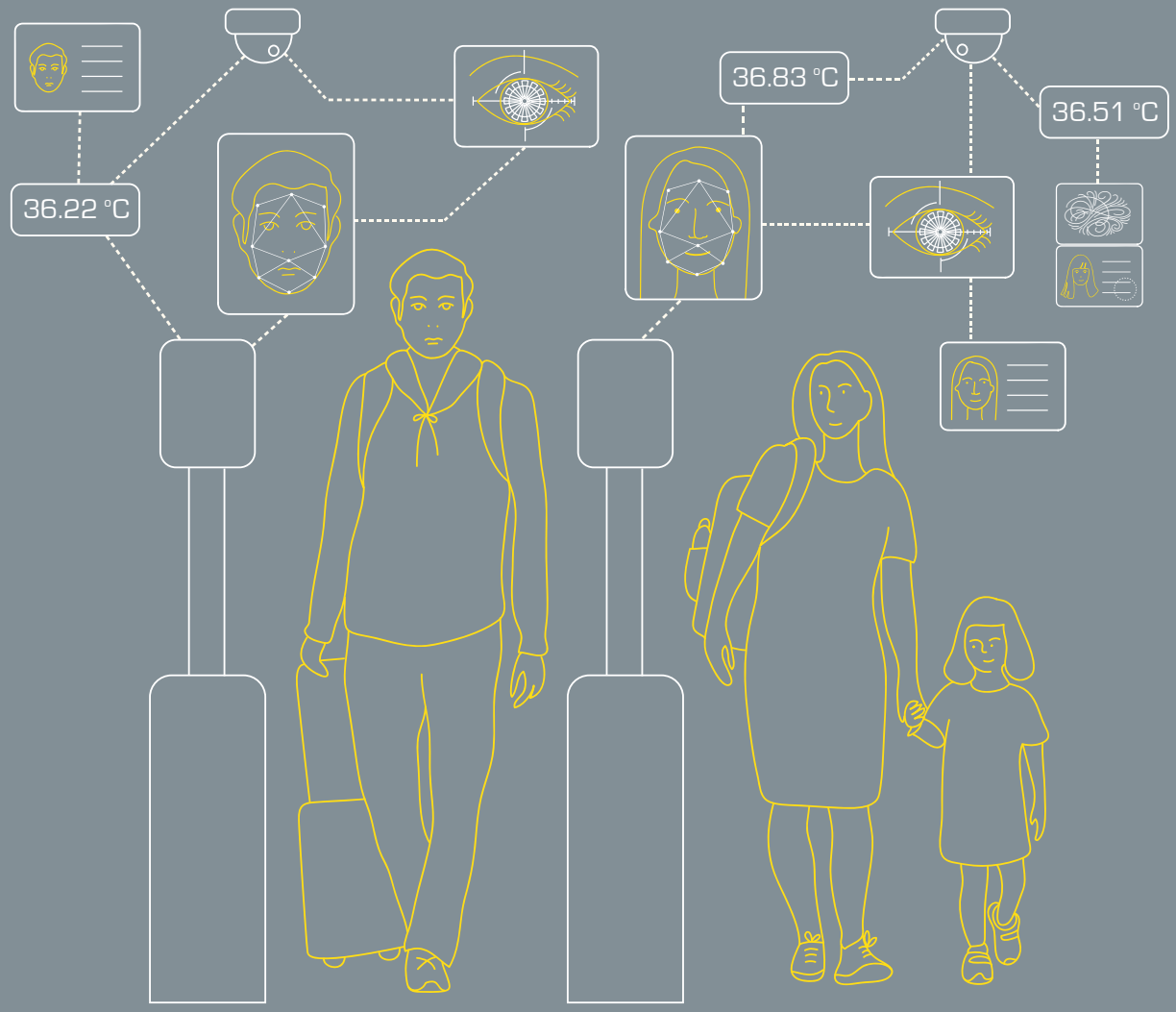
# Управление границами и права человека




## Сбор, обработка и обмен персональными данными и использование новых технологий в контексте борьбы с терроризмом и обеспечения свободы передвижения

OSCE ODIHR

# Концептуальная записка
# Управление границами и права человека

## Сбор, обработка и обмен персональными данными и использование новых технологий в контексте борьбы с терроризмом и обеспечения свободы передвижения

Опубликовано Бюро ОБСЕ по демократическим институтам и правам человека (БДИПЧ)

OSCE Office for Democratic Institutions and Human Rights (ODIHR)
Miodowa 10
00–251 Warsaw
Poland

Тел.: +48 22 520 06 00
Факс: +48 22 520 0605
Электронная почта: office@odihr.pl
osce.org/odihr



ISBN 978-83-66690-52-3



Оформление и иллюстрации: В. Цомака (V. Tzomaka).

# Содержание

# Введение

В нашем глобализированном мире все больше людей пересекают границы стран, чтобы устанавливать и поддерживать контакты, использовать возможности для получения образования и профессионального роста, а также чтобы сменить страну проживания или реализовать право на убежище, спасаясь от преследования.

При этом государства все чаще используют новые технологии сбора, обработки и обмена данными в целях управления миграционными потоками и противодействия транснациональным угрозам безопасности, включая терроризм. Использование таких технологий повышает риск нарушения прав человека в контексте обеспечении пограничного контроля – в области, которая и так является весьма непрозрачной и в которой многое зависит от усмотрения отдельных сотрудников, в которой гарантии защиты прав, подотчетность и надзор являются недостаточными, а частный сектор играет существенную роль в разработке и использовании новых технологий.

В настоящей концептуальной записке представлен обзор тех последствий, к которым может привести сбор и обмен информацией в сфере пограничного контроля, а также рассматривается вопрос о том, как внедрение и постоянное использование новых технологий в данном контексте может сказаться на правах человека. В документе также содержатся рекомендации для государств-участников ОБСЕ, касающиеся защиты и соблюдения прав человека при использовании новых технологий для целей пограничного контроля. Концептуальная записка была подготовлена в рамках постоянной работы Бюро ОБСЕ по демократическим институтам и правам человека (БДИПЧ) в области миграции, свободы передвижения, прав человека и борьбы с терроризмом[1]. После того как в ходе предварительной оценки было выявлено, что рост использования новых технологий для целей управления границами требует внимания (особенно ввиду сопутствующих этим технологиям правозащитных рисков), в июне 2020 г. БДИПЧ провело ряд консультативных онлайн-совещаний экспертов, результаты которых легли в основу данной публикации[2].

1 Более подробную информации о деятельности БДИПЧ в этих областях можно найти по следующим ссылкам: https://www.osce.org/odihr/migration, https://www.osce.org/odihr/freedom-of-movement и https://www.osce.org/odihr/countering-terrorism.

2 15-25 июня 2020 г. БДИПЧ организовало серию консультативных совещаний экспертов на тему «Управление границами и права человека: сбор и обмен данными, использование новых технологий в контртеррористической деятельности и последствия для свободы передвижения». В мероприятиях участвовало в общей сложности более 80 человек. Всего было проведено четыре тематических встречи, в ходе которых рассматривалось воздействие на права человека: i) системы предварительной информации о пассажирах (API) и записи регистрации пассажиров (PNR), ii) сбора, хранения и использования биометрических данных в сфере управления границами, iii) профилирования и принятия решений на основе алгоритмов в контексте пограничного контроля; iv) контрольных списков, баз данных и другого обмена информацией для целей обеспечения пограничного режима. Среди участников были Специальный докладчик ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом (Специальный докладчик ООН по борьбе с терроризмом), Специальный докладчик ООН по вопросу о праве на неприкосновенность частной жизни, представители Управления Верховного комиссара ООН по правам человека (УВКПЧ), Исполнительного директората Контртеррористического комитета Совета Безопасности ООН (ИДКТК), ОБСЕ, Совета Европы, Агентства ЕС по основным правам (АОП), агентства «Фронтекс», Интерпола и других международных организаций, а также представители национальных органов пограничного контроля и профильные эксперты из гражданского общества и научных учреждений. Более подробную информацию об этих совещаниях можно найти по адресу: https://www.osce.org/odihr/453291.

В настоящем документе упоминаются различные цифровые технологии, используемые в управлении миграцией и контртеррористической деятельности. Речь идет о сборе данных о пассажирах и сборе биометрических данных, принятии решений на основе алгоритмов, а также о технологиях искусственного интеллекта, поскольку эти инновационные системы в настоящее время разрабатываются и внедряются в сферу управления миграцией, в пограничный контроль, а также в деятельность по борьбе с транснациональной организованной преступностью и терроризмом.

# Пограничный контроль, безопасность и борьба с терроризмом

Государства несут международные обязательства, касающиеся пограничного контроля в контексте борьбы с терроризмом. Резолюция 2396 (2017) Совета Безопасности ООН возлагает на государства правовые обязательства по созданию систем сбора, обработки и анализа больших объемов персональных данных для выявления террористов и их перемещений. Государства должны принимать такие меры, как создание и внедрение систем для обработки биометрических данных, сбора предварительной информации о пассажирах (Advance Passenger Information – API) и данных записей регистрации пассажиров (Passenger Name Records – PNR), а также создание и использование контрольных списков и баз данных с информацией о лицах, «которые, как было установлено, являются террористами или которые подозреваются в террористической деятельности»[3]. Резолюция также призывает государства делиться этой информацией друг с другом и, при необходимости, с международными организациями[4]. Совет министров ОБСЕ в своих решениях рекомендует государствам-участникам ОБСЕ предотвращать перемещение террористов, в том числе так называемых «иностранных боевиков-террористов»[5], посредством эффективного пограничного контроля[6], а также выдавать гражданам машиносчитываемые проездные документы, содержащие биометрические данные, и принимать другие меры по укреплению безопасности проездных документов[7]. Помимо этого, государства-участники ОБСЕ обязались создать национальные системы предварительной информации о пассажирах[8].

Государства имеют законное право контролировать свои границы и решать, кто может попасть на их территорию. При этом усиленный пограничный контроль, в том числе в целях борьбы с терроризмом, не должен осуществляться в ущерб соблюдению прав человека и основных свобод[9]. Резолюции Совета Безопасности ООН и обязательства ОБСЕ неизменно говорят о том, что все действия по борьбе с терроризмом должны осуществляться с

3 Резолюция 2396 (2017), принятая Советом Безопасности ООН, пункты 11-13 и 15, http://undocs.org/S/RES/2396(2017).

4 *Там же.*

5 Определение понятия «иностранные боевики-террористы» вызывает споры из-за его размытости и возможности широкого толкования и соответствующих последствий этого для прав человека. Более подробная информация содержится в издании «Руководство по выработке ответов на угрозы и вызовы, связанные с «иностранными боевиками-террористами», в контексте защиты прав человека», БДИПЧ, 12 сентября 2018 г., https://www.osce.org/odihr/393503.

6 См.: Решение Совета министров ОБСЕ № 5/14 «Декларация о роли ОБСЕ в противодействии феномену иностранных боевиков-террористов в контексте выполнения резолюций 2170 (2014) и 2178 (2014) Совета Безопасности ООН», Базель, 5 декабря 2014 г., https://www.osce.org/mc/130546, Решение Совета министров ОБСЕ № 1/01 «Бухарестский план действий по борьбе с терроризмом», 4 декабря 2001 г., https://www.osce.org/atu/42524.

7 Решение Совета Министров ОБСЕ № 7/03 «Надежность документов на въезд и выезд», Маастрихт, 1-2 декабря 2003 г., https://www.osce.org/mc/18445, и Решение Совета Министров ОБСЕ № 4/04 «Передача информации об утерянных/похищенных паспортах в службу автоматизированного поиска/базу данных о похищенных документах на въезд и выезд (САП-БДПД) Интерпола», София, 7 декабря 2004 г., https://www.osce.org/mc/16414.

8 Решение Совета Министров ОБСЕ № 6/16 «Более широкое использование предварительной информации о пассажирах», Гамбург, 9 декабря 2016 г., https://www.osce.org/cio/288256.

9 См.: Решение Совета Министров ОБСЕ № 2/05 «Концепция в области безопасности границ и пограничного режима: рамки для сотрудничества государств-участников ОБСЕ», Любляна, 6 декабря 2005 г., https://www.osce.org/mc/17452.

соблюдением международного права, в том числе международного права прав человека и беженского права[10].

На встрече Совета министров в 2005 г. в Любляне государства-участники подтвердили свое обязательство содействовать свободному передвижению людей через границы одновременно поставив перед собой цель сокращения угрозы терроризма. Была подчеркнута необходимость с уважением обращаться с лицами, пересекающими границу, в соответствии с нормами международного и национального права и международным стандартам в области прав человека. Государства-участники также обязались активизировать свои усилия, направленные на то, чтобы их национальное законодательство, политика и принимаемые меры обеспечивали всем лицам равную и эффективную защиту и запрещали акты нетерпимости и дискриминации[11]. В соответствии с этими обязательствами ОБСЕ управление границами не должно быть увязано с контртеррористическими мерами, основанными на предположениях об опасности отдельных лиц или групп лиц, желающих перемещаться из одной страны в другую.

10 См.: Резолюция 2396 (2017) Совета Безопасности ООН; Решение Совета Министров ОБСЕ № 1/16 «Декларация о наращивании усилий ОБСЕ по предупреждению терроризма и противодействию ему», Гамбург, 9 декабря 2016 г., https://www.osce.org/cio/288176; Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063) 2012 года, https://www.osce.org/pc/98008.

11 Решение Совета Министров ОБСЕ № 2/05, Любляна, указ. соч., п. 9.

# Права человека, находящиеся под угрозой

Согласно всеобъемлющей концепции безопасности ОБСЕ, эффективные меры по борьбе с терроризмом и соблюдение прав человека не противоречат другу, а являются дополняющими друг друга задачами. Устойчивая безопасность невозможна без защиты прав человека[12]. Таким образом, обеспечение безопасности и защита жизни сами по себе являются обязательствами в области прав человека.

В связи с этим в настоящей концептуальной записке будут рассмотрены некоторые касающиеся прав человека соображения, которые государствам следует учитывать при использовании новых технологий для управления границами и борьбы с терроризмом.

## Общие принципы прав человека: правовая база, эффективные средства правовой защиты и надзор

Международные нормы в области прав человека допускают ограничение некоторых из этих прав – например, права на неприкосновенность частной жизни и права на свободу передвижения, но только при строгом соблюдении определенных условий. Любое вмешательство в эти права должно быть **предписанным законом, строго необходимым для достижения законной цели, соразмерным** этой цели и **недискриминационным.** Государства ни при каких обстоятельствах не должны вводить ограничения, ущемляющие саму суть конкретного права[13]. Аналогичным образом, запрещается ограничивать такие **абсолютные права человека и принципы**, как **право на достойное и недискриминационное обращение** при пересечении границ[14].

Международное право прав человека не только запрещает государствам нарушать права человека, но и обязывает их **защищать людей** от неправомерного вмешательства других

12 См.: Решение Совета Министров ОБСЕ № 3/15 «Декларация министров о наращивании усилий ОБСЕ по борьбе с терроризмом в свете недавних атак террористов», Белград, 4 декабря 2015 г., https://www.osce.org/cio/207261. Смотрите также: Решение Совета Министров ОБСЕ № 3/07 «Заявление Совета министров о поддержке глобальной контртеррористической стратегии Организации Объединенных Наций», Мадрид, 30 ноября 2007 г., https://www.osce.org/mc/29544. Продвижение и защита прав человека в контексте контртеррористической деятельности определены в качестве стратегического направления в Консолидированной концептуальной базе ОБСЕ для борьбы с терроризмом (PC.DEC/1063) 2012 года.

13 Комитет по правам человека ООН (ПГПП), «Замечание общего порядка № 31: характер общего юридического обязательства, налагаемого на государства-участники Пакта», 26 мая 2004 г., CCPR/C/21/Rev.1/Add.13, п. 6, https://undocs.org/CCPR/C/21/Rev.1/Add.13.

14 См.: «Рекомендуемые принципы и руководящие положения по правам человека на межгосударственных границах» УВКПЧ, 2014 г. www.ohchr.org/Documents/Issues/Migration/OHCHR_Recommended_Principles_Guidelines.pdf. Государства-участники ОБСЕ обязались поощрять достойное обращение с лицами, пересекающими границу, См.: Решение Совета Министров ОБСЕ № 2/05, Любляна, указ. соч., сноска 9.

