РУКОВОДСТВО ОБСЕ ДЛЯ СПЕЦИАЛИСТОВ-ПРАКТИКОВ В ОБЛАСТИ УГОЛОВНОГО ПРАВОСУДИЯ

Обеспечение Соблюдения Прав Человека при Расследовании Киберпреступлений

ОБСЕ Организация по безопасности и сотрудничеству в Европе

Вена, октябрь 2023 год

Международная Стандартная Нумерация Книг: 978-92-9271-375-1

Опубликовано:
Секретариат ОБСЕ
Департамент по противодействию транснациональным угрозам
Отдел стратегических вопросов полицейской деятельности
Вальнерштрассе 6
1010 Вена, Австрия
Tel: +43-1 514 36 180
Fax: +43-1 514 36 105
email: info@osce.org | spmu@osce.org

www.osce.org

РУКОВОДСТВО ОБСЕ ДЛЯ СПЕЦИАЛИСТОВ-ПРАКТИКОВ В ОБЛАСТИ УГОЛОВНОГО ПРАВОСУДИЯ

Обеспечение Соблюдения Прав Человека при Расследовании Киберпреступлений

ОБСЕ Организация по безопасности и сотрудничеству в Европе

БЛАГОДАРНОСТЬ

Данное учебное пособие было разработано Департаментом по противодействию транснациональным угрозам/Отделом стратегических вопросов полицейской деятельности (ДТУ/ОСВП) Секретариата ОБСЕ при участии Бюро по демократическим институтам и правам человека (БДИПЧ) ОБСЕ. ДТУ/ОСВП хотели бы поблагодарить г-на Роберта Голобинека и г-на Хайна Дриса за их вклад в составление данного руководства. Руководство было разработано в рамках внебюджетного проекта ОБСЕ «Развитие потенциала по противодействию киберпреступлениям в Центральной Азии», финансируемого Соединенными Штатами Америки, Германией и Республикой Корея.

СОДЕРЖАНИЕ

АББРЕВИАТУРЫ

CEC	Суд Европейского Союза
СЕ	Совет Европы
СБСЕ	Совещание по Безопасности и Сотрудничеству в Европе
ЕКПЧ	Европейская Конвенция по Правам Человека
ЕСПЧ	Европейский Суд по Правам Человека
ЕС	Европейский Союз
ФАТФ	Группа Разработки Финансовых Мер по Борьбе с Отмыванием Денег
GPS	Глобальная Система Позиционирования
МПГПП	Международный Пакт о Гражданских и Политических Правах
IP адрес	Адрес Интернет-Протокола
ИП	Интернет Провайдер
НПО	Неправительственная Организация
БДИПЧ	Бюро по Демократическим Институтам и Правам Человека (ОБСЕ)
УВКПЧ	Управление Верховного комиссара ООН по Правам Человека
ОБСЕ	Организация по Безопасности и Сотрудничеству в Европе
ВДПЧ	Всеобщая Декларация Прав Человека (ООН)
ООН	Организация Объединенных Наций
УНП	Управление ООН по Наркотикам и Преступности
VPN	Виртуальная Частная Сеть VPN

ВСТАВКИ С ТЕКСТОМ

1

Введение

Наши общества все больше полагаются на цифровые технологии во всех аспектах жизни: от бизнеса, науки и образования до общения, путешествий, отдыха и развлечений. Быстрое развитие этих технологий в последние годы принесло много возможностей, но также и новые риски и проблемы безопасности. Одной из областей, на которую эти события существенно повлияли, является преступность.

Цифровые технологии изменили криминальный ландшафт. Они породили новые формы преступности (например, киберзависимые преступления, такие как программы-вымогатели, фишинг, криптоджекинг) и изменили способы совершения существующих форм преступлений (например, киберпреступления, такие как сексуальная эксплуатация в Интернете или онлайн-торговля незаконными товарами и услугами). Многие цифровые технологии также стали полезными инструментами для борьбы с традиционными преступлениями в физическом мире (например, кража со взломом, воровство и мошенничество). Кроме того, широкое использование цифровых устройств (персональных компьютеров, ноутбуков, планшетов, мобильных телефонов, умных часов и т. д.) означает, что электронные доказательства теперь играют важную роль практически во всех видах уголовных расследований.

Киберпреступность имеет некоторые специфические особенности, которые отличают расследование киберпреступлений от расследования других видов преступлений. В частности, преступнику не обязательно физически присутствовать на месте преступления или рядом с жертвой, и он может находиться в иностранной юрисдикции. Кроме того, Интернет предоставляет преступникам множество возможностей скрыть свою личность за псевдонимами и украденными учетными данными, а для сокрытия преступной деятельности можно использовать различные инструменты шифрования или анонимизации. Криптовалюты позволяют пользователям совершать безопасные платежи без прямой связи с реальной личностью, что упрощает приобретение незаконных товаров и услуг и отмывание доходов, полученных преступным путем.

