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

INTERPOL

При финансовой поддержке Европейского союза

Кибербезопасность и новые технологии

Руководство по основанному на правах человека подходу к борьбе с использованием новых технологий в целях терроризма

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 принципа 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 следующим лицам:

- **Виктору Кипкоечу** — младшему специалисту по программам, Глобальный центр по вопросам сотрудничества в области безопасности (ГЦСБ);
- **Полу Мэддену** – руководителю проектов по борьбе с терроризмом программы PHARE, Международный институт правосудия и верховенства права (IIJ);
- **Тому Паркеру** — координатору проектов, Сектор по предупреждению терроризма Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН);
- **Томазо Фальчетта** — руководителю отдела адвокации и политики организации Privacy International; а также
- **Камелю эль-Хилали** – доктору философии в области права Университета Париж Пантеон-Асса.

Термины и определения

Виртуальные активы	Термины «виртуальные активы» или «криптоактивы» означают цифровые формы валюты и других активов[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 общепризнано, что даркнет содержит множество криминальных веб-сайтов и сервисов, размещенных в этих сетях[2].
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.
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.

1 Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ), «Виртуальные активы». Веб-сайт Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (дата обращения: 8 июня 2024 г.).

2 Европейский центр киберпреступности (EC3), «Оценка угроз организованной преступности в Интернете за 2019 год» (Европол, 2019 г.), URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

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

Новые технологии	Термин «новые технологии» охватывает широкий спектр различных технологий[4], 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[5].
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 с соблюдением обязательств государств-членов по международному праву прав человека.
Отстранение	Процесс, в ходе которого человек, проявляющий признаки радикализации, убеждается в необходимости либо «покинуть свою группу, либо отвергнуть насилие, при этом не обязательно целью ставится изменение его основополагающей экстремистской точки зрения или идеологии»[6].
Подстрекательство к терроризму	Умышленное и противозаконное распространение или направление иным образом обращения к общественности с целью подстрекательства к совершению террористического преступления, если такое поведение, являющееся или не являющееся прямой пропагандой террористических преступлений, создает угрозу того, что такое преступление или преступления могут быть совершены.
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 реинтеграцию правонарушителей в общество.
Реинтеграция	Комплексный процесс возвращения человека в социальную и (или) функциональную среду.
Терроризм	Преступные деяния, в том числе против гражданского населения, совершаемые с намерением причинить смерть или тяжкие 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.
VLOP	Очень большие онлайн-платформы и системы поиска.

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

5 Проектный документ CT TECH – Приложение I. Описание действия, URL: https://www.interpol.int/Crimes/Terrorism/Counter-terrorism-projects/Project-CT-Tech

6 Европейский центр киберпреступности (EC3), «Оценка угроз организованной преступности в Интернете за 2019 год» (Европол, 2019 г.), с. 8, URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

7 См. S/RES/1566 (2004), пункт 3. Более подробную информацию см. в разделе 5.1.

Краткое содержание

Международное право прав человека налагает на государства-члены прямое обязательство предпринимать соответствующие шаги для защиты лиц, находящихся под их юрисдикцией, от разнообразных угроз их безопасности, включая угрозу терроризма. Разработка надлежащих подходов к борьбе с терроризмом становится все более сложной задачей по мере того как террористы осваивают все больше новых технологий для поддержки, подготовки и осуществления террористических актов, а также для распространения дезинформации, подстрекательства к насилию и вербовки. В связи с этим некоторые меры, предпринимаемые государствами-членами, могут противоречить международному праву прав человека, включая, помимо прочего: меры, основанные на недостаточно четких или слишком широких определениях терроризма; уголовное преследование отдельных лиц или групп, таких как представители гражданского общества, правозащитники, журналисты или политическая оппозиция, за осуществление ими своих прав человека, включая свободу выражения мнений в Интернете; незаконное или произвольное наблюдение в Интернете; необоснованное ограничение доступа к услугам или контенту, например, путем отключения Интернета, блокирования веб-сайтов или замедления скорости подключения. Учитывая, что такие меры наносят ущерб широкому спектру прав человека и принципу верховенства права, существует реальная опасность того, что контртеррористические усилия, предпринимаемые в нарушение международного права, могут привести к неправильному или неэффективному использованию ресурсов, усугубить существующее недовольство и способствовать созданию условий, благоприятствующих радикализации к насилию.

Данный доклад об основанных на правах человека подходах к противодействию использованию новых технологий в террористических целях призван помочь разработчикам политики и тем, кто ее осуществляет, обеспечить, чтобы контртеррористические меры основывались на положениях закона, преследовали законную цель, были необходимы и соразмерны соответствующей угрозе, чтобы они не нарушали права человека отдельных лиц и (или) не усиливали существующее недовольство.

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)[8] в июле 2021 года государства-члены выразили глубокую озабоченность «использованием Интернета и других информационно-коммуникационных технологий, включая платформы социальных сетей, в террористических целях, в том числе непрекращающимся распространением террористического контента», и попросили Контртеррористическое управление 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)[9] и 2396 (2017)[10] Совета Безопасности призывают государства-члены сотрудничать при принятии национальных мер, призванных воспрепятствовать использованию террористами технологий и средств связи для совершения террористических актов. Резолюция 2396 (2017) 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 ООН[11] 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». Платформы, на которые ссылаются государства-члены, включают Telegram, Rocket, Chat, Hoop и TamTam, среди прочих. В докладе также говорится о том, что **сторонники ИГИЛ (ДАИШ) 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[12].

8 Глобальная контртеррористическая стратегия Организации Объединенных Наций: седьмой обзор (A/RES/75/291), URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F75%2F291&Language=E&DeviceType=Desktop&LangRequested=False

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

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

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

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

КТК **«с озабоченностью отметил 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, а также противодействием такому их использованию»**, особо отметив **«необходимость сохранения глобальной цифровой связности и свободного, 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 уважении прав человека и принципа верховенства права.
 **Компонент 1.2**	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 уважении 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 уважении 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

Данный документ призван помочь разработчикам политики и тем, кто ее осуществляет, обеспечить, чтобы контртеррористические меры основывались на положениях закона, преследовали законную цель, были необходимы и соразмерны соответствующей угрозе, чтобы они не нарушали права человека отдельных лиц и тем самым не нарушали обязательства по международному праву и не подрывали эффективность и устойчивость контртеррористических усилий.

1.3.1 Сфера охвата

В докладе рассмотрен ряд новых технологий, включая социальные сети, Интернет в целом, распознавание лиц и алгоритмическое профилирование, технологии обхода и шпионские программы.

1.3.2 Целевая аудитория

Разработчики политики в области национальной безопасности и старшие должностные лица, ответственные за реализацию этой политики.

1.3.3 Ограничения

За исключением технологий распознавания лиц и профилирования, в настоящем документе не анализируются преимущества или риски, связанные с использованием искусственного интеллекта.

[III]

Подход

2.1 Обзор

Цель настоящего доклада заключается в обеспечении и улучшении соблюдения международных норм и стандартов в области прав человека и защиты гражданских свобод индивидов при противодействии использованию новых технологий в террористических целях и применении технологических средств для предотвращения терроризма и борьбы с ними в соответствии с Глобальной контртеррористической стратегией Организации Объединенных Наций и при полном соблюдении прав человека и принципа верховенства права.

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 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, политики, 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 может способствовать 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 терроризме 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

В качестве информационных источников при разработке и составлении настоящего документа был использован широкий спектр материалов, включая документы проекта CT TECH, консультации с заинтересованными сторонами, данные внутреннего анализа, кабинетные исследования, совещания экспертных групп, сотрудничество с различными структурами в рамках Глобального договора по координации контртеррористической деятельности, а также руководящая основа, описанная выше в разделе 2.2. На основании полученных результатов в настоящем документе рассматриваются основные проблемы и вопросы в области прав человека в связи с разработкой, внедрением и использованием новых технологий, которые могут нарушать права человека. Этот анализ подкрепляется рядом тематических исследований.

2.3.1 Совещания экспертных групп и консультации

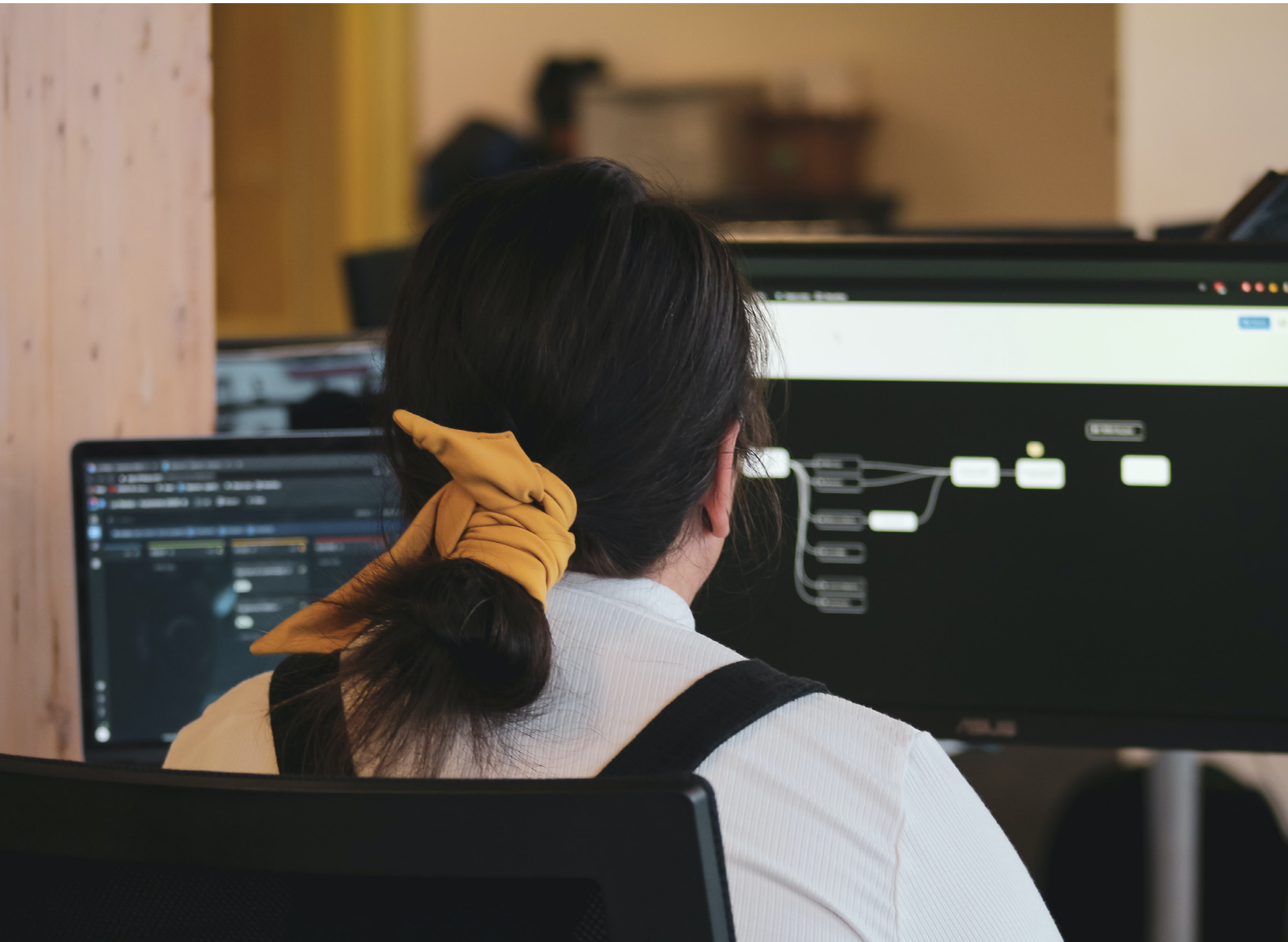
Данное руководство было разработано при участии экспертов в рамках совещаний экспертных групп (СЭГ), а также по результатам индивидуальных консультаций и обзоров. СЭГ объединили экспертов и практиков из контртеррористических служб и правоохранительных органов (ПО), экспертов в области прав человека, 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 в соответствии с международным правом прав человека, международным гуманитарным и международным беженским правом.

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	Международный пакт о гражданских и политических правах
2	Международная конвенция о ликвидации всех форм расовой дискриминации
3	Резолюции 1566 и 1624 Совета Безопасности и резолюция 69/166 Генеральной Ассамблеи
4	Прецедентное право Африканского суда по правам человека и народов, Европейского суда по правам человека и Суда Европейского союза, Межамериканского суда по правам человека, а также соответствующие региональные политические документы и заявления
5	Глобальная контртеррористическая стратегия Организации Объединенных Наций
6	Доклады уполномоченных Советом по правам человека Специальных докладчиков по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом
7	Документы по вопросам политики в области неприкосновенности частной жизни и новых технологий Управления Верховного комиссара Организации Объединенных Наций по правам человека



[III]

Введение

3.1 Права человека, борьба с терроризмом и новые технологии

Развитие, широкое распространение и использование целого ряда новых и новейших цифровых технологий в последние десятилетия изменили привычный уклад жизни общества. Во многих странах доступ к Интернету и ИКТ и их использование стали неотъемлемой частью государственной деятельности, бизнеса и повседневной жизни людей. В связи с этим Советом по правам человека Организации Объединенных Наций был признан потенциал этих новых и новейших технологий в содействии реализации мер по ускорению человеческого прогресса, создании условий для развития, укреплении демократических институтов, расширении возможностей для участия общественности и открытого и свободного обмена идеями. Им также были признаны возможности, которые эти технологии открывают в области продвижения и защиты прав человека, наряду с рисками, которые несет в себе злоупотребление ими[13].

> **„Государства-члены должны обеспечивать, чтобы любые меры, принимаемые в целях борьбы с терроризмом, согласовывались со всеми их обязательствами по международному праву, в частности международному праву в области прав человека, международному беженскому праву и международному гуманитарному праву, […] уважение прав человека, основных свобод и верховенства права дополняют и усиливают меры по борьбе с терроризмом и являются существенной составной частью успешной контртеррористической деятельности“.**
>
> Глобальная контртеррористическая стратегия Организации Объединенных Наций (резолюция 75/291 Генеральной Ассамблеи, пункт 9)

И действительно, злоупотребление этими технологиями может привести к значительным рискам для безопасности. В последние годы мы наблюдаем примеры того, как некоторые технологии используются в преступных целях и применяются, помимо прочего, для продвижения и поддержки террористических актов путем распространения пропаганды, онлайн-вербовки, радикализации и подстрекательства к терроризму, для финансирования, а также для осуществления атак. Террористические группировки используют мобильные платежные системы, онлайновый краудфандинг и виртуальные активы для обхода финансового контроля. Они также пользуются социальными сетями и игровыми онлайн-платформами для распространения языка ненависти и террористического контента. Для затруднения проверки личности и разжигания заговоров могут использоваться технологии синтеза изображения или голоса (deep fake).

13 A/HRC/RES/53/29.

Кибератаки на важнейшие объекты инфраструктуры могут нарушить жизненно важные функции общества и привести к далеко идущим последствиям для широкого спектра прав человека, от права на жизнь и личную неприкосновенность до права на здоровье и здоровую окружающую среду, права на образование, а также на воду, санитарию и другие аспекты права на достаточный жизненный уровень. Технологии 3D-печати и размещенные в Интернете технические инструкции могут облегчить террористам доступ к оружию[14].

В то же время эти же технологии способствуют сбору и сохранению информации и доказательств террористической деятельности, а также позволяют осуществлять наблюдение за подозреваемыми в терроризме, их коммуникациями, перемещениями и финансами. Они облегчают мониторинг поставок оружия и тактики вербовки, а также позволяют быстро распространять контртеррористические материалы. Однако государства-члены уже сталкивались с проблемами при использовании новых технологий в борьбе с терроризмом, например, в обеспечении полного соблюдения своих обязательств, предусмотренных международным правом прав человека, при сокращении масштабов применения указанных технологий в целях терроризма[15].

Генеральная Ассамблея и Совет Безопасности неоднократно подчеркивали, что соблюдение прав человека и принципа верховенства закона дополняют и усиливают эффективные меры по борьбе с терроризмом и являются неотъемлемой частью успешных и устойчивых контртеррористических усилий. Международное право прав человека налагает на государства-члены обязательство проявлять должную осмотрительность и принимать надлежащие меры по защите лиц, находящихся под их юрисдикцией, от обоснованно прогнозируемых террористических актов и привлекать к ответственности лиц, совершивших такие акты[16].

Принятие эффективных мер по защите населения от угроз безопасности при одновременном обеспечении защиты прав человека в контексте предотвращения терроризма и насильственного экстремизма и борьбы с ними может стать для государств сложной задачей. Однако государства могут эффективно выполнять свои обязательства по международному праву, используя гибкие механизмы международного права прав человека, в частности, путем надлежащего применения отступлений и ограничений.

В случае чрезвычайного положения, при котором «жизнь нации находится под угрозой», государства имеют право законно отступать от определенных обязательств в области прав человека при соблюдении ряда условий[17]. Более того, даже вне чрезвычайного положения государства могут вводить ограничения на осуществление определенных прав. Указанные ограничения должны быть предусмотрены законом и необходимы для достижения законной цели (охраны государственной безопасности, общественного порядка, безопасности, прав и свобод других лиц). Любые меры должны также основываться на принципах необходимости и соразмерности и согласовываться с другими гарантированными правами человека.

Эти условия, определенные в международном праве прав человека для законного ограничения определенных прав, применяются, например, к использованию государствами особых методов расследования. Совет Европы определяет особые методы расследования как «методы, применяемые компетентными органами в области уголовных расследований в целях раскрытия и расследования тяжких преступлений и установления

14 Выступление Генерального Секретаря на второй Конференции высокого уровня с участием руководителей контртеррористических ведомств государств-членов. 28 июня 2021 г. URL: https://www.un.org/sg/en/content/sg/statement/2021-06-28/secretary-generals-remarks-the-second-high-level-conference-of-heads-of-counter-terrorism-agencies-of-member-states-delivered

15 Глобальная контртеррористическая стратегия Организации Объединенных Наций, (A/RES/75/29) URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F75%2F29&Language=E&DeviceType=Desktop&LangRequested=False

16 Управление Верховного комиссара Организации Объединенных Наций по правам человека. Права человека, терроризм и борьба с терроризмом (УВКПЧ ООН, Изложение фактов № 32, 2008 г.), Введение и пп. 19 и 20.

17 Например, согласно Статье 4 МПГПП, государства могут принимать меры в отступление от своих обязательств по Пакту «во время чрезвычайного положения в государстве, при котором жизнь нации находится под угрозой» при условии соблюдения ряда условий (например, указанные меры должны приниматься только в такой степени, в какой это требуется остротой положения). Это обязательство отражает принцип соразмерности, обычно применяемый к полномочиям по использованию отступлений и ограничений. Любые принятые таким образом меры должны быть действительно направлены на урегулирование ситуации и на восстановление конституционного порядка, уважающего права человека, и должны быть полностью оправданы обстоятельствами. См. также Замечание общего порядка № 29 Комитета по правам человека о чрезвычайном положении (статья 4), CCPR/C/21/Rev.1/Add.11. Другие пакты о правах человека, содержащие положения об отступлении, включают Европейскую конвенцию о правах человека и Американскую конвенцию о правах человека. Однако многие договоры по правам человека не предусматривают возможности отступления от их положений в случае чрезвычайного положения. К ним относятся, в частности, Международный пакт об экономических, социальных и культурных правах, Международная конвенция о ликвидации всех форм расовой дискриминации, Конвенция о ликвидации всех форм дискриминации в отношении женщин и Африканская хартия прав человека и народов.

подозреваемых и направленные на сбор информации таким образом, чтобы не вызвать подозрений у объекта расследования»[18]. К ним относятся: 1) секретные расследования с публичным взаимодействием и без маскировки (например, с привлечением источников или информаторов); 2) секретные расследования без публичного взаимодействия и без маскировки (например, электронная слежка); 3) секретные расследования с публичным взаимодействием и с маскировкой (например, с использованием внедренных оперативников); и 4) секретные расследования без публичного взаимодействия и с маскировкой (операции под прикрытием)[19].

Однако, стремясь выполнить свои обязательства по борьбе с терроризмом, многие государства принимали законодательные и практические меры в ускоренном порядке, что привело к нарушению их обязательств по международному праву человека и незаконному вмешательству в права человека[20].

