают за проверку полномочий исполнительной власти, они часто создают постоянные или специальные надзорные комитеты и инициируют расследования для проверки секретных программ наблюдения.

Некоторые государства-члены также создали независимые экспертные органы, в том числе национальные институты по правам человека, институты уполномоченных по правам человека, или ведомства по защите данных специально для надзора за программами наблюдения. Конкретная форма надзорного органа не регулируется международным правом, однако указанные органы должны быть независимыми и обладать достаточными полномочиями, включая получение всей информации, относящейся к полным циклам наблюдения, а также предоставлять обязательные для исполнения публичные рекомендации.

Система надзора может иметь различные формы, включая административный надзор, судебный и/или парламентский надзор. Санкционирующие и надзорные органы должны быть институционально разделены, хотя один судебный орган может санкционировать операцию, а другой — обеспечивать компенсацию ущерба потерпевшим.

59 CCPR/C/ITA/CO/6, п. 37. См. также резолюцию 73/179 Генеральной Ассамблеи. См. также Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина. Подборка оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью, A/HRC/14/46, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

Независимые надзорные органы должны иметь доступ к информации, полученной в результате наблюдения, и проводить периодические обзоры возможностей и технологических изменений в сфере наблюдения. 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 наблюдения[60]. Надзорные механизмы могут давать рекомендации по проведению институциональных и законодательных реформ, которые должны быть надлежащим образом рассмотрены соответствующими исполнительными и законодательными органами.

Надзорные учреждения должны принимать все необходимые меры для защиты конфиденциальной информации и персональных данных, к которым они получают доступ в ходе своей работы; за нарушение этих требований членами надзорных учреждений должны предусматриваться меры наказания[61].

5.4 Механизм подачи и рассмотрения жалоб

Наличие механизмов, с помощью которых частные лица могут оспорить законность предполагаемого вмешательства в их права человека, имеет фундаментальное значение и будет способствовать развитию принципов эффективного расследования. Привлечение к этому процессу потерпевших и общественный контроль способствуют росту осведомленности об интересах субъектов данных. Для обеспечения и поддержания доверия общества к системе подачи и рассмотрения жалоб необходимо, чтобы жалобы рассматривались адекватно и соразмерно содержанию жалобы.

В мировой практике существует пять основных типов механизмов рассмотрения жалоб на действия полиции: внутренняя полиция; министерство полиции или внутренних дел; прокурор; омбудсмен; гражданский надзор. Нередко в одной юрисдикции действуют несколько механизмов[62].

Создание независимого органа внешнего гражданского надзора, в обязанности которого входит прием и расследование жалоб на действия полиции, жизненно необходимо для обеспечения большей подотчетности и прозрачности, а в некоторых случаях — для устранения недостатков неэффективного внутреннего контроля и надзора. Стандартной предусмотренной законом целью в юрисдикциях, где системы рассмотрения жалоб на действия полиции кодифицированы, является привлечение сотрудников правоохранительных органов к ответственности в рамках уголовного и дисциплинарного производства на основании доказательств, полученных в ходе расследования жалобы. Механизмы, аналогичные используемым для расследования заявлений о применении полицией излишней силы, могут также применяться для расследования заявлений о незаконном вмешательстве в частную жизнь или незаконном сборе персональных данных в Интернете, хотя для этого может потребоваться дополнительная техническая экспертиза. Эффективная система подачи жалоб на действия полиции обеспечивает фундаментальную защиту от формирования культуры безнаказанности. Кроме того, жалобы являются важным ресурсом, который можно изучать и анализировать для извлечения уроков из прошлых ошибок в целях повышения качества работы в будущем. Жалобы дают возможность извлечь уроки на уровне отдельных сотрудников и служб[63].

60 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/39/29, п. 40, URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F39%2F29&Language=E&DeviceType=Desktop&LangRequested=False

61 Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина. Подборка оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью, A/HRC/14/46, п. 14, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

62 Там же.