Выявление, изъятие и анализ электронных доказательств киберпреступления или другого вида преступлений также во многом отличаются от обработки вещественных доказательств. Соответствующие электронные доказательства могут храниться не на отдельном устройстве, а на облачных серверах, контролируемых частными компаниями, которые часто базируются за границей. Более того, электронные данные нестабильны и могут быть легко перемещены, изменены или удалены.

Таким образом, киберпреступность[1] и электронные доказательства создают серьезные проблемы для систем уголовного правосудия и верховенства закона во всем регионе ОБСЕ. Расследование киберпреступлений и электронных доказательств требует особых знаний и навыков, адекватных технических средств и законодательной базы, а также эффективного и действенного международного сотрудничества с иностранными субъектами уголовного правосудия и частными организациями. Государства адаптируются к этим изменениям, внося поправки в свои законы, наращивая свой технический потенциал и вводя новые процессуальные следственные полномочия. Все эти меры и инструменты должны разрабатываться и применяться в соответствии с обязанностями государств согласно международному праву прав человека.

Примечание: Доступ ко всем электронным ресурсам был осуществлен 1 июня 2023 г.

1 В этом тексте «киберпреступность» используется как общий термин, который относится как к киберзависимым, так и к киберпреступлениям, если не указано иное.

Как и любое другое уголовное расследование, расследование киберпреступлений и использование определенных процессуальных полномочий затрагивают права и свободы человека, изложенные в международных документах на глобальном и региональном уровнях. К ним относятся Всеобщая Декларация Прав Человека (ВДПЧ), Международный Пакт о Гражданских и Политических Правах (МПГПП) и Европейская Конвенция по Правам Человека (ЕКПЧ).

Хотя эти права и свободы необходимо уважать и защищать в ходе любого уголовного расследования, эта необходимость, возможно, становится еще более актуальной в контексте киберпреступлений и электронных доказательств. Данные, которые цифровые устройства и онлайн-сервисы собирают о своих пользователях, беспрецедентны как в масштабе, так и в объёме. Эти данные могут предоставить множество личных подробностей о жизни людей, включая их здоровье, экономическую деятельность, личные отношения и политические предпочтения. Собирая электронные доказательства в ходе расследования, специалисты по уголовному правосудию часто находят соответствующие доказательства наряду с большим количеством других, часто личных данных. Таким образом, этот тип расследования потенциально гораздо более интрузивен, чем традиционные «автономные» расследования, в ходе которых осуществляется сбор только вещественных доказательств.

Поэтому осведомленность о последствиях расследований киберпреступлений и других расследований, включающих электронные доказательства, для прав человека важна для следователей полиции, прокуроров и судей. Нарушение прав человека в ходе уголовных расследований и разбирательств может привести к неправомерному осуждению или к отклонению представленных доказательств, что приведет к оправданию преступника. Отсутствие уважения к правам человека также подрывает доверие на национальном и международном уровнях. Это является препятствием для международного сотрудничества, как с правоохранительными и другими органами в странах-партнерах, так и с частными компаниями, расположенными за рубежом. Кроме того, уважение и защита прав человека на практике помогает укрепить доверие между органами уголовного правосудия и обществом в целом и, таким образом, побуждает людей сотрудничать со следователями, занимающимися делами по киберпреступлениям и предоставлять им важную информацию. Таким образом, применение подхода, основанного на правах человека, повышает эффективность расследований киберпреступлений.

Настоящее Руководство направлено на повышение осведомленности специалистов уголовного правосудия о последствиях, которые могут повлиять на соблюдение прав человека и помогут им оказывать поддержку в защите прав человека в их повседневной следственной работе по расследованию киберпреступлений и других преступлений, включающих электронные доказательства. Это делается путем сосредоточения внимания на тех правах человека, которые особенно затрагиваются расследованиями киберпреступлений и других преступлений, включающих электронные доказательства, а именно:

- Право на неприкосновенность частной жизни;
- Право на справедливое судебное разбирательство;
- Право на свободу выражения мнений/слова;
- Право на защиту собственности.

Руководство опирается на судебную практику Европейского Суда по Правам Человека (ЕСПЧ), а иногда и Суда Европейского Союза (СЕС), чтобы объяснить и проиллюстрировать, как права человека применяются в контексте расследований киберпреступлений, а также при сборе и использовании электронных доказательств.