В одних случаях последствия проблемной политики, законодательства и практических мер были непреднамеренными, в то время как в других государствах намеренно злоупотребляли контртеррористическими мерами для преследования политической оппозиции, средств массовой информации, гражданского общества, правозащитников или расовых, этнических, религиозных или других меньшинств. Воздействие широкого определения и неправильного применения контртеррористических мер на гражданское пространство, верховенство закона и демократические процессы не является второстепенной или чисто теоретической проблемой. Хотя оценки разнятся, группы, отслеживающие состояние демократического пространства и гражданского общества в разных странах мира, сходятся во мнении, что более половины населения планеты живет в государствах, где основные свободы либо отсутствуют, либо существенно подавляются[21]. Некоторые из этих государств принимают контртеррористические меры, предоставляющие властям широкие или неограниченные полномочия по наблюдению, включая возможность следить за критиками правительства, правозащитниками, борцами с коррупцией, журналистами или большими группами населения; возможность ограничивать или перекрывать каналы финансирования групп гражданского общества; возможность ограничивать доступ к отдельным социальным сетям или их значительному количеству; возможность принуждения к удалению законного контента из социальных сетей; возможность закрывать доступ в Интернет без достаточных оснований; и возможность контролировать СМИ, подвергать их цензуре или препятствовать законным формам выражения мнений. Было доказано, что онлайн-атаки открывают путь для нарушений прав человека и злоупотреблений, включая убийства, пытки, насильственные исчезновения и произвольное лишение свободы[22].

Незаконное или произвольное наблюдение, необоснованные ограничения законного выражения мнений, в том числе путем незаконного или произвольного удаления онлайн-контента, блокирования веб-сайтов, прекращения доступа в Интернет, блокирования технологий обхода, а также допускающие расширительное толкование в силу нечетких формулировок законы, устанавливающие уголовную ответственность за выражение мнений, могут оказывать сильное отрицательное воздействие не только на свободу выражения мнений,

---

18 Рекомендация Rec(2005)10 Комитета министров Совета Европы государствам-членам об «особых методах расследования» тяжких преступлений, в том числе террористических актов, раздел «Определения и сфера применения». URL: https://www.refworld.org/pdfid/43f5c6094.pdf

19 Tom Parker, *Avoiding the Terrorist Trap: Why Respect for Human Rights is the Key to Defeating Terrorism* («Избегая ловушки терроризма: почему соблюдение прав человека является ключом к победе над терроризмом»). World Scientific Publishing Company, July 2, 2019.

20 Управление Верховного комиссара Организации Объединенных Наций по правам человека. Права человека, терроризм и борьба с терроризмом (УВКПЧ ООН, Изложение фактов № 32, 2008 г.), Введение и п. 20. URL: https://www.ohchr.org/ru/publications/fact-sheets/fact-sheet-no-32-terrorism-and-counter-terrorism

21 По оценкам Freedom House, 20 процентов населения планеты живут в свободных странах; 38 процентов — в несвободных странах; остальные — в частично свободных. См. Freedom in the World, 2022, URL: https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf. По оценкам этой же организации, из 4,5 миллиарда человек, имеющих доступ к Интернету, 76 процентов живут в странах, где люди подвергались аресту или тюремному заключению за размещение материалов на политические, социальные или религиозные темы. См. Freedom on the Net, *Annual Survey 2022*, URL: https://freedomhouse.org/report/freedom-net/. По оценкам Civicus, 3,1 процентов населения мира живут в странах с открытым гражданским пространством, а 70 процентах — в странах, где гражданское общество либо отсутствует, либо подавляется. URL: https://monitor.civicus.org/quickfacts/#:~:text=CIVIC%20SPACE%20IN%202022,decimal%20point%20to%20the%20percentages

22 См., например, A/HRC/52/39; Документ с изложением позиции Специального докладчика ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом. Глобальное регулирование торговли технологиями шпионских программ контртеррористического назначения: предложения по разработке подхода, отвечающего требованиям прав человека. См. также Совместное заявление США и ЕС о защите правозащитников. URL: https://www.eeas.europa.eu/eeas/useu-joint-statement-protecting-human-rights-defenders-online_en

включая право на доступ к информации, но и на процессы, связанные с общественными интересами, а также на свободу мирных собраний и объединений.

В настоящем руководстве затрагиваются вопросы воздействия на права человека ряда новых технологий, включая социальные сети, даркнет, криптовалюты и технологии распознавания лиц, однако не рассматривается весь масштаб использования искусственного интеллекта (ИИ) в борьбе с терроризмом или применением дистанционно управляемого оружия.

Использование новых технологий в борьбе с терроризмом может повлиять на широкий спектр прав человека, включая право на неприкосновенность частной жизни, право на свободу выражения мнений и объединений, право на участие в политической деятельности, право на равную защиту закона без дискриминации и право на справедливый суд, и не только на них. Структуры и механизмы Организации Объединенных Наций особенно подчеркивают роль прав на неприкосновенность частной жизни и свободу выражения мнений в данной связи как прав-проводников, позволяющих осуществлять целый ряд взаимосвязанных прав человека.

Принятие и реализация законов, политических и практических мер, соответствующих международному праву прав человека, — это не только юридическое обязательство, но и стратегический императив для успешных и устойчивых усилий по борьбе с терроризмом. Генеральная Ассамблея и Совет Безопасности давно признали, что нарушения прав человека являются одним из условий, способствующих терроризму, и что неспособность государств соблюдать свои обязательства по международному праву прав человека — это один из факторов, содействующих росту радикализации к насилию. Законы, политические и практические меры, противоречащие указанным обязательствам, таким образом, являются контрпродуктивными, поскольку могут разжечь недовольство, которое может быть использовано террористами в целях вербовки.

[IV] Общие соображения

4.1 Обзор

Меры по предотвращению терроризма и борьбе с ним зачастую закреплены в широком спектре внутренних нормативных документов, включающих в себя не только контртеррористическое законодательство, но и связанные с ним законы, правила, положения, директивы и прокламации, такие как уголовные и уголовно-процессуальные кодексы; законы об Интернете и телекоммуникациях; законы о кибербезопасности; законодательство о безопасности, включая законы, регулирующие деятельность спецслужб; законы о защите информации; финансовые законы и правила и т. д. Поскольку контртеррористические меры часто приводят к ограничению прав человека, государства-члены сталкиваются с проблемами обеспечения полного соблюдения обязательств по международному праву прав человека при принятии эффективных мер по борьбе с угрозами, связанными с терроризмом. Тем не менее свойственная механизмам международного права прав человека гибкость[23] позволяет государствам выполнять свои обязательства по соблюдению прав человека, принимая при этом необходимые и соразмерные меры по борьбе с террористическими угрозами, в том числе для обеспечения того, чтобы любое лицо, участвующее в финансировании, планировании, подготовке или совершении террористических актов или в поддержке таких актов, было привлечено к ответственности.

В частности, согласно международному праву прав человека, государства могут отступать от определенных прав и налагать ограничения на их осуществление. Условия, применяемые к отступлениям и ограничениям, коротко описаны ниже.

В то же время некоторые права человека носят абсолютный характер. К ним относятся запрет на применение пыток и жестокие, бесчеловечные или унижающие достоинство виды обращения или наказания, на рабство и подневольное состояние, а также принцип законности, согласно которому нет наказания без закона. 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.

4.2 Отступления

В чрезвычайных ситуациях, при которых «жизнь нации находится под угрозой»[24], государства имеют право временно корректировать некоторые обязательства в области прав человека[25] при соблюдении ряда условий. Меры, отступающие от прав человека, должны приниматься только в такой степени, в какой это требуется остро-

23 См., например, УВКПЧ ООН, Изложение фактов № 32: Терроризм и борьба с терроризмом; K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' («Использование биометрических данных для идентификации террористов: передовая практика или рискованное предприятие?») (2020), URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 18.

24 Специальным докладчиком ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом были рассмотрены практики государств-членов, связанные с осуществлением чрезвычайных полномочий в условиях борьбы с терроризмом, и соответствующие проблемы соблюдения прав человека. См. в данном отношении A/HRC/37/52.

25 Следует отметить, что возможность отступления в чрезвычайной ситуации предусматривается лишь несколькими договорами о правах человека. К ним относятся Международный пакт о гражданских и политических правах, Европейская конвенция о правах человека и Американская конвенцию о правах человека. Другие документы, такие как Международный пакт об экономических, социальных и культурных правах и Африканская хартия прав человека и народов, не предусматривают корректировки обязательств в связи с наличием чрезвычайного положения.

той положения, и должны быть действительно направлены на урегулирование ситуации и на восстановление конституционного порядка, а также полностью оправданы обстоятельствами[26]. Более того, должны быть созданы надлежащие гарантии для защиты от произвольного и несоразмерного вмешательства в права человека[27]; процессуальные гарантии не могут быть ограничены в обход защиты не допускающих отступлений прав[28].

Меры, отступающие от прав человека, не должны противоречить «другим обязательствам государства по международному праву», в частности по международному гуманитарному праву[29]. В этой связи ряд деяний запрещен при любых обстоятельствах, и поэтому они не могут быть предметом законных отступлений в условиях чрезвычайного положения. Это касается запрета на захват заложников; тайное задержание; депортацию или насильственное перемещение населения, т. е. насильственное перемещение лиц, ставших объектом выселения или других принудительных действий, из района, в котором они законно проживают, без каких бы то ни было оснований, допускаемых международным правом; пропаганду войны или организацию выступлений в пользу национальной, расовой или религиозной ненависти, представляющих собой подстрекательство к дискриминации, вражде или насилию[30].

4.3 Ограничения

Даже вне чрезвычайного положения государства могут вводить ограничения на осуществление определенных прав[31]. Такие ограничения должны быть предусмотрены законом и необходимы для законной цели (включая обеспечение государственной безопасности, общественного порядка, защиты населения, прав и свобод других лиц). Любые меры должны также основываться на принципах необходимости и соразмерности и согласовываться с другими гарантированными правами человека.

4.3.1 Законная цель

Ограничения прав человека должны быть необходимы для достижения законных целей охраны государственной безопасности, общественного порядка/защиты, здоровья и морали, равно как и основных прав и свобод других лиц. Ограничения могут устанавливаться лишь для тех целей, для которых они предназначены[32], и должны быть прямо связаны с конкретной целью, достижение которой ими преследуется[33]. Совет по правам

26 Замечание общего порядка № 29 Комитета по правам человека о чрезвычайном положении (статья 4), CCPR/C/21/Rev.1/Add.11. Также следует отметить, что только лишь тот факт, что отступление от конкретного положения договора может быть обосновано остротой положения, не отменяет требования продемонстрировать необходимость конкретных мер, принятых в соответствии с указанным отступлением.

27 Замечание общего порядка № 29 Комитета по правам человека о чрезвычайном положении (статья 4), CCPR/C/21/Rev.1/ Add.11, п. 4.

28 Это предусмотрено в Замечании общего порядка № 29 Комитета по правам человека о чрезвычайном положении (статья 4), CCPR/C/21/Rev.1/ Add.11, и в новом Замечании общего порядка № 35 Комитета по правам человека о свободе и личной неприкосновенности (Статья 9), CCPR/C/GC/35, в котором Комитет недвусмысленно заявил, что отступление от принципа habeas corpus не допускается (пп. 65-67).

29 Замечание общего порядка № 29 Комитета по правам человека о чрезвычайном положении (статья 4), CCPR/C/21/Rev.1/ Add.11, п. 9.

30 Там же, п. 13.

31 Некоторые права человека не могут быть ограничены. К ним относятся запрет на применение пыток и жестокое, бесчеловечное или унижающее достоинство обращение или наказание, на рабство и подневольное состояние, а также принцип законности (права, являющиеся абсолютными). Абсолютный характер этих прав означает, что их нельзя ограничивать, уравновешивая их осуществление с нарушениями свободы мысли, совести и религии, а также свободы убеждений. Однако в этой связи следует отметить, что право исповедовать религию или веру, а также право на свободу выражения мнений могут быть ограничены в соответствии с условиями, установленными законодательством о правах человека.

32 Законные цели, служащие в качестве обоснования ограничений, относятся к конкретным правам, согласно положениям международных и региональных договоров о правах человека. Например, право исповедовать религию или веру может быть подвержено ограничениям, установленным законом и необходимым для защиты общественной безопасности, порядка, здоровья или морали или основных прав и свобод других лиц. Следует отметить, что, например, в отличие от свободы выражения мнений или свободы мирных собраний, свобода исповедовать религию или веру не может быть ограничена в интересах государственной безопасности.

33 См., например, Замечание общего порядка № 22 Комитета по правам человека, Статья 18, CCPR/C/21/Rev.1/Add.4, п. 8; Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 22.

человека отметил, что «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 силой или ее применения»[34]. В то же время, если безопасность государства ослаблена как раз по причине подавления прав человека, данный критерий не может служить основанием для дальнейших ограничений[35]. При этом известны случаи, когда государства неправомерно ссылались на императивы государственной безопасности, в частности на борьбу с терроризмом, в качестве предлога для расплывчатого оправдания произвольного вмешательства в права человека. Эта проблема не раз озвучивалась различными структурами и механизмами Организации Объединенных Наций по правам человека. Специальный докладчик ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение отметил следующее:

«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 является 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 транспарентности и подотчетности»[36].

4.3.2 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.

Предсказуемость означает, что закон должен быть сформулирован достаточно четко, с тем чтобы дать лицу возможность предвидеть, в разумной с учетом обстоятельств степени, последствия определенного действия и соответствующим образом следить за своим поведением[37]. Это требование предполагает не абсолютную предсказуемость, а то, что закон должен давать людям «адекватное указание на обстоятельства, при которых органы государственной власти имеют право вмешиваться в их права»[38]. Законы должны предоставлять лицам, которым поручено их осуществление, достаточные руководящие указания для того, чтобы они могли определить, когда права могут быть ограничены, а также должны устанавливать объем любых дискреционных полномочий, предоставленных компетентным органам, и порядок их осуществления[39]. Они также должны предусматривать достаточные гарантии против возможных злоупотреблений, такие как независимые проверки и надзор. Они должны содержать эффективные средства правовой защиты на случай нарушения прав человека. И, наконец, требование о достаточной доступности закона означает, что лица, на которых распространяется соответствующее законодательство, должны иметь возможность ознакомиться с его содержанием (в большинстве случаев это означает, что закон должен быть общедоступным)[40].

---

34 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.

35 Там же.

36 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

37 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.

38 См., например, Европейский суд по правам человека, *Мейлоун* против *Великобритании*, жалоба № 8691/79, 2 августа 1984 г., §§ 66–68.

39 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.

40 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, *«Гроппера Радио АГ» и другие* против *Швейцарии*, жалоба № 10890/84, Серия А № 173, 28 марта 1990 г., §§ 65–68.

В отношении наблюдения со стороны государства, которое может нарушать право на неприкосновенность частной жизни, например, Европейский суд по правам человека счел, что требование предсказуемости «не может быть абсолютно одинаковым в особом контексте перехвата сообщений в целях производства следствия полицией», пояснив далее, что это требование в данном конкретном контексте «не должно быть таким, чтобы позволять индивиду предвидеть, как и когда его сообщения подвергаются риску быть прослушанными властями с тем, чтобы он не мог вследствие этого менять свое поведение». Тем не менее Суд обратил внимание на то, что «закон должен использовать достаточно ясные термины, чтобы всем дать достаточное представление, при каких обстоятельствах и условиях он наделяет публичную власть правом проводить такое скрытое и, в буквальном смысле слова, опасное вмешательство в право на уважение частной жизни и тайны корреспонденции». Соответственно, «закон должен определить объем и условия осуществления таких полномочий компетентных органов с достаточной ясностью по отношению в установленной законом цели с тем, чтобы обеспечить индивиду адекватную защиту против произвольных действий»[41]. Секретные правила, руководства или толкования таких правил не обладают необходимыми качествами «закона»[42]. Решение о санкционировании такого вмешательства, например, посредством выдачи ордера, должно приниматься только конкретным органом, предусмотренным законом, и строго индивидуально[43].

4.3.3 Соразмерность

Любое вмешательство в ограничиваемое право не только должно осуществляться для достижения законной цели, но также должно быть необходимо для защиты этой цели. Требование необходимости устанавливает более высокий порог, чем просто «разумность или целесообразность». По сути, мера нарушает критерий необходимости, если защита может быть обеспечена другими способами, не ограничивающими рассматриваемое право.

Меры по ущемлению ограничиваемого права должны быть соразмерны преследуемой законной цели; 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[44]. Соответственно, в отношении ограничений права на неприкосно-

41 См., например, Европейский суд по правам человека, *Мейлоун* против *Великобритании*, жалоба № 8691/79, 2 августа 1984 г., §§ 67–68.

42 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/27/37, п. 29.

43 Замечание общего порядка № 16 Комитета по правам человека о праве на неприкосновенность частной жизни (статья 17), п. 8.

44 Межамериканский суд по правам человека использует термин «адекватные», а не «соразмерные». 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

венность частной жизни Европейский суд по правам человека постановил, что «всеобъемлющая без каких-либо оговорок» возможность 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[45].

4.3.4 Отсутствие дискриминации

Запрет на дискриминацию в международном праве прав человека является абсолютным, и никакие ограничения права на свободу от дискриминации и отступления от него не допускаются, независимо от того, имеет ли место чрезвычайная ситуация[46]. Основаниями, по которым запрещена дискриминация, являются пол, расовая принадлежность, цвет кожи, язык, религия, политические или иные убеждения, национальное или социальное происхождение, этническое происхождение[47], имущественное, сословное или иное положение.

В связи с этим ограничения прав человека всегда должны осуществляться с учетом запрета на дискриминацию[48]. Национальное законодательство, устанавливающее условия, при которых права человека могут быть ограничены, таким образом, должны содержать достаточные гарантии против дискриминационного применения.

4.3.5 Типовые положения о соответствии контртеррористической практики праву прав человека, беженскому праву и гуманитарному праву

Специальным докладчиком ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом (Специальным докладчиком по правам человека в условиях борьбы с терроризмом) были сформулированы типовые положения, касающиеся соответствия контртеррористических мер государств праву прав человека, беженскому праву, а также применимым нормам международного гуманитарного права (см. текстовую вставку ниже)[49].

---

45 Европейский суд по правам человека, *S. и Марпер* против *Соединенного Королевства* (2009) 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 С № 403, п. 53.

46 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 ОС-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.

47 Хотя «этническое происхождение» не включено в Международный пакт о гражданских и политических правах (ст. 26) в качестве основания, по которому запрещена дискриминация, оно указано в качестве такового в Статье 1 Международной конвенции о ликвидации всех форм расовой дискриминации.

48 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, 46; Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 32.

49 Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом Мартина Шейнина (A/HRC/16/51), Практика 2. URL: https://undocs.org/Home/Mobile?FinalSymbol=a%2Fhrc%2F16%2F51&Language=E&DeviceType=Desktop&LangRequested=False

ВСТАВКА 1. **Специальный докладчик ООН по правам человека в условиях борьбы с терроризмом: ограничение прав и свобод**

1. Осуществление функций и полномочий должно быть основано на четких положениях закона, в которых исчерпывающе перечисляются данные полномочия.
2. Ни при каких обстоятельствах осуществление таких функций и полномочий не может нарушать императивных или не допускающих отступлений норм международного права или умалять сущность любого из прав человека.
3. В тех случаях, когда осуществление функций и полномочий предполагает ограничение права человека, которое можно ограничивать, любое такое ограничение должно быть как можно менее интрузивным и:
   - быть необходимым в демократическом обществе для осуществления определенной законной цели, если это допускается международным правом;
   - быть соразмерным пользе, получаемой в случае достижения этой законной цели.
4. Если государство принимает участие в происходящем вооруженном конфликте как одна из его сторон, вышеуказанные положения применяются также для обеспечения соблюдения принципов и положений международного гуманитарного права, причем без ущерба для обязательства соблюдать международное право прав человека и беженское право.
5. Если веские причины требуют наделения некоторых органов конкретными полномочиями:
   - такие полномочия должны быть частью специального законодательства, которое может быть признано единственным исключением из обычного правового ограничения;
   - требования, в соответствии с которыми устанавливаются такие полномочия, должны подчиняться положениям об истечении срока действия и подвергаться регулярному обзору; и
   - использование таких полномочий в целях, не относящихся к борьбе с терроризмом, должно быть запрещено.

[V]

Определения терроризма и подстрекательства к терроризму

5.1 Определение терроризма

Механизмы Организации Объединенных Наций по правам человека и другие заинтересованные стороны неоднократно выражали свою обеспокоенность по поводу последствий чрезмерно широких определений терроризма и связанных с ним преступлений[50], которые в некоторых случаях включали действия, защищаемые международным правом прав человека.

Одним из обязательных условий контртеррористических усилий, не нарушающих право прав человека, является присутствие политико-правовых основ, базирующихся на четких и ясных определениях терроризма и связанных с ним преступлений, включая подстрекательство к терроризму. Эти определения не должны быть чрезмерно широкими или расплывчатыми и не должны включать в себя ненасильственные действия или законные высказывания, включая инакомыслие, критику или нонконформизм. Нечеткие формулировки в законах часто используются для причисления представителей гражданского общества к террористам и преследования их за преступления, связанные с терроризмом. В других случаях контртеррористические меры вводятся для ограничения доступа организаций гражданского общества к финансированию и, следовательно, сужения их деятельности[51].