лиц, в том числе физических лиц и частных компаний[15]. Государства должны создать **нормативные-правовые и институциональные рамки**, гарантирующие эффективное осуществление прав человека на практике, в том числе (и особенно) в контексте управления границами и борьбы с терроризмом, – ввиду особых обстоятельств принятия решений на границе, для которых характерна высокая степень свободы усмотрения. Должны существовать **эффективные средства правовой защиты и надежные механизмы контроля и возмещения ущерба**[16] для обеспечения подотчетности и предупреждения нарушений прав человека. Крайне важной частью такой системы является **образование и обучение в области прав человека**, ориентированное на тех, кто участвует в разработке и осуществлении мер пограничного контроля и борьбы с терроризмом и принимает решения в этой области[17].

В разработке и эксплуатации систем пограничного контроля с использованием технологий искусственного интеллекта и биометрических технологий все большую роль играет частный сектор, поскольку важные функции в области управления границами и обеспечения безопасности передаются на аутсорсинг частным предприятиям[18]. При этом государственное регулирование и контроль в этой сфере пока не успевают за темпами развития новых технологий и реализуются недостаточно эффективно. Нормативно-правовая база, касающаяся использования новых технологий, требует доработки, поскольку данная сфера характеризуется дискреционным принятием решений, ее развитие зависит от частного бизнеса, а определенность относительно возможных правовых последствий отсутствует[19]. **Государства несут основную ответственность за обеспечение соблюдения прав человека и должны создать четкие, основанные на правах человека рамки для использования технологий. Руководящие принципы предпринимательской**

---

15 Что касается частных предприятий, то государствам следует четко заявить, что они ожидают от всех предприятий, имеющих офисы на их территории и/или находящихся под их юрисдикцией, соблюдения прав человека в рамках своей деятельности. В целях выполнения корпоративных обязательств по защите прав человека предприятия должны проводить тщательную проверку своей деятельности с точки зрения прав человека и соответствующую оценку воздействия. См.: Доклад Специального представителя Генерального секретаря по вопросу о правах человека и транснациональных корпорациях и других предприятиях «Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций, касающихся «защиты, соблюдения и средств правовой защиты», UN Doc. A/HRC/17/31, 23 марта 2011 г., принципы 2 и 17, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf.

16 Статья 2(3) Международного пакта о гражданских и политических правах (МПГПП) предоставляет каждому, чьи признаваемые в Пакте права или свободы были нарушены, право на эффективное средство правовой защиты. В отношении соответствующих обязательствах ОБСЕ см. также: Итоговый документ Венской встречи 1986 года представителей государств-участников совещания по безопасности и сотрудничеству в Европе, состоявшейся на основе положений заключительного акта, относящихся к дальнейшим шагам после совещания, 1989 г., п. 13.9, https://www.osce.org/files/f/documents/9/1/40885.pdf; Документ Копенгагенского совещания Конференции по человеческому измерению СБСЕ, 29 июня 1990 г., п. 5, 5.10 и 5.11, https://www.osce.org/files/f/documents/d/0/14305.pdf; Документ Московского совещания Конференции по человеческому измерению СБСЕ, 3 октября 1991 года, пункт 18.2 и 18.4, https://www.osce.org/files/f/documents/8/a/14314.pdf.

17 Согласно Статье 2(1) МПГПП, государства обязаны принимать законодательные, судебные, административные, образовательные и другие соответствующие меры для выполнения принятых ими правовых обязательств в рамках МПГПП; см.: Комитет по правам человека ООН, Замечание общего порядка № 31, указ. соч., сноска 13, п. 7. Помимо этого, в решениях Совета Министров ОБСЕ говорится о необходимости проведения обучающих программ, в том числе по вопросам недискриминации, и обмена хорошей практикой в этой области.

18 Доклад Специального докладчика ООН по вопросу о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости (далее – Специальный докладчик ООН по вопросу о современных формах расизма), UN Doc. A/75/590, 10 ноября 2020 г., https://undocs.org/en/A/75/590. В пункте 16 упоминается термин «пограничный промышленный комплекс», который используется для описания растущей приватизации пограничного контроля и управления миграцией, а также использования все более строгих проверок. См. также: Доклад Рабочей группы ООН по вопросу об использовании наемников как средстве нарушения прав человека и противодействия осуществлению права народов на самоопределение (Рабочая группа по вопросу об использовании наемников), UN Doc. A/HRC/45/9, 9 июля 2020 г., пп. 75-77, https://undocs.org/en/A/HRC/45/9.

19 См.: Petra Molnar, Technological Testing Grounds – Migration Management Experiments and Reflections from the Ground Up [Технологические испытательные площадки – эксперименты по управлению миграцией и размышления по всем вопросам], November 2020, EDRi and the Refugee Law Lab, https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.

**деятельности в аспекте прав человека ООН (Принципы Ругги) также определяют обязанности коммерческих предприятий в отношении прав человека.** Компании должны проводить тщательную проверку своей деятельности с точки зрения прав человека, с тем чтобы она не приводила к негативным последствиям для этих прав[20].

Технологии и системы, применяемые в сфере управления границами и в борьбе с терроризмом, могут оказывать воздействие на целый ряд прав человека, охраняемых международным правом. В рассматриваемом контексте особенно актуальны некоторые из этих прав человека.

## Свобода передвижения

Согласно статье 12 Международного пакта о гражданских и политических правах (МПГПП), каждый человек имеет **право покинуть любую страну, включая свою собственную, и также въехать в свою собственную страну**[21]. Свобода передвижения является одним из неотъемлемых условий свободного развития личности[22]. Въезд иностранца на территорию государства может быть ограничен только тогда, когда применяемые ограничения не нарушают международных обязательств в области прав человека. **Иностранные граждане также могут пользоваться защитой МПГПП в отношении въезда или проживания в той или иной стране**, а при ограничении свободы передвижения следует учитывать другие права – такие, например, как защита от дискриминации, запрет жестокого, бесчеловечного или унижающего достоинство обращения и недопущение вмешательства в семейную жизнь[23].

20 См.: Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН, указ. соч., сноска 15.

21 Право покинуть какую-либо страну может ограничиваться только тогда, когда такое ограничение предписано законом и соответствует принципам необходимости, соразмерности и недискриминации. Что касается права вернуться в свою собственную страну, то Комитет по правам человека подчеркивает, что понятие «своя собственная страна» шире понятия «страна своего гражданства». Оно распространяется на иностранных граждан, которые имеют особые связи с рассматриваемой страной (например, проживали в ней длительное время); см.: Комитет по правам человека ООН, Замечание общего порядка №27: Статья 12 (свобода передвижения), UN Doc. CCPR/C/21/Rev.1/Add.9, 2 ноября 1999 г., п. 20, см.: https://www2.ohchr.org/english/bodies/icm-mc/docs/8th/hri.gen.1.rev9_ru.pdf. См. также обязательства ОБСЕ в отношении свободы передвижения, Вена, 1989 г., указ. соч., сноска 16, п. 20.

22 Там же, пункт 1.

23 Комитет по правам человека, Замечание общего порядка №15: Положение иностранцев в соответствии с Пактом, 11 апреля 1986 г., п. 5, https://www.refworld.org/pdfid/45139acfc.pdf.

## Право искать убежище

Право искать убежища и пользоваться им закреплено в статье 14 Всеобщей декларации прав человека (ВДПЧ). Оно получило дальнейшее развитие в Конвенции о статусе беженцев 1951 года и ее соответствующем Протоколе[24]. Система международной защиты, созданная Конвенцией, предусматривает основные права беженцев и связанные с ними обязательства государств, среди которых – **запрет на принудительное возвращение** в страну, где жизни или свободе человека угрожает опасность (принцип **невысылки**)[25].

## Равенство и недискриминация

Статья 1 Всеобщей декларации прав человека гласит, что все люди рождаются свободными и равными в своем достоинстве и правах. Статья 2(1) МПГПП обязывает государства уважать и обеспечивать права, признаваемые в Пакте, «без какого бы то ни было различия, как-то в отношении расы, цвета кожи, пола, языка, религии, политических и иных убеждений, национального или социального происхождения, имущественного положения, рождения или иного обстоятельства». В статье 26 МПГПП гарантируется равенство всех людей перед законом и их право на равную защиту закона без какой-либо дискриминации[26]. Государства не должны отступать от принципа равенства и недискриминации даже во время чрезвычайного положения[27]. **Дискриминация – это любое различие, исключение, ограничение или предпочтение, которое основано на любых вышеупомянутых признаках и которое имеет целью или следствием уничтожение или умаление признания, использования или осуществления всеми лицами, на равных началах, всех прав и свобод**[28]**.** Обеспечение пограничного режима может предполагать различное обращение с лицами, например, в зависимости от их гражданства, но ни при каких обстоятельствах не должно приводить к дискриминации. Ниже будет более подробно рассмотрен вопрос о том, как использование новых технологий в контексте пограничного контроля может на деле усилить проблему расизма, расовой дискриминации и ксенофобии и привести к другим формам социальной изоляции[29]. Государства-участники ОБСЕ категорически не приемлют отождествление терроризма с какой-либо этнической группой, гражданством, религией

---

24 Конвенция о статусе беженцев, 1951 г., https://www.unhcr.org/3b66c2aa10. Также см. обязательства ОБСЕ в отношении права на поиск убежища, Стамбульский документ (Хартия европейской безопасности), ноябрь 1999 г., п. 22, https://www.osce.org/files/f/documents/7/1/39573.pdf.

25 Конвенция о статусе беженцев 1951 г., статья 33. Запрет на принудительное возвращение (высылку) также закреплен в других международных нормах в области прав человека, которые запрещают возвращение человека в страну, где он может подвергнуться риску пыток или других серьезных нарушений прав человека. Абсолютный запрет пыток предполагает абсолютный запрет на высылку человека туда, где к нему могут применяться пытки. См. обзор этих вопросов в: OHCHR, The Principle of non-refoulement under international human rights law [УВКПЧ , Принцип невысылки в международном праве прав человека], https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/ThePrincipleNon-RefoulementUnderInternationalHumanRightsLaw.pdf.

26 Помимо этого, МПГПП гарантирует равные права мужчин и женщин (статья 3) и права детей на защиту без дискриминации по какому-либо признаку (статья 24).

27 В том числе при реагировании на угрозы безопасности или в контексте борьбы с терроризмом.

28 Комитет по правам человека, Замечание общего порядка № 18: Недискриминация, 10 ноября 1989 г., п. 7, https://www.refworld.org/docid/453883fa8.html. Определения дискриминации в рамках Международной конвенции о ликвидации всех форм расовой дискриминации (МКЛРД) и Конвенции о ликвидации всех форм дискриминации в отношении женщин (КЛДЖ) см. в статье 1 обеих Конвенций.

29 Комитет ООН по ликвидации расовой дискриминации (КЛРД), Общая рекомендация № 36 о предупреждении расового профилирования со стороны сотрудников правоохранительных органов и борьбе с ним, CERD/C/GC/36, 24 ноября 2020 г., п. 12, https://undocs.org/CERD/C/GC/36.

или убеждениями и неизменно подтверждают важность соблюдения принципов равенства и недискриминации в контексте борьбы с терроризмом.[30]

## Право на неприкосновенность частной жизни и защиту персональных данных

Обеспечение права на неприкосновенность частной жизни является **обязательным условием** для обеспечения других прав человека, поскольку нарушение этого права ставит под угрозу множество других прав. Право на неприкосновенность частной жизни гарантируется статьей 17 МПГПП. **Защита персональных данных является важной составляющей права на неприкосновенность частной жизни**, и это особенно актуально в контексте использования новых технологий в сфере управления границами и в борьбе с терроризмом[31]. Согласно изложенным в международных нормах **основополагающим принципам защиты данных**, персональные данные, проходящие автоматизированную обработку, должны: (а) собираться и обрабатываться на справедливой и законной основе; (б) храниться для конкретных и законных целей; (в) быть достаточными, относящимися к делу и не быть избыточными; (г) быть точными и, при необходимости, обновляться; и (д) храниться не дольше, чем это необходимо. **Конфиденциальные данные** (например, данные, раскрывающие этническое происхождение, политические взгляды, религиозные или другие убеждения, состояние здоровья или интимную жизнь, наличие судимости) требуют особенно высокого уровня защиты. Необходимо обеспечивать безопасность данных и их защиту от несанкционированного доступа. Помимо этого, лица имеют **право знать о хранении их персональных данных**, иметь к ним доступ и в случае необходимости добиваться их исправления[32]. Государства-участники обязались защищать право на неприкосновенность личной и семейной жизни, жилища, переписки и электронных сообщений, а также не допускать произвольного вмешательства в личную сферу индивидуума[33].

## Другие права

Применение новых технологий в обеспечении пограничного контроля может прямо и косвенно затронуть множество других прав, в том числе права лиц, особо нуждающихся в защите, – беженцев, соискателей убежища, детей и жертв торговли людьми[34]. В

30 См., например: Решение Совета министров ОБСЕ № 1/01, указ. соч., сноска 6; Решение Совета Министров ОБСЕ № 10/02 «Хартия ОБСЕ о предупреждении терроризма и борьбе с ним», Порто, 2002 г., https://www.osce.org/mc/42536.

31 См.: Комитет по правам человека, Замечание общего порядка № 16 – Статья 17 (право на личную жизнь), 8 апреля 1988 г., п. 10, https://www.refworld.org/docid/453883f922.html.

32 См. статьи 5-8 Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера (далее Конвенция 108), Страсбург, 28 января 1981 г., Ref.: ETS No.108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. При толковании обязательств государств по соблюдению статьи 17 МПГПП Комитет ООН по правам человека привел ряд соответствующих принципов защиты данных, см. там же: МПГПП, п. 10. В Европейском союзе дополнительно к статье 8 Хартии ЕС об основных прав также применяется более полный набор принципов, содержащихся в Общем регламенте защиты персональных данных ЕС, см.: Регламент ЕС 2016/679, 27 апреля 2016 г., https://eur-lex.europa.eu/eli/reg/2016/679/oj. Конвенция 108 была ратифицирована всеми 47 государствами-членами Совета Европы, то есть большинством государств-участников ОБСЕ, а также открыта для ратификации государствами, не являющимися членами Совета Европы.

33 Документ Московского совещания ОБСЕ 1991 года, указ. соч., сноска 16, п. 24; Документ Копенгагенского совещания 1990 года в части обязательств, связанных с доступом к информации и защитой частной жизни, указ. соч., сноска 16, п. 26.

34 Как указано в Конвенции о статусе беженцев 1951 года, Конвенции о правах ребенка (КПР), статье 8 МПГПП, запрещающей рабство и принудительный труд, и Конвенции Совета Европы о противодействии торговле людьми, призванной защитить жертв торговли людьми и обеспечить их права.

зависимости от того, как и какие решения принимаются в рамках обеспечения пограничного контроля, использование новых технологий может затронуть **права лиц на свободу и на справедливое судебное разбирательство**. Помимо этого, возможно нарушение **стандартов надлежащей правовой процедуры**[35], в том числе права быть выслушанным, права на рассмотрение ситуации справедливым, беспристрастным и независимым лицом, принимающим решения; права получать соответствующую информацию и знать причины принятия того или иного решения, а также права обжаловать это решение. Как будет показано ниже, как такое положение вещей может подвергать людей риску **применения к ним пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения** в результате нарушения **абсолютного запрета пыток**[36], а также приводить к неправомерному вмешательству в **свободу религии или убеждений**[37]. Помимо этого, косвенным образом могут быть затронуты и многие другие права, не связанные со сферой управления границами, – например, возможен демотивирующий эффект в отношении осуществления права на **свободу выражения мнения и свободу собраний и объединений**[38].

35 Статьи 9 и 14 МПГПП, а также статья 2(3), предусматривающая, как отмечалось выше, право на эффективное средство правовой защиты в случае нарушения прав, устанавливаемое компетентными судебными, административными или законодательными властями.

36 Статья 7 МПГПП.

37 Статья 18 МПГПП. Право иметь или принимать какую-либо религию или убеждения является абсолютным правом. Определенным ограничениям может подлежать только свобода их исповедовать.

38 Статьи 19, 21 и 22 МПГПП.

# Новые технологии, используемые в управлении границами, и их последствия для прав человека

Государства-участники ОБСЕ в той или степени внедряют новые технологии и системы сбора и обработки данных в деятельность по управлению границами. В данном разделе представлен краткий обзор того воздействия, которое подобные системы и технологии могут оказать на права человека.