2

Правовая база в области прав человека, применимая к расследованиям киберпреступлений

2.1 ЧТО ТАКОЕ ПРАВА ЧЕЛОВЕКА?

Права человека – это законные права человека на защиту своего достоинства и свобод. Они присущи всем людям, без различия расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного положения, рождения или любого другого статуса. Все права человека, будь то гражданские и политические права (например, право на жизнь, равенство перед законом и свобода выражения мнений); экономические, социальные и культурные права (такие как право на труд, социальное обеспечение и образование); или коллективные права (такие как право на развитие и самоопределение) неделимы, взаимосвязаны и взаимозависимы. Улучшение одного права облегчает развитие других.

Всеобщие права человека выражаются и гарантируются законом в форме договоров, обычного международного права, общих принципов и других источников международного права. Международное право в области прав человека налагает конкретные обязательства на государства, включая парламенты, министерства, местные органы власти, правоохранительные органы и органы уголовного правосудия, как на «носителей обязанностей», ответственных за уважение, защиту и реализацию прав человека. Сюда входят как так называемые «негативные» обязательства воздерживаться от определенных действий (например, от незаконного вмешательства в частную жизнь человека), а также обязанности предпринимать «позитивные» действия для защиты прав человека (например, путем эффективного расследования и преследования преступлений) и продвижения прав человека и основных свобод (например, путем предоставления общественной информации и обучения соответствующих государственных чиновников).

2.2 МЕЖДУНАРОДНЫЕ ПРАВОВЫЕ ИНСТРУМЕНТЫ И ОРГАНЫ ПО ВОПРОСАМ ПРАВ ЧЕЛОВЕКА

Государства признали важность защиты прав человека после Второй мировой войны с созданием Организации Объединенных Наций (ООН) и Совета Европы (СЕ) и разработкой международных инструментов по правам человека в рамках этих организаций. Европейский Союз (ЕС) также подчеркнул важность прав человека, приняв специальную хартию прав человека. Во Вставке 1 представлены международные правовые документы по правам человека, особенно актуальные в контексте киберпреступности.

ВСТАВКА 1 МЕЖДУНАРОДНЫЕ ПРАВОВЫЕ ДОКУМЕНТЫ ПО ПРАВАМ ЧЕЛОВЕКА ОСОБЕННО АКТУАЛЬНЫЕ ДЛЯ РАССЛЕДОВАНИЙ КИБЕРПРЕСТУПЛЕНИЙ

- Всеобщая Декларация Прав Человека 1948[2] года (ВДПЧ) ООН (в частности, статьи 8–11, 12 и 19);
- Международный Пакт о Гражданских и Политических Правах 1966[3] года (МПГПП) ООН (в частности, статьи 14, 17 и 19);
- Европейская Конвенция по Правам Человека 1950[4] года (ЕКПЧ) Совета Европы (в частности, статьи 6, 8 и 10);
- Хартия Основных Прав Европейского Союза[5] 2000 года.

В Дополнении 1 представлен полный текст упомянутых выше статей МПГПП и ЕКПЧ.

За исключением Святого Престола, все государства-участники ОБСЕ ратифицировали МПГПП и поэтому обязаны соблюдать его положения. Большинство государств-участников ОБСЕ также являются членами Совета Европы и, следовательно, участниками ЕКПЧ. Некоторые государства-участники ОБСЕ также являются государствами-членами ЕС и, следовательно, связаны Хартией Основных Прав Европейского Союза при применении законодательства ЕС (пункт 1 статьи 51 Хартии).

Существует ряд правозащитных учреждений, уполномоченных интерпретировать и продвигать права человека, закрепленные в этих юридических текстах. На уровне ООН Комитет по правам человека является договорным органом МПГПП. В его состав входят 18 независимых экспертов, которые следят за выполнением МПГПП государствами-участниками.[6] Он рассматривает выполнение Пакта посредством периодических докладов и может рассматривать индивидуальные жалобы относительно предполагаемых нарушений МПГПП государствами, присоединившимися к Факультативному Протоколу к Пакту.[7]

На региональном уровне Европейский суд по правам человека (ЕСПЧ) выносит решения по заявлениям, поданным отдельными лицами, группами лиц или одним или несколькими государствами-членами Совета Европы, в которых утверждается о нарушениях прав, изложенных в ЕКПЧ. Хотя решения ЕСПЧ имеют юридическую силу для соответствующих государств-членов Совета Европы, его судебная практика также может служить важным руководством для других стран относительно объема и применения гражданских и политических прав. Суд Европейского Союза (СЕС) интерпретирует законодательство ЕС,

2 Всеобщая декларация прав человека, 10 декабря 1948 г., Резолюция Генеральной Ассамблеи ООН. 217 A (III).