Согласно пункту 3 резолюции 1566 (2004) Совета Безопасности, терроризм определяется как «преступные деяния, в том числе против гражданского населения, совершаемые с намерением причинить смерть или тяжкие 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»[52].

Специальным докладчиком ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом (Специальным докладчиком по правам человека в условиях борьбы с терроризмом) было предложено схожее типовое определение, отражающее передовую практику в борьбе с терроризмом и разработанное по результатам анализа, проведенного на основе консультаций и различных форм взаимодействия с многочисленными заинтересованными сторонами, включая правительства[53].

---

50 См., например, «Защита прав человека и основных свобод в условиях борьбы с терроризмом». Доклад Генерального секретаря. (A/68/298); Доклад Верховного комиссара Организации Объединенных Наций по правам человека о защите прав человека и основных свобод в условиях борьбы с терроризмом. (A/HRC/28/28); Международная комиссия юристов. (2009). Доклад Группы видных юристов по вопросам терроризма, борьбы с терроризмом и прав человека.

51 Доклад Генерального секретаря «Терроризм и права человека», A/76/273 (2021), пп. 22, 24. URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F273&Language=E&DeviceType=Desktop&LangRequested=False

52 Актуальным также является определение терроризма, представленное в резолюции 51/210 Генеральной Ассамблеи: «...преступные акты, направленные или рассчитанные на создание обстановки террора среди широкой общественности, группы лиц или конкретных лиц в политических целях... какими бы ни были соображения политического, философского, идеологического, расового, этнического, религиозного или любого другого характера, которые могут приводиться в их оправдание».

53 Доклад Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом, 2010, A/HRC/16/51. URL: https://undocs.org/Home/Mobile?FinalSymbol=a%2Fhrc%2F16%2F51&Language=E&DeviceType=Desktop&LangRequested=False

ВСТАВКА 2. **Определение терроризма**

Терроризм означает действие или попытку совершения действия, когда: 1. Действие: *a*) представляет собой преднамеренный захват заложников; или *b*) имеет целью причинить смерть или тяжкое телесное повреждение одному или нескольким представителям населения в целом или некоторых его слоев; или *c*) повлекло за собой смерть или было связано с серьезным физическим насилием в отношении одного или нескольких представителей населения в целом или некоторых его слоев; 2. Действие осуществлено или предпринята попытка его осуществления с целью: *a*) вызвать состояние страха среди широкой общественности или какого-либо сегмента населения; или *b*) принудить правительство или международную организацию совершить какое-либо действие или воздержаться от его совершения; и 3. Действие соответствует: *a*) определению тяжкого преступления в национальном законодательстве, принятого в целях соблюдения международных конвенций и протоколов, касающихся терроризма, или резолюций Совета Безопасности, касающихся терроризма; или *b*) всем элементам тяжкого преступления, определенного в национальном законодательстве.

И пункт 3 Резолюции 1566 (2004) Совета Безопасности, и типовое определение, разработанное по мандату Специального докладчика по правам человека в условиях борьбы с терроризмом, по своему охвату ограничиваются действиями, направленными на то, чтобы: *a*) создать обстановку террора или вызвать состояние ужаса у широких слоев населения или группы лиц и *b*) незаконно принудить правительство или международную организацию к совершению или отказу от совершения какого-либо действия.

Специальным докладчиком по правам человека в условиях борьбы с терроризмом неоднократно подчеркивалась важность сужения определений борьбы с терроризмом и вытекающих из них мер до действий, которые действительно носят террористический характер. Таким образом, все контртеррористические законы «должны ограничиваться борьбой с преступлениями, являющимися таковыми, по смыслу и согласно определениям международных конвенций и протоколов, касающихся терроризма, или борьбой со связанными с этими деяниями, о которых идет речь в резолюциях Совета Безопасности и в которых присутствуют элементы намерения и цели, указанные в резолюции 1566 (2004) Совета Безопасности»[54]. В частности, «[н]а преступления, которые не подпадают под категорию терроризма (…), независимо от того, насколько они серьезны, не должно распространяться действие законодательства о борьбе с терроризмом»[55].

ВСТАВКА 3. **По мандату Специального докладчика было разработано типовое определение подстрекательства к терроризму, основанное на передовом опыте**

Это преступление заключается в умышленном и противозаконном распространении или направлении иным образом обращения к общественности с целью подстрекательства к совершению террористического преступления, если такое поведение, являющееся или не являющееся прямой пропагандой террористических преступлений, создает угрозу того, что такое преступление или преступления могут быть совершены[56].

Защита свободы выражения мнений по международному праву прав человека включает даже такую форму выражения мнений, которая может рассматриваться как глубоко оскорбительная[57]. В то же время некоторые формы выражения мнений, которые не могут считаться истинно террористическими и не подпадают под вышеуказанное определение, могут, тем не менее, быть незаконными. В частности, они могут включать пропаганду национальной, расовой или религиозной ненависти, представляющую собой подстрекательство к дискриминации, вражде или насилию, и должны рассматриваться в соответствии со статьями 20 и 19(3) Международного пакта о гражданских и политических правах и стандартами, изложенными в Рабатском плане действий по запрещению пропаганды национальной, расовой и религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию[58].

54 E/CN.4/2006/98, п. 39.

55 Там же, п. 47.

56 A/HRC/16/51, Практический метод 8.

57 Замечание общего порядка № 34 Комитета по правам человека. Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, п. 11.

58 A/HRC/22/17/Add.4, в частности, п. 29.

ВСТАВКА 4. **Определение терроризма МАСПЧ***

Контртеррористическое законодательство страны X включало положение, согласно которому «если не установлено иное, намерение посеять страх среди населения в целом презюмируется, если преступление было совершено с использованием взрывчатых веществ или зажигательных устройств…».

Межамериканский суд по правам человека постановил, что данная формулировка, включающая презумпцию намерения, является нарушением основополагающего принципа презумпции невиновности, а также принципа законности.

Норин Катриман и др. против *Чили,* пп. 170-171 и 174.

* Межамериканский суд по правам человека

ВСТАВКА 5. **ЕСПЧ* о качестве национального законодательства**

В деле против Турции Суд отметил, что ему «известно о сложностях борьбы с терроризмом и разработки уголовного законодательства о противодействии терроризму. Государства-участники в силу необходимости используют достаточно общие выражения», и, «осуществляя толкование соответствующих правовых норм, суды обязаны обеспечивать человеку достаточную защиту от произвола». Согласно тексту решения Суда, Комиссар по правам человека отметил, что в Турции доказательства, которые используются в качестве обоснования заключения под стражу, все чаще сводятся исключительно к высказываниям и действиям, которые «явно не имеют насильственного характера», и что во многих случаях турецкие суды принимают решения о заключении под стражу по обвинению в принадлежности человека к вооруженной организации на основании весьма неубедительных доказательств. Суд заключил, что диапазон действий, которые могли бы оправдать заключение заявителя под стражу в связи с тяжкими преступлениями, ответственность за которые предусмотрена Уголовным кодексом Турции, такими как членство в вооруженной организации, настолько широк, что содержание этой статьи в сочетании с ее толкованием турецкими судами не обеспечивает надлежащей защиты от произвольного вмешательства властей. По мнению Суда, такое широкое толкование «уголовно-правовой нормы нельзя оправдать, когда оно приводит к тому, что ставится знак равенства между осуществлением права на свободу выражения мнения и принадлежностью к вооруженной террористической организации, созданием такой организации или руководством ею в отсутствие каких-либо конкретных доказательств такой связи». На этом основании он постановил, что вмешательства в свободу выражения мнений заявителя не соответствовали требованию о качестве закона.

Селахаттин Демирташ против *Турции* (№ 2), пп. 279–281.
* Европейский суд по правам человека

5.1.1 Определение подстрекательства к терроризму

В резолюции 1624 Совета Безопасности Организации Объединенных Наций содержится призыв к государствам ввести законы, запрещающие подстрекательство к терроризму, однако не приводится определение подстрекательства. Специальный докладчик по борьбе с терроризмом и правам человека предложил следующее определение:

> Это преступление заключается в умышленном и противозаконном распространении или направлении иным образом обращения к общественности с целью подстрекательства к совершению террористического преступления, если такое поведение, являющееся или не являющееся прямой пропагандой террористических преступлений, создает угрозу того, что такое преступление или преступления могут быть совершены.

ВСТАВКА 6. **ЕСПЧ* постановил, что обвинительный приговор за одобрение терроризма не нарушает свободу выражения мнений заявителя**

Заявитель, будучи карикатуристом, был признан виновным в одобрении терроризма после публикации рисунка, изображающего атаку на Всемирный торговый центр с подписью: «Мы все мечтали об этом — ХАМАС сделал».

Суд счел, что карикатура не ограничивается критикой американского империализма, но поддерживает и прославляет его разрушение с помощью насилия в отношении тысяч гражданских лиц. Суд также одобрительно отметил, что заявитель был приговорен к разумному штрафу.

Леруа против *Франции*, пп. 43 и 47.

* Европейский суд по правам человека

[VI] Наблюдение в Интернете и неприкосновенность частной жизни

6.1 Нормы и стандарты международного права в области прав человека, касающиеся мер наблюдения

Право на неприкосновенность частной жизни защищено международными и региональными договорами о правах человека. Статья 17 Международного пакта о гражданских и политических правах предусматривает следующее:

> **„Никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств“.**

Право на неприкосновенность частной жизни также защищено статьей 8 Европейской конвенции по правам человека и статьей 11 Американской конвенции по правам человека. Африканская комиссия по правам человека и народов утверждает, что элементы права на неприкосновенность частной жизни могут быть выведены из Африканской конвенции о правах человека и народов[59]. В седьмом обзоре Глобальной контртеррористической стратегии Организации Объединенных Наций государства-члены призвали «соблюдать и защищать право на неприкосновенность частной жизни, [...] в том числе в контексте цифровой связи и в условиях борьбы с терроризмом, и принимать меры для обеспечения того, чтобы препятствия для осуществления этого права или его ограничения не были произвольными, надлежащим образом регулировались законом, подпадали под действенный надзор и охватывались механизмами надлежащей правовой защиты, в том числе с использованием судебного надзора или других правовых средств»[60].

Вмешательство в право на неприкосновенность частной жизни для оказания помощи правоохранительным органам и спецслужбам в охране общественного порядка, общественной или национальной безопасности может соответствовать международному праву прав человека в том случае, если соответствующие меры предусмотрены законом, являются необходимыми и соразмерными. Новые технологии значительно расширили возможности наблюдения, поскольку информация больше не хранится в закрытых помещениях, а может находиться на компьютерах, телефонах, аккаунтах в социальных сетях, устройствах геолокации и т. д. Конституционный суд ЮАР отметил, что: «[с]овременные технологии позволяют правоохранительным органам не только физически вторгаться в интимную личную сферу жизни людей (в отличие от электронного вторжения), но также и поддер-

59 Африканская комиссия по правам человека и народов, Принципы и руководящие положения по правам человека и народов в условиях борьбы с терроризмом в Африке, раздел 11, URL: https://achpr.au.int/sites/default/files/files/2021-05/principlesandguidelinesonhumanandpeoplesrightswhilecounteringterrorisminafrica.pdf

60 A/RES/77/298, п. 11.

живать и укреплять свое присутствие в ней, постоянно собирая, сохраняя и — при необходимости — используя информацию»[61].

ВСТАВКА 7. ЕСПЧ* о скрытом наблюдении

Ввиду риска того, что система секретного наблюдения, призванная защищать национальную безопасность (и другие важнейшие национальные интересы), может нанести урон надлежащему функционированию демократических процессов или даже уничтожить их под предлогом их защиты, Суд должен убедиться в существовании адекватных и эффективных гарантий против злоупотреблений. Эта оценка зависит от (...) содержания, объема и продолжительности возможных мер, оснований, необходимых для санкционирования таких мер, органов, компетентных разрешать, выполнять и контролировать такие действия, и от вида средств правовой защиты, предусмотренных национальным законодательством.

Big Brother Watch и другие против *Соединенного Королевства*

* Европейский суд по правам человека

ВСТАВКА 8. Пример законодательства о сборе данных, предоставляющего правоохранительным органам чрезмерные полномочия по наблюдению

В государстве-члене F новый закон о кибербезопасности обязывает все онлайн-платформы сохранять сведения о гражданах: имена пользователей, даты рождения, гражданство, данные удостоверений личности, номера кредитных карт, биометрические файлы и медицинские записи. Власти могут получить доступ к данным на основании нечетко сформулированных соображений национальной безопасности и общественного порядка.

Еще в 1978 году Европейский суд по правам человека рассматривал вопрос об опасности нерегулируемого наблюдения при борьбе с терроризмом, отметив, что «[о]сознавая опасность, что [нерегулируемое наблюдение] может подорвать и даже уничтожить демократию под предлогом ее защиты, Суд утверждает, что [...] Стороны не могут во имя борьбы против шпионажа и терроризма предпринимать любые действия, которые они считают подходящими»[62]. Он также отметил, что риски произвола и злоупотребления присущи любой системе тайного наблюдения, и поскольку осуществление скрытых мер наблюдения не подлежит проверке со стороны заинтересованных лиц или широкой общественности, исполнительная власть или судья не могут быть наделены неограниченной свободой действий[63].

Аналогичным образом, Межамериканский суд выразил опасение, что «законы, разрешающие перехват и мониторинг... сообщений, которые были разработаны для борьбы с преступностью, могут стать инструментом для шпионажа и преследования в случае неправильной интерпретации и применения. Поэтому, учитывая опасность злоупотреблений в любой системе мониторинга, эта мера должна быть основана на особенно четком законодательстве с ясными и подробными правилами». Он также постановил, что «наблюдение, вмешательство, запись и распространение сообщений запрещены, за исключением случаев, установленных законом, которые адаптированы к объектам и целям Американской конвенции[64].

Эти опасения оправдались, поскольку было доказано, что национальные власти в нескольких государствах-членах по всему миру используют как старые, так и новые технологии для незаконного или произвольного наблюдения за деятельностью журналистов, правозащитников, борцов с коррупцией, студенческих активистов, диссидентов и других категорий лиц, которые считаются помехой или угрозой для государственной политики или легитимности конкретных правительств.

Новые технологии и методы сбора данных оказывают неблагоприятное воздействие на меньшинства и тесно связаны с гендерной проблематикой. В ходе контртеррористических операций семья и домашнее пространство часто являются неотъемлемой частью мер наблюдения; кроме того, незаконное использование контр-

61 Конституционный суд ЮАР, Решение по делу Центра журналистских расследований Амабхунгане, дело CCT 278/19, п. 2. URL: https://privacyinternational.org/sites/default/files/2021-02/%5BJudgment%5D%20CCT%20278%20of%2019%20and%20279%20of%2019%20AmaBhungane%20Centre%20for%20Investigative%20Journalism%20v%20Minister%20of%20Justice%20and%20Others.pdf

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

63 См., например, Европейский суд по правам человека, *Роман Захаров* против *России*, пп. 299–231.

64 Межамериканский суд по правам человека, *Эшер* против *Бразилии*, п. 118. URL: https://corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf

террористических мер также продемонстрировало модели установления наблюдения за целыми семьями, что напрямую влияет на право на неприкосновенность частной жизни. Например, женщины сразу же считаются подозреваемыми в силу семейных или социальных связей с определенными мужчинами. Матери и жены неизменно ассоциируются с насильственными действиями своих детей или мужей, их дома часто становятся местом навязчивых и сопровождающихся жестокостями обысков со стороны государства, а сами они нередко подвергаются постоянным преследованиям и слежке. Были выявлены массовые нарушения и злоупотребления в области применения законодательства о наблюдении, когда наблюдение устанавливается за определенными общинами и группами на основе этнического происхождения, расы и религии[65].

В отношении слежения за цифровыми сообщениями Генеральная Ассамблея призвала государства внедрить нормативно-правовую базу, которая должна быть доступной для общественности, ясной, точной, всесторонней и недискриминационной[66]. В резолюции 42/15 о праве на неприкосновенность частной жизни в цифровой век Совет по правам человека более подробно рассмотрел эти вопросы, призвав государства[67]:

- обеспечивать, чтобы любые меры, принимаемые для борьбы с терроризмом и насильственным экстремизмом, создающим питательную среду для терроризма, которые нарушают право на неприкосновенность частной жизни, отвечали принципам законности, необходимости и соразмерности;
- создавать новые или продолжать использовать уже имеющиеся независимые, эффективные, обеспеченные надлежащими ресурсами и беспристрастные внутренние механизмы судебного, административного и (или) парламентского надзора, позволяющие обеспечивать транспарентность, сообразно обстоятельствам, и подотчетность в связи с осуществлением государствами слежения за сообщениями, их перехвата и сбора персональных данных;
- разрабатывать или продолжать применять и осуществлять надлежащие законы, предусматривающие эффективные санкции и средства правовой защиты, для защиты лиц от нарушений и ущемлений права на неприкосновенность частной жизни, заключающихся в противоправных или произвольных действиях по сбору, обработке, хранению или использованию персональных данных физическими лицами, правительствами, коммерческими предприятиями и частными организациями.

Руководящие принципы, установленные Европейским судом по правам человека, содержат дополнительные полезные положения в данном отношении. Суд определил следующие минимальные гарантии, которым должен отвечать закон о наблюдении, чтобы быть совместимым с правом на уважение частной и семейной жизни[68]:

- характер преступлений, в связи с которыми может быть выдан ордер на перехват, должен быть изложен четко и ясно;
- закон должен четко указывать категории лиц, за которыми может вестись наблюдение;
- операции по наблюдению должны быть строго ограничены по времени;
- должны быть разработаны процедуры, предписывающие изучение, использование, хранение и сохранение данных, полученных в результате наблюдения;
- в законе должны быть прописаны меры предосторожности, которые необходимо соблюдать при передаче данных третьим лицам;
- должны существовать правила хранения перехваченной информации; тот факт, что фрагмент информации может однажды оказаться полезным, не оправдывает бессрочного хранения тысяч единиц такой информации;
- должны существовать независимые органы, ответственные за надзор за программами наблюдения.

65 См., например, A/HRC/46/36, пп. 11 и 26.

66 A/Res/ 73/179.

67 A/HRC/RES/42/15, п. 6.

68 Статья 8 Европейской конвенции о правах человека. См. также 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. 17, URL: https://www.law.berkeley.edu/wp-content/uploads/2022/05/Amicus-Brief-CCAJAR-v.-Colombia.pdf; ЕСПЧ, *Класс и другие* против *Германии*, № 5029/71, 6 сентября 1978 г., пп. 42 и 49, *Либерти и другие* против *Соединенного Королевства*, № 58243/00, 1 июля 2008 г. и *Ротару* против *Румынии*, № 28341/95,[GC], 4 мая 2000 г., о наблюдении, осуществляемом спецслужбами.

Специальные докладчики по вопросу свободы выражения мнений Организации Объединенных Наций и Организации американских государств (OAS) выпустили совместную декларацию, в которой был принят аналогичный подход[69]:

> Государства должны гарантировать, что перехват, сбор и использование персональной информации, включая все ограничения права затронутого лица на доступ к этой информации, должны быть четко санкционированы законом, чтобы защитить их от произвольного или неправомерного вмешательства в их частные интересы. Закон должен устанавливать ограничения в отношении характера, объема и продолжительности этих видов мер; основания для их принятия; органы, уполномоченные санкционировать, осуществлять и контролировать их применение; а также правовые механизмы, с помощью которых они могут быть оспорены.
>
> Учитывая важность осуществления этих прав для демократической системы, закон должен разрешать доступ к сообщениям и личной информации только в самых исключительных обстоятельствах, определенных законодательством. Если в качестве основания для наблюдения за корреспонденцией и сбора персональной информации указывается национальная безопасность, в законе должны быть четко прописаны критерии, которые должны использоваться для определения случаев, когда указанные меры являются законными. Они должно быть разрешены только в случае, если присутствует явный риск для защищаемых интересов и если ущерб, который может быть нанесен, превышает общий интерес общества в поддержании права на неприкосновенность частной жизни и свободное распространение идей и информации. Сбор данной информации должен осуществляться под контролем независимого надзорного органа и регулироваться достаточными гарантиями соблюдения процессуальных норм и судебным надзором в рамках ограничений, допустимых в демократическом обществе.