## Система предварительной информации о пассажирах (API) и записи регистрации пассажиров (PNR)

Предварительная информация о пассажирах (Advance Passenger Information – API) – это биографическая информация, хранящаяся в паспорте пассажира[39]. Она собирается авиакомпаниями при регистрации пассажира перед вылетом, а затем передается пограничным службам и соответствующим ведомствам стран вылета, транзита и назначения при условии, что подобный обмен разрешен внутренним законодательством этих стран. Пограничные службы могут использовать данные API для выполнения автоматического поиска – например, в базах данных Интерпола. Обычно данные пассажиров одного рейса передаются властям все вместе, за одну операцию передачи данных. Однако при использовании интерактивной системы (iAPI), данные пассажира передаются от авиакомпании органам пограничного контроля стран вылета и стран назначения в индивидуальном порядке при регистрации пассажира перед вылетом. Это позволяет пограничным службам реагировать на случаи, касающиеся отдельных пассажиров[40].

Данные записей регистрации пассажиров (Passenger Name Records – PNR) формируются во время покупки или бронирования авиабилета. Они могут включать имя и фамилию пассажира, маршрут, информацию о билете, предпочтения в отношении питания на борту

39 Данные API обычно включают фамилию и имя пассажира, гражданство, дату рождения, пол, номер официального проездного документа, выдавшее его государство или организацию, тип проездного документа, срок его действия.

40 Более подробно о формате, технических стандартах и применении API см: World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO), Guidelines on Advance Passenger Information (API) [Всемирная таможенная организация (ВТамО), Международная ассоциация воздушного транспорта (ИАТА) и Международная организация гражданской авиации (ИКАО), Руководство по системе API], 2014 г., https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf; ICAO, Traveller Identification Programme (TRIP) Guide on Border Management Control [ИКАО, Руководство по пограничному контроля в рамках Программы идентификации пассажиров], 2018 г., https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf. См. также: Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (ИДКТК) / Контртеррористическое управление ООН (КТУ ООН), Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом (далее – Сборник ООН), 2018 г., https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf.

и выбора места в салоне, общую контактную информацию и способ оплаты, а также другие сведения[41]. В отличие от данных API, которые генерируются на основе официальных проездных документов, данные записей регистрации пассажиров вводятся пассажиром или туристическим агентством вручную и могут содержать неточности или ошибки. Авиакомпания хранит эти данные и отправляет их пограничным службам стран вылета и прилета перед отправлением рейса, кроме тех случаев, когда нормы национального законодательства или другие требования по защите данных запрещают такую передачу данных[42]. Государства используют данные записи регистрации пассажиров для проверки лиц в базах данных с информацией о лицах, «которые, как было установлено, являются террористами или которые подозреваются в террористической деятельности» или совершении других преступлений, и анализа данных с целью выявления закономерностей в перемещениях человека, которые могли бы указать на преступное поведение. Это также позволяет пограничным службам реагировать и работать с авиалиниями в отношении отдельных пассажиров до вылета рейса[43].

Сбор и автоматизированная обработка данных предварительной информации о пассажирах и записи регистрации пассажиров государственными органами (через авиакомпании) является существенным вмешательством в право на неприкосновенность частной жизни; чтобы не нарушить прав человека, это вмешательство должно опираться на четкую правовую базу, предусматривающую необходимые гарантии защиты прав; должно быть **необходимым** и **соразмерным** законной цели, а также **недискриминационным**.

## Сокращение объемов собираемых конфиденциальных данных, их хранение и защита

Система записи регистрации пассажиров (PNR) подразумевает сбор и обработку большего объема информации, чем в системе предварительной информации о пассажирах (API), и может быть сопряжена с бóльшим вмешательством и получением и обработкой более конфиденциальной персональной информации, в том числе информации о предстоящей поездке, номере мобильного телефона, данных о платеже и банковской карте. Сбор и передача данных PNR затрагивают право на неприкосновенность частной жизни каждого человека, совершающего международный перелет[44]. Помимо этого, передача данных PNR государственным органам в правоохранительных целях значительно отличается от коммерческих целей, для которых они собирались изначально. Это поднимает вопрос о необходимости ограничения целей их сбора и использования. С учетом объема и типа тех данных, к которым государства требуют доступа, а также последствий такого вмешательства для

41 Национальное законодательство стран и двусторонние соглашения определяют, какие именно данные PNR перевозчики обязаны предоставлять властям; при этом в Рекомендации ИКАО в отношении записей регистрации пассажиров (PNR) содержится список из 19 категорий таких данных. См.: WCO/IATA/ICAO API Contact Committee, Air Transport & Travel Industry Principles, Functional and Business Requirements PNRGOV [Контактный комитет ВТамО/ИАТА/ИКАО по API, Принципы авиаперевозок и туристической индустрии, Функциональные и бизнес-требования PNRGOV], 2013 г., p. 11, https://www.icao.int/Security/FAL/Documents/2-PNRGOV-Principles_13-1version_FIRST.pdf.

42 Сборник ООН, указ. соч., сноска 40, с. 59; C. Hanab, R. McGaurana and H. Nelen, API and PNR data in use for border control authorities [Использование данных API и PNR органами пограничного контроля], Security Journal, Vol. 30, 2016, p. 1050.

43 WCO/IATA/ICAO API Contact Committee, указ. соч., сноска 41.

44 Последствия для людей, совершающих международные поездки, будут еще более масштабными, если в будущем данные API/PNR станут использоваться и для других видов транспорта, что в настоящее время рассматривается Европейским союзом. См., например: Peter Teffer, EU may extend 'passenger name records' to rail and sea [ЕС может распространить PNR на железнодорожный и морской транспорт], EU Observer, Brussels, 6 August 2019, https://euobserver.com/justice/145602.

каждого пассажира высказываются опасения относительно того, что сбор и обработка данных PNR являются нецелевыми и чрезмерными, а также нарушают принцип, согласно которому любое вмешательство должно быть настолько минимальным, насколько это возможно[45].

В системе PNR содержится подробная информация, которая также может раскрывать конфиденциальные данные о человеке – при том, что защита этих данных при помощи соответствующих правовых гарантий признана особенно важной. К такой информации относятся данные, касающиеся этнического происхождения, политических взглядов, религии или убеждений, а также здоровья и интимной жизни лица, и их раскрытие может подвергнуть данное лица риску дискриминации или других нарушений прав человека[46]. Даже если законодательство запрещает обработку конфиденциальных данных PNR[47], остается риск того, что на основании этих данных могут быть сделаны те или иные выводы о человеке: например, предпочтения в еде могут указывать на его религиозные убеждения, а история поездок или данные попутчиков – на политические взгляды или сексуальную ориентацию[48]. Предварительный обмен данными API или PNR может привести к ограничению свободы передвижения, например, политических диссидентов, или же может помешать людям успешно просить убежища.

45 Критики называют эту ситуацию «массовой слежкой без оснований» и оспаривают ее в судах. См.: EDRI ICAO mandates worldwide government surveillance of air travellers [ИКАО разрешает правительствам вести глобальную слежку за авиапассажирами], 10 September 2020, https://edri.org/our-work/icao-mandates-worldwide-government-surveillance-of-air-travelers/. Директива ЕС об использовании данных регистрации пассажиров (EU PNR Directive) была оспорена в судах Германии и Австрии и в настоящее время находится на рассмотрении в Суде Европейского союза. См.: EDRi CJEU to decide on processing of passenger data under PNR Directive [Суд Европейского союза примет решение об обработке данных пассажиров в соответствии с Директивой об использовании данных регистрации пассажиров], 29 January 2020, https://edri.org/our-work/cjeu-to-decide-on-processing-of-passenger-data-under-PNR-directive/. Более подробную информацию о судебном процессе можно найти по адресу: https://noPNR.eu/en/home/.

46 Конвенция 108 Совета Европы, статья 6.

47 Как предусмотрено, например, в Директиве ЕС об использовании данных регистрации пассажиров. См.: Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [Директива Европейского Парламента и Совета 2016/681 от 27 апреля 2016 г. об использовании данных регистрации пассажиров (PNR) в целях предупреждения, выявления, расследования и уголовного преследования преступлений террористической направленности и тяжких преступлений], 4 May 2016, п. 37 и ст. 13, http://data.europa.eu/eli/dir/2016/681/oj.

48 Исследование, подготовленное для Консультативного комитета по Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера (Консультативный комитет по Конвенции 108): Douwe Korff, Passenger Name Records, data mining & data protection: the need for strong safeguards [Записи регистрации пассажиров, анализ данных и их защита: необходимость надежных гарантий защиты прав], Strasbourg, 15 June 2015, p. 79, https://rm.coe.int/16806a601b. См. также: Evelien Brouwer, The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom? [Система записи регистрации пассажиров в ЕС: передача данных или свободы?], CEPS Working Document No. 320/ September 2009, p. 25, http://aei.pitt.edu/11485/1/1903.pdf.

В регионе ОБСЕ не существует единого подхода в отношении того, как долго разрешается хранить данные API или PNR[49]. Консультативный комитет по Конвенции Совета Европы о защите частных лиц в отношении автоматизированной обработки данных личного характера (Консультативный комитет по Конвенции 108) подчеркнул, что сроки хранения данных должны быть четко определены и ограничены периодом, строго необходимым для предусмотренной цели их использования[50]. Хотя Комитет и отметил, что маскировка данных пассажира спустя определенное время после поездки может сократить некоторые риски, возникающие в случае более длительного хранения данных, он тем не менее напомнил, что и маскированные данные позволяют идентифицировать человека. Таким образом, подобные данные продолжают быть персональными данными и срок их хранения должен подлежать надлежащим ограничениям, с тем чтобы не допустить постоянной и всеобщей слежки[51]. В контексте пандемии COVID-19 сбор данных о состоянии здоровья в дополнение к другим уже собранным персональным данным может вызывать дополнительную обеспокоенность относительно соблюдения прав человека пассажиров, совершающих международные поездки воздушным, сухопутным и морским транспортом.

- С учетом серьезности вмешательства, сопряженного со сбором и обработкой данных API и особенно PNR, а также того факта, что это вмешательство может затронуть большое число людей, государствам необходимо **в ясной и убедительной форме продемонстрировать, что эти данные будут использоваться исключительно для того, что является строго необходимым** для достижения законной цели – такой, например, как предупреждение, выявление или расследование преступлений террористической направленности и других тяжких преступлений[52].

49 В Канаде данные API и PNR хранятся в течение трех с половиной лет. Если в отношении лица ведется расследование, его данные хранятся шесть лет. Более подробную информацию см. на странице Управления пограничных служб Канады: Canada Border Services Agency, Advance Passenger Information / Passenger Name Record Data [Система предварительной информации о пассажирах / Записи регистрации пассажиров], https://www.cbsa-asfc.gc.ca/security-securite/API_ipv-eng.html. В США данные записей регистрации пассажиров хранятся в течение 15 лет, последние 10 лет из этого срока они находятся в спящем режиме. Подробнее см.: How long is PNR information retained and what access restrictions apply? (U.S. Customs and Border Protection, Passenger Name Record (PNR)) [Как долго хранятся данные PNR и какие ограничения доступа применяются (в разделе «Записи регистрации пассажиров» на веб-сайте Службы таможенного и пограничного контроля Соединенных Штатов], https://www.cbp.gov/travel/clearing-cbp/passenger-name-record. Согласно Директиве ЕС об использовании данных регистрации пассажиров, данные должны быть деперсонализированы через полгода, а срок их хранения не может превышать пяти лет. Однако пятилетний период хранения данных был подвергнут критике как слишком длительный. Также был поднят вопрос о том, насколько деперсонализация данных может служить эффективной гарантией защиты права на неприкосновенность частной жизни – ввиду того, что при необходимости возможна их реперсонализация.

50 См.: Council of Europe Consultative Committee of Convention 108, Opinion on the Data protection implications of the processing of Passenger Name Records [Заключение Консультативного комитета Совета Европы по Конвенции 108 о последствиях обработки записей регистрации пассажиров (PNR) для защиты данных], Strasbourg, 19 August 2016, p. 8-9, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b051e.

51 Там же. Это соответствует решениям Суда Европейского союза в других областях, согласно которым «общее и неизбирательное хранение данных» в целях борьбы с преступностью или обеспечения национальной безопасности подлежит судебной и другой независимой проверке и обязано осуществляться только на временной основе, за исключением тех случаев, когда речь идет о реальной или прогнозируемой серьезной угрозе национальной безопасности. См.: CJEU, Press Release No 123/20 [Пресс-релиз №123/20 Суда Европейского союза], Luxembourg, 6 October 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf.

52 См.: Council of Europe Consultative Committee of Convention 108, указ. соч., сноска 50, с. 6.

- Для защиты лиц от чрезмерного сбора данных государствам необходимо **свести к минимуму объем собираемых данных и сроки их хранения**, а обработка данных должна быть строго **ограничена целью их использования**. Следует запретить сбор и обработку **конфиденциальных данных** в рамках системы записи регистрации пассажиров (PNR)[53].

## Точность и надежность данных и обмен данными между странами

Неверные или некорректно введенные данные в системе предварительной информации о пассажирах и в системе записи регистрации пассажиров могут отразиться на праве человека на свободу передвижения и других правах. Например, если имя человека введено с ошибкой в систему данных API, его могут не пустить на борт самолета или в страну назначения. В отличие от данных API, основанных на официальных проездных документах, данные PNR вводятся совершающим поездку лицом или туристическим агентом вручную. По этой причине точность данных PNR обычно не установлена. Но ошибки возможны и при вводе и обработке данных API. Расхождения в данных могут вызвать подозрение и привести к тому, что об отдельных лицах, совершающих поездки, будет безосновательно сообщено властям как о подозреваемых в причастности к преступлениям террористической направленности или другим тяжким преступлениям[54].

Данные систем API и PNR используются для выявления среди пассажиров лиц, подозреваемых в терроризме, путем сравнения их данных со специальными контрольными списками и базами данных (см. раздел о контрольных списках и системах предупреждения ниже). Неверная идентификация человека может привести к нарушению права на свободу передвижения. Данные PNR также используются для общего анализа данных о путешественнике, а также для оценки действий с точки зрения конкретных рисков в целях выявления вызывающих подозрение закономерностей. Это может привести к дискриминационному профилированию. Ситуация может усугубиться, если анализ данных проводится в целях прогнозирования рисков. В этом случае человек может быть отнесен к категории лиц, представляющих риск, не только на основании действий, которые он мог совершить, но и на основании предположений о том, что он может сделать в будущем[55]. Такой подход вызывает дополнительную обеспокоенность относительно возможных нарушений прав человека (см. ниже раздел о принятии решений на основе алгоритмов).

Отсутствие надлежащих стандартов и гарантий защиты прав мешает эффективному обмену информацией между государствами-участниками ОБСЕ. Обмен данными PNR между странами может считаться правомерным только при условии соблюдения стандартов конфиденциальности и защиты данных как в отправляющей, так и в принимающей стране[56]. Однако «как представляется, лишь несколько стран задумались о создании эффективных

53 Там же, с. 7 и 11.

54 Там же, с. 4.

55 Там же, с. 8. См. также выступление Специального докладчика ООН по борьбе с терроризмом на консультативных совещаниях, организованных БДИПЧ, 15 июня 2020 г., https://www.ohchr.org/Documents/Issues/Terrorism/SR/OSCEODIHRExpertMeetingAPI_PNRdata.pdf; Passenger Name Records, data mining & data protection: the need for strong safeguards, указ. соч., сноска 48.

56 См.: Council of Europe Consultative Committee of Convention 108, указ. соч., сноска 50, с. 9, где говорится, что «любая передача данных PNR государствам, не являющимся сторонами Конвенции 108, должна соответствовать условиям, гарантирующим надлежащую защиту субъектов данных в таких государствах».

механизмов, в том числе по возмещению ущерба»[57]. Обмен данными в такой ситуации не только подрывает стандарты защиты данных, но и может привести к нарушению других прав человека (например, к неправомерному ограничению свободы передвижения, дискриминации, незаконному задержанию или бесчеловечному и унижающему достоинство обращению или наказанию), если защита прав человека в принимающей стране является недостаточной. Это может подвергнуть риску не только само лицо, совершающее поездку, но и его семью и близких. Передача данных беженцев и соискателей убежища, в таком случае подвергает их особому риску, поскольку в результате им могут не позволить покинуть свою или другую страну.