3 Международный Пакт о Гражданских и Политических Правах, 16 декабря 1966 г., Резолюция Генеральной Ассамблеи ООН. 2200A (XXI), вступил в силу 23 марта 1976 г.

4 Конвенция о Защите Прав Человека и Основных Свобод от 4 ноября 1950 г., СДСЕ № 5, вступила в силу 3 сентября 1953 г.

5 Хартия Европейского Союза об Основных Правах, 18 декабря 2000 г., ОЖЕС 2012/C 326/02, вступила в силу 1 декабря 2009 г.

6 УВКПЧ (без даты), Комитет по правам человека, доступно по адресу https://www.ohchr.org/en/treaty-bodies/ccpr.

7 Факультативный Протокол к Международному Пакту о Гражданских И Политических Правах, 16 декабря 1966 г., Резолюция Генеральной Ассамблеи ООН. 2200A (XXI), вступил в силу 23 марта 1976 г.

включая Хартию Основных Прав Европейского Союза.[8] Его решения имеют обязательную юридическую силу для государств-членов ЕС.

Другие органы имеют консультативный мандат по усилению продвижения и защиты прав человека. На международном уровне к ним относятся Совет ООН по правам человека[9] и различные специальные процедуры, созданные при нем, включая специальных докладчиков, специальных представителей, независимых экспертов и рабочие группы.[10] Кроме того, Управление Верховного комиссара ООН по правам человека (УВКПЧ) продвигает и защищает все права человека посредством исследований, образования, пропаганды и помощи правительствам.

Уважение прав человека и основных свобод также является ключом к всеобъемлющей концепции безопасности ОБСЕ. С момента подписания Хельсинкского Заключительного акта в 1975 году, Совещание по Безопасности и Сотрудничеству в Европе (СБСЕ), а затем и ОБСЕ накопили значительный объем обязательств в области прав человека, демократии, верховенства закона и национальных меньшинств, принятых различными директивными органами СБСЕ, а затем и ОБСЕ.[11] Многие из этих обязательств имеют отношение к работе органов уголовного правосудия, в том числе в контексте расследования и преследования киберпреступлений и других преступлений, включающих электронные доказательства. Хотя обязательства ОБСЕ не носят характер юридически обязывающих договоров в соответствии с международным правом, они представляют собой важные политически обязывающие обязательства, принятые консенсусом всеми государствами-участниками.

2.3 НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО И УЧРЕЖДЕНИЯ ПО ПРАВАМ ЧЕЛОВЕКА

Чтобы быть эффективными, международные стандарты в области прав человека должны внедряться и защищаться национальным законодательством, политикой и практикой. Обеспечение того, чтобы национальная законодательная база отражала и включала международные стандарты в области прав человека, является, прежде всего, задачей законодателей. Обычно защита прав человека интегрирована в конституцию страны и другие сквозные или отраслевые законы. Процессуальные права обычно включаются в уголовно-процессуальные кодексы посредством различных условий и гарантий.

Национальное законодательство в области прав человека интерпретируется национальными судами, в том числе, если речь идет о конституционных положениях, конституционными судами. В национальном прецедентном праве содержатся важные рекомендации о том, как внутреннее законодательство в области прав человека следует применять на практике.

8 Протокол 3 к Статуту Суда Европейского Союза, 16 декабря 2004 г., ОЖЕС 310/210.

9 Совет ООН по правам человека, 15 марта 2006 г., Резолюция Генеральной Ассамблеи ООН. 60/251, заменивший Комиссию ООН по Правам Человека 16 июня 2006 г.

10 Совет ООН по правам человека (без даты), Специальные процедуры Совета по Правам Человека, доступно по адресу: https://www.ohchr.org/EN/HRBodies/SP/Pages/ Welcomepage.aspx.

11 Подробный обзор см. в ОБСЕ/БДИПЧ, Обязательства ОБСЕ в области Человеческого Критерия: Том 1 – Тематический сборник, 4-е издание (Варшава, 2023 г.); и ОБСЕ/БДИПЧ, Обязательства ОБСЕ в области Человеческого Критерия: Том 2 – Хронологический сборник, 4-е издание (Варшава, 2023 г.).

Национальные органы по правам человека (такие как национальные правозащитные учреждения или омбудсмены) также выполняют важную функцию по защите прав человека на национальном уровне, предоставляя консультации и действуя в отдельных случаях нарушений. Кроме того, гражданское общество, включая неправительственные организации (НПО) и средства массовой информации, играют решающую роль в повышении осведомленности о правах человека, отстаивая общественные интересы и способствуя общественному контролю за соблюдением прав человека.