63 Совет Европы, «Реформа международной системы обжалования действий полиции», URL: https://rm.coe.int/16806dbbbd

5.4.1 Средства правовой защиты и возмещение ущерба

Статья 2 Международного пакта о гражданских и политических правах устанавливает право на эффективное средство правовой защиты в случае нарушения обязательств в области прав человека[64]. Таким образом, лица, пострадавшие от незаконных действий сотрудника правоохранительного органа или самого органа, должны иметь возможность обратиться в учреждение, которое может предоставить эффективное средство правовой защиты, включая полное возмещение ущерба за причиненный ущерб. Внесудебные органы могут быть уполномочены принимать и расследовать жалобы, а также издавать обязательные для исполнения постановления или предоставлять эффективные средства правовой защиты, в то время как судебные учреждения могут предписать принятие мер по устранению допущенного нарушения. Для обеспечения практического применения данного права государства обязаны гарантировать, чтобы отдельные лица также могли обращаться в учреждение, уполномоченное выносить юридически обязательные для исполнения постановления о сотрудничестве, включая информацию, полученную от иностранных органов или направленную им. Учреждения, ответственные за рассмотрение жалоб и требований о применении эффективных средств правовой защиты, возникающих в связи с деятельностью спецслужб, должны быть независимыми от правоохранительных органов и исполнительной власти. Такие учреждения также должны иметь полный беспрепятственный доступ ко всей соответствующей информации, необходимые ресурсы, знания и опыт для проведения расследований, а также способность выносить обязательные для исполнения постановления[65].

5.4.2 Прозрачность

Прозрачность является важнейшим условием деятельности демократического правительства. Таким образом, общая правовая основа, касающаяся наблюдения всех видов, а также процедуры, которым необходимо следовать при выдаче разрешения на наблюдение, выборе объектов наблюдения, использовании, обмене, хранении и уничтожении перехваченных материалов, должны быть доступны для общественности[66].

Органы государственной власти и надзорные органы должны участвовать в информировании общественности о существующих законах, политике и практике наблюдения, перехвата сообщений и других формах обработки персональных данных, поскольку для понимания преимуществ и недостатков методов наблюдения необходимы открытые дебаты и тщательный контроль[67].

Лица, ставшие объектом наблюдения, должны быть уведомлены об этом, и разъяснения о вмешательстве в их право на неприкосновенность частной жизни должны быть предоставлены им постфактум, если одновременное уведомление невозможно. Объекты наблюдения также должны иметь право изменять и/или удалять персональную информацию, если она неактуальна, неточна или в ней больше нет необходимости для целей текущего или готовящегося расследования[68].

---

64 Согласно статье 2 Международного пакта о гражданских и политических правах, государства обязуются: *a*) обеспечить любому лицу, права и свободы которого, признаваемые в настоящем Пакте, нарушены, эффективное средство правовой защиты, даже если это нарушение было совершено лицами, действовавшими в официальном качестве; *b*) обеспечить, чтобы право на правовую защиту для любого лица, требующего такой защиты, устанавливалось компетентными судебными, административными или законодательными властями или любым другим компетентным органом, предусмотренным правовой системой государства, и развивать возможности судебной защиты; *c*) обеспечить применение компетентными властями средств правовой защиты, когда они предоставляются.

65 Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина. Подборка оптимальных практических методов, применяемых в отношении законодательной и институциональной основы и мер, которые обеспечивают соблюдение прав человека специальными службами в условиях борьбы с терроризмом, в том числе касающихся надзора за их деятельностью, A/HRC/14/46, пп. 16 и 17, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

66 Принцип 10. E Тшванских принципов национальной безопасности и права на информацию, URL: https://www.justiceinitiative.org/publications/tshwane-principles-national-security-and-right-information-overview-15-points#:~:text=June%202013-,The%20Tshwane%20Principles%20on%20National%20Security%20and%20the%20Right%20to,and%20national%20law%20and%20practices

67 Доклад Специального докладчика о праве на неприкосновенность частной жизни, A/HRC/34/60, п. 38, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/260/54/PDF/G1726054.pdf?OpenElement

68 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/39/29, URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement

Процессы надзора также должны быть прозрачными и подвергаться соответствующему общественному контролю, а решения надзорных органов должны подлежать обжалованию или независимым проверкам[69]. Надзорные органы в соответствии с законом должны публиковать публичные версии своих периодических отчетов и отчетов о проведении расследований. Кроме того, правоохранительные органы и надзорные органы не должны освобождаться от действия законодательства о свободе информации. Напротив, решения не предавать определенную информацию гласности должны приниматься в каждом случае в отдельности, должным образом обосновываться и подлежать контролю со стороны независимого органа.