- При разработке и внедрении систем API и PNR государствам необходимо обеспечить **действенные гарантии защиты прав человека**, с тем чтобы защитить людей от **необоснованного подозрения** в причастности к терроризму или другим преступлениям. Прежде всего государствам следует **избегать дискриминационного профилирования** на основе данных PNR.
- Перед заключением соглашений об обмене данными API и PNR государства обязаны убедиться в том, что в странах-партнерах, с которыми предполагается обмен такой информацией, в полном объеме существуют и соблюдаются надлежащие гарантии защиты данных, неприкосновенности частной жизни и других прав человека.

## Системы биометрических данных

Биометрические данные – это индивидуальные и обычно неизменные характеристики человека (такие, как отпечатки пальцев, черты лица, радужная оболочка глаз, голос, рисунок вен и ДНК). Эти данные могут быть отсканированы или получены иным способом для определения личности человека. После их сбора они преобразуются в числовые

57 OSCE Parliamentary Assembly, ad hoc Committee on Countering Terrorism, Strengthening Border Security and Information Sharing in the OSCE Region: A Parliamentary Oversight Exercise [Специальный комитет по противодействию терроризму Парламентской ассамблеи ОБСЕ, Повышение безопасности границ и обмен информацией в регионе ОБСЕ: осуществление парламентского надзора], October 2019, p. 11, https://www.oscepa.org/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/3905-strengthening-border-security-and-information-sharing-in-the-osce-region/file. Согласно существующим стандартами защиты данных (например, Директиве ЕС об использовании данных регистрации пассажиров, данные PNR могут передаваться третьим странам только в особых случаях при тщательном рассмотрении каждой отдельной ситуации. В 2017 г. Суд Европейского союза изучил планируемое соглашение между ЕС и Канадой об обмене данными PNR и постановил, что предлагаемый документ нарушает право на неприкосновенность и защиту частной жизни. Суд постановил, что положения соглашения, касающиеся хранения, использования и возможной последующей передачи данных государственным органам Канады, Европы или других стран являются неправомерным вмешательством в упомянутые права, поскольку «некоторые из положений соглашения не предусматривают ограничения этих действий принципом строгой необходимости», также не предусмотрена надлежащая защита конфиденциальных данных от их дальнейшей передачи. В итоге соглашение не было заключено. В 2018 г. были начаты новые переговоры, однако окончательный вариант документа пока не подготовлен. На настоящий момент подобные соглашения были заключены с Соединенными Штатами и Австралией. См.: CJEU, Press Release No 84/17 [Пресс-релиз Суда Европейского союза №84/17], Luxembourg, 26 July 2017, https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf; European Commission, Report “On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime” [Отчет Европейской комиссии «О пересмотре Директивы ЕС 2016/681 об использовании записей регистрации пассажиров (PNR) для предотвращения, выявления, расследования и уголовного преследования преступлений террористической направленности и тяжких преступлений»], Brussels, 24 July 2020, pp. 2-3, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf.

стандартизированные образцы, которые являются машиносчитываемыми и могут храниться и сравниваться с другими образцами биометрических данных[58].

Эти данные могут сравниваться с информацией, хранящейся в различных базах данных (например, в ИТ-системах, дающих разрешение на поездку), или с данными, собранными с помощью технологии LiveCapture – например, используемой в автоматизированных турникетах eGate[59]. Сравнение биометрических данных может принимать форму «верификации», то есть проверки принадлежности двух наборов биометрических данных одному и тому же лицу, или «идентификации» – выяснения факта совпадения биометрических данных проверяемого лица с записью, существующей в определенной базе данных. Система может выдавать ошибки в виде «ложного подтверждения» или «ложного отказа» при некорректном результате сопоставления двух образцов биометрических данных[60].

Помимо использования отпечатков пальцев и изображений лица для верификации и идентификации (это уже стало обычной практикой), государства все чаще экспериментируют с новыми биометрическими системами для обнаружения потенциальных угроз безопасности при пограничном контроле[61].

Использование биометрических систем вызывает серьезные вопросы относительно соблюдения прав человека, в том числе относительно последствий для права на неприкосновенность частной жизни – особенно если речь идет о лицах, находящихся в уязвимом положении (например, мигрантах, беженцах, соискателях убежища и детях). **Все системы, работающие с биометрическими данными, должны рассматриваться как технологии, сопряженным с высоким риском нарушения прав человека.** В связи с этим они должны проходить **тщательную и независимую оценку с точки зрения возможных последствий для прав человека**[62].

58 Обзор биометрических систем и сопоставления биометрических данных см., например, в: OSCE and Biometrics Institute, Outcome Document of the ID@ Borders & Future of Travel Conference 2019 [Итоговый документ конференции «Установление личности на границе и будущее путешествий», организованной ОБСЕ и Институтом биометрии], 14 May 2019, https://www.osce.org/secretariat/419552?download=true.

59 LiveCapture – это процесс сбора биометрического образца и преобразования его в шаблон биометрических данных. При этом полученные данные обычно не сохраняются в базе данных, а сразу же сравниваются с другими шаблонами биометрических данных (например, с тем, который хранится в чипе биометрического паспорта).

60 Сборник ООН, указ. соч., сноска 40, с. 14 и 16.

61 Например, распознавание лиц в движении, распознавание походки или даже предиктивный анализ биометрических данных (то есть помимо верификации или идентификации использования биометрии также для прогнозирования). См.: Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? [Использование биометрических данных для идентификации террористов: успешная практика или рискованное дело?], 22 July 2020, p. 9, https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf. О «технологических экспериментах», проводимых государственными и негосударственными субъектами при работе с беженцами, мигрантами и лицами без гражданства см. также в: Доклад Специального докладчика ООН по вопросу о современных формах расизма, указ. соч., сноска 18, пп. 38-39; Technological Testing Grounds, указ. соч., сноска 19.

62 Там же, с. 36 и 38. См. также: Доклад Специального докладчика ООН по вопросу о современных формах расизма, указ. соч., сноска 18.

## Принципы защиты данных

Биометрические данные относятся к персональным данным, и поэтому их сбор, хранение и обработка являются вмешательством в право на неприкосновенность частной жизни. Всеобщее и неизбирательное хранение биометрических данных было признано несовместимым с правом на неприкосновенность частной жизни[63]. Помимо этого, биометрические данные являются конфиденциальными[64] и могут также раскрыть другие конфиденциальные данные о человеке; в связи с этим необходимо обеспечить их особую защиту для недопущения дискриминации[65].

Сбор, хранение и обработка данных во всех случаях должны осуществляться на основании закона, быть необходимыми и соразмерными законной цели[66]. Однако во многих странах сбор и обработка биометрических данных, особенно в контексте деятельности по борьбе с терроризмом и другими преступлениями, все еще недостаточно регулируются национальной правовой базой[67].

Во многих государствах иностранцы, въезжающие в страну, обязаны на пограничном контроле предоставить отпечатки пальцев и изображения лица. Согласно международным стандартам в области защиты данных, любое лицо, чьи данные собираются, имеет право получить информацию о том, какие данные собираются, с какой целью, как долго они будут хранится и как они обрабатываются[68]. Таким образом, тайный сбор и хранение

63 Решение Европейского суда по правам человека (ЕСПЧ) по делу «С. и Марпер против Соединенного Королевства» (S and Marper v. The United Kingdom), заявления № 30562/04 и 30566/04, 4 декабря 2008 г., п. 125 (в отношении отпечатков пальцев, образцов клеток и профилей ДНК), https://rm.coe.int/168067d216.

64 См.: Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Совет Европы, Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 223)], Article 8. В Протоколе был расширен перечень категорий конфиденциальных данных, с тем чтобы в обновленной Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера (так называемой «Конвенции 108+») к ним были также отнесены биометрические данные. В ожидании вступления этого документа в силу государства могут объявить о применении измененных положений Конвенции 108+ в предварительном порядке. Текст обновленной Конвенции 108+: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Что касается законодательства ЕС, то в Общем регламенте ЕС по защите персональных данных (General Data Protection Regulation – GDPR) биометрические данные также отнесены к конфиденциальным (статья 9, п. 4). См. также: Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, указ. соч., сноска 61, с. 16; Privacy International, Responsible use and sharing of biometric data in counter-terrorism [Ответственное использование биометрических данных и обмен ими в рамках борьбы с терроризмом], July 2020, p. 8, https://privacyinternational.org/sites/default/files/2020-07/Responsible%20use%20and%20sharing%20of%20biometric%20data%20in%20counter-terrorism.pdf.

65 Изучение определенных биометрических данных также позволяет получить другую информацию, которая отнесена к «особой категории персональных данных». Например, с помощью образцов ДНК и средств распознавания голоса или радужной оболочки глаза можно получить информацию о состоянии здоровья, поле, возрасте и этнической принадлежности человека. См.: Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, указ. соч., сноска 61, с. 24.

66 Обзор прецедентного права см. в: ECtHR, Factsheet – Personal data protection [ЕСПЧ, Защита персональных данных (информационная справка)], October 2020, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

67 По данным организации Privacy International, примерно в двух третях государств мира действует всестороннее законодательство по вопросам защиты данных. Однако в большинстве случаев в нем не учтены биометрические данные. Помимо этого, в законодательстве многих стран предусмотрены исключения, связанные с обеспечением национальной безопасности или борьбой с терроризмом и преступностью. См.: Privacy International, указ. соч., сноска 64, с. 8.

68 Конвенция 108 Совета Европы, статья 8; обновленная Конвенция 108+, статьи 8 и 9. Общий регламент ЕС по защите персональных данных ЕС, статьи 13 и 14.

данных запрещены[69]. При сборе и обработке биометрических данных государства обязаны сообщать людях об их правах в качестве субъекта данных в понятной и доступной им форме – например, с помощью специальных памяток, наглядных материалов, а также информации, расположенной на видном месте там, где происходит сбор данных[70].

Суд Европейского союза постановил, что снятие и хранение отпечатков пальцев в чипе паспорта является юридически правомерным действием, так как не предполагает какой-либо обработки данных, выходящей за рамки того, что необходимо для достижения законной цели – защиты от мошеннического использования паспортов[71]. Однако это применимо только до тех пор, пока данные используются по назначению (для проверки подлинности паспорта и определения личности его владельца согласно применимому законодательству)[72]. В случае использования этих данных для других целей или если их обработка подразумевает их хранение в централизованных базах отпечатков пальцев, может иметь место неправомерное вмешательство в право на неприкосновенность частной жизни[73]. Такое возможно, как представляется, если эти данные, использованные для «идентификации» (то есть для проверки наличия в контрольных списках или системах предупреждения), или снятые на пограничном контроле (например, при помощи турникетов eGate с использованием технологии LiveCapture) отпечатки пальцев не удаляются сразу после того, как личность пассажира была установлена, а вместо этого сохраняются и хранятся в базах[74].

---

69 Возможны исключения из этого правила – например, для защиты национальной безопасности и охраны общественного порядка. См., например, положение об ограничениях в статье 9 Конвенции 108 Совета Европы и статье 11 обновленной Конвенции 108+. Тем не менее, в отношении системы PNR Консультативный комитет по Конвенции 108 заключил, что лица, которые не подозреваются в том, что они совершили или совершат преступление террористической направленности или другое тяжкое преступление, в полном объеме пользуются правом на информацию о собираемых данных, а также на доступ к этим данным, их исправление или удаление. См.: Council of Europe, Consultative Committee of Convention 108, указ. соч., сноска 50, с. 9. В странах ЕС при сборе и обработке персональных данных в правоохранительных целях применяется не Общий регламент ЕС по защите персональных данных, а Директива об обработке персональных данных правоохранительными органами.

70 Применительно к ЕС см., например: EU Fundamental Rights Agency (FRA), Under watchful eyes: biometrics, EU IT systems and fundamental rights [Агентство ЕС по основным правам, Под бдительным оком: биометрия, ИТ-системы ЕС и основные права], 2018, pp. 10 and 29-41, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf.

71 CJEU, Michael Schwarz v Stadt Bochum, Case C-291/12, Judgment of 17 October 2013 [Решение Суда Европейского союза от 17 октября 2013 г. по делу C-291/12 «Михаэль Шварц против города Бохум»], paras. 63-64, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0291&from=EN.

72 Там же, п. 56.

73 Там же, пп. 61 и 62; European Data Protection Supervisor (EDPS), EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents [Европейский надзорный орган по защите данных, Заключение EDPS 7/2018 о предложении по Регламенту ЕС о усилении надежности документов, удостоверяющих личность граждан ЕС, и других документов], 10 August 2018, para 42, https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf. Об опасениях, связанных с хранением генетических данных всех лиц, задержанных иммиграционными службами (например, в отношении того, что «будут храниться для целей раскрытия преступлений генетические данные людей, которым не были предъявлены обвинения в совершении какого-либо преступления»), см. Доклад Специального докладчика ООН по вопросу о современных формах расизма, указ. соч., сноска 18, п. 41.

74 Отпечатки пальцев и изображения лица граждан не входящих в ЕС стран, въезжающих в Шенгенскую зону на основании визы или электронного разрешения на въезд, будут храниться в электронной системе въезда/выезда (Electronic Entry/Exit System – EES). Ее запуск запланирован на 2021 г. См.: Statewatch, Automated Suspicion – The EU's New Travel Surveillance Initiatives [Автоматизированное подозрение – новые инициативы ЕС по отслеживанию путешественников], July 2020, p. 27, https://www.statewatch.org/media/1235/sw-automated-suspicion-full.pdf.

В связи с растущим развитием больших баз биометрических данных и повышающейся централизацией и операционной совместимостью различных видов баз данных[75] повышается риск расширения их первоначально определенной миссии, задач и функций[76]. Само по себе наличие биометрических данных или возможность легко их получить ведет к расширению их использования[77]. Это увеличивает риск изменения целей использования этих наборов данных, то есть использования их не для той цели, для которой они были собраны[78]. Помимо этого, рост взаимодействия между базами данных правоохранительных органов и иммиграционных служб способствует восприятию иммиграции как угрозы безопасности и создает риск стигматизации для лиц, находящихся в уязвимом положении, – мигрантов, беженцев, соискателей убежища, лиц без гражданства и лиц, имеющих нестабильный иммиграционный статус[79].

- Государства должны создать четкую **и основанную на правах человека правовую базу**[80], которая рассматривает **биометрические данные как конфиденциальные** по своей природе и строго регулирует использование биометрических технологий.
- Правовая база обязательно должна предусматривать ограничения на расширение использования биометрических данных и увеличение **централизации и операционной совместимости** систем, а также действенную **защиту от повторного использования** биометрических данных **в других целях** и от **тайного сбора** таких данных (право на информацию). Сбор и обработка биометрических данных должны быть **предусмотрены законодательством** и должны быть **строго необходимыми, соразмерными и недискриминационными**.
- Особое внимание следует уделять недопущению стигматизации групп, находящихся в особенно уязвимом положении, – беженцев, соискателей убежища и лиц с нестабильным иммиграционным статусом.

75 См.: Privacy International, указ. соч., сноска 64, с. 5. Например, ИДКТК ООН подчеркнул необходимость сопоставления биометрических данных, собранных в рамках пограничного и иммиграционного контроля и расследований, с более широким массивом данных, получаемых с помощью национальных и международных биометрических инструментов, в целях идентификации террористов и рекомендовал государствам обеспечить совместимость этих систем биометрических данных с другими национальными и международными базами биометрических данных. См.: ИДКТК ООН, Приложение 2018 года к Мадридским руководящим принципам 2015 года, UN Doc. S/2018/1177, декабрь 2018 г., п. 14 и Руководящий принцип 3, https://undocs.org/ru/S/2018/1177.

76 См.: Privacy International, указ. соч., сноска 64, с. 14 и 16; Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, указ. соч., сноска 61, с. 24 и 28; Доклад Специального докладчика ООН по вопросу о современных формах расизма, указ. соч., сноска 18, п. 35.

77 См.: Privacy International, указ. соч., сноска 64, с. 14.

78 Там же. Было задокументировано использование данных для других целей (для мониторинга беженцев, а затем при моделировании распространения COVID-19). См.: Crofton Black, Monitoring being pitched to fight Covid-19 was tested on refugees [Мониторинг, предлагаемый для борьбы с Covid-19, был опробован на беженцах], 28 April 2020, https://www.thebureauinvestigates.com/stories/2020-04-28/monitoring-being-pitched-to-fight-covid-19-was-first-tested-on-refugees.