69 Совместная декларация о программах наблюдения и их воздействии на свободу выражения мнений, выпущенная Специальным докладчиком ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение и Специальным докладчиком по вопросу свободы выражения мнений Межамериканской комиссии по правам человека, июнь 2013 г., пп. 8 и 9, URL: http://www.oas.org/en/iachr/expression/showarticle.as p?artID=927&lID=1

ВСТАВКА 9. **ЕСПЧ* констатирует отсутствие достаточных гарантий от злоупотреблений в законодательстве о наблюдении**

Оценивая законодательство государства о наблюдении, Суд отметил опасность современных средств наблюдения, указав, что «естественным последствием форм, принимаемых современным терроризмом, является то, что правительства прибегают к передовым технологиям в предотвращении террористических атак, включая массовое наблюдение за сообщениями, способными содержать показатели приближающихся инцидентов.... [однако] парадоксальная замена террористической угрозы угрозой вторжения неограниченной исполнительной власти в частную жизнь людей путем техник и прерогатив неконтролируемого, но далеко идущего наблюдения, будет противоречить цели правительственных усилий по борьбе с терроризмом и восстановлению веры граждан в способность правительства поддерживать общественную безопасность.... С учетом риска того, что система тайного наблюдения, созданная для защиты национальной безопасности, может повредить или даже уничтожить демократию под прикрытием ее защиты, Суд должен быть удовлетворен тем, что существуют надлежащие и эффективные гарантии против злоупотребления». Следовательно, Суд заключил, что закон должен обозначать объем любого такого усмотрения, предоставленного компетентным органам, и способ его осуществления с достаточной ясностью.

Рассматривая соблюдение государством этого принципа, Суд отметил, что в государстве почти любой человек может подвергнуться наблюдению, поскольку не существует никакого требования, чтобы власти продемонстрировали фактическую или предполагаемую связь между объектами наблюдения и предотвращением террористической угрозы. Отсутствие требования о предоставлении просителем разрешения на наблюдение достаточной фактической базы сделало процесс утверждения неактуальным, поскольку оценка необходимости интрузивных мер на основании индивидуального подозрения в отношении конкретного человека не представлялась возможной. Суд также отметил, что закон не предусматривает судебного санкционирования ордеров или их продления, и что вместо этого санкционирование осуществляется Министерством юстиции, а не независимым органом. Суд также выразил обеспокоенность отсутствием положений, касающихся возможности возмещения ущерба лицам, незаконно подвергшимся тайному наблюдению, а также отсутствием независимого надзорного механизма. Суд также не нашел положения о хранении, обработке и удалении данных осуществимыми при данных обстоятельствах.

Таким образом, суд пришел к выводу, что законодательство не обеспечивает достаточно точных, эффективных и всеобъемлющих гарантий в отношении авторизации и осуществления мер наблюдения, а также потенциальных мер по возмещению ущерба.

Сабо и Виши против *Венгрии*

*Европейский суд по правам человека

6.2 Метаданные/массовое наблюдение

Метаданные (коммуникационные данные) обычно определяют 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. Однако из-за развития технологий метаданные, включая идентификацию владельца IP-адреса, абонентских данных, идентификатора мобильного устройства или IP-адреса электронной почты, идентификатора мобильного абонента (IMSE) и адреса электронной почты, могут быть весьма информативными в экосистеме, где люди оставляют свои электронные следы в создаваемом ими цифровом контенте. В связи с этим метаданные могут позволить определить контент, к которому они относятся, в результате чего сбор и использование таких данных могут быть в высокой степени интрузивными[70]. Соответственно, любые различия между метаданными и контентом будет все труднее обосновать, что неоднократно подчеркивалось международными и региональными механизмами и организациями в области прав человека. Верховный комиссар Организации Объединенных Наций по правам человека отметил, что метаданные «могут дать даже еще более полное представление о поведении человека, его социальных отношениях, личных предпочтениях и личности, чем то, что можно было бы узнать из самого содержания частного общения»[71] и заявил, что усиление защиты неприкосновенности частной жизни требу-

70 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

71 A/HRC/27/37, п. 19.

ет эквивалентной защиты метаданных. Аналогичные изменения нашли отражение, помимо прочего, в прецедентном праве Европейского суда по правам человека и Межамериканского суда по правам человека[72].

В отношении массового сбора и использования метаданных органами безопасности и разведки Суд Европейского союза постановил, что «данные, взятые в целом, могут позволить сделать очень точные выводы о частной жизни лиц, чьи данные были сохранены, в том числе об их повседневных привычках, постоянном или временном месте жительства, ежедневных или иных передвижениях, выполняемых видах деятельности, социальных связях этих людей и общественных местах, которые они посещают»[73].

В рассматриваемом деле он отметил, что оспариваемое законодательство, предусматривающее неизбирательное хранение массовых данных, не требовало установления какой-либо связи между данными, подлежащими хранению, и угрозой общественной безопасности[74]. Следовательно, он постановил, что национальное законодательство, требующее от поставщиков услуг электронной связи хранения указанных данных в общем и неизбирательном порядке для целей охраны национальной безопасности, является незаконным[75]. В отношении национальных ведомств, желающих получить доступ к таким данным, Суд постановил, что «общий доступ ко всем хранящимся (частными компаниями) данным, независимо от наличия какой-либо связи, хотя бы косвенной, с преследуемой целью, не может рассматриваться как ограниченный строгой необходимостью» и, соответственно, доступ может быть предоставлен только к «данным лиц, подозреваемых в планировании или совершении тяжкого преступления или в причастности тем или иным образом к такому преступлению» и что такой доступ также требует предварительного разрешения судебного или независимого административного органа[76].

Однако он добавил, что государством может быть принято законодательство, разрешающее целевое хранение данных о трафике и местоположении в качестве превентивной меры и для целей борьбы с тяжкими преступлениями, при условии, что «хранение будет ограничено строгой необходимостью в отношении категорий данных, подлежащих хранению, затрагиваемых средств связи, соответствующих лиц и установленного периода хранения»[77].

72 См., например, *Big Brother Watch и другие* против *Соединенного Королевства* [GC], *№№ 58170/13, 62322/14 и 24960/15*, Решение от 25 мая 2021 г.; *Эшер и другие* против *Бразилии*, Решение от 6 июля 2009 г.

73 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. 99.

74 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, пп. 103, 106.

75 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. 107.

76 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. 119, 125.

77 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. 108.

6.3 Выдача разрешений, надзор и средства правовой защиты

ВСТАВКА 10. **Резолюция 75/176* Генеральной Ассамблеи о праве на неприкосновенность частной жизни в цифровую эпоху**

Эта резолюция призывает государства-члены, помимо прочего, создавать новые или продолжать использовать уже имеющиеся независимые, эффективные, обеспеченные надлежащими ресурсами и беспристрастные внутренние механизмы судебного, административного и (или) парламентского надзора, позволяющие при необходимости обеспечивать транспарентность, сообразно обстоятельствам, и подотчетность в связи с осуществлением государствами слежения за сообщениями, их перехвата и сбора персональных данных...

и в соответствии с международными обязательствами в области прав человека предоставлять лицам, чье право на неприкосновенность частной жизни было нарушено в результате противоправного или произвольного слежения, доступ к эффективным средствам правовой защиты.

В Замечании общего порядка № 16 по статье 17 (право на неприкосновенность частной жизни) Комитет по правам человека отметил, что решение о санкционировании вмешательства в право на неприкосновенность частной жизни должно приниматься только конкретным органом, предусмотренным законом, и строго индивидуально[78]. Европейский суд по правам человека указал на то, что санкционирование наблюдения со стороны несудебного органа допускается, если этот орган достаточно независим от исполнительной власти. В то же время Суд отметил, что вмешательство властей в права человека должно «подлежать эффективному контролю, который обычно должен быть закреплен в судебном порядке, хотя бы в крайнем случае, судебный контроль предоставляет лучшие гарантии независимости, беспристрастности и надлежащей процедуры»[79]. Как подчеркивалось Комитетом по правам человека, такое санкционирование должно осуществляться в индивидуальном порядке[80]. Более того, оно должно основываться на фактах. Например, в деле *Эшер* против *Бразилии* Межамериканский суд по правам человека выразил обеспокоенность по поводу того, что суд выдал разрешение на наблюдение, несмотря на то что запрос на него не был основан на каких-либо фактах или причинах. Он также отметил, что органы, запросившие разрешение, не указали, что менее интрузивные средства получения информации были недоступны[81].

ВСТАВКА 11. **Тшванский принцип[82] 10. E**

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.

78 Замечание общего порядка № 16, п. 8.

79 См., например, *Сабо и Виши* против *Венгрии*, п. 77.

80 Замечание общего порядка № 16, п. 8.

81 Пп. 92, 134, 135, 140. 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, URL: https://espchhelp.ru/blog/4219-varga-protiv-slovakii

82 Тшванские принципы национальной безопасности и права на информацию, выпущенные в июне 2013 года, представляют собой руководство для законодателей и должностных лиц, занимающихся разработкой, пересмотром и внедрением законов или положений, касающихся полномочий государств в области сокрытия информации по соображениям национальной безопасности и наказания за раскрытие указанной информации. Они были составлены на основе международного и национального права, стандартов и практики по результатам широких консультаций, проведенных при содействии фонда Open Society Justice с участием широкого круга экспертов из правительственных учреждений, сферы национальной безопасности, международных организаций, гражданского общества и научных кругов. Свой вклад в процесс консультаций внесли четыре мандатария специальных процедур ООН, включая Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение и Специального докладчика по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом. Парламентская ассамблея Совета Европы одобрила указанные принципы в октябре 2013 года, призвав государства — члены Совета Европы принять их «во внимание при модернизации своего законодательства и практики» (резолюция 1954 (2013).

В соответствии с международными нормами и стандартами в области прав человека, наблюдение должно быть разрешено только на ограниченный срок, хотя разрешение может быть продлено или возобновлено при условии, что будет доказана необходимость и соразмерность мер. Кроме того, разрешение должно быть четко сформулированным. Так, например, если разрешение дается только на сбор данных с телефона субъекта, данные с его компьютера сбору не подлежат.

Вопрос о прослушивании телефонных разговоров рассматривался Европейским судом по правам человека в ряде дел. Гарантии, установленные Судом для обеспечения реализации указанных мер в соответствии с нормами и стандартами в области прав человека, применимы и к другим формам наблюдения, включая наблюдение в Интернете. Разрешение на наблюдение должно содержать следующую информацию:

- данные о лицах, за коммуникациями которых будет вестись наблюдение;
- характер преступлений, позволяющий использование наблюдение;
- продолжительность наблюдения;
- процедуру составления кратких отчетов о содержании перехваченных сообщений;
- меры предосторожности, которые необходимо принимать в целях передачи записей в нетронутом и полном виде;
- обстоятельства, в том числе предельные сроки, при которых перехваченная информация должна быть стерта или уничтожена, например, после снятия обвинения или оправдания обвиняемого[83].

6.3.1 Механизмы надзора[84]

Комитет по правам человека отметил, что законодательство, регулирующее осуществление мер наблюдения, включая перехват личных коммуникаций, и использование хакерских технологий, должно предусматривать четко определенные гарантии от злоупотреблений, в число которых должны входить надежные и независимые системы надзора[85].

Надзор за деятельностью субъектов сферы безопасности может принимать различные формы, включая внутренний надзор, независимый внешний надзор (внесудебный и судебный) и парламентский надзор[86].

Первая степень контроля в любой системе подотчетности правоохранительных органов — 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;
- внутреннюю отчетность и дисциплинарные меры.

Поэтому 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 или контролироваться судебным представителем или органом либо аналогичным независимым механизмом, до начала такой деятельности, насколько это возможно. Европейский суд по правам человека постановил, что в той области, где

83 См. *Хювик* против *Франции*, 24 апреля 1990 г., § 34, Серия A № 176 B и *Крюслен* против *Франции*, 24 апреля 1990 г., § 35, Серия A № 176-A; ЕСПЧ, *Гройтер* против *Нидерландов*, жалоба № 40045/98, 19 марта 2002 г. Также см. ОБСЕ/БДИПЧ, Права человека в антитеррористических расследованиях: практическое руководство для сотрудников правоохранительных органов, сноска 48, цитата из публикации «Борьба с терроризмом и защита прав человека: руководство», с. 246.

84 См. Управление Организации Объединенных Наций по наркотикам и преступности, URL: https://www.unodc.org/e4j/en/crime-prevention-criminal-justice/module-5/key-issues/2--key-mechanisms-and-actors-in-police-accountability-and-oversight.html

85 CCPR/C/ITA/CO/6, п. 37. См. также резолюцию 73/179 Генеральной Ассамблеи.

86 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

велика потенциальная вероятность злоупотреблений в конкретных делах, что может иметь пагубные последствия для демократического общества в целом, в принципе желательно, чтобы надзорные функции выполнял суд[87]. Суд выразил мнение, что орган, санкционирующий перехват, должен быть независимым, либо должен существовать контроль за деятельностью санкционирующего органа со стороны судьи или независимого органа. Соответственно, в этой области, контроль со стороны независимого органа, обычно судьи с особым опытом, должен быть правилом, а запасные методы — исключением, обеспечивающим пристальный контроль[88]. В некоторых системах континентальной правовой традиции существует институт судьи-следователя, ответственного за надзор за текущей деятельностью правоохранительных органов. И во всех системах судебная власть призвана рассматривать обвинения в неправомерных действиях полиции 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 всеобъемлющей правовой базы для программ наблюдения, осуществляемых правоохранительными органами, которая соответствовала бы международному праву 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 скрытых операций или программ наблюдения.

Некоторые государства-члены также создали независимые экспертные органы или ведомства по защите данных специально для надзора за программами наблюдения. Конкретная форма надзорного органа не регулируется международным правом, но указанные органы должны быть независимыми, располагать необходимыми ресурсами, бюджетом, специальными знаниями и материалами, должны обладать достаточными полномочиями, предусмотренными законом, включая инициирование и проведение независимых расследований с полным и беспрепятственным доступом к информации, сотрудникам и объектам, а также правом на вынесение постановления о прекращении мер по сбору информации[89].

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. Надзорные механизмы могут давать рекомендации по проведению институциональных и законодательных реформ, которые должны быть надлежащим образом рассмотрены соответствующими исполнительными и законодательными органами[90]. Надзорные механизмы могут давать рекомендации по проведению институциональных и законодательных реформ, которые должны быть надлежащим образом рассмотрены соответствующими исполнительными и законодательными органами.

6.3.2 Право на эффективные средства правовой защиты

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; и *c*) обеспечить применение компетентными властями средств правовой защиты, когда они предоставляются.

87 Европейский суд по правам человека, *Класс и другие* против *Германии*, № 5029/71, 6 сентября 1978 г., п. 56.

88 Европейский суд по правам человека, *Думитри Попеску* против *Румынии*, № 71525/01, 26 апреля 2017 г., пп. 70–73; Европейский суд по правам человека, *Сабо и Виши* против *Венгрии*, № 37138/14, п. 77.

89 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://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F14%2F46&Language=E&DeviceType=Desktop&LangRequested=False

90 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://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement

Средства правовой защиты могут включать, среди прочего, штрафы и санкции в отношении соответствующего лица или органа, причастного к противоправному поведению, а также компенсацию пострадавшему(-им). Растет консенсус в отношении того, что для практической реализации этого права люди должны иметь возможность получать информацию об осуществлявшемся в их отношении наблюдении постфактум.

Эффективность средств правовой защиты предполагает, что любое лицо, считающее, что его права были нарушены, имеет возможность обратиться с жалобой в суд или надзорное учреждение для получения необходимой защиты, включая полное возмещение причиненного вреда. 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. Эти институты должны быть независимы от правоохранительных органов и исполнительной власти, иметь полный и беспрепятственный доступ ко всей необходимой информации, необходимые ресурсы и специальные знания для проведения расследований, а также право издавать обязательные для исполнения приказы[91]. Европейский суд по правам человека уточнил, что в контексте скрытого наблюдения эффективное средство правовой защиты должно означать, что «данное правовое средство эффективно настолько, насколько это возможно, принимая во внимание особый порядок обращения в суд, при любой системе скрытого наблюдения»[92]. Растет консенсус в отношении того, что для практической реализации этого права люди должны иметь возможность получать информацию об осуществлявшемся в их отношении наблюдении постфактум. Отметив, что отдельные лица лишены возможности оспаривать конкретные меры, предписанные или осуществленные против них в процессе реализации указанных мер, Суд далее указал, что «это не означает, что предоставление ограниченной правовой защиты совершенно невозможно [...] даже на этом этапе»[93].

6.4 Особые методы расследования

Особые методы расследования означают оперативные ресурсы, которые могут быть задействованы как превентивно, так и в порядке реагирования в целях раскрытия и расследования тяжких преступлений и установления подозреваемых для сбора информации таким образом, чтобы не вызвать подозрений у объекта расследования[94]. Применение ОМР также может быть связано с определенной степенью маскировки. Советом Европы была разработана классификация особых методов расследования, в которой выделяются четыре отдельные категории такой деятельности[95]:

1. Секретные расследования с публичным взаимодействием и без маскировки (например, с привлечением информаторов).
2. Секретные расследования с публичным взаимодействием и с маскировкой (например, с использованием внедренных оперативников).
3. Секретные расследования без публичного взаимодействия и с маскировкой (например, операции под прикрытием).
4. Секретные расследования без публичного взаимодействия и без маскировки (например, прослушивание).

91 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://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F14%2F46&Language=E&DeviceType=Desktop&LangRequested=False. См. также Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/27/37, пп. 40–41.

92 Европейский суд по правам человека, *Класс и другие* против *Германии*, № 5029/71, 6 сентября 1978 г., пп. 50 и 69.

93 Европейский суд по правам человека, «Ассоциация за европейскую интеграцию и права человека» и *Экимджиев* против *Болгарии*, № 62540/00, 28 июня 2007, пп. 99–100.

94 Рекомендация Rec(2005)10 Комитета министров Совета Европы об «особых методах расследования» тяжких преступлений, в том числе террористических актов (Рекомендация по ОМР), 20 апреля 2005 г.

95 Эта классификация была разработана на основании работы профессора Г. Маркса и профессора де Валкенера. См. Совет Европы, *Terrorism: Special Investigation Techniques* («Терроризм: особые методы расследования (апрель 2005 г.), сс. 13–15.

Как указано в начале раздела, использование особых методов расследования (ОМР) — включая привлечение источников в режиме онлайн и офлайн или использование вводящих в заблуждение приемов в режиме онлайн и офлайн — может быть необходимо как для сбора оперативной информации, так и для расследования тяжких преступлений, включая терроризм. Однако применение таких методов нарушает права на неприкосновенность частной жизни тех, кто им подвергается, а в некоторых случаях и третьих лиц. Использование ОМР может также повлиять на другие права, такие как право на надлежащую правовую процедуру и право на справедливое судебное разбирательство. Следовательно, государства-члены должны определить в своем национальном законодательстве обстоятельства и условия, при которых компетентные органы имеют право прибегать к особым методам расследования, должным образом учитывая последствия для прав человека, связанные с их интрузивным характером.

Кроме того:

- Особые методы расследования должны использоваться, только если есть достаточные основания полагать, что тяжкое преступление совершено, подготовлено или готовится одним или несколькими конкретными лицами или еще не установленным лицом или группой лиц.
- Компетентные органы должны применять меньше сопряженных с вмешательством методов расследования, чем особых методов расследования, если первые позволяют эффективно раскрыть, предотвратить или преследовать преступление в судебном порядке.
- Необходимо обеспечить соразмерность между последствиями использования особых методов расследования и поставленной целью. В этом отношении при принятии решения об их использовании необходимо оценить тяжесть правонарушения и учесть, что особые методы расследования имеют характер вмешательства.
- Государства-члены должны, в принципе, принять надлежащие законодательные меры, разрешающие представление доказательств, полученных в результате использования особых методов расследования, в суде. Процессуальные нормы, регулирующие представление и допустимость таких доказательств, должны гарантировать право обвиняемого на справедливое судебное разбирательство[96].

И, наконец, используя вводящие в заблуждение приемы, сотрудники правоохранительных органов должны различать методы, способствующие сбору доказательств, и методы, которые могут подтолкнуть к совершению преступления. Последние, включая использование агентов-провокаторов или заманивание подозреваемых в ловушку, могут нарушить целостность доказательств, что приведет к их недопустимости в суде. Это относится и к скрытым операциям, проводимым в Интернете, – например, путем внедрения на конкретные форумы, которые, как предполагается, пропагандируют насильственные и радикальные взгляды.

Провоцирование имеет место, если полиция делает следующее:

- дает какому-либо лицу возможность совершить преступление, при этом не имея обоснованного подозрения, что данное лицо уже занимается преступной деятельностью, или другого достаточного основания;
- имея обоснованное подозрение или другое достаточное основание, склоняет человека к совершению преступления.

В отношении указанных методов Европейский суд по правам человека подчеркнул принципиальную разницу между сотрудниками, скрывающими свою личность с целью получения информации и доказательств преступления, и активным подстрекательством человека к его совершению и отметил, что «хотя рост организованной преступности, несомненно, требует принятия соответствующих мер, право на справедливое отправление правосудия, тем не менее, занимает столь важное место [...], что им нельзя жертвовать в угоду целесообразности»[97].