3

Права человека и расследования киберпреступлений

3.1 ПОЧЕМУ ПРАВА ЧЕЛОВЕКА ВАЖНЫ В КОНТЕКСТЕ РАССЛЕДОВАНИЙ КИБЕРПРЕСТУПЛЕНИЙ?

Государственные субъекты, в том числе министерства и специалисты по уголовному правосудию, несут основную ответственность за уважение, защиту и соблюдение прав человека. Это включает в себя обеспечение реализации на практике стандартов прав человека, включенных в международные конвенции, стороной которых является государство. Обязательства государств распространяются на все аспекты реагирования уголовного правосудия на киберпреступность. Они включают в себя обеспечение того, чтобы внутреннее законодательство соответствовало правам человека и содержало необходимые процессуальные гарантии, информирование специалистов-практиков об их ответственности за соблюдение прав человека, мониторинг реализации прав человека на практике и предоставление людям возможностей для обращения за помощью в случае нарушения их прав человека.

Помимо ответственности по международному праву, защита прав человека имеет явные практические преимущества для расследования киберпреступлений и работы органов уголовного правосудия в целом, как показывают следующие примеры.

Во-первых, уважение прав человека важно для получения необходимых доказательств из-за рубежа и обеспечения международного сотрудничества между органами уголовного правосудия и частными компаниями. Несоблюдение стандартов прав человека может, например, стать причиной отказа в просьбе о взаимной правовой помощи. Для многих государств необходимым условием предоставления официальной помощи является то, что запрашивающее государство гарантирует справедливое судебное разбирательство и уважение прав человека, закрепленных в международных и региональных документах по правам человека. Частные компании, в том числе крупные поставщики услуг, такие как Microsoft, Google или Meta, также учитывают ситуацию с правами человека в государстве при принятии решения о том, как реагировать на запрос о сохранении или передаче данных для использования в уголовном расследовании.[12]

Во-вторых, несоблюдение прав человека и процессуальных гарантий при проведении расследования может привести к признанию доказательств недопустимыми в суде. Это особенно актуально при расследованиях киберпреступлений, которые могут включать интрузивные методы расследования и необходимость полагаться на нестабильные электронные доказательства. Таким образом, обеспечение соблюдения стандартов прав человека на протяжении всего расследования увеличивает вероятность успешного осуждения преступников.

В-третьих, органы уголовного правосудия, которые не проводят расследования киберпреступлений в соответствии со стандартами прав человека, могут быть подвергнуты процедурам подачи жалоб или судебным искам. Например, отдельные сотрудники полиции и менеджеры могут быть подвергнуты административным или уголовным санкциям, если они причастны к расследованиям, которые, как будет установлено, проводились незаконно. Это

12 См., например, УНП ООН, Практическое Руководство по Запросу Электронных Доказательств из Других Стран (Вена, 2021 г.), стр. 12. 18, 37

может оказать разрушительное воздействие на моральный дух и репутацию властей, а также на вероятность добиться осуждения лиц, совершивших киберпреступления.

Наконец, нарушения прав человека в ходе расследований киберпреступлений могут привести к потере общественного доверия к органам уголовного правосудия, что затрудняет достижение уровня сотрудничества, необходимого для эффективной борьбы с киберпреступностью. Отсутствие доверия не только подрывает действия по предотвращению киберпреступности, но также может негативно повлиять на готовность общественности сообщать о таких преступлениях или давать свидетельские показания.

Поэтому уважение и защита прав человека в контексте расследований киберпреступлений имеет важное значение для обеспечения того, чтобы усилия по борьбе с киберпреступностью были устойчивыми, эффективными и в конечном итоге успешными.

3.2 ПРАВА ЧЕЛОВЕКА, КОТОРЫЕ ОСОБЕННО СТРАДАЮТ В ВРЕЗУЛЬТАТЕ РАССЛЕДОВАНИЙ КИБЕРПРЕСТУПЛЕНИЙ

Расследования киберпреступлений могут повлиять на реализацию многочисленных прав человека. Следующие права человека особенно актуальны в контексте расследований киберпреступлений:

- Право на неприкосновенность частной жизни;
- Право на справедливое судебное разбирательство;
- Право на свободу выражения мнений/слова;
- Право на защиту собственности.

Полный текст статей МПГПП и ЕКПЧ, устанавливающих эти права, можно найти в Дополнении 1.

Другие права, которые могут быть прямо или косвенно затронуты расследованиями киберпреступлений, включают: недискриминацию, свободу религии или убеждений, свободу ассоциаций, право на свободу и права ребенка.

ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Право на неприкосновенность частной жизни закреплено в статье 17 МПГПП и статье 8 ЕКПЧ, где оно упоминается как право на уважение частной и семейной жизни. В дополнение к своим обязательствам по этим документам, государства-участники ОБСЕ обязались в Московском документе 1991 года обеспечить право на защиту частной и семейной жизни, места жительства, переписки и электронных коммуникаций, а также на предотвращение

незаконного вторжения в сферу личности.[13]

Право на неприкосновенность частной жизни играет важную роль в демократическом обществе. Оно включает в себя защиту конфиденциальности сообщений, телефонных звонков и электронной почты, а также защиту от незаконного и ненужного государственного надзора. Для реализации права на неприкосновенность частной жизни государства имеют как позитивное обязательство (защищать это право), так и негативное обязательство (воздерживаться от вмешательства в это право). Право на неприкосновенность частной жизни также позволяет людям предпринимать шаги для защиты своей частной жизни, например, используя технологии повышения конфиденциальности, такие как шифрование и виртуальные частные сети (VPN).

Важность права на неприкосновенность частной жизни заключается в том, что оно рассматривается, как некий «шлюз». Без уважения частной жизни полное пользование широким спектром других прав оказывается под угрозой, например, право выражать свое мнение, общаться с другими людьми или свободно участвовать в общественной и политической жизни.[14]

Защита данных является важной частью права на неприкосновенность частной жизни, как это признано Комитетом ООН по правам человека[15] и ЕСПЧ.[16] Ряд международных и региональных документов содержат конкретные принципы защиты данных, которые необходимо соблюдать для обеспечения полного соблюдения права на неприкосновенность частной жизни.[17] К ним относятся, например, принципы, согласно которым персональные данные, подвергающиеся автоматической обработке, должны:

- Быть получены и обработаны честным и законным путем;
- Храниться для определенных и законных целей (ограничение цели);
- Быть адекватными, актуальными и не чрезмерными (минимизация данных);
- Храниться не дольше, чем требуется (ограниченное хранение данных);
- Быть защищены от несанкционированного доступа.

Как и многие другие права, право на неприкосновенность частной жизни не является абсолютным и может быть ограничено при определенных обстоятельствах. Любое вмешательство в осуществление этого права должно быть основано на законе, необходимом в демократическом обществе, например, для защиты национальной или общественной

13 ОБСЕ/СБСЕ, Московский документ 1991 г., 3 октября 1991 г., СБСЕ/CHDM.49/вер..1, п. 24; ОБСЕ/СБСЕ, Копенгагенский документ 1990 г., 27 июня 1990 г., CSCE/CHDC.43, пункт 26, примечание 16

14 УВКПЧ (2018 г.), Всеобщая Декларация Прав Человека 70: 30 статей по 30 статьям, статья 12, доступно по адресу: https://www.ohchr.org/en/press- releases/2018/11/universal-declaration-human-rights-70-30-articles-30-articles-article-12.

15 См. Комитет ООН по Правам Человека, Замечание общего порядка № 16 к статье 17, Право на неприкосновенность частной жизни, 8 апреля 1988 г., Док. HRI/GEN/1/Вер.1, стр. 21–23, пункт 10.

16 ЕСПЧ, Руководство по Статье 8 Европейской Конвенции по Правам Человека: Право на уважение частной и семейной жизни, жилища и переписки (Страсбург, 2022 г.); см. также ЕСПЧ (2023), Информационный Бюллетень о Защите Персональных Данных, доступный по адресу https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

17 См., например, Конвенцию о Защите Частных Лиц в отношении Автоматической Обработке Персональных Данных, 28 января 1981 г., CETS (серия договоров Совета Европы) № 108; Хартия ЕС об Основных Правах, Статья 8 в сочетании с Общим Регламентом ЕС по Защите Данных, 27 апреля 2016 г., Рег. (ЕС) 2016/679 о Защите Физических Лиц в Отношении Обработки Персональных Данных и Свободного Перемещения Таких Данных.

безопасности или для предотвращения беспорядков или преступлений, и должно быть соразмерным (см. также раздел 3.3). Например, компетентный судебный орган может разрешить полиции перехватывать сообщения человека, если у полиции есть разумные основания полагать, что это лицо собирается совершить серьезное преступление.