79 См.: Privacy International, указ. соч., сноска 64, с. 14-15. В документе упоминается, например, Европейская база данных дактилоскопии просителей убежища (EURODAC), которая была создана в 2004 г. для обеспечения применения Дублинского регламента. Как было отмечено Европейским надзорным органом по защите данных (EDPS), с 2009 г. база данных также используется в правоохранительных целях, в частности для борьбы с терроризмом. Об участии частных компаний и стремлении к совместимости баз данных правоохранительных органов и иммиграционных служб см.: Доклад Рабочей группы ООН по вопросу об использовании наемников, указ. соч., сноска 18, п. 40; Statewatch and PICUM, Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status [Защита данных, правоприменение в области иммиграции и основные права: как правила ЕС об операционной совместимости систем повлияют на людей с неурегулированным статусом], 18 November 2019, https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf.

80 Как также признано ИДКТК ООН в Дополнении 2018 года к Мадридским руководящим принципам, указ. соч., сноска 75, Руководящий принцип 3, пункт (d).

## Биометрические данные, уязвимость и человеческое достоинство

Пересекая границы, беженцы, соискатели убежища и дети подвергаются особому риску нарушения их прав человека, связанному с использованием их биометрических данных. Помимо возможного нарушения их права на неприкосновенность частной жизни и защиту персональных данных, могут быть затронуты и абсолютные права: возникает риск высылки, применения жестокого, бесчеловечного и унижающего достоинство обращения и других посягательств на человеческое достоинство. Упомянутые риски могут возникнуть не только в связи с хранением или использованием биометрических данных, но и в связи с тем способом, которым эти данные собираются.

При подаче прошения о предоставлении убежища обычным требованием является снятие отпечатков пальцев и снимок лица[81]. Как отметил Специальный докладчик ООН по вопросу о современных формах расизма, «в связи со сбором данных в контекстах, характеризующихся очевидным неравенством возможностей, возникают вопросы информированного согласия и способности отказаться»[82]. Если снятие отпечатков пальцев является обязательным условием для подачи прошения об убежище (как, например, в ЕС), отказ предоставить их способен на практике привести к тому, что человек не сможет добиваться убежища[83]. В некоторых странах отказ также может привести к помещению под стражу или другим принудительным мерам для целей снятия отпечатков пальцев[84]. В ряде стран были задокументированы сообщения о случаях применения силы, и эти случаи, по утверждениям, представляли собой жестокое, бесчеловечное или унижающее достоинство обращение[85].

Спасаясь от преследования, беженцы и соискатели убежища уже находятся в ситуации повышенного стресса, особенно если они добираются по опасным маршрутам или, как это часто бывает, попадают во враждебно настроенную среду. Эта ситуация еще больше усугубляется, если человека принуждают предоставить биометрические данные и если ему не объясняют, почему необходимо снятие отпечатков пальцев, где информация будет храниться, как можно получить к ней доступ, внести в нее исправления или добиться ее удаления[86]. Есть риск, что дети и представители других уязвимых групп, в том числе жертвы торговли людьми и лица, пережившие гендерно-обусловленное насилие, не смогут дать свободное и информированное согласие на сбор их данных. Люди также могут отказаться от снятия отпечатков пальцев, если будут опасаться, что их данные могут быть переданы стране происхождения[87]. Управление Верховного комиссара ООН по делам беженцев подчеркивает опасность передачи данных лица, ищущего убежища, его стране происхождения, так как человек может быть подвергнут репрессиям после возвращения в страну или его родственники, оставшиеся в стране, могут столкнуться с преследованиями[88]. Хотя вышесказанное применимо ко всем видам данных, биометрические данные, как представляется, связаны с повышенными рисками, так как они могут в более значительной

81 Например, в ЕС; см.: Under watchful eyes: biometrics, указ. соч., сноска 70.

82 Доклад Специального докладчика ООН по вопросу о современных формах расизма, указ. соч., сноска 18, п. 34.

83 См.: Under watchful eyes: biometrics, указ. соч., сноска 70, с. 51.

84 Там же, с. 53 и 55-56.

85 Там же, с. 53-54.

86 Примеры см. в: Technological Testing Grounds, указ. соч, сноска 19, с. 12-14.

87 См.: Under watchful eyes: biometrics, указ. соч., сноска 70, с. 10, 49 и 77-79.

88 Управление Верховного комиссара ООН по делам беженцев (УВКБ ООН), Решение проблем безопасности без отрицательных последствий для защиты беженцев – точка зрения УВКБ ООН, 17 декабря 2015 г., пункт 17, https://www.refworld.org/docid/5672aed34.html; Under watchful eyes, указ. соч., сноска 70, с. 77-78.

степени использоваться для дальнейшей изоляции, дискриминации и слежки за человеком в стране происхождения[89].

Рост использования биометрических данных также привел к тому, что тело человека становится формой идентификации личности. Это может угрожать физической неприкосновенности людей. Например, человек может прибегнуть к членовредительству, если он боится рисков, связанных с идентификацией его личности[90]. Риск кражи персональных данных также может создать долгосрочные проблемы, поскольку биометрические данные в случае их похищения невозможно заменить.

Пандемия COVID-19 и связанные с ней расширение сбора данных и стремление к реагированию на кризис с использованием новых технологий вызывают обеспокоенность, поскольку это может иметь далеко идущие последствия для прав человека и гражданских свобод. Данные, собираемые для целей сдерживания пандемии COVID-19, могут использоваться для дальнейшего ущемления прав людей, особенно если собранные данные используются вместе с биометрическими данными и в ситуациях, содержащих высокий риск нарушения прав человека – например, в отношении уязвимых групп лиц, находящихся в процессе транзита[91].

- При сборе и обработке биометрических данных (например, отпечатков пальцев), государства обязаны обеспечить, чтобы принцип **свободного и информированного согласия**, а также **право на информацию** были гарантированы на практике, особенно **лицам, находящимся в ситуации повышенной уязвимости** (включая мигрантов и соискателей убежища).
- Сбор и использование биометрических данных ни при каких обстоятельствах не должны приводить к ограничению абсолютных прав. Необходимо обеспечить полное уважение **человеческого достоинства, соблюдение запрета жестокого, бесчеловечного или унижающего достоинство обращения**, а также **принципа невысылки**.
- Государства должны следовать общепринятому принципу **не передавать биометрические данные соискателей убежища стране происхождения**[92].

## Вопрос надежности и дискриминационной предвзятости биометрических систем

Часто считается, что биометрические данные человека неизменны, но это не так. Они могут меняться с течением времени в зависимости от того, как меняется тело человека. Например, качество отпечатков пальцев может снизиться с возрастом, при кожных заболеваниях или в результате выполнения тяжелого физического труда. Про системы распознавания лиц,

89 См.: например: The Institute of Statelessness and Inclusion, Locked in and locked out: The impact of digital identity systems on Rohingya populations [Ни выйти, ни зайти: последствия цифровых систем идентификации для рохинджа], November 2020, p. 3, https://files.institutesi.org/Locked_In_Locked_Out_The_Rohingya_Briefing_Paper.pdf.

90 См.: Under watchful eyes: biometrics, указ. соч., сноска 70, с. 50 и 56; Technological Testing Grounds, указ. соч., сноска 19, с. 12-14.https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf

91 Technological Testing Grounds указ. соч., сноска 19, с. 21-22.

92 УВКБ ООН, Решение проблем безопасности без отрицательных последствий для защиты беженцев, указ. соч., сноска 88, п. 17.

использующие биометрические данные, говорят, что они неизбежно несут в себе возможность ошибки, поскольку в их основе лежит статистическая вероятность[93].

Степень погрешности у алгоритмов биометрического распознавания лиц в значительной степени зависит от пола, цвета кожи и возраста человека. В ходе исследований было выявлено, что существующим алгоритмам сложнее распознавать женские лица и они выдают больше ложных отказов и ложных подтверждений для женщин. Помимо этого, они лучше распознают лица со светлым тоном кожи. Показатель ошибок был выше всего для смуглых женских лиц[94]. Это может привести, например, к интерсекциональной дискриминации чернокожих женщин, поскольку результаты анализа биометрических данных именно этой группы содержат самый большой процент ошибок[95].

Полученные от биометрических систем некорректные результаты, связанные с полом, цветом кожи, этнической принадлежностью или другими защищаемыми характеристиками, могут привести к дискриминации и другим серьезным последствиям для лиц, совершающих поездки. Как ложноотрицательные, так и ложноположительные результаты (например, при распознавании лица при проходе через автоматизированные турникеты eGate или при сканировании отпечатков пальцев) могут стать причиной стигматизации, укрепить негативные стереотипы и привести к неправомерному определению человека как подозрительного лица. Из-за этого затронутые лица могут столкнуться с более подробными проверками. Могут возникнуть и другие сложности при пересечении границы, вплоть до невозможности совершить поездку[96]. В ходе последующих проверок непосредственно персоналом ошибки автоматизированной системы могут быть устранены, однако тенденция больше доверять технологиям, чем другим источникам информации и человеческому суждению (так называемый «выбор в пользу автоматизированных решений») может помешать этому и укрепить дискриминационное отношение[97].

---

93 Sandra Azria and Frédéric Wickert, Facial Recognition: Current Situation and Challenges [Распознавание лиц: текущая ситуация и вызовы], Strasbourg, 13 November 2019, pp. 15-16, https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1 (исследование, подготовленное для Консультативного комитета по Конвенции 108).

94 Joy Buolamwini and Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification [Гендерные оттенки: интерсекциональные расхождения в точности коммерческих инструментов классификации пола], Proceedings of Machine Learning Research 81:1–15, 2018 Conference on Fairness, Accountability, and Transparency, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. См. также: Patrick Grother, Mei Ngan and Kayee Hanaoka for the National Institute of Standards and Technology (NIST), U.S. Department of Commerce NISTIR 8280 Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects [Министерство торговли Соединенных Штатов – Испытание алгоритмов распознавания лиц, часть 3: демографические результаты] декабрь 2019 г., https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

95 В прошлом также было выявлено, что алгоритмы распознавания лиц лучше всего распознают лица, наиболее распространенные в том регионе, где разрабатывалась система. Например, алгоритмы, разработанные в Восточной Азии, лучше всего распознавали азиатский тип внешности, а алгоритмы, разработанные в Западном полушарии лучше всего справлялись с лицами со светлым тоном кожи. Вместе с тем, более поздние исследования показывают, что обучение таких алгоритмов на более разнообразных массивах данных может повысить их точность и снизить количество ошибок. См.: Patrick Grother, Mei Ngan and Kayee Hanaoka, указ. соч., сноска 94. Более подробную общую информацию о связи между предвзятостью искусственного интеллекта (machine bias) и системным расизмом см. также в: Ruha Benjamin, Race After Technology: Abolitionist Tools for the New Jim Code [Раса в эпоху технологий: инструменты аболиционизма и новое неравенство], 2019.

96 Некорректная обработка биометрических данных соискателей убежища может привести к тому, что они не смогут въехать в страну, предоставляющую убежище (в случае ЕС – к неверному применению Дублинского регламента), а также к риску неправомерного задержания. В случае нарушения принципа невысылки может иметь место риск применения пыток и других видов жестокого обращения, а также нарушения других прав человека.

97 Подробнее о выборе в пользу автоматизированных решений см. в следующем разделе и в: Petra Molnar, Technology on the margins: AI and global migration management from a human rights perspective [Технологии за рамками: искусственный интеллект и управление глобальной миграцией с точки зрения прав человека], 2019, Cambridge Journal of International Law, Vol. 8, No.2, p. 324.

Также наблюдается растущая тенденция к разработке средств прогнозирования на основе биометрических данных – например, автоматизированного распознавания лжи или эмоций человека, сканирования мимики и анализа голоса. Эта тенденция в значительной степени увеличивает риски для прав человека[98]. Подобные технологии недостаточно надежны и точны. При этом помимо проблемы возможных ошибок системы здесь возникают и другие серьезные опасения. Например, использование биометрических данных для анализа эмоционального или психологического состояния человека либо для определения вероятности совершения им преступления ущемляет его право на свободу мысли и право на психическую неприкосновенность[99].

- Государствам следует пересмотреть использование ими биометрических технологий (таких, как системы распознавания лиц), способных **усилить предвзятость и привести к дискриминации.**
- Также следует отказаться от внедрения и использования **непроверенных или неточных технологических средств**, особенно в таких областях, как пограничный контроль или управление миграцией, которые сами по себе сопряжены с повышенными рисками нарушения прав человека.
- Если же после тщательной оценки возможного воздействия было принято решение о внедрении и использовании биометрической системы, государству необходимо принять надлежащие меры для **снижения потенциальных рисков для прав человека**. Необходимо, помимо прочего, противодействовать **«выбору в пользу автоматизированных решений»**, а также обеспечить процессуальные гарантии защиты прав и соответствующее обучение сотрудников.

98 См.: Доклад Специального докладчика ООН по вопросу о современных формах расизма, указ. соч., сноска 18, п. 39 (о пробном внедрении системы iBorderCtrl на границах в некоторых государствах-членах ЕС). См. также: Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, указ. соч., сноска 61, с. 25;

99 Гарантируемые статьей 18 МПГПП и статьей 3 Хартии ЕС об основных прав, соответственно. Об опасениях насчет неточности таких систем см., например: Ryan Gallagher and Ludovica Jona, We tested Europe's new lie detector for travelers — and immediately triggered a false positive [Мы проверили новый европейский детектор лжи для путешественников и сразу же получили ложноположительный результат], The Intercept, 26 July 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/; Samuel Stolton, MEP: Public has a 'right to know' about Commission's lie detector tech [Депутат Европарламента: «Общественность имеет право знать о технологии распознавании лжи, используемой Комиссией»], EURACTIV, 1 April 2020, https://www.euractiv.com/section/digital/news/mep-public-has-a-right-to-know-about-commissions-lie-detector-tech/. Об опасениях по поводу использования технологий предиктивного анализа в работе правоохранительных органов см., например: PACE, Resolution 2342 "Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems" [ПАСЕ, Резолюция 2342 «Правосудие по алгоритму – роль искусственного интеллекта в системе охраны правопорядка и уголовного правосудия»], 22 October 2020, https://pace.coe.int/en/files/28805/htm.

## Принятие решений на основе алгоритмов: системы выдачи виз и разрешений на поездки и системы проверки по базам данных

Алгоритмы – это системы, которые запрограммированы в соответствии с определенным набором правил и должны выполнять статистический анализ данных, составлять прогнозы и рекомендации или служить основой для принятия решений[100]. Автоматизированные системы принятия решений на основе алгоритмов разрабатываются людьми и могут быть обучены со временем автоматически меняться и адаптироваться, реагируя на различные наборы данных. На практике это означает, что алгоритмы могут научиться назначать определенные свойства тем или иным конкретным характеристикам[101]. Например, алгоритм на основе определенного массива наборов данных может научиться определять, что все лица выше определенного роста являются мужчинами, чтобы затем автоматически определять всех таких людей как мужчин. Подобное машинное обучение и внесение изменений в систему может происходить с различной степенью автономности или контроля[102].

Применительно к пограничному контролю рекомендации или прогнозы, сделанные алгоритмами, иногда используются для принятия решения о том, можно ли разрешить тому или иному лицу совершить поездку или въехать в страну[103], необходимы ли дополнительные проверки в отношении конкретного человека и представляет ли этот человек угрозу. Если речь идет о системах, обрабатывающих запросы на получение визы или выдающих разрешение на поездку, проводится анализ персональных данных путешественника, помогающий принять решение о выдаче или отказе в выдаче визы/разрешения[104]. Аналогичным образом, при проведении проверок и оценки рисков с точки зрения терроризма, а также для других целей службами пограничного контроля используются алгоритмы анализа персональных данных, предназначенные для обнаружения индикаторов предполагаемой угрозы[105]. В связи с этим

---

100 FRA, #BigData: Discrimination in data-supported decision making [Агентство ЕС по основным правам, #BigData: дискриминация при принятии решений на основе данных], 2018, pp. 3-4, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf; о различных значениях и определении термина «алгоритм» в специализированных сферах (математика и информатика) и его широком использовании в общественном дискурсе см.: Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter and Luciano Floridi, The ethics of algorithms: Mapping the debate [Этика алгоритмов: систематизация споров], Big Data & Society, December 2016, pp. 2-4, https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679.

101 Там же, The ethics of algorithms, с. 2-4.

102 О различных значениях понятий «машинное обучение» и «искусственный интеллект» и разнице между контролируемым и неконтролируемым обучением см.: там же, с. 3; Privacy International, Submission on Draft General Recommendation No. 36: Preventing and Combating Racial Profiling [Предложение к проекту Общей рекомендации № 36 о предупреждении расового профилирования и борьбы с ним], June 2019, pp. 2-4, https://privacyinternational.org/sites/default/files/2019-07/PI%20submission_CERD%20General%20Comment%2036_June%202019.pdf; Комиссар Совета Европы по правам человека, Раскрытие искусственного интеллекта: 10 шагов для защиты прав человека, 2019, с. 24, https://rm.coe.int/-10-/16809a42e4. В документах Privacy International и Комиссара Совета Европы по правам человека есть полезный глоссарий соответствующих терминов и понятий.