96 Рекомендация Rec(2005)10 Комитета министров Совета Европы о «специальных методах расследования» в отношении серьезных преступлений, включая акты терроризма.

97 *Тейшейра де Кастро* против *Португалии*, Европейский суд по правам человека, жалоба № 44/1997/828/1034, Решение от 9 июня 1998 г., § 36.

Таким образом, для обеспечения допустимости доказательств и права на справедливое судебное разбирательство, применяя вводящие в заблуждение практики, представители правоохранительных органов должны воздерживаться от провокаций[98].

ВСТАВКА 12. **Соблюдение прав человека при использовании ОМР***

- Судебные власти или другие независимые органы должны осуществлять достаточный контроль за использованием ОМР — в форме предварительного разрешения, контроля за ходом операции или последующего анализа и оценки. Характер и уровень контроля будет зависеть от степени вмешательства в права человека.
- ОМР должны использоваться только в делах о тяжких преступлениях.
- ОМР должны использоваться соразмерным образом, исходя из тяжести расследуемого деяния; при этом степень вмешательства в права должна быть важнейшим вопросом, который следует принимать во внимание.
- В случае если цель операции может быть «достаточно эффективно» достигнута при помощи средств, сопряженных с меньшим вмешательством в права человека, или обычных методов расследования, предпочтение всегда должно отдаваться этим вариантам.
- Процессуальные нормы, регулирующие получение и допустимость доказательств, полученных при помощи ОМР, должны гарантировать соблюдение права на справедливое судебное разбирательство.
- Лица, участвующие в оперативном использовании ОМР, должны проходить соответствующую подготовку.

* Организация по безопасности и сотрудничеству в Европе, Права человека в антитеррористических расследованиях: практическое руководство для сотрудников правоохранительных органов, с. 32. osce.org/odihr/108930

98 Организация по безопасности и сотрудничеству в Европе, Права человека в антитеррористических расследованиях: практическое руководство для сотрудников правоохранительных органов, сс. 40–45. osce.org/odihr/108930

[VII]

Распознавание лиц, неприкосновенность частной жизни и недопущение дискриминации

7.1 Распознавание лиц

В резолюции 2396 Совет Безопасности постановил, что государства-члены должны «разрабатывать и внедрять системы сбора биометрических данных, которые могут включать отпечатки пальцев, фотографии, данные распознавания лиц и другие соответствующие идентификационные биометрические данные, для ответственного и надлежащего выявления террористов, включая иностранных боевиков-террористов, в соответствии с внутренним законодательством и нормами международного права в области прав человека».

Хотя биометрические инструменты способны внести существенный вклад в повышение целенаправленности, точности и, следовательно, эффективности контртеррористических усилий[99], «[п]рименение этих технологий порождает целый комплекс проблем правового и политического характера, имеющих отношение как к усилиям государств по борьбе с терроризмом, так и к их обязательствам в области прав человека»[100]. В дополнении 2018 года к Мадридским руководящим принципам 2015 года также подчеркивается, что для выполнения требований резолюции 2396 «нужны нормативно-правовая база, навыки, потенциал, специальные знания и оборудование, которыми [некоторые государства-члены] в настоящее время не располагают»[101].

Действительно, сбор, хранение, обработка, передача и другое использование биометрических данных как данных, относящихся к физическим, физиологическим или поведенческим характеристикам человека, должны быть подкреплены соответствующими законодательными и оперативными гарантиями. В частности, сбор и обработка таких данных должны осуществляться в соответствии с применимыми международными нормами и стандартами в области прав человека, а также признанными принципами защиты данных[102].

Биометрические технологии, которые применяются государственными и частными структурами для целей верификации и идентификации, используют возможности искусственного интеллекта. Биометрическое распознавание основано на сравнении цифрового представления определенных черт человека, таких как лицо, отпечаток пальца, радужная оболочка глаза, голос или походка, с другими такими представлениями в базе

99 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' («Использование биометрических данных для идентификации террористов: передовая практика или рискованное предприятие?») (2020), URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 14.

100 S/2018/1177.

101 Там же.

102 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' («Использование биометрических данных для идентификации террористов: передовая практика или рискованное предприятие?») (2020), URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 16.

данных[103]. На основе сравнения делается вывод о большей или меньшей вероятности того, что человек действительно является тем, кого нужно идентифицировать[104].

Под распознаванием лиц понимают множество технологий, позволяющих выполнять различные задачи для различных целей. При рассмотрении вопроса о применении мер по распознаванию лиц важно проводить различие между технологиями, предназначенными для верификации, и технологиями, предназначенными для идентификации[105]. Верификацию часто называют совпадением «один к одному». Она позволяет сравнивать два биометрических образца, которые обычно считаются принадлежащими одному и тому же человеку. Проводится сравнение двух биометрических образцов, чтобы определить, является ли человек на двух изображениях одним и тем же лицом. Этот тип верификации используется, например, на автоматизированных пунктах пограничного контроля в аэропортах. Человек сканирует свой паспорт, и специальное оборудование делает снимок документа на месте. При помощи технологии распознавания лиц осуществляется сравнение двух изображений лица, и если вероятность того, что на обоих из них изображен один и тот же человек, превышает определенный порог, личность считается верифицированной. Этот тип проверки не требует хранения биометрических данных в центральной базе данных. Они могут храниться, например, на карте или в удостоверении личности/проездном документе человека[106].

Также существуют технологии распознавания лиц, предназначенные для сравнения изображения лица человека с другими изображениями для целей его идентификации. При помощи указанных технологий осуществляется оценка каждого сравнения и определяется процент вероятности того, что на двух изображениях фигурирует один и тот же человек. В некоторых случаях изображение анонимного человека сравнивается с изображениями идентифицированных лиц в базе данных, исходя из того, что этот человек находится в базе данных (идентификация на замкнутом множестве); в других случаях неизвестно, есть ли этот человек в базе данных (идентификация на открытом множестве). Последняя используется, например, при сравнении человека со списком подозреваемых в терроризме.

ИИ также может создавать базы данных или наборы данных, используя информацию, собранную с платформ социальных сетей и миллионов других веб-сайтов, которые могут включать миллиарды изображений.

Изображения лиц на видеозаписях также могут быть извлечены и сравнены с изображениями в базе данных, чтобы определить, присутствует ли человек на видео в базе данных изображений (например, в списке преступников в розыске). Такие системы называют технологией распознавания лиц в реальном времени (LFRT). Качество изображений лиц, полученных с видеокамер, невозможно контролировать, и поэтому в случае применения LFRT вероятность ложных совпадений выше, чем при использовании изображений, полученных в контролируемой среде, например, на пограничном пункте или в полицейском участке[107].

Многочисленные заинтересованные стороны, включая механизмы по правам человека, выражали обеспокоенность в отношении использования технологий распознавания лиц, отмечая, что указанные технологии наглядно продемонстрировали «гендерную и расовую предвзятость, приводящую к менее надежным резуль-

---

103 Европейская служба парламентских исследований, «Регулирование распознавания лиц в Европейском союзе», URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

104 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/48/31, URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F48%2F31&Language=E&DeviceType=Desktop&LangRequested=False

105 Технологии распознавания лиц также используются для получения информации о характеристиках человека. Этот процесс иногда называют «анализом лица». Поэтому он также может использоваться для профилирования людей, что подразумевает распределение их по категориям на основе их личных характеристик. По изображениям лиц обычно определяют пол, возраст и этническое происхождение. Категоризация означает, что технология используется для идентификации или сопоставления не конкретных людей, а только их характеристик, которые не всегда позволяют идентифицировать личность. Технология распознавания лиц также может быть использована для определения эмоций. Серьезные последствия для основных прав, связанные с категоризацией людей на основе изображения лица, не рассматриваются в данном руководстве.

106 Агентство Европейского союза по основным правам, «Технология распознавания лиц: соображения об основных правах в контексте правоохранительной деятельности», раздел 3.1, URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

107 Там же, раздел 3.2, URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

татам при идентификации женщин и лиц с темным цветом кожи»[108]. В то же время характер и серьезность опасений зависят от различных способов использования таких технологий. Особую тревогу вызывает удаленное распознавание лиц в режиме реального времени, которое все чаще используется властями по всему миру для целей идентификации[109]. Несмотря на реальные преимущества использования таких систем распознавания лиц для обеспечения общественной безопасности, их повсеместное распространение и интрузивный характер, а также подверженность ошибкам вызывают ряд проблем в области прав человека с особым риском негативного воздействия на права на неприкосновенность частной жизни и недискриминацию.

В отличие от отпечатков пальцев и анализа ДНК, например, существуют серьезные опасения по поводу точности распознавания лиц не только в целом, но и в отношении групповых характеристик. Как правило, технологии считают нейтральными и объективными по умолчанию. На самом же деле технологии отражают ценности и интересы лиц, влияющих на их разработку и использование, а это значит, что они могут формироваться под воздействием тех же структур неравенства, которые присутствуют в обществе. Например, проведенный в 2019 году обзор 189 алгоритмов распознавания лиц, созданных 99 разработчиками по всему миру, показал, что «многие из этих алгоритмов имели в 10–100 раз большую вероятность неточно идентифицировать фотографию чернокожего или восточноазиатского лица по сравнению с белокожим лицом». При поиске в базе данных заданного лица большинство из них выбирали неправильные изображения среди чернокожих женщин значительно более часто, чем среди других категорий населения[110]. Ошибки приводили к ложноположительным результатам, т. е. случаям, когда людей выделяют и подвергают дополнительной проверке на основании ошибочного предположения, что они представляют собой угрозу, и к ложноотрицательным результатам, при которых лица, представляющие реальный риск в контексте операций правоохранительных органов или пограничного контроля, не идентифицируются системой как таковые[111]. В 2019 году в США система распознавания лиц ошибочно опознала студента университета как подозреваемого в терроризме при взрывах в церкви на Пасху в Шри-Ланке. Хотя полиция позже опубликовала заявление с признанием своей ошибки, пострадавший столкнулся с угрозами расправы и подвергся дополнительной проверке со стороны полиции[112].

Как и другие технологии наблюдения, которые, как сообщается, продаются для борьбы с терроризмом и тяжкими преступлениями, возможности распознавания лиц применяются в отношении представителей меньшинств, журналистов, правозащитников, политических оппонентов и диссидентов[113]. Государственные органы по всему миру используют технологии распознавания лиц для мониторинга акций протеста, включая мирные, в том числе для отслеживания и идентификации их участников.

В одном из государств-членов (США) шесть федеральных агентств использовали программное обеспечение для распознавания лиц, чтобы идентифицировать протестующих, которые вышли на демонстрацию после особенно серьезного инцидента, связанного с жестокостью полиции[114], который также вызвал осуждение со стороны правозащитных механизмов и организаций ООН. В другом государстве-члене (Китай) национальные власти приняли программу, предусматривающую сбор обширных биометрических данных, включая взятие образцов ДНК и сканирование радужной оболочки глаза, для отслеживания перемещений представителей

---

108 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' («Использование биометрических данных для идентификации террористов: передовая практика или рискованное предприятие?») (2020), URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 25.

109 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Право на неприкосновенность личной жизни в цифровой век», A/HRC/48/31. URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F48%2F31&Language=E&DeviceType=Desktop&LangRequested=False. См. также Европейский совет по защите данных, «Руководство 05/2022 по использованию технологии распознавания лиц в правоохранительной деятельности» (12 мая 2022 г.), [103]–[104].

110 Доклад Специального докладчика по вопросу о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости. Расовая дискриминация и инновационные цифровые технологии, A/HRC/44/57, п. 12. URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F44%2F57&Language=E&DeviceType=Desktop&LangRequested=False

111 Агентство Европейского союза по основным правам, «Предотвращение незаконного профилирования сегодня и в будущем: руководство», с. 22, URL: https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide. См. также Европейская служба парламентских исследований, «Регулирование распознавания лиц в Европейском союзе», с. 7. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

112 См. веб-сайт организации Algorithmic Justice League: https://www.ajl.org/facial-recognition-technology

113 Доклад Верховного комиссара Организации Объединенных Наций по правам человека. Терроризм и права человека, A HRC/50/49, п. 27, URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F50%2F49&Language=E&DeviceType=Desktop&LangRequested=False

114 URL: https://thehill.com/policy/technology/560805-watchdog-6-federal-agencies-used-facial-recognition-software-to-id-george/

определенного этнического меньшинства[115]. Идентификация осуществляется на основе общих биометрических признаков, характерных для этой группы[116]. Еще в одном государстве-члене (Израиле) власти используют сложнейшие технологии распознавания лиц для наблюдения за деятельностью отдельной группы населения на территории, находящейся под его контролем[117]. Как отмечалось выше, запрет на дискриминацию в международном праве прав человека является абсолютным.

Использование распознавания лиц должно регулироваться внутренним законодательством, соответствующим международным нормам и стандартам в области прав человека и предусматривающим достаточные гарантии защиты неприкосновенности частной жизни и персональных данных. Учитывая «высокий риск, связанный с использованием биометрических инструментов, из-за конфиденциального характера биометрических данных и возможности эксплуатации и злоупотреблений», передовой практикой считается проведение комплексных оценок рисков в области прав человека[118]. В данном отношении Специальным докладчиком по правам человека в условиях борьбы с терроризмом рекомендуется в рамках указанных оценок рисков «изучать последствия для права на неприкосновенность частной жизни субъектов данных и побочные эффекты для третьих сторон, а также рассматривать вопрос соответствия признанным принципам защиты данных»[119]. В Руководстве по распознаванию лиц Совета Европы отмечается, что уровень интрузивности данных технологий и связанные с ними нарушения прав человека различаются «в зависимости от конкретной ситуации их использования, и существуют случаи, когда закон строго ограничивает или даже полностью запрещает такое использование»[120]. В документе также подчеркивается, что использование технологий распознавания лиц в режиме реального времени в «неконтролируемой обстановке» (местах, к которым у физических лиц есть свободный доступ, через которые они также могут проходить, в том числе общественные или квазиобщественные пространства, такие как торговые центры, больницы, школы) «должно быть предметом демократического обсуждения, и должна существовать возможность моратория на время, необходимое для полного анализа» в свете их интрузивности и риска негативных последствий для прав человека[121].

Учитывая вышесказанное, в неконтролируемой обстановке технологии распознавания в реальном времени должны применяться только в результате демократического обсуждения, в ходе которого должным образом рассматривается их воздействие, в том числе с точки зрения прав человека, и при условии, что власти продемонстрируют, что их использование необходимо и соразмерно обстоятельствам[122]. В этом контексте органы власти должны также учитывать уязвимость субъектов данных, на которых могут повлиять принимаемые меры, и способы эффективного снижения соответствующих рисков.

Поскольку технологии распознавания лиц могут использоваться без согласия или даже без ведома субъектов данных, прозрачность и справедливость обработки имеют первостепенное значение. В законодательстве о распознавании лиц или сборе, хранении, обработке, передаче или ином использовании аналогичных биометрических данных должно быть указано, по меньшей мере, следующее:

- что получение и обработка данных должны быть справедливыми и законными;
- что хранение данных может осуществляться только для конкретных и законных целей, и запрещается их использование способом, несовместимым с этими целями;

---

115 См., например, OL CHN 18/2019.

116 Доклад Специального докладчика по вопросу о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости. Расовая дискриминация и инновационные цифровые технологии, A/HRC/44/57, п. 39, URL: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F44%2F57&Language=E&DeviceType=Desktop&LangRequested=False

117 См. статью «Израиль усиливает слежку за палестинцами с помощью программы распознавания лиц на Западном берегу», *Washington Post*, 8 ноября 2021 г., URL: https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

118 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' («Использование биометрических данных для идентификации террористов: передовая практика или рискованное предприятие?») (2020), URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 42.

119 Там же.

120 Совет Европы, Консультативный комитет по Конвенции 108 о защите данных, Руководство по распознаванию лиц. URL: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

121 Там же.

122 В этом отношении см. также Европейский совет по защите данных, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* («Руководство 05/2022 по использованию технологии распознавания лиц в правоохранительной деятельности», 12 мая 2022 г.), [103]–[104].

- что собираемые данные должны быть адекватными, релевантными и не чрезмерными по отношению к целям, для которых они хранятся;
- что данные должны быть точными и, при необходимости, обновляться;
- что хранение данных в форме, позволяющей идентифицировать субъектов данных, разрешается осуществлять не дольше, чем это требуется для целей, для которых эти данные хранятся; это означает, что законодательство должно включать руководящие принципы по хранению, удалению или анонимизации данных;
- в законодательстве должно быть определено, в каких случаях и в каком объеме разрешается передача биометрических данных третьим сторонам.

Государства также должны предоставлять информацию о контактных лицах, к которым можно обратиться с вопросами о сборе, хранении, использовании и передаче биометрических данных, включая данные, полученные с помощью технологий распознавания лиц, и принимать меры для обеспечения безопасности биометрических систем и предотвращения потери данных или несанкционированного доступа к ним.

Поскольку распознавание лиц основано на обработке персональных данных, субъекты данных должны иметь: право на информацию, право на доступ, право на получение информации о причинах, лежащих в основе сбора и (или) хранения данных, право на возражение и право на исправление. В случае если личные или конфиденциальные данные были собраны или использованы в нарушение международного права прав человека, субъектам данных должны быть предоставлены эффективные средства правовой защиты.

Наконец, как неоднократно подчеркивалось механизмами по защите прав человека, включая Специального докладчика по правам человека в условиях борьбы с терроризмом, трансграничный обмен данными, в том числе биометрическими, вызывает озабоченность с точки зрения прав человека. Специальный докладчик назвал указанные договоренности «черным ящиком в практике международного права, при этом имеется мало информации о том, происходит ли обмен биометрическими данными и какого типа, а также, что в большей мере относится к практической стороне вопроса, о содержании соглашений об обмене данными»[123]. По этой причине Специальный докладчик отмечает, что практика обмена данными должна основываться на принципе подотчетности и подлежать всестороннему независимому надзору[124].

123 A/HRC/ 52/39, п. 26.

124 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' («Использование биометрических данных для идентификации террористов: передовая практика или рискованное предприятие?») (2020), URL: https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 43.

[VIII]

Незаконно полученные доказательства

8.1 Незаконно полученные доказательства

При определении способов ведения наблюдения с помощью новых технологий, правоохранительные органы должны учитывать, что незаконное получение доказательств подрывает целостность судебного разбирательства в отношении лиц, подозреваемых или обвиняемых в преступной деятельности. Международное право прав человека гарантирует право на справедливое разбирательство, и хотя оно не содержит подробных положений о допустимости доказательств (это прерогатива национального законодательства), оно все же дает рекомендации, касающиеся обеспечения справедливости разбирательства в целом и той роли, которую играют в этом отношении доказательства и правила допустимости. Важно отметить, что использование доказательств, полученных с помощью пыток или жестокого, бесчеловечного или унижающего достоинство обращения, несовместимо с международным правом прав человека, включая право на справедливое судебное разбирательство. В отношении других незаконных доказательств в разных юрисдикциях применяются разные подходы: в некоторых из них такие доказательства автоматически исключаются из использования в уголовном процессе, а в других такие доказательства не являются априори недопустимыми, но их допустимость определяется способом и обстоятельствами, при которых они были получены, а также их надежностью и влиянием на целостность разбирательства. Например, Европейский суд по правам человека постановил, что вопрос заключается в том, было ли разбирательство справедливым в целом, включая способ получения доказательств.

[IX]

Алгоритмическое профилирование и недопущение дискриминации

9.1 Алгоритмическое профилирование и недопущение дискриминации

Развитие технологий привело к расширению использования профилирования в самых разных контекстах, включая правоохранительную деятельность, пограничный контроль и безопасность. Сотрудники правоохранительных органов и пограничной службы обычно используют профилирование для предотвращения и расследования уголовных преступлений. Такие практики используются для «установления корреляции между определенными характеристиками и конкретными результатами или поведением» [125], и результат их применения может не быть верным для всех индивидов, причисленных к определенному профилю. Профилирование используется 1) для идентификации известных лиц на основе оперативных данных о конкретном индивиде (полицейская деятельность на основе конкретных оперативных данных) и 2) в качестве предиктивного метода для идентификации неизвестных лиц, которые могут представлять интерес для правоохранительных органов и органов пограничного контроля (предиктивная полицейская деятельность)[126].

Хотя существуют различные определения профилирования, эту практику принято описывать как «любой вид автоматической обработки персональных данных, состоящий в том, что персональные данные используются для оценки тех или иных личностных аспектов физического лица, в частности, для анализа и прогнозирования аспектов, связанных с работоспособностью, экономическим положением, состоянием здоровья, личными предпочтениями, интересами, надежностью, поведением, местом проживания или переменами места жительства данного физического лица»[127]. За последние годы участилось использование алгоритмического профилирования на основе данных, хранящихся в различных базах данных и информационных системах управления.