ПРАВО НА СПРАВЕДЛИВОЕ СУДЕБНОЕ РАЗБИРАТЕЛЬСТВО

Право на справедливое судебное разбирательство является ключевым элементом защиты прав человека и служит процессуальным средством защиты верховенства закона.[18] И статья 14 МПГПП, и Статья 6 ЕКПЧ устанавливают ряд отдельных требований, которые вместе составляют право на справедливое судебное разбирательство, в том числе для всех обвиняемых в совершении уголовного преступления:[19]

- Имеют право на справедливое и публичное разбирательство дела независимым и беспристрастным судом;
- Должны считаться невиновным, пока его вина не будет доказана в соответствии с законом;
- Должны иметь достаточно времени и возможностей для подготовки своей защиты;
- Должны иметь возможность защищать себя лично или через выбранного ими самими адвоката;
- Дело должно быть рассмотрено в разумные сроки без неоправданной задержки.

Определенные элементы права на справедливое судебное разбирательство могут быть ограничены при определенных условиях. Другие – такие как презумпция невиновности, право на слушание дела компетентным, независимым и беспристрастным судом, а также требование справедливости суда в целом – считаются абсолютными и не могут быть ограничены ни при каких обстоятельствах.[20]

ПРАВО НА СВОБОДУ ВЫРАЖЕНИЯ

Свобода выражения мнения, закрепленная в статье 19 МПГПП и статье 10 ЕКПЧ, является одной из важнейших основ демократического общества. Она включает право искать, получать и распространять информацию и идеи любыми средствами, независимо от границ и без вмешательства со стороны государственных властей. Важно отметить, что свобода выражения мнений распространяется не только на информацию и идеи, которые воспринимаются положительно, но и на те, которые могут оскорбить или обеспокоить.[21]

---

18 См. Комитет ООН по Правам Человека, Замечание Общего Порядка № 32 к Статье 14: Право на равенство перед судами и трибуналами и на справедливое судебное разбирательство, 23 августа 2007 г., Док. ООН. CCPR/C/GC/32, пункт 2.

19 ЕСПЧ, Руководство по статье 6 Европейской Конвенции по Правам Человека: Право на справедливое судебное разбирательство (уголовная ответственность) (Страсбург, 2022 г.).

20 См. Комитет ООН по Правам Человека, Замечание общего порядка № 32 к статье 14: Право на равенство перед судами и трибуналами и на справедливое судебное разбирательство, 23 августа 2007 г., Док. ООН. CCPR/C/GC/32, пункт 6, 19.

21 Департамент СЕ по исполнению решений Европейского суда по правам человека, Тематический информационный бюллетень: Свобода выражения мнений, апрель 2021 г., доступно по адресу https://rm.coe.int/thematic-factsheet-freedom-expression-eng/1680a235d0

Государства-участники ОБСЕ подтвердили, что «каждый будет иметь право на свободу выражения мнений, включая право на общение» и «свободу придерживаться своих убеждений, а также получать и распространять информацию и идеи без вмешательства со стороны государственных властей и независимо от государственных границ».[22]

Свобода выражения мнения может подлежать исключениям в ограниченных обстоятельствах, например, для защиты национальной безопасности или общественного порядка или для предотвращения беспорядков или преступлений. Прецедентное право подчеркивает, что эти исключения следует толковать узко. Это помогает избежать чрезмерного вмешательства и так называемого «сдерживающего эффекта», когда люди подвергают себя самоцензуре из страха подвергнуться уголовному преследованию (см. вставку 4).

Интернет создал новые возможности для людей реализовать свое право на свободу выражения мнения, обмениваясь информацией очень широко и с беспрецедентной скоростью. Благодаря своей доступности и способности хранить и передавать огромные объемы информации Интернет играет важную роль в улучшении общественного доступа к новостям и содействии распространению информации.[23] Эти преимущества, однако, сопровождаются рядом опасностей, в частности, тем, что незаконные высказывания, в том числе высказывания, разжигающие ненависть, и высказывания, подстрекающие к дискриминации, вражде или насилию, могут распространяться по всему миру за считанные секунды и часто остаются постоянно доступными в Интернете.[24]

Как и в офлайн мире, государства обязаны обеспечить, чтобы любые ограничения на выражение мнения в Интернете были **предусмотрены законом, были необходимыми и соразмерными.**[25]

ПРАВО НА ЗАЩИТУ СОБСТВЕННОСТИ

ЕКПЧ устанавливает, что люди – и компании – имеют право владеть собственностью, которая принадлежит им по закону. Сюда входят физические объекты, которыми человек владеет, финансовые ресурсы, такие как банковские счета. депозиты и акции, а также интеллектуальная собственность.[26] Собственность также включает в себя виртуальные активы, такие как криптовалюты.

Государства не могут лишить отдельных лиц или компании их собственности, если это не отвечает общественным интересам и не соответствует условиям, изложенным в законе.