103 Все больше стран используют электронные системы подачи заявок на получение визы. Некоторые страны используют электронные системы выдачи разрешений на поездки для тех стран, с которыми установлен безвизовый режим. Среди таких систем – ESTA в Соединенных Штатах и eTA в Канаде. ЕС создает аналогичную ИТ-систему (ETIAS – European Travel Information and Authorisation System), запуск которой запланирован на 2022 год.

104 Эти данные могут включать, помимо прочего, персональную информацию (фамилию и имя, дату и место рождения, пол, профессию), различные вопросы (цель поездки, ее продолжительность, возможная история судимости), биометрические данные и информацию о спутниках. Для сравнения требований в отношении предоставления данных в различных странах см.: веб-сайт Tactical Tech, раздел Applying for a Visa, https://ourdata-ourselves.tacticaltech.org/posts/40-applying-for-a-visa.

105 Это может касаться и данных PNR, которые анализируются специализированными отделами, работающими с данными пассажиров в целях обнаружения лиц, намеревающихся совершить «поездку с террористической целью», еще до их появления на пограничном контроле.

алгоритмы могут оказывать огромное воздействие на соблюдение индивидуальных прав в контексте управления границами.

## Предвзятость алгоритмов и выбор в пользу автоматизированных решений

В контексте пограничного контроля алгоритмы часто воспринимаются как нейтральное техническое решение, которое помогает проверять пассажиров и служит для последующего принятия решений в их отношении (например, о допуске в страну) на основе корреляций и закономерностей, выявленных в объективных данных. Однако технологии не являются нейтральными, поскольку существует риск внесения предвзятости в алгоритм из-за его обучения на предвзятых наборах данных и это будет воспроизведено при дальнейшем анализе данных алгоритмом, а затем повлияет на окончательное решение[106].

Консультативный комитет по Конвенции 108 подчеркнул, что правильность индивидуальных результатов автоматизированной оценки должна тщательно проверяться человеком без применения средств автоматизации, с тем чтобы не допустить неправильной идентификации людей, совершающих поездки, как подозрительных лиц или лиц, представляющих угрозу с точки зрения терроризма[107]. Выполняющие такую проверку сотрудники должны пройти надлежащую подготовку и быть соответствующим образом проинформированы о возможной предвзятости системы, а также о последствиях ошибочной идентификации рисков для затронутых лиц[108]. При этом проблема «выбора в пользу автоматизированных решений», или склонности лиц, принимающих решения, полагать, что заключения, выдаваемые автоматизированными техническими средствами, являются более объективными и нейтральными, чем решения людей, создает дополнительные проблемы, которые сложно выявить, а тем более устранить.

Алгоритмы также могут самостоятельно создавать усиливающуюся внутреннюю предвзятость. Динамичное развитие алгоритмов через (автономное) машинное обучение делает отслеживание предвзятости системы и ее коррекцию все более сложной или даже невозможной задачей. Если алгоритм самообучается на базе «тренировочных наборов данных», возникает «серьезный риск непроизвольного воспроизведения имеющихся в данных стереотипных установок, и это может усилить социальное неравенство и стигматизацию определенных групп»[109]. Например, если алгоритм выдачи виз работает на наборе данных, содержащих предвзятость в отношении лиц с гражданством определенных стран, то он «выучит», что гражданам именно этих стран реже выдаются визы, и в результате это усилии изначально существующую предвзятость системы[110]. Подобную усиливающуюся

106 #BigData: Discrimination in data-supported decision making, 2018, указ. соч., сноска 100, с. 5.

107 См.: Заключение Консультативного комитета Совета Европы по Конвенции 108, указ. соч., сноска 50, с. 8. Это также предусмотрено Директивой ЕС об использовании записей регистрации пассажиров (PNR), указ. соч., сноска 57.

108 Помимо этого, затронутым лицам должны быть обеспечен доступ к эффективным средствам правовой защиты, а также право на информацию о сборе данных, исправление своих данных и т. д. См.: Заключение Консультативного комитета Совета Европы по Конвенции 108, указ. соч., сноска 50, с. 9-10. Это также подчеркнуто ИДКТК ООН в Приложении 2018 года к Мадридским руководящим принципам 2015 года, указ. соч., сноска 75, с. 6-7.

109 FRA, Preventing unlawful profiling today and in the future: a guide [Агентство ЕС по основным правам, Предупреждение незаконного профилирования сейчас и в будущем: руководство], 2018, p. 110, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf.

110 См., например: Home Office drops 'racist' algorithm from visa decisions [Министерство внутренних дел перестало использовать «расистский» алгоритм при принятии решений о выдаче виз], BBC News, 4 August 2020, https://www.bbc.co.uk/news/technology-53650758; Henry McDonald, AI system for granting UK visas is biased, rights groups claim [Система ИИ для выдачи виз в Соединенное Королевство необъективна, утверждают правозащитные группы], The Guardian, 29 октября 2019 г., https://www.theguardian.com/uk-news/2019/oct/29/ai-system-for-granting-uk-visas-is-biased-rights-groups-claim.

предвзятость алгоритма сложно устранить, так как не всегда понятно, почему он принимает то или иное решение. Если это приводит к произвольному отказу в выдаче визы или разрешения на поездку, такая ситуация не только дискриминирует человека, но и может повлиять на его свободу передвижения и другие права, в том числе право на семейную жизнь.

- Алгоритмические/автоматизированные системы принятия решений всегда **должны контролироваться людьми и быть прозрачными**[111]. Результат оценки, ставящий человека в невыгодное положение, должен быть тщательно изучен и проверен без использования средств автоматизации.
- Алгоритмические системы перед их запуском, а также на регулярной основе после запуска должны проходить **обязательную проверку в целях выявления возможного дискриминационного эффекта**. Помимо этого, необходимо оценить, как выбор наборов данных, их обработка, методы принятия решений и получаемые результаты влияют на права человека.
- Государства должны возложить обязательства по проведению такой оценки на **частные компании, а также на государственные органы**, участвующие в разработке и эксплуатации таких систем. Оценка должна включать **независимую проверку воздействия на права человека** и быть **прозрачной и основанной на широком участие** различных сторон, в том числе национальных институтов[112], НПО, отражающих многообразие общества, а также тех групп и общин, права которых затронуты в наибольшей степени.
- Сотрудники пограничной службы и другие лица, участвующие в разработке и эксплуатации алгоритмических систем, должны пройти соответствующую **подготовку по вопросам прав человека и борьбы с дискриминацией**. Пользователи должны быть обучены видеть риски и ограничения систем и распознавать как **личные предубеждения, так и склонность делать «выбор в пользу автоматизированных решений»**.

## Оценка рисков и дискриминационное профилирование

Риск предвзятости, неизбежно заложенный в алгоритмах и тех данных, на которых обучаются алгоритмы, может привести к дискриминирующему профилированию[113]. Распределение лиц по категориям риска на основании предположений о конкретных группах или воспринимаемых моделях поведения, с которыми эти группы предположительно связаны, может привести к стигматизации людей в результате безосновательного отождествления их с конкретным риском, а также может укрепить стереотипы в отношении целых групп или общин[114].

111 Комиссар Совета Европы по правам человека, Раскрытие искусственного интеллекта: 10 шагов для защиты прав человека, указ. соч., сноска 102, с. 13.

112 Например, национальные правозащитные учреждения, органы по защите информации и по вопросам равенства.

113 Для целей настоящего документа профилирование определяется как составление предположений о поведении человека на основе присущих ему характеристик и/или его предыдущих действий. См.: FRA, Towards More Effective Policing – Understanding and Preventing Discriminatory Ethnic Profiling: A Guide [На пути к более эффективной деятельности полиции – понимание проблемы дискриминационного этнического профилирования и его предупреждение: руководство], 2010, pp. 9-10, https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf.

114 Там же. См. также: Council of Europe Commissioner for Human Rights, Ethnic profiling: a persisting practice in Europe [Комиссар Совета Европы по правам человека, Этническое профилирование: сохраняющаяся практика в Европе], 9 May 2019, https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe; Комитет ООН по ликвидации расовой дискриминации (КЛРД), Общая рекомендация № 36, указ. соч., сноска 29.

Включение определенных характеристик людей в «модель риска» может представлять собой дискриминационное профилирование, особенно если речь идет о защищаемых признаках – этнической принадлежности, цвете кожи, поле, языке, религии, политических или других убеждениях, национальном или социальном происхождении или другом статусе. Дискриминирующее профилирование является незаконным.

Совокупность личной информации о человеке, которая используется в системах выдачи виз и разрешений на поездки, также может раскрыть защищаемые характеристики. Например, из информации об уровне образования и текущем месте работы (данные, запрашиваемые новой системой ETIAS – European Travel Information and Authorisation System), можно сделать вывод о вероисповедании человека – если он сообщил, что получил религиозное образование и/или работает в религиозном учреждении[115]. Если алгоритмы используют подобные выводы при оценке рисков или проверках и в результате могут определить конкретного человека как потенциальную угрозу, это может являться дискриминационным профилированием и может привести к ограничению свободы передвижения и других прав этого лица.

Присваивание лицам определенной категории и уровня риска на основании того или иного сочетания характеристик может привести к неверным выводам. Например, пассажиры из определенной страны или региона, занимающиеся низкоквалифицированным трудом, могут быть восприняты системой как лица, вписывающиеся в модель незаконной миграции, хотя характер их поездки и личные характеристики могут быть типичными для их страны или региона. Даже если присвоение категории риска не основано на защищаемых признаках, может иметь место непреднамеренная дискриминация – в тех случаях, когда та или иная группа оказывается непропорционально затронутой на фоне всего остального населения или когда она затронута косвенно[116]. Люди, подвергшиеся уголовному преследованию за свою сексуальную ориентацию в стране происхождения, столкнутся, скорее всего, с дополнительной дискриминацией во время поездки, если алгоритм не будет обучен определять вид «совершенных в прошлом уголовных правонарушений»[117]. Использование алгоритмов для выявления таких характеристик, как сексуальная ориентация, является совершенно недопустимым.

Как правило, отождествление человека с определенным профилем риска может иметь серьезные последствия для прав человека этого лица – ему могут запретить въезд или выезд, его могут дискриминационным образом подвергнуть дополнительным проверкам и даже задержать при попытке пересечь границу. Если же затрагиваются права соискателей убежища, то в результате такой практики они могут подвергнуться риску применения в их отношении пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения или же в опасности может оказаться их жизнь (в случае их возвращения в страну происхождения или получения отказа на выезд из нее)[118].

---

115 FRA, The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS): Opinion of the European Union Agency for Fundamental Rights [Агентство ЕС по основным правам, Влияние на основные права предлагаемого Регламента о Европейской системе информации о поездках и выдачи разрешений на поездки (ETIAS): мнение Агентства ЕС по основным правам], Vienna, 30 June 2017, p. 19, https://fra.europa.eu/sites/default/files/fra_uploads/fra-opinion-02-2017-etias.pdf.

116 Например, если среди людей с низким уровнем образования в конкретной стране слишком много представителей определенных этнических групп и низкий образовательный уровень определяется системой как характеристика, указывающая на высокий риск нелегальной миграции. Там же, с. 28-29.

117 FRA, Preventing unlawful profiling today and in the future: a guide, указ. соч., сноска 109, с. 117-118; FRA Opinion on the ETIAS Regulation, указ. соч., сноска 115, с. 21.

118 Petra Molnar and Lex Gill, Bots at the Gate - A Human Rights Analysis of Automated Decision-making in Canada's immigration and refugee system [Боты у ворот – анализ влияния на права человека автоматизированного принятия решений в системе управления иммиграцией и приема беженцев Канады], 2018, https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.

- Государства **обязаны не допускать дискриминационного профилирования** при использовании алгоритмов для анализа данных путешественников в целях проверки и оценки рисков[119].
- Для действенного предупреждения дискриминации и дискриминационного профилирования государствам необходимо создать **четкие и основанные на правах человека правовые рамки**, обеспечивающие строгое регулирование разработки и эксплуатации инструментов оценки рисков на основе алгоритмов, а также **использования полученных результатов или возможного обмена ими**.
- В нормативно-правовой базе необходимо предусмотреть **гарантии защиты прав человека** для защиты субъектов данных, в том числе для обеспечения **права на информацию** (о том, как и с какой целью собираются данные), а также **эффективные средства правовой защиты**, дающие возможность оспаривать сбор и использование данных и любые решения, принятые на основе данных, полученных с помощью указанных систем.
- Эксплуатация алгоритмических систем должна подлежать **эффективному и независимому надзору** на всех ее этапах.

119 Это также указано в Резолюции 2396 (2017) Совета Безопасности ООН, пункт 4,а также в: ИДКТК ООН, Приложение 2018 года к Мадридским руководящим принципам 2015 года, указ. соч., сноска 75, Руководящий принцип 1, пункт (d).

## Контрольные списки и системы предупреждения

На сегодняшний день существует множество различных информационных систем, используемых для различных целей в контексте обеспечения безопасности границ[120]. Предусмотренные Резолюцией 2396 (2017) Совета Безопасности ООН контрольные списки и другие базы данных лиц, «которые, как было установлено, являются террористами или которые подозреваются в террористической деятельности», представляют собой системы предупреждения для правоохранительных органов. Они используются «для проверки пассажиров и проведения оценки рисков и расследований»[121].

Доступ к контрольным спискам и к базам данных правоохранительных органов предоставляется внутри страны соответствующим правоохранительным органам и органам пограничного контроля; при этом Резолюция 2396 также призывает государства обмениваться информацией на международном уровне через двусторонние и многосторонние механизмы. Такие многосторонние механизмы могут включать в себя региональные и международные системы предупреждения – например, системы, управляемые Интерполом. На основе информации, предоставленной национальными органами полиции, Интерпол выпускает различные виды циркуляров, касающиеся разыскиваемых преступников и других лиц[122]. В контексте обеспечения безопасности границ данные о поездках (данные систем API и PNR и информация из систем выдачи виз и разрешений на поездки) проверяются с использованием соответствующих национальных и международных контрольных списков или баз данных правоохранительных служб в целях обнаружения лиц, находящихся в розыске, подозреваемых в совершении преступлений или рассматриваемых как представляющих террористическую угрозу или другую угрозу, связанную с преступностью[123].

120 Обзор различных ИТ-систем в ЕС для обмена информацией, касающейся безопасности, миграции и пограничному контролю, см. в: EU Information Systems – Security and Border [Информационные системы ЕС – безопасность и границы], European Commission, February 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190205_security-union-eu-information-systems_en.pdf.

121 Резолюция 2396 (2017), принятая Советом Безопасности 21 декабря 2017 г., пп. 13 и 15, https://undocs.org/en/S/RES/2396(2017).

122 Интерпол выпускает так называемые «красные уведомления» (в основном для ареста разыскиваемых лиц) и «синие уведомления» (для сбора дополнительной информации о личности человека, его местонахождении или действиях в связи с каким-либо преступлением). См.: Interpol, About Notices [Интерпол, Об уведомлениях], https://www.interpol.int/en/How-we-work/Notices/About-Notices. Помимо уведомлений, Интерпол ведет различные базы данных – судебных экспертиз (биометрические данные, связанные с совершенными преступлениями), данных потерянных и украденных паспортов и т. д. См.: Interpol, Our 18 Databases [Интерпол, Наши 18 баз данных], https://www.interpol.int/en/How-we-work/Databases/Our-18-databases.

123 В ЕС будет запущена информационная система выдачи разрешений на поездки ETIAS (European Travel Information and Authorisation System). При рассмотрении заявлений система будет сопоставлять полученные данные с целым рядом баз данных ЕС в области безопасности, управления миграцией и пограничного контроля, а также с данными Интерпола и Европола. В ETIAS также будет специальный контрольный список лиц. См.: Council of the EU, European travel information and authorisation system (ETIAS): Council Presidency and European Parliament provisionally agree on rules for accessing relevant databases, Press Release, 18 March 2021 [Пресс-релиз Совета ЕС от 18 марта 2021 г. «Европейская система информации о поездках и выдачи разрешений на поездки (ETIAS): председательство Совета и Европарламент предварительно согласовали правила доступа к базам данных], https://www.consilium.europa.eu/en/press/press-releases/2021/03/18/european-travel-information-and-authorisation-system-etias-council-presidency-and-european-parliament-provisionally-agree-on-rules-for-accessing-relevant-databases.