Чтобы профилирование и связанные с ним практические методы соответствовали принципу верховенства права и международным нормам и стандартам в области прав человека, они должны иметь достаточно предсказуемую и доступную правовую базу, одним из главных принципов которой является объективное и разумное обоснование[128], и осуществляться в соответствии с процедурой, предусматривающей адекватные

125 Агентство Европейского союза по основным правам, «Предотвращение незаконного профилирования сегодня и в будущем: руководство» (2018), с. 16, URL: https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide

126 Там же, сс. 16 и 18.

127 См., например, Директиву ЕС 2016/680.

128 Объективное и разумное обоснование требует, чтобы профилирование преследовало законную цель и соответствовало принципам необходимости и соразмерности «между применяемыми средствами и преследуемой целью». См., например, Агентство Европейского союза по основным правам, «Предотвращение незаконного профилирования сегодня и в будущем: руководство» (2018), с. 23; Европейский суд по правам человека, Руководство по Статье 14 Европейской Конвенции по правам человека и Статье 1 Протокола № 12 к Конвенции, URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_14_art_1_protocol_12_eng. См. также Замечание общего порядка № 31 2004 Комитета по правам человека, п. 6, и *Дженеро* против *Италии*, п. 7.6; а также Комитет по экономическим, социальным и культурным правам, Замечание общего порядка № 20 (2009), п. 13, и *Трухильо Калеро* против *Эквадора*, п. 19.5. См. также Комитет по ликвидации расовой дискриминации, Общая рекомендация № 32 (2009), п. 8.

гарантии против злоупотребления и подлежащей полноценному надзору. С профилированием связан целый ряд соображений, касающихся прав человека, таких как неприкосновенность частной жизни, защита данных, надлежащая процедура, справедливое судебное разбирательство и т. д. Важно отметить, что методы профилирования должны быть разработаны и применяться на практике в соответствии с правом на недискриминацию. Учитывая это, профилирование, которое в первую очередь или в значительной степени основывается на защищенных от дискриминации характеристиках, таких как пол, раса, этническая принадлежность, религия, возраст и т. д., или которое приводит к прямой или косвенной дискриминации лиц на основе таких характеристик, противоречит запрету на дискриминацию и не допускается.

В контексте борьбы с терроризмом неоднократно поднимался вопрос использования расового и этнического профилирования. Согласно определению Комитета Организации Объединенных Наций по ликвидации расовой дискриминации, «расовое профилирование: *a*) совершается правоохранительными органами; *b*) не имеет под собой объективных критериев или разумных оснований; *c*) осуществляется по признакам расы, цвета кожи, родового, национального или этнического происхождения или их пересечения с другими соответствующими признаками, такими как религия, пол или гендер, сексуальная ориентация и гендерная идентичность, инвалидность и возраст, миграционный статус или трудовой или иной статус; *d*) используется в конкретных контекстах, таких как иммиграционный контроль и борьба с преступностью, терроризмом или другими видами деятельности, которые предположительно нарушают или могут привести к нарушению закона»[129]. Специальным докладчиком по правам человека в условиях борьбы с терроризмом было отмечено, что когда сотрудники правоохранительных органов используют «схематичные профили, отражающие неизученные обобщения», такая практика может представлять собой несоразмерное вмешательство в сферу прав человека. Специальный докладчик также подчеркнул, что «профилирование, основанное на стереотипных предположениях, что лица определенной „расы", национального или этнического происхождения или религии особенно склонны к совершению преступлений, может привести к действиям, несовместимым с принципом недискриминации». У Специального докладчика вызывает серьезную озабоченность факт применения методов борьбы с терроризмом, основанных на использовании профилей террористов, которые включают такие характеристики, как презюмируемая „раса", этническая принадлежность, национальное происхождение или религия того или иного лица»[130]. Он обратил внимание на то, что подобная практика не только является «неадекватным и неэффективным средством выявления потенциальных террористов, но и влечет за собой серьезные негативные последствия, способные сделать эти меры бесполезными в борьбе с терроризмом»[131].

Комитет по ликвидации расовой дискриминации отметил, что расовое профилирование связано со «стереотипами и предрассудками, которые могут быть осознанными или неосознанными, а также индивидуальными или институциональными и структурными» и что стереотипизация становится нарушением международного права прав человека, когда стереотипные представления «на практике используются для подрыва осу-

129 Комитет по ликвидации расовой дискриминации, Общая рекомендация № 36 о предупреждении расового профилирования со стороны сотрудников правоохранительных органов и борьбе с ним, п. 13. Комитет описывает этническое профилирование как «использование правоохранительными органами, без объективных и разумных оснований, таких признаков как раса, цвет кожи, язык, религия, гражданство или национальное или этническое происхождение при контроле, слежении или проведении расследований». См. там же, п. 13. См. также Европейская комиссия по борьбе с расизмом и нетерпимостью, Общеполитическая рекомендация № 11 о борьбе с расизмом и расовой дискриминацией в работе правоохранительных органов, CRI (2007)39, 29 июня 2007 г., с. 4. См. также Комитет по ликвидации расовой дискриминации, Общая рекомендация № 36 о предупреждении расового профилирования со стороны сотрудников правоохранительных органов и борьбе с ним, п. 13: См. также Межамериканская комиссия по правам человека, «Положение лиц африканского происхождения в Северной и Южной Америке» (2011), п. 143: расовое профилирование определяется как тактика, принятая по предполагаемым мотивам общественной безопасности и защиты на основе стереотипов, касающихся расы, цвета кожи, этнической принадлежности, языка, происхождения, религии, гражданства или места рождения или сочетания этих факторов, а не объективных подозрений, при которой отдельные лица или группы людей выделяются дискриминационным образом исходя из ошибочного представления о том, что люди с такими характеристиками будто бы склонны к совершению конкретных видов преступлений. Арабский комитет по правам человека сообщил, что расовое профилирование можно определить как использование сотрудниками правоохранительных органов обобщений или стереотипов, связанных с предполагаемой расой, цветом кожи, происхождением, гражданством, местом рождения, национальным или этническим происхождением, вместо объективных доказательств или индивидуального поведения, в качестве основы для констатации того, что данное конкретное лицо занимается или занималось преступной деятельностью, что приводит к дискриминационному принятию решений (см. Замечание общего порядка № 36, п. 15).

130 A/HRC/4/26, п. 34. См. также A/HRC/29/46, п. 2.

131 A/HRC/4/26, п. 83.

ществления прав человека»[132]. Другие исследования показали, что профилирование на дискриминационной почве не только неточно, но и неэффективно. Например, террористические группы доказали свою способность обходить профилирование, вербуя людей, которые с меньшей вероятностью подвергнутся розыску по предиктивным профилям. Кроме того, в исследовании, проведенном Организацией по безопасности и сотрудничеству в Европе, сделан вывод о том, что тщательный идентификационный контроль в мечетях, проводимый некоторыми государствами — членами ОБСЕ, а также мероприятия по сбору данных по этническому признаку и программы задержания и обыска не привели ни к одному случаю осуждения по делам о борьбе с терроризмом[133].

Комитет по ликвидации расовой дискриминации также отметил, что, хотя в некоторых областях искусственный интеллект может способствовать повышению эффективности принятия решений, существует реальный риск проявления алгоритмической предвзятости, в частности, в контексте правоохранительной деятельности[134]. Даже если стереотипы могут отражать некоторую статистическую истину, профилирование является проблематичным, если выводы о людях делаются на основе их принадлежности к группе, а не индивидуальных характеристик и поведения. Алгоритмическое профилирование вызывает серьезную озабоченность, а его последствия для прав пострадавших могут быть очень серьезными. Учитывая непрозрачность алгоритмического анализа и методов принятия решений, в частности, с использованием искусственного интеллекта, дискриминационные результаты алгоритмического профилирования нередко могут быть менее очевидными и более трудными для обнаружения, чем в случае решений, принимаемых человеком, и, следовательно, оспорить их может быть сложнее[135]. Это может иметь серьезные последствия для прав пострадавших. По этой причине, согласно рекомендациям, национальные структуры по правам человека, включая органы по обеспечению равенства, а также независимые службы по надзору за полицией, должны играть активную роль в «выявлении и снижении рисков, связанных с использованием алгоритмов в системах уголовного правосудия»[136].

По мере того как использование алгоритмов машинного обучения в системах уголовного правосудия становится все более распространенным в области «предиктивной» полицейской деятельности, сотрудники правоохранительных органов все чаще прибегают к алгоритмическим методам профилирования. Они используются для прогнозирования мест совершения преступлений и оптимального распределения полицейских ресурсов, а также оценки риска повторного совершения преступления в контексте процессов уголовного правосудия, в том числе в связи с принятием решений о заключении под стражу, назначении наказания и условно-досрочном освобождении. Хотя методы прогнозирования должны фокусироваться на поведении, на практике «часто акцент делается не на поведении (или не только на нем), а на видимых физических характеристиках, таких как возраст, пол или этническая принадлежность»[137]. Прогнозирование преступного поведения, в частности, должно основываться не только на статистике, генерируемой алгоритмами, но и подтверждаться другими признаками и фактами.

Исследование последней технологии в США, проведенное в 2016 году, показало, что она допускает ошибки примерно с одинаковой частотой как для белых, так и для чернокожих людей, но гораздо чаще давала ложноположительные результаты (ошибочное предсказание «высокого риска») для чернокожих и чаще давала ложноотрицательные результаты для белых[138].

Особые риски возникают, когда алгоритмическое профилирование используется для определения вероятности преступной деятельности либо в определенных населенных пунктах, либо определенными группами

---

132 Комитет по ликвидации расовой дискриминации, Общая рекомендация № 36 о предупреждении расового профилирования со стороны сотрудников правоохранительных органов и борьбе с ним, п. 20.

133 Бюро ОБСЕ по демократическим институтам и правам человека, Доклад совещания экспертов по вопросам безопасности, радикализации и предупреждения терроризма, 28–29 июля 2008 г., п. 25. URL: www.osce.org/odihr/34379

134 Комитет по ликвидации расовой дискриминации, Общая рекомендация № 36 о предупреждении расового профилирования со стороны сотрудников правоохранительных органов и борьбе с ним, п. 12, URL: https://digitallibrary.un.org/record/3897913

135 Там же, п. 32.

136 Совет Европы, Комиссар по правам человека, «Этническое профилирование: сохраняющаяся практика в Европе», URL: https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe

137 Агентство Европейского союза по основным правам, «Предотвращение незаконного профилирования сегодня и в будущем: руководство» (2018), с. 18.

138 Совет Европы, Комиссар по правам человека, «Этническое профилирование: сохраняющаяся практика в Европе», URL: https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe

или отдельными лицами. Например, исторические данные об арестах в том или ином районе могут отражать предвзятую с расовой точки зрения полицейскую практику. Включение этих данных в предиктивную модель охраны порядка порождает риск получения прогнозов, отражающих столь же предвзятые оценки, на основе которых в данном квартале будет развернуто чрезмерное полицейское присутствие, что, в свою очередь, может привести к еще большему числу задержаний в том же квартале, завершив тем самым опасный порочный круг обратной связи[139]. В то же время в ситуациях, когда члены определенной этнической группы или религиозной общины могут находиться под угрозой, выделение необходимых правоохранительных ресурсов на защиту этой группы не является дискриминационным или несоразмерным.

Помимо того, что дискриминация является незаконной, она способна снизить эффективность контртеррористических усилий. Дискриминационные меры могут привести к отчуждению групп и вызвать или усугубить недовольство, которое может способствовать росту террористической угрозы. Профилирование может вызвать возмущение в особенно пострадавших сообществах и снизить доверие к полиции и пограничным службам. Это, в свою очередь, может подорвать эффективность методов, основывающихся на сотрудничестве с общественностью.

Использование слишком широких критериев также может привести к значительному числу бесполезных ложноположительных результатов, то есть к ошибочному причислению людей к определенному профилю риска. Некоторые из таких ложноположительных результатов также могут носить дискриминационный характер. Например, Агентство Европейского союза по основным правам отмечает, что если профиль риска, касающийся риска нелегальной миграции, основан на сочетании определенной национальности и профессиональной группы, это может привести к тому, что объектом преследования станет этническая группа или национальность, которая в определенной стране обычно работает в определенном экономическом секторе, например, в строительстве или сельском хозяйстве. В других случаях широкое определение критерия «судимость в прошлом» может привести к тому, что ЛГБТИ+ люди будут «обязаны сообщать о судимостях, связанных с определенным сексуальным поведением, за которое в некоторых странах предусмотрена уголовная ответственность»[140].

---

139 Комитет по ликвидации расовой дискриминации, Общая рекомендация № 36 о предупреждении расового профилирования со стороны сотрудников правоохранительных органов и борьбе с ним, п. 33. URL: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-36-2020-preventing-and

140 Агентство Европейского союза по основным правам, «Предотвращение незаконного профилирования сегодня и в будущем: руководство», с. 27–28, URL: https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide. См. также Совет Европы, Комиссар по правам человека, «Этническое профилирование: сохраняющаяся практика в Европе», сс. 117–118. URL: https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe

[X]

Социальные сети, Интернет, свобода выражения мнений и объединений и подстрекательство

10.1 Общие вопросы

Новые технологии сыграли важную роль в расширении доступа общественности к поиску, получению и передаче информации. Эти технологии и инструменты могут также стать платформой для людей и групп, которые в меньшей степени участвуют в обсуждениях, представляющих общественный интерес, например, женщин или лиц, принадлежащих к маргинализированным или недостаточно представленным группам. Они также могут создавать и укреплять социальные связи, расширять доступ к здравоохранению, образованию и средствам социального обеспечения, способствовать распространению знаний, направленных на устойчивое развитие, позволять маргинализированным сообществам устанавливать связи, а также способствовать формированию более открытых, инклюзивных и разнообразных общественных сфер[141].

В то же время ИКТ и Интернет, включая социальные сети, неоднократно использовались террористами и применялись, помимо прочего, для продвижения и поддержки террористических актов путем распространения пропаганды, онлайн-вербовки, радикализации и подстрекательства к терроризму, для финансирования, а также для осуществления атак, в том числе путем распространения технических инструкций о получении оружия и совершении насильственных действий.

В 2013 году в ходе атаки на торговый центр Westgate в Найроби террористическая группировка «Аш-Шабаб» опубликовала серию сообщений в Twitter[142]. Она также использовала Интернет для сбора пожертвований от сомалийской диаспоры и не только, получив таким образом более 40 000 долларов[143]. В аккаунте пользователя, связанного с «Аль-Каидой», было опубликовано фото беспилотника с подписью: «Российский разведывательный самолет упал в Латтакии [Сирия] неподалеку от места дислокации суннитских боевиков! Было бы здорово, если бы боевики смогли воспроизвести его!»[144]. В 2016 году был запущен Telegram-канал под названием «Ученые и инженеры Исламского государства». Его официальными целями является: «i) собрать как можно больше ученых и инженеров халифата со всего мира и познакомить их друг с другом; и ii) использовать их для создания мощной всемирной промышленной сети для поддержки военной промышленности Исламского государства»[145]. 16 октября 2014 года ведущий англоязычный аккаунт ИГИЛ в Twitter разместил ссылку на PDF-файл, озаглавленный «Руководство по мультикоптерам для начинающих», в котором

141 Рекомендация CM/Rec (2022)13 Комитета Министров Совета Европы государствам-членам о воздействии цифровых технологий на свободу выражения мнений, URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a61729

142 См. URL: https://www.cbc.ca/news/world/kenya-attack-why-al-shabaab-live-tweeted-the-assault-1.1865566

143 Доклад Группы контроля по Сомали за 2010 год, представленный в соответствии с резолюцией 1853 (2008) Совета Безопасности, п. 92. URL: https://www.securitycouncilreport.org/un-documents/document/somalia-s-res-1853.php

144 Институт исследований средств массовой информации Ближнего Востока (MEMRI), «Десятилетие использования беспилотников джихадистскими организациями», 1027, URL: https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda

145 Там же.

рассказывалось о том, как построить мультироторные беспилотники базовой конфигурации[146]. Аналогичным образом, группа технических специалистов, поддерживающих «Исламское государство», использовала Telegram для обсуждения того, как обычные детали двигателя могут быть адаптированы для использования в ракетах или ударных беспилотниках военного типа[147]. Интернет-журнал «Талибана» призывал «наших искусных братьев-мусульман, инженеров и ученых, не оставаться в стороне и приложить все усилия, чтобы выяснить, как разорвать связь между беспилотником и GPS. Проведите эксперимент в любом уголке мира, где бы вы ни жили, и если он окажется удачным, снимите весь процесс на видео, выложите запись в Интернет и защитите ее паролем. Затем отправьте нам ссылку на нее и пароль. Или просто подготовьте хорошую... презентацию PowerPoint и отправьте ее нам. Даже если вы добились хороших результатов в эксперименте, но столкнулись с какими-то сложностями, обратитесь к нам и, возможно, мы сможем подсказать вам что-то полезное»[148].

В отношении пределов свободы выражения мнений в соответствии с международным правом прав человека Европейский суд по правам человека постановил, что «[т]ерпимость и уважение равного достоинства всех людей составляют основу демократического, плюралистического общества. Исходя из этого в определенных ситуациях может считаться принципиально необходимым в определенных демократических обществах налагать санкции или даже предупреждать возникновение таких форм выражения мнения, которые распространяют, разжигают, продвигают или оправдывают чувство ненависти, основанное на нетерпимости, при условии, что любые «формальности», «условия», «ограничения» или «санкции» соразмерны преследуемой законной цели[149].

Хотя ограничения свободы выражения мнений и других соответствующих прав, таких как право на свободу объединений, необходимы как часть законных антитеррористических усилий, в некоторых юрисдикциях существуют необоснованные ограничения на контент или услуги в Интернете, в том числе путем отключения интернет-сервисов или выборочного блокирования доступа к интернет-ресурсам и веб-сайтам. В некоторых юрисдикциях журналисты, представители политической оппозиции, правозащитники, активисты борьбы с коррупцией и другие лица сталкивались с преследованиями или подвергались нападкам, в том числе с применением мер уголовного правосудия, только за то, что осуществляли свое право на выражение мнений в Интернете. В 2018 году Верховный комиссар ООН по правам человека отметила, что «Интернет все больше становится пространством, угрожающим правозащитникам»[150].

10.2 Оперативная информация из открытых источников

Благодаря современным технологиям объем информации, получаемой правоохранительными органами и спецслужбами в ходе расследований с использованием открытых источников (OSINT), существенно увеличился. OSINT действительно являются одним из важнейших инструментов, используемых современными следователями и аналитиками как для предотвращения террористических актов, так и для судебного преследования лиц или групп, обвиняемых в совершении указанных актов. Это особенно верно, когда OSINT используется в дополнение к другим видам деятельности по сбору информации. Используя растущее число онлайновых баз данных и Интернет в целом, в рамках OSINT следователи могут просматривать веб-сайты СМИ, аккаунты в социальных сетях, карты, спутниковые снимки, видео, фотографии и другой цифровой контент на своих компьютерах для выявления террористической пропаганды и информации о террористических операциях, методах и лидерах.

146 Институт исследований средств массовой информации Ближнего Востока (MEMRI), «Десятилетие использования беспилотников джихадистскими организациями», 1027, URL: https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda

147 Там же.

148 Там же.

149 Европейский суд по правам человека, *Эрбакан* против *Турции*, Решение от 6 июля 2006 г., § 56.

150 URL: https://www.ohchr.org/en/statements/2018/11/human-rights-new-era

Как и любое другое расследование, OSINT должно служить законной цели, быть соразмерным этой цели и недискриминационным. Указанные методы не должны использоваться для сбора информации с целью мониторинга, слежки, преследования или запугивания лиц, занимающихся законной деятельностью. Властям также следует принимать во внимание проблемные вопросы, связанные с использованием OSINT, такие как объем и достоверность доступных данных; ограничения и гарантии, которые должны сопровождать автоматизированный анализ; и персональный и конфиденциальный характер информации[151].

10.3 Террористический контент в Интернете, включая подстрекательство к терроризму

Резолюция 1624 (2005) Совета Безопасности призывает государства ввести законодательный запрет на подстрекательство к совершению террористического акта или актов. Однако, учитывая то, что государства оправдывают ограничения на все формы выражения мнений соображениями борьбы с подстрекательством к совершению террористических актов, очень важно, чтобы государства подходили к выполнению указанной резолюции с осторожностью. Как уже упоминалось ранее, Специальным докладчиком по правам человека в условиях борьбы с терроризмом было предложено типовое определение подстрекательства к терроризму[152]. Специальный докладчик, а также механизмы Организации Объединенных Наций по правам человека и другие заинтересованные стороны неоднократно подчеркивали необходимость четкого определения подстрекательства к терроризму, а также других преступлений, связанных с пропагандой терроризма, включая «прославление», «одобрение», «восхваление» или «оправдание» терроризма, во избежание слишком широкой сферы применения или уголовной ответственности за действия, не относящиеся к подстрекательству к терроризму или выступлению в пользу национальной, расовой или религиозной ненависти, представляющему собой подстрекательство к насилию[153].