5.5 Данные, агрегированные в коммерческих целях

Несмотря на то что в соответствии с международным правом для получения доступа к персональным данным сотрудники государственных органов обязаны получать ордера или аналогичные разрешения, предусмотренные ясным, четким, доступным, всеобъемлющим и недискриминационным внутренним законодательством, данный вопрос осложняется существованием коммерчески доступных данных, которые агрегируют общедоступную и частную информацию. Государственные учреждения, желающие приобрести данные, зачастую используют в своих заказах и контрактах такие термины, как «открытый источник» и «общедоступный», предполагая, что им нужна только такая информация, как публичные сообщения в социальных сетях, которые частные лица сознательно делают общедоступными. Тем не менее в государственных заказах и контрактах эти термины часто используются для включения информации, собранной специально для конкретного органа, которая на самом деле не является доступной для общественности или любого другого потребителя. Широкое и вводящее в заблуждение использование этих терминов подрывает заявления правительства о том, что государственным органам разрешено осуществлять сбор такой информации на том основании, что она уже доступна общественности, и поэтому у частных лиц не имеется разумных ожиданий относительно конфиденциальности таких уязвимых данных[70]. Как минимум, если государственные органы приобретают данные, включающие, например, финансовую или медицинскую информацию, которая в соответствии с обоснованными ожиданиями частного лица является частной, эти данные должны приобретаться в строгом соответствии с принципами, изложенными в данном отчете. «Руководящие принципы предпринимательской деятельности в аспекте прав человека» Организации Объединенных Наций более подробно описывают обязательства государств при заключении контрактов с предприятиями, а также ответственность таких предприятий за соблюдение прав человека, предотвращение и устранение любых неблагоприятных последствий для прав человека, непосредственно связанных с их деятельностью, продукцией или услугами[71]. Такие обязательства находятся за рамками данного документа.

69 Там же, п. 40.

70 Центр демократии и технологий, «Правовые лазейки и данные за доллары: Как правоохранительные и разведывательные органы покупают ваши данные у брокеров», URL: https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/

71 «Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты» | Управление Верховного комиссара ООН по правам человека. См. также Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/39/29, п. 42–49.

[VI] Заключение

6.1 Основные выводы

1. Государства-члены должны создать как внутренние, так и независимые надзорные механизмы для осуществления контроля за деятельностью сотрудников правоохранительных органов в отношении сбора данных в Интернете и цифрового наблюдения. Ответственность за надзор за сбором данных в Интернете и наблюдением может быть включена в обязанности существующих надзорных механизмов. Гражданский надзор способствуют обеспечению более полных подотчетности и прозрачности.
2. Внешние надзорные механизмы должны быть независимыми, иметь надлежащие ресурсы и полный и беспрепятственный доступ ко всей соответствующей информации, инфраструктуре и должностным лицам. Они могут включать в себя сочетание административных, исполнительных, законодательных и независимых органов, хотя последние должны обладать полномочиями по проведению расследований и предоставлению эффективных средств правовой защиты.
3. Различия между сбором и обработкой персональных данных и сбором и обработкой метаданных становятся все более размытыми.
4. Аналогичным образом, трудно обозначить правовое различие между государственным сбором персональных данных и покупкой персональных данных у коммерческих организаций.
5. Право на доступ к персональным данным и обстоятельства, при которых такой доступ может быть получен, должны быть установлены ясным, четким, доступным, всеобъемлющим и недискриминационным законом или внутренним регламентом и доведены до сведения всех сотрудников правоохранительных органов. Нарушения таких правил должны влечь за собой санкции с использованием существующих или новых дисциплинарных механизмов.
6. В интересах прозрачности правительства должны предоставлять общественности информацию о своей деятельности по сбору и обработке данных. Насколько это возможно, деятельность и выводы надзорных механизмов должны быть доступны общественности.
7. Государства должны гарантировать, чтобы любые жертвы незаконного сбора данных и наблюдения в Интернете могли подать жалобу в независимый суд или надзорный орган и обратиться в учреждение, которое может предоставить эффективное средство правовой защиты, включая полное возмещение причиненного ущерба.
8. Гражданское общество является ключевым партнером в работе по обеспечению соблюдения прав человека при сборе и обработке персональных данных. Государствам рекомендуется создавать и поддерживать благоприятные условия для гражданского общества, включая правовую базу, обеспечивающую защиту и продвижение прав человека в соответствии с международным правом прав человека. Они должны гарантировать, чтобы любые официальные препятствия, мешающие гражданскому обществу осуществлять надзор за сбором и обработкой персональных данных правительством, подлежали независимому судебному рассмотрению.

Контртеррористическое управление Организации Объединенных Наций
Центральные учреждения Организации Объединенных Наций
New York, NY 10017

www.un.org/counterterrorism

КОНТРТЕРРОРИСТИЧЕСКОЕ УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ
Контртеррористический центр ООН (КТЦ ООН)

24-09822