В Резолюции 2396 Совета безопасности ООН подчеркивается, что эффективное внедрение механизмов более тщательной проверки и международное сотрудничество в области обмена информацией имеют первостепенное значение для выявления лиц, «которые, как было установлено, являются террористами или которые подозреваются в террористической деятельности», и пресечения поездок в террористических целях[124]. Однако контрольные списки террористов также **могут использоваться неправомерным образом, и это представляет собой очень серьезную проблему с точки зрения прав человека и верховенства права**, и государства, выполняя Резолюцию 2396, должны принимать меры по решению этой проблемы[125].

## Слишком широкие критерии для включения лиц в контрольные списки и произвольное использование этих списков

Ошибочное включение лиц в контрольные списки для отслеживания террористов приводит к серьезным последствиям для прав человека этих лиц[126]. В зависимости от того, какие меры были использованы в качестве реагирования на предупреждение на основе контрольного списка (запрет на поездки, отказ во въезде или пребывании в стране, допрос, слежка или даже арест), может быть затронут широкий спектр прав, в том числе свобода передвижения, доступ к международной защите, право на неприкосновенность частной жизни, право на свободу, право на справедливое судебное разбирательство и право на надлежащую правовую процедуру. Это также может прямо или косвенно повлиять на весь спектр гражданских, политических, экономических, социальных и культурных прав членов семьи, включая детей, и близких того лица, которое было необоснованно внесено в контрольный список[127].

Существует риск использования слишком широких критериев для включения в контрольные списки и риск произвольного включения в такие списки. Отчасти это связано с отсутствием общепринятого международного определения понятия «терроризм». Слишком широкие определения этого понятия в законах разных стран о борьбе с терроризмом может приводить к его избыточному и даже неправомерному использованию[128].

---

124 См., например: Global Counterterrorism Forum (GCTF), New York Memorandum on Good Practices for Interdicting Terrorist Travel [Глобальный контртеррористический форум, Нью-Йоркский меморандум о хорошей практике в области пресечения поездок террористов], 25 September 2019, p. 1, https://toolkit.thegctf.org/Portals/1/Documents/En/New_York_Memorandum_on_Good_Practices_for_Interdicting_Terrorist_Travel.pdf.

125 В соответствии также с пунктом 11 Приложения к Мадридским руководящим принципам, см.: ИДКТК ООН, Приложение 2018 года к Мадридским руководящим принципам, указ. соч., сноска 75, пункт 11.

126 См., например: ECtHR, Nada v Switzerland [Европейский суд по правам человека (ЕСПЧ), дело «Нада против Швейцарии»], Application no. 10593/08, 12 September 2012, http://hudoc.echr.coe.int/fre?i=001-113118; CCPR, Sayadi and Vinck vs Belgium [Комитет по правам человека ООН, дело «Саяди и Винк против Бельгии»], UN Doc. CCPR/C/94/D/1472/2006, 22 October 2008, https://juris.ohchr.org/Search/Details/1477. См. также: Руководство по выработке ответов на угрозы и вызовы, связанные с «иностранными боевиками-террористами», в контексте защиты прав человека, указ. соч., сноска 5, с. 22-23.

127 Специальный докладчик ООН по борьбе с терроризмом подчеркнул, что следует, как правило, избегать включения детей в списки. См.: UN Special Rapporteur on counter-terrorism, Human Rights Principles Applicable to Watchlisting [Специальный докладчик ООН по борьбе с терроризмом, Правозащитные принципы, относящиеся к контрольным спискам], 2020, Principle 9, https://www.ohchr.org/Documents/Issues/Terrorism/ApplicablWatchlisting.docx.

128 См., например: Доклад Специального докладчика по борьбе с терроризмом «Влияние мер по борьбе с терроризмом и насильственным экстремизмом на гражданское пространство и права акторов гражданского общества и правозащитников», 1 марта 2019 г., UN Doc. A/HRC/40/52, https://undocs.org/A/HRC/40/52; БДИПЧ ОБСЕ, Ответственность государств: защита правозащитников в регионе ОБСЕ (2014-2016 гг.), 14 сентября 2017 г., https://www.osce.org/odihr/341366.

В Резолюции 2396 особое внимание уделяется лицам, «которые, как было установлено, являются террористами или которые подозреваются в террористической деятельности», в связи с чем возникают вопросы относительно степени доказанности вины, необходимой для включения лица в контрольные списки, а также может возникнуть обеспокоенность по поводу соблюдения презумпции невиновности[129]. Особая озабоченность была высказана в отношении «заблаговременных» контрольных списков, в которые включаются «потенциальные» террористы и преступники, то есть лица, не совершавшие правонарушений, но предположительно способные сделать совершить преступление в будущем[130]. Включение в контрольные списки для отслеживания террористов может быть сопряжено с серьезными ограничениями прав человека, и поэтому такое решение не должно приниматься на основе представлений об абстрактной или гипотетической опасности совершения преступления в будущем. Для того чтобы соответствовать принципам необходимости и соразмерности, подобное решение должно касаться «реальной, явной и измеримой террористической угрозы»[131] и должны существовать достаточные доказательства причастности лица к совершению реального уголовного преступления.

Во избежание слишком широкого применения контрольных списков террористов **необходимо четко определить критерии включения лиц в такие списки, используя узкое и точное определение преступлений террористической направленности**[132].

## Отсутствие процессуальных гарантий защиты прав при включении в контрольные списки и в процессе исключения из них

Несмотря на то, что в последние годы были достигнуты определенные улучшения, серьезной критике подвергается практика внесения лиц в контрольные списки даже таких международных институтов, как Совет безопасности ООН и Европейский союз[133].

---

129 Определить конкретного человека как лицо, которое, «как было установлено, явля[е]тся террорист[ом]», возможно при наличии решения суда, признавшего это лицо виновным в совершении преступления террористической направленности; вина должна быть доказана вне всяких разумных сомнений. Требования для признания лица подозреваемым всегда ниже и зависят от уровня подозрения (разные уровни предполагаются для инициирования уголовного преследования, для получения ордера на арест или начала расследования).

130 Automated Suspicion – The EU's New Travel Surveillance Initiatives, указ. соч., сноска 74, с. 22 и 33 (о новом контрольном списке в системе ETIAS, который будет введены в 2021 г. и будет содержать данные не только тех лиц, которые подозреваются в совершении преступлений, но и тех, кто предположительно может нарушить закон в будущем).

131 Как отметила Специальный докладчик ООН по борьбе с терроризмом, см.: Human Rights Principles Applicable to Watchlisting, указ. соч., сноска 127, принцип 2.

132 БДИПЧ последовательно призывает обеспечить, чтобы законодательство, касающееся борьбы с терроризмом, основывалось на определении терроризма в соответствии с подходом, принятым в Резолюции 1566 (2004) Совета безопасности ООН; см., например: Руководство по выработке ответов на угрозы и вызовы, связанные с «иностранными боевиками-террористами», в контексте защиты прав человека БДИПЧ, указ. соч., сноска 5, с. 21-24. Предлагаемое типовое определение терроризма согласно этим критериям можно найти в Докладе Специального докладчика ООН по борьбе с терроризмом «Десять элементов наилучшей практики в области борьбы с терроризмом:, 22 декабря 2010 г., UN Doc. A/HRC/16/51, п. 28, https://undocs.org/A/HRC/16/51. Об определении терроризма см. также: БДИПЧ, Предупреждение терроризма и борьба с насильственным экстремизмом и радикализацией, ведущими к терроризму: подход, основанный на взаимодействии полиции с населением, февраль 2014 г., с. 27-30, https://www.osce.org/ru/secretariat/116413.

133 См., например: ПАСЕ, Резолюция 1597 «Черные списки» Совета Безопасности ООН и Европейского союза», 23 января 2008 г., https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2008]/%5BJan2008%5D/Res1597_rus.asp#TopOfPage. В ответ на такую обеспокоенность Совет Безопасности ООН создал независимую Канцелярию омбудсмена для рассмотрения просьб от отдельных лиц и групп, добивающихся исключения из санкционного списка ООН. См.: Канцелярия Омбудсмена по Комитету Совета Безопасности по санкциям в отношении ИГИЛ (ДАИШ) и Аль-Каиды, https://www.un.org/securitycouncil/ombudsperson.

Минимальные стандарты надлежащей правовой процедуры должны применяться ко всем механизмам (как национальным, так и международным) внесения лиц в контрольные списки и использования других ограничительных мер. Это подразумевает обязательное и незамедлительное информирование физического или юридического лица о включении его в список и об основаниях для такой меры, а также право затронутого лица ходатайствовать об исключении из списка и право на судебный пересмотр решения о включении в список после подачи такого ходатайства – с полным соблюдением гарантий надлежащей правовой процедуры, включая раскрытие заявителю информации о соответствующем деле[134].

Практика показала, что исключение из списка является особенно сложной задачей, если имеет место международный обмен контрольными списками и базами данных. Даже если человек успешно оспорит включение себя в список в одной стране, это необязательно приведет к удалению его данных из списков во всех других странах. Могут потребоваться подача отдельных заявлений и судебные разбирательства в других юрисдикциях, а это подрывает право на эффективное средство правовой защиты[135]. Таким образом, исключение лица из контрольного списка в одной стране должно запускать процесс пересмотра списков в других странах. У затронутых лиц должен быть доступ к эффективному оспариванию в юридическом порядке продолжающегося присутствия их данных в контрольных списках в других юрисдикциях[136]. Также рекомендуется предусмотреть положения об истечении срока действия, согласно которым включение в список автоматически теряет силу, если оно не было продлено[137].

В связи с тем, что попавшие в контрольный список лица могут столкнуться с серьезными последствиями для их прав человека, необходимо предусмотреть **строгие процессуальные гарантии** для защиты от произвола. В частности, должны существовать **действенные средства правовой защиты,** позволяющие оспорить необоснованное включение в контрольный список, а также **эффективные механизмы, обеспечивающие исключение из контрольного списка на практике**, в том числе в случае международного обмена данными.

134 Эти рекомендации были предложены Специальным докладчиком ООН по борьбе с терроризмом еще в 2010 г., см.: Десять элементов наилучшей практики в области борьбы с терроризмом, указ. соч., сноска 132, Практический метод 9. См. также: UN Special Rapporteur on counter-terrorism, Human Rights Principles Applicable to Watchlisting, указ. соч., сноска 127, принцип 7.

135 Это относится и к случаям, когда контрольные списки воспроизводятся и распространяются частными субъектами (например, используются авиакомпаниями или финансовыми учреждениями). В результате этого люди могут сталкиваться с ограничениями (например, при открытии банковских счетов) даже после исключения из списка. См.: Gavin Sullivan, Submission to the UN Special Rapporteur on counter-terrorism [Представление Специальному докладчику ООН по вопросам борьбы с терроризмом], 2019, https://www.ohchr.org/Documents/Issues/Terrorism/SR/Submissions/Gavin%20Sullivan_GA74CT.pdf.

136 UN Special Rapporteur on counter-terrorism, Human Rights Principles Applicable to Watchlisting, указ. соч., сноска 127, принцип 8. ПАСЕ предложила аналогичные рекомендации, а именно обеспечить удаление из национальных баз данных всех копий красных уведомлений и специальных запросов, признанных Интерполом необоснованными. См.: PACE Resolution 2315 “Interpol reform and extradition proceedings: building trust by fighting abuse” [ПАСЕ, Резолюция 2315 «Реформа Интерпола и процедура выдачи: укрепление доверия путем борьбы со злоупотреблениями»], 29 November 2019, https://pace.coe.int/en/files/28303/html.

137 Специальный докладчик ООН по борьбе с терроризмом рекомендовал ввести пункт о прекращении действия санкций по прошествии 1 года, см.: Десять элементов наилучшей практики в области борьбы с терроризмом, указ. соч., сноска 132, Практический метод 9.

## Проблемы, касающиеся неприкосновенности частной жизни и защиты данных

В целях обнаружения лиц, подозреваемых в терроризме (и совершении других преступлений), данные пассажиров сравниваются не только с национальными и международными контрольными списками, составленными для борьбы с терроризмом. Они также проверяются по другим базам данных правоохранительных органов, в которых содержится информация о большом числе людей. Эти базы данных формируются многочисленными ведомствами (полиция, спецслужбы, органы пограничного контроля и т. д.); при этом субъекты данных необязательно знают о том, что их данные были включены в базу[138]. В таких обстоятельствах надзор является трудной задачей, и обеспечение эффективных средств правовой защиты и возможности оспорить ошибочное включение в списки и потребовать исправления ситуации тоже серьезно затруднено.

Часто в положениях законодательства о защите данных предусмотрены широкие исключения для правоохранительных органов, однако любое вмешательство в право на неприкосновенность частной жизни должно быть предписано законом и быть необходимым и соразмерным поставленной законной цели[139]. В связи с этим создание и ведение баз данных правоохранительных органов должно осуществляться согласно законодательству, предусматривающему эффективные гарантии защиты от неправомерного использования данных[140]. В частности, должны быть определены предельные сроки хранения данных и специальные механизмы защиты конфиденциальных данных (например, информации о политических взглядах)[141]; также должна быть обеспечена реальная возможность запрашивать удаление данных[142] и исправление неправильных данных[143].

---

138 В ЕС помимо списка террористов используются, например, базы данных Шенгенской информационной системы (ШИС) и Европола. В данных, введенных в ШИС, могут содержаться различные инструкции для пользователей системы. Система может дать указание сотрудникам не только задержать человека или запретить ему въезд, но и провести скрытые или специальные проверки. В случае скрытых проверок затронутое лицо не будет знать о том, что в его отношении было выпущено предупреждение о необходимости проверки. См.: Automated Suspicion – The EU's New Travel Surveillance Initiatives, указ. соч., сноска 74, с. 22. Об опасениях по поводу секретных списков террористов/лиц, не допускаемых к полетам, см. также: American Civil Liberties Union (ACLU), Wilwal v. Bielsen – Lawsuit challenging abusive border detention of American family [Американский союз защиты гражданских свобод, дело «Уилвэл против Билсена» – иск, оспаривающий неправомерное содержание под стражей американской семьи на границе], 29 September 2020, https://www.aclu.org/cases/wilwal-v-nielsen-lawsuit-challenging-abusive-border-detention-american-family; ACLU, Kashem, et al. v. Barr, et al. – ACLU challenge to Government No Fly List [Дело «Кашем и др. против Барра и др.» – Американский союз защиты гражданских свобод оспаривает составленный правительством черный список лиц, не допускаемых к полетам], 13 March 2018, https://www.aclu.org/cases/kashem-et-al-v-barr-et-al-aclu-challenge-government-no-fly-list; ACLU, Trapped in a Black Box: Growing Terrorism Watchlisting in Everyday Policing [Американский союз защиты гражданских свобод, В западне черного ящика: расширенное использование списков террористов в правоохранительной деятельности], April 2016, https://www.aclu.org/sites/default/files/field_document/wirac_9-11_clinic_trapped_in_a_black_box.pdf.

139 Например, в законодательстве ЕС предусмотрено, что деятельность правоохранительных органов регулируется не Общим регламентом ЕС о защите персональных данных, а Директивой 2016/680 об обработке персональных данных правоохранительными органами. Помимо этого, национальные правила в отношении защиты данных часто содержат значительные исключения для правоохранительных органов. См. раздел о биометрических данных в настоящем документе. Тем не менее, как подчеркнула Специальный докладчик ООН по борьбе с терроризмом, международные стандарты защиты данных должны в полной мере соблюдаться при составлении контрольных списков; см.: Human Rights Principles Applicable to Watchlisting, указ. соч., сноска 127, принцип 6.

140 См., например: ECtHR, Shimovolos v. Russia [Европейский суд по правам человека (ЕСПЧ), дело «Шимоволос против России»], Application no. 30194/09, 21 June 2011, http://hudoc.echr.coe.int/eng?i=001-105217 (о внесении правозащитника в базу данных «Сторожевой контроль», в которую собиралась информация о передвижениях этого лица на внутреннем железнодорожном и воздушном транспорте).