Постановление ЕС 2021/784 определяет террористический контент как контент, который[154]:

- побуждает кого-либо совершить или способствовать совершению террористических преступлений или участвовать в деятельности террористической группы;
- подстрекает к совершению террористических актов или пропагандирует совершение террористических преступлений, например, путем их прославления;
- дает инструкции о том, как осуществлять атаки.

Борьба с террористическим контентом, включая подстрекательство к совершению террористических актов, подразумевает вмешательство в такие права человека как свобода выражения мнений, и их ограничение. Контент может быть удален или частично заблокирован, а свобода выражения мнения ограничена, если такие меры необходимы для соблюдения прав или репутации других лиц либо для защиты национальной

151 См., например, URL: https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/

152 См. раздел V.

153 Статья 20 МПГПП.

154 Регламент 2021/784 Европейского парламента и Совета о борьбе с распространением террористического контента в Интернете, статья 2 (7): Террористический контент означает…:

a) подстрекает к совершению какого-либо из преступлений, о которых говорится в пунктах (a)–(i) статьи 3 (1) Директивы ЕС 2017/541, при этом такой материал прямо или косвенно, например путем прославления террористических актов, пропагандирует совершение террористических преступлений, тем самым создавая опасность совершения одного или нескольких таких преступлений;

b) побуждает лицо или группу лиц к совершению одного из преступлений, о которых говорится в пунктах (a)–(i) статьи 3 (1) Директивы ЕС 2017/541, или содействию ему;

c) побуждает лицо или группу лиц к участию в деятельности террористической группировки в значении пункта (b) статьи 4 Директивы ЕС 2017/541;

d) дает инструкции о создании или использовании взрывчатых веществ, огнестрельного или иного оружия, а также вредных или опасных веществ, или о иных конкретных методах или способах для целей совершения или содействия совершению одного из террористических преступлений, о которых говорится в пунктах (a)–(i) статьи 3 (1) Директивы ЕС 2017/541. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32021R0784

безопасности, общественного порядка, здоровья населения или общественной морали. Более того, в соответствии со статьей 20 Международного пакта о гражданских и политических правах, всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом. При выполнении своих обязательств по статье 20 (2) МПГПП государствам-членам предлагается учитывать указания, содержащиеся в Рабатском плане действий по запрещению пропаганды национальной, расовой и религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию, в частности[155], пороговый тест, описанный в указанном документе. В этом тесте рассматриваются шесть критериев при оценке высказываний, которые могут представлять собой пропаганду преступлений или ненависти: 1) контекст, 2) статус говорящего, 3) намерение, 4) содержание и форму речи, 5) степень воздействия речи и 6) вероятность причинения вреда, включая его неотвратимость[156].

В распоряжении государств имеется целый ряд инструментов для борьбы с террористическим контентом: i) требовать от поставщиков услуг удаления соответствующего контента; ii) привлекать виновных к гражданско-правовой ответственности; iii) преследовать в судебном порядке виновное лицо или группу лиц.

10.3.1 Удаление контента

Как упоминалось ранее в настоящем Руководстве, в соответствии с международным правом государства-члены обязаны принимать меры по предотвращению террористических актов и борьбе с ними. Это обязательство также связано с предусмотренным правом прав человека обязательством государств проявлять должную осмотрительность и принимать надлежащие меры для защиты лиц, находящихся под их юрисдикцией, от необоснованного вмешательства в их права третьих сторон, включая террористов, а в случае если предотвратить такое вмешательство не удается, привлекать виновных лиц к ответственности. Таким образом, государства-члены обязаны принимать меры для обеспечения регулирования размещаемого в Интернете контента в соответствии с международным правом прав человека, в том числе обязывать корпоративных субъектов осуществлять свою деятельность без нарушений прав лиц, находящихся под юрисдикцией соответствующего государства.

При том, что ряд государств-членов и региональных организаций приняли законодательство о размещении контента в Интернете, включая контент террористического характера, государства-члены также обязали технологические компании, которые предоставляют платформу для контента третьих лиц и курируют его, отслеживать и контролировать от имени государства контент, создаваемый или распространяемый пользователями в Интернете. В некоторых случаях соответствующие правовые и политические рамки не учитывали всесторонне вопросы прав человека и не давали корпоративным субъектам рекомендаций по обеспечению соблюдения прав человека.

Хотя государства-члены несут основную ответственность за обеспечение поощрения и защиты прав человека всех лиц, находящихся под их юрисдикцией, растущая роль корпоративных субъектов и их увеличивающееся влияние на осуществление прав человека были отмечены в Руководящих принципах предпринимательской деятельности в аспекте прав человека, разработанных ООН, которые представляют собой авторитетный глобальный стандарт по предотвращению и устранению негативного воздействия на права человека, связанного с предпринимательской деятельностью[157]. Согласно Руководящим принципам, предприятия обязаны проявлять должную осмотрительность и проводить оценку рисков своей деятельности, изучая фактическое и потенциальное воздействие на права человека, как прямое, так и косвенное. Это позволит компаниям в случае необходимости разработать и реализовать меры по снижению указанного воздействия. Компании должны создавать внутренние механизмы подотчетности за реализацию политики

155 A/HRC/22/17/Add.4.

156 A/HRC/22/17/Add.4, п. 29.

157 Хотя Руководящие принципы были одобрены Советом по правам человека (резолюция 17/4), они не имеют обязательной силы. Это значит, что *обязанности, предусмотренные* Руководящими принципами, *не подлежат принудительному исполнению без их транспонирования в национальное законодательство. В то же время* Руководящие принципы представляют собой важный шаг к тому, чтобы соотнести воздействие бизнеса на права человека с соответствующим уровнем корпоративной ответственности. Они также задают направление развитию нормативной базы на международном и внутреннем уровне, и их признает, принимает и внедряет все большее число предприятий, включая технологические компании. В данной связи см. также OL OTH 46/ 2018; OL OTH 71/2018.

в области прав человека и внедрять процессы, позволяющие устранить неблагоприятные последствия для прав человека, которые компания вызвала или которым способствовала. Они должны информировать общественность о мерах, принимаемых ими для устранения воздействия на права человека, связанного с их деятельностью, особенно в случаях получения жалоб от пострадавших лиц или их представителей, посредством регулярной отчетности о прозрачности.

Успешная борьба с использованием Интернета в террористических целях требует конструктивного сотрудничества между государственными органами и широким кругом частных субъектов, включая технологические компании. Пересечение ролей и обязанностей государства и корпораций в цифровую эпоху остается проблемой как для государств-членов, так и для корпоративных субъектов, что особенно заметно в контексте борьбы с терроризмом.

Компания Meta учредила независимый орган, в состав которого входят ученые и эксперты по вопросам технологий и свободы слова, целью которого является рассмотрение, помимо прочего, ответов Facebook и Instagram на запросы об удалении контента и консультирование по вопросам политики. Его решения способствуют более широкому обсуждению путей обеспечения уважения прав человека, включая свободу выражения мнений в Интернете.

ВСТАВКА 13. **Дело Надзорного совета Meta № 1**

В 2021 году пользователь Facebook поделился сообщением с проверенной страницы Al Jazeera Arabic, состоящим из текста на арабском языке и фотографии. На фотографии были изображены двое мужчин в камуфляжной форме с закрытыми лицами и головными повязками с эмблемой группы, входящей в список опасных лиц и организаций сообщества Facebook.

Текст гласил: «Руководство сопротивления в общем зале дает оккупантам отсрочку до 18:00, чтобы они вывели своих солдат из (названной) мечети… В противном случае оставляем за собой право принять соответствующие меры». — Представитель Группы по военным вопросам.

Надзорный совет подтвердил решение Facebook о восстановлении первоначально удаленного контента. При этом он отметил, что сообщение не содержало восхваления, поддержки опасной организации или ее контента. Сообщение лишь воспроизводило новость легального новостного канала по срочному вопросу, затрагивающему общественные интересы. Кроме того, Facebook сообщила Совету, что не получала законного запроса от государственных органов на удаление контента, а это значит, что ни один государственный орган не был призван обосновать запрос на удаление.

ВСТАВКА 14. **Дело Надзорного совета Meta № 2**

В другом решении Надзорный совет отменил решение Facebook удалить пост в Instagram, призывавший людей обсуждать одиночное заключение лидера опасной организации. В соответствии с политикой Facebook и организация, и ее лидер были отнесены к категории «опасных субъектов».

Один из пользователей Instagram опубликовал фотографию лидера со словами «Вы все готовы к этому разговору». Пользователь призвал читателей вступить в дискуссию о заключении лидера в тюрьму и бесчеловечной природе одиночного заключения.

После первоначального решения об удалении Facebook проинформировала Совет о том, что правила социальной сети были изменены, и пользователям было разрешено обсуждать права человека лиц, признанных опасными. Надзорный совет отменил первоначальное решение Facebook об удалении контента и предписал Facebook в обновленном руководстве «более подробно описать «реальный вред, который политика стремится предотвратить и устранить, когда подавляется чей-то голос», и добавить четкое пояснение о том, какие действия не относятся к «поддержке».

ВСТАВКА 15. **Дело Надзорного совета Meta № 3**

В 2022 году одна из газет сообщила на своей странице в Facebook, что представитель опасной организации объявил о скором открытии школ для женщин и девочек в районе, находящемся под контролем этой организации.

Meta сочла, что это сообщение нарушает политику в отношении опасных лиц и организаций, которая запрещает «восхвалять» организации, которые, как считается, «занимаются серьезным вредительством вне сети Интернет».

Позднее Meta отменила решение об удалении и пришла к выводу, что стандарт сообщества разрешает контент, который «сообщает» об опасных организациях. Надзорный совет отменил первоначальное решение Facebook об удалении контента, отметив, что право получать и распространять информацию, в том числе о террористических группировках, особенно важно во время конфликтов и кризисов, в том числе когда террористические группировки устанавливают контроль над страной.

10.3.2 Наложение гражданско-правовых санкций

Любые гражданско-правовые санкции, налагаемые на лиц или организации, виновные в подстрекательстве к террористическим актам, должны быть предусмотрены законом и соответствовать принципам необходимости и соразмерности, а также подлежать независимому административному или судебному надзору и обжалованию.

ВСТАВКА 16. **МАСПЧ* постановил, что наложение гражданско-правовых санкций нарушает свободу выражения мнений**

Межамериканским судом по правам человека было рассмотрено судебное решение государства о лишении лиц, признанных виновными в совершении террористических актов, права «пользоваться средством социальной коммуникации, быть его директором или администратором, а также выполнять функции, связанные с публикацией и распространением мнений и информации», на 15 лет.

Суд постановил, что данное наказание нарушает принцип соразмерности, особенно учитывая то, что обвиняемые являлись лидерами маргинализированного сообщества, права человека членов которого постоянно нарушались, и подобное наказание ограничило бы их способность принимать участие в распространении мнений, идей и информации, что, в свою очередь, ограничило бы их право на свободу мысли и выражения мнений при выполнении ими своих функций в качестве лидеров или представителей своих сообществ.

Кроме того, Суд постановил, что неправильное применение государством контртеррористического законодательства может иметь запугивающий и сдерживающий эффект на осуществление свободы выражения мнений другими членами маргинализированного сообщества, который может быть вызван страхом подвергнуться гражданскому или уголовному наказанию, которое не является необходимым или является несоразмерным в демократическом обществе, и которое может привести к самоцензуре человека, на которого наложено наказание, и других членов общества. Согласно заключению Суда, то, как закон о борьбе с терроризмом был применен к членам маргинализированного сообщества, может вызвать обоснованные опасения у других членов этого сообщества, участвующих в социальных протестах с целью признания их территориальных прав.

Норин Катриман против *Чили*, пп. 374–376.

* Межамериканский суд по правам человека

ВСТАВКА 17. **ЕСПЧ* постановил, что наложение гражданско-правовых санкций не нарушает свободу выражения мнений**

Судом было рассмотрено решение национального суда о наложении штрафа на телекомпанию государства-члена в размере около 671 000 евро за поддержку группировки, которая была внесена в список террористических организаций ЕС, Канадой, США, Австралией и Соединенным Королевством. Национальный суд отклонил ходатайство об отзыве лицензии вещателя.

ЕСПЧ счел, что национальные суды тщательно оценили представленные им доказательства и провели анализ, в ходе которого было учтено право компании-заявителя на свободу выражения мнения. В национальные суды были представлены доказательства, подтверждающие, что при освещении вооруженного конфликта между третьим государством-членом и обозначенной группировкой вещание в основном опиралось на информацию, полученную от сторонников группировки без привлечения каких-либо других источников. В ряде программ лидеры группировки рассказывали о своих взглядах и подстрекали к восстанию, а телеведущий пассивно слушал их. Телекомпания не предприняла никаких усилий, чтобы дистанцироваться от подстрекательства или отразить другие мнения, например, задавая острые вопросы. Эффект от предвзятого освещения деятельности группировки и предоставления ей эфирного времени для подстрекательства и пропаганды усиливался формулировками, которые использовал ведущий: например, он назвал арест лидера группировки «международным заговором». В программах погибших членов группировки называли «героями» и «мучениками» и упоминали конкретные действия, совершенные группировкой, которые привели к жертвам среди полицейских и военных сил третьего государства. Национальные суды постановили, что предвзятое вещание в сочетании с «неоднократным подстрекательством к участию в боях и акциях, подстрекательством к присоединению к организации/повстанцам» было равносильно пропаганде от имени террористической группы, а не простому сочувствию ей. Национальный суд также установил, что вещательная компания в значительной степени финансировалась террористической организацией. Национальные суды также отметили, что другие программы, транслируемые компанией, касались общего положения маргинализованной группы, связанной с террористической группой, в том числе их языка, культуры и политики. ЕСПЧ постановил, что, учитывая 1) характер оспариваемых программ, которые включали в себя подстрекательство к насилию и поддержку террористической деятельности, 2) тот факт, что выраженные в них взгляды были распространены среди широкой аудитории посредством телевизионного вещания и 3) то, что они непосредственно касались вопроса, имеющего первостепенное значение для современного европейского общества — предотвращения терроризма и связанных с терроризмом высказываний, пропагандирующих применение насилия — жалоба компании-заявителя не подпадает под защиту, предоставляемую Конвенцией в отношении свободы выражения мнений. Соответственно, ЕСПЧ объявил жалобу неприемлемой для рассмотрения по существу.

ROJ TV/AS против *Дании*, пп. 9 и 39–49.

* Европейский суд по правам человека

10.3.3 Уголовное преследование

Государства обязаны запрещать и должным образом пресекать подстрекательство к терроризму и пропаганду национальной, расовой или религиозной ненависти, представляющей собой подстрекательство к дискриминации, вражде или насилию. Указанные действия, в зависимости от конкретных обстоятельств, могут потребовать принятия мер уголовного правосудия в отношении виновных. В то же время в ряде государств были вынесены жесткие приговоры лицам в связи с контентом, распространяемым ими в Интернете. В одном из государств-членов (Иран) власти вынесли смертный приговор руководителю популярного новостного канала в Telegram, после того как он был осужден за подстрекательство к протестам и связь с иностранными спецслужбами[158].

И Африканский суд по правам человека и народов, и Европейский суд по правам человека рассматривали дела о назначении уголовных наказаний и оценивали правомерность приговоров, вынесенных по уголовным делам, в свете стандартов в области прав человека.

При рассмотрении преступлений, связанных с высказываниями, важно учитывать, что судебное преследование на основании выражения мнения может оказать сдерживающее воздействие на других людей в том, что касается интерпретации ими своего права на свободу выражения мнений, что обычно приводит к самоцензуре.

Хотя некоторые оспариваемые высказывания, описанные во вставках ниже, были сделаны не в Интернете, данные примеры и их анализ, тем не менее, одинаково актуальны для онлайн- и для офлайн-высказываний.

158 См. Amnesty International, 12 декабря 2020 г: Iran: Execution of journalist Rouhollah Zam a 'deadly blow' to Freedom of Expression («Иран: казнь журналиста Рухоллы Зама — «смертельный удар» по свободе выражения мнений»).

ВСТАВКА 18. **ЕСПЧ* постановил, что уголовное наказание нарушает свободу выражения мнений**

Дело касалось участия бывшего баскского политика-сепаратиста в церемонии почтения памяти бывшего члена террористической организации, в результате чего он был приговорен к одному году тюремного заключения за публичную поддержку терроризма.

Суд постановил, что, хотя обвиняемый сделал определенные заявления на церемонии в память бывшего члена террористической организации в напряженном политическом и социальном контексте, содержание и формулировки его высказываний показывали, что он не намеревался подстрекать людей к насилию, одобрять или защищать терроризм, и поэтому не было установлено ни прямого, ни косвенного подстрекательства к насилию. Напротив, в оспариваемой речи на церемонии прозвучала поддержка использования демократических средств для достижения конкретной политической цели. Поэтому ограничения свободы выражения мнений не могут считаться «необходимыми в демократическом обществе».

Эркизия Альмандос против *Испании*, пп. 42–50.

* Европейский суд по правам человека

ВСТАВКА 19. **АСПЧН* постановил, что осуждение по уголовному делу нарушает свободу выражения мнений**

На основании ряда публичных выступлений обвиняемый, оппозиционный политический лидер, был признан виновным и приговорен к 15 годам тюремного заключения за «пособничество или содействие в терроризме», «попытку прибегнуть к терроризму... и другим формам насилия для дестабилизации установленной власти и нарушения конституционных принципов» и «подрыв внутренней безопасности государства, распространение слухов, способных настроить население против политических властей и настроить граждан друг против друга».

Суд рассмотрел заявления обвиняемого и заключил, что, хотя они могут «быть оскорбительными» и могут дискредитировать честность и неподкупность должностных лиц и государственных институтов, «государственные институты и должностные лица не могут быть закрыты для критики, и рассматриваемые высказывания не могут обоснованно считаться способными «разжечь вражду»... или «угрожать безопасности государства».

Ингабире Виктуар Умухоза против *Республики Руанда*, пп. 160–161.

* Африканский суд по правам человека и народов

ВСТАВКА 20. **ЕСПЧ* признал несоразмерным приговор, вынесенный за восхваление терроризма**

Обвиняемый являлся бывшим членом террористической группировки. В радиопередаче, которая была записана и впоследствии размещена на веб-сайте, он назвал исполнителей теракта «храбрыми» и сказал, что они «храбро сражались». Он был признан виновным в публичной защите террористического акта и приговорен к 18 месяцам тюремного заключения, десять из которых были отсрочены.

Суд постановил, что хотя высказывания заявителя не являлись прямым подстрекательством к насилию, они создали положительный образ исполнителей террористических актов и прозвучали в то время, когда французское общество еще не оправилось от смертоносных терактов 2015 года, а уровень террористической угрозы оставался высоким. Однако Суд также установил, что в конкретных обстоятельствах дела вынесенный приговор был несоразмерен преследуемой законной цели и не являлся необходимым в демократическом обществе.

Руйян против *Франции*, пп. 60, 69–71, 75–76.

* Европейский суд по правам человека

[XI] Технологии обхода

11.1 Технологии обхода

Хотя тот факт, что правонарушители используют шифрование в злонамеренных целях, является неоспоримым, существует множество законных причин, по которым отдельные лица или группы лиц могут использовать технологии, защищающие анонимность или позволяющие избежать обнаружения, включая виртуальные частные сети (VPN), даркнет, криптовалюты и системы обмена сообщениями с шифрованием.

Например, правозащитники могут прибегать к помощи даркнета, когда государства запрещают деятельность других поставщиков услуг или иным образом жестко ограничивают свободу выражения мнений. Правоохранительные органы, правозащитники, врачи и журналисты могут использовать системы обмена сообщениями с шифрованием для защиты источников и информаторов, а также другой конфиденциальной информации, такой как медицинские записи. Отдельные лица и группы могут прибегать к одноранговым криптовалютным операциям для обхода хищнических банковских практик или несоразмерно обременительных требований к финансовой отчетности.

Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ ООН) предупреждало правительства о недопустимости подрыва шифрования, отметив, что «[ш]ифрование является одним из основных факторов обеспечения конфиденциальности и безопасности в Интернете и необходимо для защиты прав. В последние годы правительства разных стран предприняли действия, которые, преднамеренно или нет, могут подорвать безопасность и конфиденциальность зашифрованных сообщений. Это имеет серьезные последствия для осуществления права на неприкосновенность частной жизни и других прав человека»[159].