141 См.: ECtHR, Catt v The United Kingdom [Европейский суд по правам человека (ЕСПЧ), дело «Кэтт против Соединенного Королевства»], Application no. 43514/15, 24 January 2019, http://hudoc.echr.coe.int/eng?i=001-189424 (о сборе и хранении данных лица, в течение многих лет бывшего гражданским активистом, в полицейской базе данных «внутренних экстремистов».

142 См., например: ECtHR, Brunet v. France [Европейский суд по правам человека (ЕСПЧ), дело «Бруне против Франции], Application no. 21010/10, 18 September 2014, http://hudoc.echr.coe.int/eng?i=001-146389.

143 См., например: ECtHR, Khelili v. Switzerland [Европейский суд по правам человека (ЕСПЧ), дело «Хелили против Швейцарии»], Application no. 16188/07, 18 October 2011, http://hudoc.echr.coe.int/eng?i=001-107032.

- Учитывая тот факт, что использование контрольных списков и других баз данных правоохранительных органов оказывает очень серьезное воздействие на права человека, очень важно создать надлежащие процедуры для **регулярной проверки данных**, с тем чтобы они оставались правильными и чтобы информация, ставшая ненужной или устаревшей удалялась в соответствии с четко **установленными сроками хранения**[144].
- Помимо этого, у субъектов данных должна быть **возможность эффективно запрашивать исправление данных** и должны быть созданы механизмы особой защиты **конфиденциальных данных**.

## Международное сотрудничество

Обмен контрольными списками и другими базами данных в рамках международного (двустороннего или многостороннего) сотрудничества правоохранительных органов создает дополнительные потенциальные риски для прав человека[145]. Сбор, обмен и получение информации от государств, в которых существует реальный риск того, что эта информация была добыта с помощью пыток или других видов жестокого обращения, делает государство, принимающее эти данные, соучастником этих актов[146]. Это также касается ситуации, когда принимаются данные, полученные в результате других серьезных нарушений прав человека в государстве-отправителе. Аналогичным образом, передача информации государству, в котором существует реальный риск того, что эта информация будет использована для нарушения международного права прав человека, может сделать отправляющее информацию государство соучастником этих нарушений.

Таким образом, прежде чем передавать или получать данные от властей другой страны, государство должно убедиться в существовании там эффективных гарантий защиты прав человека и соблюдении этих гарантий[147].

Резолюция 2396 Совета Безопасности ООН призывает государства регулярно пользоваться базами данных Интерпола для проверки пассажиров в воздушных, наземных и морских пунктах въезда[148]. Многие выразили обеспокоенность по поводу возможного неправомерного использования «красных циркуляров» и так называемых «запросов» Интерпола (то есть просьб о сотрудничестве с другими правоохранительными органами) в отношении подозреваемых лиц в качестве инструмента для «экспорта угнетения» или в качестве

144 См.: Права человека в антитеррористических расследованиях: практическое руководство для сотрудников правоохранительных органов, Варшава/Вена, БДИПЧ ОБСЕ, 2013 г., с. 30, https://www.osce.org/files/f/documents/4/1/117891.pdf.

145 Точно так же, как обмен данными API, PNR или биометрическими данными между странами может создать новые или усугубить существующие правозащитные риски.

146 Доклад Специального докладчика по вопросу о пытках и других жестоких, бесчеловечных или унижающих достоинство видах обращения или наказания, UN Doc. A/HRC/25/60, 10 апреля 2014 г., п. 76, https://undocs.org/A/HRC/25/60.

147 Доклад Специального докладчика по борьбе с терроризмом «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», UN Doc. A/HRC/14/46, 17 мая 2010 г., Метод 33, https://undocs.org/A/HRC/14/46. См.: Руководство по выработке ответов на угрозы и вызовы, связанные с «иностранными боевиками-террористами», в контексте защиты прав человека, указ. соч., сноска 5, с. 34, 42 и 43.

148 Резолюция 2396 (2017) Совета Безопасности ООН, п. 16.

оружия против критиков правительства, находящихся в других странах[149]. Возможные последствия такой ситуации, в том числе для мигрантов, беженцев и соискателей убежища, очевидны и хорошо задокументированы[150]. В целом, усилия Интерпола по решению этой проблемы и предупреждению неправомерного использования его механизмов получили широкое признание[151]. Однако риск злоупотребления его системами по-прежнему высок и соответствующие проблемы остаются. В этом контексте международные институты и гражданское общество подчеркнули, что Интерполу необходимо дополнительно ужесточить проверку циркуляров и запросов, а также повысить подотчетность стран, злоупотребляющих его системой[152].

Как подчеркивает ПАСЕ, «международное сотрудничество в уголовно-правовой сфере требует высокой степени взаимного доверия, основанного на общих стандартах и практике»[153]. Нарушения прав человека в какой-либо стране подрывают доверие к ней других стран, а также сказываются на эффективности международного сотрудничества (двустороннего и многостороннего) и в итоге ставят под удар эффективность совместных усилий по борьбе с терроризмом и другими транснациональными угрозами.

149 См.: например: PACE Resolution 2315, указ. соч., сноска 136; ПАСЕ, Резолюция 2161 «Злоупотребление системой Интерпола: необходимость ужесточения правовых гарантий», 26 апреля 2017 г., https://rm.coe.int/session-april-17-ru/16807161f2; Fair Trials, Dismantling the Tools of Oppression: Ending the Misuse of INTERPOL [Устранение инструментов угнетения: прекращение неправомерного использования системы Интерпола], 4 October 2018, https://www.fairtrials.org/sites/default/files/publication_pdf/Dismantling%20the%20tools%20of%20oppression.pdf; Fair Trials, Strengthening respect for human rights, strengthening INTERPOL [Укрепление соблюдения прав человека, укрепление деятельности Интерпола], 26 November 2013, https://www.fairtrials.org/publication/strengthening-respect-human-rights-strengthening-interpol; Nate Schenkkan and Isabel Linzer, Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression [Вне поля зрения, но не вне досягаемости: глобальные масштабы и сфера применения транснациональных репрессий], Freedom House, February 2021 (описаны случаи из России, Турции и других стран, а также общая ситуация в разных регионах мира), https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.

150 См.: конкретные примеры в: Fair Trials, Dismantling the Tools of Oppression, там же. В связи с этим также стоит отметить, что, как сообщается, другие механизмы Интерпола (например, базы данных потерянных и украденных проездных документов) используются в похожих целях (см.: Freedom House, February 2021, там же). Помимо этого, как отмечает ПАСЕ, неправомерно использоваться могут и межгосударственные механизмы взаимного правового сотрудничества (например, Шенгенская информационная система), что может привести к вторжению в частную жизнь, нарушению имущественных и профессиональных прав, а также к лишению свободы, см.: PACE Resolution 2315, указ. соч., сноска 136, п. 5.

151 Например, укрепление Комиссии по контролю за архивами Интерпола (Commission for the Control of Interpol's Files – CCF), куда могут обращаться лица, в отношении которых существуют уведомления и специальные запросы. См.: PACE Resolution 2315, указ. соч., сноска 136, п. 7; Fair Trials, Dismantling the Tools of Oppression, указ. соч., сноска 149.

152 См.: PACE Resolution 2315, указ. соч., сноска 136, пп.8 и 10.1. По мере того, как защита от злоупотребления инструментами Интерпола будет улучшаться, государствам также следует проявлять бдительностью в отношении возможного и альтернативных механизмов, которые могут быть не так защищены от злоупотреблений и при этом использоваться государствами в целях преследования своих оппонентов в других странах. См.: Fair Trials, Dismantling the Tools of Oppression, указ. соч., сноска 149, с. 67-68.

153 См.: PACE Resolution 2315, указ. соч., сноска 136, п. 4.

- До заключения **соглашения об обмене информацией** с другими странами и до обмена информацией по отдельным делам необходимо провести оценку **положения с правами человека и защитой данных в государстве-партнере**[154].
- Когда речь идет о **многостороннем обмене информацией**, государства должны с особой бдительностью относится к запросам о сотрудничестве, поступающим от государств, в которых плохо обеспечиваются права человека и соблюдается принцип верховенства права, в том числе от стран с недостаточно независимой системой уголовного преследования и судебной системой. Необходимо предпринимать действенные меры по недопущению неправомерного использования таких запросов[155].

154 Эта рекомендация была предложена Специальным докладчиком ООН по борьбе с терроризмом Мартином Шейнином в отношении обмена информацией между спецслужбами, однако она также применима к любому обмену информацией между государствами, в том числе к обмену данными API/PNR, биометрическими и другими данными для целей правоохранительной деятельности. См.: Доклад Специального докладчика по борьбе с терроризмом, Подборка оптимальных практических методов, указ. соч., сноска 147, Метод 33.

155 См.: PACE Resolution 2315, указ. соч., сноска 136, пп. 9.6, 10.1 и 10.2.

# Заключение

При том, что государства имеют право контролировать, кто въезжает на их территорию, и несут обязанность по борьбе с терроризмом и другими преступлениями, деятельность в этих областях должна осуществляться с полным соблюдением всех международных стандартов в области прав человека. Появление и рост использования пограничными службами новых технологий по сбору и обработке больших объемов персональных данных для целей отслеживания, идентификации и контроля за лицами, пересекающими границы[156], создает новые вызовы в сфере защиты прав человека. Технологические решения вовсе не являются нейтральными[157]. Причисление людей к категории подозрительных лиц на основе предположений, сгенерированных алгоритмами, а также дискриминационное профилирование, слежка, вторжение в частную жизнь и нарушения других прав человека, ставшие результатом сбора и обработки биометрических данных, данных API/PNR и другой информации, имеющей отношение к поездкам, и обмена такими данными, – вот лишь некоторые из рисков для прав человека, возникающие в связи с использованием указанных технологий.

Эти риски увеличиваются при отсутствии прозрачности и надзора за системами, разработанными для пограничного контроля. При этом лица, находящиеся в особенно уязвимом положении (например, мигранты, соискатели убежища и беженцы), подвергаются наибольшим рискам. Использование излишне строгих мер безопасности в рамках пограничного контроля приводит к тому, что людям отказывают в их правах, и эта ситуация затрагивает прежде всего тех, кто остро нуждается в защите. Такой подход ведет к утрате доверия со стороны общин, которым система должна служить. Результатом является не укрепление безопасности, а снижение ее уровня. Защита прав человека является важнейшим инструментом для действенного обеспечения трансграничной безопасности.

Таким образом, государствам настоятельно рекомендуется:

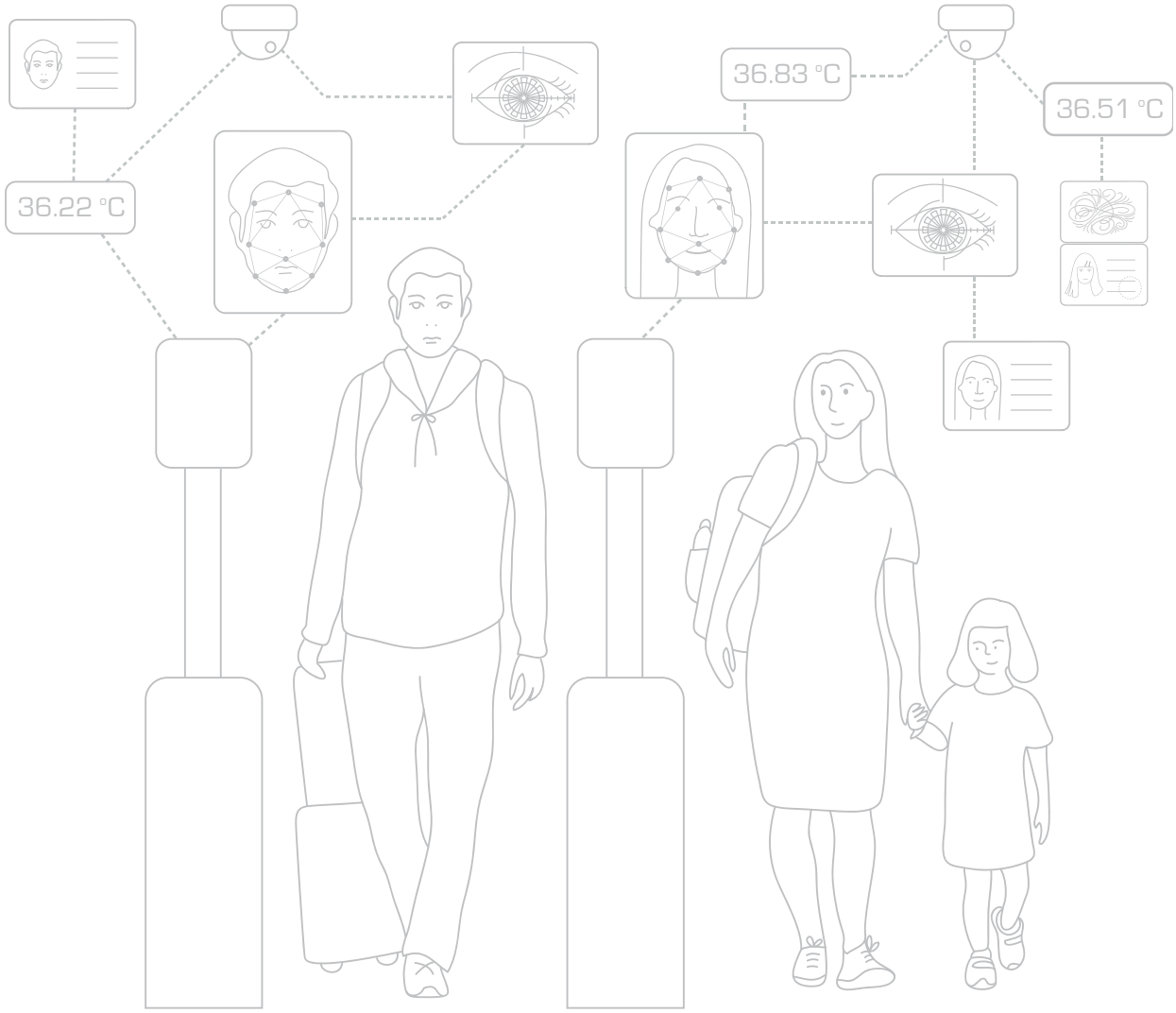
- создать надлежащую **законодательную базу**, регулирующую использование новых технологий в пограничном контроле и обеспечивающую **надежные гарантии защиты прав человека**, а также включить эти гарантии во все соответствующие международные и транснациональные соглашения о сотрудничестве, в том числе в области обмена данными;
- гарантировать прозрачность и подотчетность при разработке и использовании технологических решений и систем, предназначенных для сбора, обработки и обмена персональными данными в сфере пограничного контроля и обеспечения безопасности;
- создать действенные **независимые механизмы внешнего надзора**, регулярного мониторинга и анализа, а также обеспечить эффективные средства правовой защиты для тех, чьи права были затронуты;

156 Technological Testing Grounds, указ. соч., сноска 19, с. 2.
157 Там же, с. 37.

- в целью выявления рисков в области прав человека и реагирования на эти риски обязать стороны, занимающиеся разработкой, закупкой и эксплуатацией указанных систем, во время их разработки и до введения их в эксплуатацию **проводить их комплексную проверку с точки зрения прав человека**, а также обязательную **тщательную оценку возможных последствий для прав человека**; обеспечить регулярное проведение такой оценки после введения системы в эксплуатацию;
- обеспечить, чтобы проведение **оценки всегда было основано на широком участии** неправительственных организаций, отражающих многообразие общества, а также групп и общин, права которых затрагиваются в наибольшей степени;
- обеспечить, чтобы сотрудники пограничных служб и другие лица, использующие новые системы, прошли соответствующее **обучение в области прав человека** и были проинформированы о потенциальной предвзятости используемых систем и последствиях их использования для прав человека.

Помимо этого, государствам следует **воздержаться от распространения в мире** (путем экспорта или официальной поддержки разработки) тех технологий, которые оказывают неблагоприятное воздействие на права человека.

Основную ответственность за соблюдение и защиту прав человека несут государства, однако у **частных коммерческих предприятий** тоже есть обязанности в области прав человека, и должна быть обеспечена их подотчетность в данном вопросе. Это особенно касается компаний, занимающихся разработкой или применением указанных технологий или же иным образом задействованных в выполнении функций, связанных с обеспечением пограничного контроля, либо напрямую выполняющих такие функции.


36.22 °C
36.83 °C
36.51 °C

Follow OSCE and ODIHR


**OSCE Office for Democratic Institutions and Human Rights**

Ul. Miodowa 10
00-251 Warsaw
Poland

Office: +48 22 520 06 00
Fax: +48 22 520 06 05
office@odihr.pl