Специальный докладчик ООН по вопросу свободы выражения мнений отмечал, что «шифрование обеспечивает «зону приватности», которая позволяет людям формулировать мнения и обмениваться ими посредством онлайн-переписки и других цифровых средств массовой информации. Шифрование позволяет людям быть уверенными в том, что их «сообщения получат только те, кому они предназначены, без вмешательства или изменения, и чтобы получаемые ими сообщения были в равной степени свободны от посягательств». В некоторых случаях шифрование может также гарантировать анонимность: использование специально разработанных схем шифрования, таких как Tor, позволяет анонимизировать метаданные (такие как время, дата и место сообщений и действий человека в Интернете) и цифровые идентификаторы (такие как адреса электронной почты или IP-адреса)[160].

159 См., например, A/HRC/51/17, п. 21.

160 A/HRC/38/35, Add. 5, п. 6.

ВСТАВКА 21. **Закон о регулировании телекоммуникаций в стране X**

В стране X закон о регулировании телекоммуникаций затрагивает вопросы «национальной безопасности» и «всеобщей мобилизации». Одна из статей запрещает поставщикам и пользователям телекоммуникационных услуг использовать шифровальное оборудование без письменного разрешения Управления по регулированию телекоммуникаций, Вооруженных сил и органов национальной безопасности.

Принцип 40 Декларации принципов свободы выражения мнений и доступа к информации в Африке[161] запрещает государствам-членам принимать законы, которые «запрещают или ослабляют шифрование, включая бэкдоры, депонирование ключей и требования локализации данных, если только такие меры не являются оправданными и совместимыми с международным правом и стандартами в области прав человека».

Согласно рекомендациям Организации Объединенных Наций и региональных механизмов по защите прав человека, государства не должны принимать или должны пересмотреть законы и меры политики, которые предусматривают следующее[162]:

- общие запреты на шифрование и анонимность, несоразмерные и не являющиеся необходимыми, что делает их неправомерными ограничениями свободы выражения мнений, в том числе в рамках ответных мер государств на терроризм и другие формы насилия;
- меры, ослабляющие доступные средства цифровой безопасности, такие как бэкдоры и депонирование ключей, поскольку они несоразмерно ограничивают свободу выражения мнений и неприкосновенность частной жизни и делают коммуникационные сети более уязвимыми для атак.

ВСТАВКА 22. **ЕСПЧ* об обоснованном подозрении**

Бывший сотрудник полиции был заподозрен в членстве в террористической организации только на основании того, что он якобы пользовался сервисом обмена зашифрованными сообщениями, и помещен под стражу до суда.

Суд пришел к выводу, что, поскольку сервис обмена сообщениями использовался не только террористами, одного лишь факта пользования этим сервисом было недостаточно для того, чтобы вызвать обоснованные подозрения в принадлежности к террористической организации, и поэтому его задержание было незаконным.

Акгюн против *Турции*

* Европейский суд по правам человека

11.2 Агрессивные интрузивные технологии

Интрузивное ПО, позволяющее получить доступ к стационарным и мобильным устройствам для скрытого и удаленного отслеживания коммуникаций пользователя и другой информации, включая метаданные (например, местоположение, продолжительность, источник и контакты), называют «шпионскими программами».

161 URL: https://achpr.au.int/sites/default/files/files/2021-05/principlesandguidelinesonhumanandpeoplesrightswhilecounteringterrorisminafrica.pdf

162 Совместная декларация о свободе выражения мнений и противодействии насильственному экстремизму, принятая Специальным докладчиком ООН по вопросу свободы выражения мнений, Представителем Организации по безопасности и сотрудничеству в Европе по вопросам свободы средств массовой информации, Специальным докладчиком Организации американских государств по вопросам свободы выражения мнений и Специальным докладчиком Африканской комиссии по правам человека и народов по вопросам свободы выражения мнений и доступа к информации, 3 мая 2016 г. URL: https://www.osce.org/files/f/documents/e/9/237966.pdf

Если в прошлом технологии наблюдения, как правило, были прерогативой исключительно государственных учреждений, то в современную эпоху большинство таких технологий разрабатывается частными компаниями, которые затем продают их государственным учреждениям или предоставляют в их распоряжение иным образом[163].

При помощи компьютерно-технической экспертизы группы гражданского общества выявили широкое использование таких технологий репрессивными органами государств-членов во всем мире, в частности, в отношении политиков, журналистов, правозащитников и политических диссидентов. Есть свидетельства того, что некоторые из указанных лиц подвергаются и другим нарушениям прав человека, включая внесудебные казни и пытки, а также сексуальное и гендерное насилие[164].

Государства, использующие такие технологии, должны нести ответственность за все связанные с ними нарушения прав человека. Однако государства, разрешающие торговлю или передачу таких технологий на международном уровне, как минимум, обязаны в той или иной форме проявлять должную осмотрительность в отношении потенциального использования таких технологий получателями и принимать соответствующие меры, включая введение запрета на интрузивные технологии[165].

Бывший Специальный докладчик ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение отметил:

> ***"Аналоговые средства наблюдения, такие как прослушивание стационарного или мобильного телефона, обычно позволяют получить доступ к разговорам, что само по себе является потенциальной проблемой, но никак не обширный доступ к контактам, данным о местоположении, нажатиям клавиш, видео и так далее. Цели их применения можно контролировать как с помощью судебного ордера, так и с помощью технологий. В случае с шпионскими программами вроде Pegasus интрузивность ПО может быть сложно ограничить. С юридической точки зрения государству может быть трудно или даже невозможно доказать, что оно использует шпионские программы в узких целях и без «побочного» сбора персональных данных, не имеющих отношения к законной государственной цели"[166].***

Технологии наблюдения затрагивают не только тех людей, чьи данные фактически собираются, но и всех остальных, поскольку страх допустить нарушение приводит к самоцензуре. Этот сдерживающий эффект становится еще более острым, когда шпионское ПО предоставляет данные не только об объекте наблюдения, но и обо всех его контактах[167]. В решении, касающемся использования шпионского ПО Pegasus, Верховный суд Индии отметил, что «такое отрицательное воздействие на свободу слова является посягательством на жизненно важную роль прессы как общественного наблюдателя, что может подорвать способность прессы предоставлять точную и достоверную информацию»[168].

---

163 Частичный список таких компаний см. в Документе с изложением позиции Специального докладчика ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом. Глобальное регулирование торговли технологиями шпионских программ контртеррористического назначения: предложения по разработке подхода, отвечающего требованиям прав человека, п. 17. URL: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

164 Документ с изложением позиции Специального докладчика ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом. Глобальное регулирование торговли технологиями шпионских программ контртеррористического назначения: предложения по разработке подхода, отвечающего требованиям прав человека, пп. 18–24.

165 См. Замечание общего порядка № 36 Комитета по правам человека, пп. 7, 22 и 23.

166 D. Kaye, 'The Spyware State and the Prospects for Accountability' («Государство-шпион и перспективы подотчетности») (2021), 27(4) Global Governance, p. 492.

167 A/HRC/51/17, п. 12.

168 См. обзор дела *Манохар Лал Шарма* против *Союза Индии*, рассмотренного в Верховном суде Индии, Постановление от 27 октября 2021 г., п. 39, URL: https://globalfreedomofexpression.columbia.edu/cases/manohar-v-union-of-india/

Как отмечалось выше, произвольное использование технологий наблюдения может иметь особенно тяжелые последствия для женщин, поскольку они чаще подвергаются шантажу или дискредитации в результате фактического или потенциального обнародования реального или поддельного сексуализированного контента. Кроме того, нахождение сложных технологий наблюдения в частных руках повышает риск насилия со стороны близкого партнера[169].

Темпы технологического развития шпионских программ вызывают тревогу. Например, несмотря на то, что гражданское общество выражает глобальную обеспокоенность по поводу использования Pegasus, эксперты в состоянии обнаружить его наличие на устройствах. С появлением технологии, разработанной компанией Toka, все может измениться. Эта новейшая технология может не только перенаправлять видео в режиме реального времени, но и изменять старые записи и стирать любые доказательства тайной операции, не оставляя при этом никаких следов и признаков взлома. В рекламных материалах компании утверждается, что эта технология может собирать визуальную информацию из «живого и записанного видео» и может «изменять потоки» «аудио- и визуальных» записей, чтобы «маскировать действия на месте» во время «скрытых операций»[170].

Существование такой технологии вызывает серьезные опасения в отношении принципа верховенства права. Например, обычно отредактированное видео не принимается в качестве доказательства в суде. Поэтому суды и стороны разбирательства полагаются на наличие технологий, позволяющих обнаружить проведенные манипуляции. Если манипуляции невозможно обнаружить, риск того, что видео будет изменено с целью осуждения невиновного и оправдания виновного, достигнет невероятных масштабов. Более того, невозможность обнаружения технологий может нарушить право на применение средств защиты от злоупотреблений. Следовательно, использование технологии, подобной той, которую разработала компания Toka, не может соответствовать международному праву прав человека, по крайней мере, до тех пор, пока не будет разработана технология, способная обнаружить ее использование.

Что касается других форм шпионского ПО, то государства-члены должны обеспечить защиту от нарушений прав человека на своей территории и (или) под своей юрисдикцией со стороны третьих лиц, включая коммерческие предприятия, путем создания правовой базы, регулирующей использование коммерческой продукции с высокой степенью риска, такой как шпионское ПО, национальными силами безопасности путем предотвращения использования шпионского ПО дискриминационным образом и внедрения эффективного и независимого надзора, как текущего, так и ретроспективного, и обеспечения пострадавшим лицам доступа к эффективным средствам правовой защиты в случае обнаружения незаконного использования шпионских программ.

Государства обязаны принимать адекватные законодательные и оперативные меры для защиты лиц, находящихся под их юрисдикцией, от незаконного вмешательства в их права человека со стороны субъектов частного сектора[171]. Это требование также закреплено в Руководящих принципах предпринимательской деятельности в аспекте прав человека, разработанных ООН.

Тема международного регулирования индустрии коммерческих шпионских технологий и торговли ими, вероятно, будет часто обсуждаться на международном уровне в ближайшие годы[172].

---

169 Документ с изложением позиции Специального докладчика ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом. Глобальное регулирование торговли технологиями шпионских программ контртеррористического назначения: предложения по разработке подхода, отвечающего требованиям прав человека, пп. 52 и 55, URL: https://repository.graduateinstitute.ch/record/301602?v=pdf

170 URL: https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000

171 См. Замечание общего порядка № 36 Комитета по правам человека, пп. 7, 22 и 23.

172 Специальный докладчик по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом, «Глобальное регулирование торговли технологиями шпионских программ контртеррористического назначения: предложения по разработке подхода, отвечающего требованиям прав человека» (апрель 2023 г.); Европейский парламент, Комитет по расследованию использования Pegasus и аналогичных шпионских программ, предварительная версия отчета (28 ноября 2022 г.).

[XII] Отключение Интернета

12.1 Отключение Интернета

Под отключением Интернета понимают меры, предпринимаемые правительством или от его имени для намеренного нарушения доступа к информационно-коммуникационным системам в Интернете и их использования. К ним относятся действия, направленные на ограничение способности большого числа людей пользоваться средствами онлайн-коммуникаций путем массового ограничения подключения к Интернету либо путем создания препятствий для доступа и использования Интернета, социальных сетей и коммуникационных услуг путем замедления скорости подключения. В некоторых случаях отключение Интернета сопровождается отключением целых телефонных сетей, в результате чего не остается ни одного канала прямой электронной связи. В период с 2016 по 2021 год отключение Интернета было зарегистрировано в 74 странах, причем в некоторых из них неоднократно и на длительные периоды времени[173].

Результаты таких отключений часто бывают плачевными. Отключения использовались для вмешательства в право на мирные собрания, часто в контексте протестов и политических кризисов, нанося ущерб демократическим избирательным процессам и свободному распространению информации. Отключение Интернета серьезно сказывается на всех секторах экономики и влияет на доступ к основным услугам, которые все больше зависят от цифровых инструментов и коммуникаций, таким как образование, здравоохранение, социальная и гуманитарная помощь[174]. Отключение Интернета может особенно тяжело сказаться на женщинах и девочках, подрывая их доступ к важнейшей поддержке и защите, включая экстренную медицинскую помощь и информацию по вопросам репродуктивного здоровья, и усугубляя гендерный разрыв[175]. Оно также может отрицательно сказаться на возможностях карьерного продвижения и получения образования[176].

Отключение Интернета пагубно сказывается на многих правах человека, и в первую очередь на праве на свободу выражения мнений и доступ к информации. Отключение Интернета, как правило, нарушает требования законности в соответствии с национальным законодательством/правовой определенности, наличия законной цели, необходимости и соразмерности, предусмотренные международным правом прав человека[177].

Отключая Интернет, правительства часто не признаются в этом или предоставляют минимальное обоснование указанных мер, включая их правовую базу. Когда отключения происходят на основании законного приказа, они, как правило, опираются на нечетко сформулированные законы, предоставляющие властям широкую свободу действий. Официальным обоснованием большинства случаев закрытия сайтов были соображения

173 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Отключение Интернета: тенденции, причины, правовые последствия и воздействие на ряд прав человека», A/HRC/50/55, пп. 5–6 и 19. URL: https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

174 Там же, пп. 25, 26, 33, 35–37.

175 Там же, п. 38.

176 См. Access Now: URL: https://www.accessnow.org/internet-shutdowns-international-womens-day/

177 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Отключение Интернета: тенденции, причины, правовые последствия и воздействие на ряд прав человека», A/HRC/50/55, пп. 9 и 13.

общественной и национальной безопасности или необходимость ограничить распространение информации, считающейся незаконной или способной нанести вред. Согласно данным, собранным группами гражданского общества, 189 отключений в период с 2016 по 2021 год были обоснованы соображениями общественной безопасности, а 150 — соображениями национальной безопасности. За многими из этих отключений последовали всплески насилия, что, по-видимому, свидетельствует о том, что эти меры часто не достигают официально заявленных целей обеспечения охраны и безопасности[178].

ВСТАВКА 23. **Отключение Интернета и коммуникационных услуг в государстве-члене J на два года**

По соображениям борьбы с терроризмом государство-член J закрыло доступ к Интернету и коммуникационным услугам в регионе Y, где проживает 6 миллионов человек, на два года с 2020 по 2022 год. Среди многочисленных разрушительных последствий для гражданского населения этого преимущественно сельскохозяйственного региона можно отметить то, что лица, зависящие от натурального хозяйства, не могли получать метеорологическую информацию и обмениваться ею, а население в целом не могло получать денежные переводы из-за границы, которые являлись для них важным источником дохода.

ВСТАВКА 24. **Блокирование Википедии в государстве-члене L**

Государство-член L заблокировало доступ к Википедии чуть более чем на год. Объявляя об ограничении доступа к Википедии, власти государства сослались на полномочия правительства блокировать доступ к веб-страницам или целым сайтам, если это будет сочтено необходимым.

Учитывая неизбирательное и широкомасштабное воздействие отключения Интернета, оно крайне редко отвечает критерию соразмерности. Негативное воздействие отключений на многочисленные права часто выходит за пределы областей или периодов их применения, что делает их несоразмерными, даже если они осуществляются с целью реагирования на реальные угрозы[179].

Комитетом по правам человека было отмечено, что общие запреты на работу определенных веб-сайтов и систем также несовместимы с правом на свободу выражения мнений[180]. Верховный комиссар Организации Объединенных Наций по правам человека рекомендовал государствам воздерживаться от всех видов отключения Интернета, в особенности от полного отключения. Целенаправленное отключение услуг связи, предоставляемых через Интернет, может считаться соразмерным и обоснованным только в самых исключительных обстоятельствах, в качестве крайней меры, когда это необходимо для достижения законной цели, такой как национальная безопасность или общественный порядок, и когда никакие другие средства не являются эффективными для предотвращения или смягчения вреда. Если государства все же рассматривают возможность санкционирования или осуществления отключений, Верховный комиссар ООН по правам человека рекомендует строго придерживаться шести основных требований, согласно которым любые отключения Интернета должны: быть четко обоснованы в однозначном, общедоступном законе, иметь законную цель, быть соразмерными, подлежать предварительному утверждению судом или другим независимым судебным органом, быть заблаговременно объявлены общественности и телекоммуникационным компаниям или интернет-провайдерам с четким разъяснением правовой основы отключения и подробностей относительно его охвата и продолжительности, предусматривать конструктивные механизмы возмещения ущерба, доступные для тех, чьи права были затронуты отключениями, в том числе посредством судебного разбирательства в независимых и беспристрастных судах[181].

178 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Отключение Интернета: тенденции, причины, правовые последствия и воздействие на ряд прав человека», A/HRC/50/55, п. 31. URL: https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

179 Там же, пп. 13 и 59.

180 Замечание общего порядка № 34 Комитета по правам человека (Статья 19: Свобода мнений и их выражения), CCPR/C/GC/34, 12 сентября 2011 г., п. 43.

181 Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека, «Отключение Интернета: тенденции, причины, правовые последствия и воздействие на ряд прав человека», A/HRC/50/55, пп. 13, 66-67, URL: https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

ВСТАВКА 25. **Закон о наблюдении в государстве-члене K**

Законы о наблюдении, принятые в государстве-члене K после крупного теракта, позволяли национальным властям отслеживать и блокировать веб-сайты без судебного надзора.

[XIII] Заключение

13.1 Обзор

Контртеррористические программы и меры должны осуществляться без нарушений прав человека для обеспечения соответствия международному праву и предотвращения возникновения или обострения недовольства, которое может привести к насилию. Следовательно, законы и практика в государствах-членах должны соответствовать указанным ниже рекомендациям.

13.2 Краткий обзор рекомендаций

ТАБЛИЦА 2. **Краткий обзор рекомендаций**

Определения терроризма и подстрекательства к терроризму	Определения терроризма и подстрекательства к терроризму, соответствующие типовым определениям, разработанным Советом Безопасности и Специальным докладчиком по правам человека в условиях борьбы с терроризмом.
Наблюдение и сбор данных в Интернете	Наблюдение и сбор данных в Интернете представляют собой вмешательство в право на неприкосновенность частной жизни. Соответственно, необходимо учитывать следующее: • любое такое вмешательство должно: *a*) быть предусмотрено законом, *b*) преследовать законную цель и *c*) быть необходимым и соразмерным; • любое такое вмешательство должно быть санкционировано независимым органом на индивидуальной основе и иметь четкие границы во избежание чрезмерно широкого сбора и хранения данных; • программы наблюдения должны подлежать независимому надзору; • пострадавшие от незаконного наблюдения должны иметь право на эффективные средства правовой защиты; • государства-члены должны признать, что сбор и использование метаданных могут быть столь же интрузивными, как и сбор и использование содержания сообщений.

Запрет на дискриминацию	• Ни при каких обстоятельствах не допускается наблюдение или сбор данных на дискриминационных основаниях. • Ни при каких обстоятельствах не допускается использование биометрических инструментов, включая распознавание лиц, на дискриминационных основаниях. • Пострадавшие от дискриминации имеют право на применение средств правовой защиты.
Интернет и социальные сети	• Расследования с использованием открытых источников должны служить законной цели, быть соразмерными этой цели и недискриминационными. • В контексте контртеррористических мер государства-члены и их ведомства не должны осуществлять сбор данных об отдельных лицах или группах, не прибегающих к насилию или угрозе насилия в соответствии с определениями терроризма и подстрекательства к терроризму, отвечающими требованиям прав человека. • В контексте контртеррористических мер государства-члены и их ведомства не должны требовать от ИКТ-компаний удаления контента, который не подпадает под соответствующие правам человека определения терроризма и подстрекательства к терроризму, или другого контента, защищенного в соответствии с правом прав человека. Действия правоохранительных органов, включая уголовное правосудие в связи с подстрекательством к терроризму, должны соответствовать критериям законности/правовой определенности, надлежащей процедуры и справедливого судебного разбирательства, быть соразмерными и не ограничивать необоснованно права человека, включая свободу выражения мнений.
Особые методы расследования	• Государства-члены должны четко определить в своем национальном законодательстве обстоятельства и условия, при которых компетентные органы имеют право прибегать к особым методам расследования, должным образом учитывая последствия для прав человека, связанные с их интрузивным характером. По этой причине особые методы расследования должны использоваться только для борьбы с тяжкими преступлениями и сопровождаться адекватными гарантиями против злоупотреблений, включая полноценный независимый мониторинг и надзор.
Технологии обхода	• Технологии обхода используются преимущественно в законных целях и поэтому не должны запрещаться.
Отключение Интернета	• Отключение Интернета пагубно сказывается на ряде прав человека, и в первую очередь на праве на свободу выражения мнений и доступ к информации. Отключение Интернета, как правило, нарушает требования правовой определенности, наличия законной цели, необходимости и соразмерности, предусмотренные международным правом прав человека.

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)

24-09826