22 СБСЕ/ОБСЕ, Копенгагенский документ 1990 г., 27 июня 1990 г., CSCE/CHDC.43, параграф 9.1

23 См., например, ЕСПЧ, Delfi AS против Эстонии [БП], 10 октября 2013 г., № 64569/09, § 133; ЕСПЧ, Times Newspapers Ltd (№ 1 и 2) против Соединенного Королевства, 10 марта 2009 г., № 3002/03 и 23676/03, § 27.

24 См., например. , ЕСПЧ, Delfi AS против Эстонии [БП], 10 октября 2013 г., № 64569/09, § 110; ЕСПЧ, Аннен против Германии, 20 сентября 2018 г., № 3682/10, § 67

25 УВКПЧ (без даты), Информационный бюллетень о свободе мнений и их выражения, доступен по адресу https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/Factsheet_1.pdf.

26 Департамент исполнения решений Европейского суда по правам человека Совета Европы, Тематический информационный бюллетень по защите собственности, июнь 2022 г., доступен по адресу https://rm.coe.int/thematic-factsheet-protection-of-property-eng/1680a6f07f

3.3 ПРИНЦИПЫ ЗАКОННОСТИ, НЕОБХОДИМОСТИ И СОРАЗМЕРНОСТИ

Большинство прав человека, включая право на неприкосновенность частной жизни и свободу выражения мнений, не являются абсолютными и могут быть ограничены при определенных обстоятельствах. В международном праве в области прав человека существует устоявшийся принцип, согласно которому любые подобные ограничения права должны быть предусмотрены законом, являться необходимыми и соразмерными.

Принцип **законности** требует, чтобы любая мера, ограничивающая какое-либо право, имела основу в национальном законодательстве. Эта правовая основа должна быть доступной для тех, кто может быть затронут, и достаточно ясной, чтобы адекватно информировать людей об обстоятельствах и условиях, при которых государственные органы имеют право прибегнуть к мерам, затрагивающим их права. Законодательство должно содержать адекватные гарантии против произвольного применения и не должно предоставлять чрезмерную свободу действий должностным лицам, которым поручено его применение.

Принцип **необходимости** состоит из двух элементов. Во-первых, любое ограничение права **должно преследовать законную цель**. Некоторые права определяют эти законные цели. Например, ЕКПЧ допускает ограничение права на уважение частной и семейной жизни и права на свободу выражения мнения в интересах национальной безопасности, общественной безопасности или предотвращения беспорядков или преступлений, среди других целей. Во-вторых, ограничение не должно выходить за рамки того, что необходимо для достижения этой цели. Иными словами, ограничение не должно быть слишком широким или длиться дольше, чем это необходимо для достижения цели, т. е. оно должно быть узко определенным и иметь ограниченную продолжительность.

Принцип соразмерности означает, что любая мера, нарушающая какое-либо право, должна быть соразмерна преследуемой законной цели. Для этого необходимо продемонстрировать, что не существует менее ограничительных мер, что сущность права сохраняется и что ограничение права не носит дискриминационного характера. Существование и эффективное применение процессуальных гарантий является ключевым аспектом определения того, является ли ограничение права соразмерным.

4

Процессуальные полномочия, касающиеся киберпреступлений, и гарантии прав человека

4.1 ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Расследование и успешное судебное преследование киберпреступлений и других преступлений, связанных с электронными доказательствами, ставит особые задачи перед практиками уголовного правосудия. Во-первых, поскольку для совершения киберпреступлений не требуется физическое присутствие или близость к жертве, преступники могут находиться под другой национальной юрисдикцией, чем их жертвы. Действительно, преступников может быть несколько, каждый из которых находится в отдельной юрисдикции.

Во-вторых, преступники все чаще скрывают свою личность, используя такие сервисы, как Tor или виртуальные частные сети (VPN), которые позволяют им использовать интернет-ресурсы с относительной анонимностью. Они также используют различные инструменты шифрования для защиты своих данных и связи, а также для сокрытия своей преступной деятельности. Операторы мобильных сетей используют такие технологии, как Трансляция Сетевых Адресов, которые затрудняют идентификацию пользователей Интернета по их адресам интернет-протокола (IP). Все это делает установление виновных в преступных действиях в киберпространстве все более сложной задачей.

Кроме того, большинство доказательств киберпреступлений – и, по сути, важнейших доказательств многих офлайн-преступлений – находится в форме цифровых данных, которые по своей природе изменчивы и могут быть легко перемещены, изменены или удалены. Более того, данные часто хранятся в «облаке» на серверах, которые могут находиться в одной или нескольких иностранных юрисдикциях. Различные частные поставщики услуг могут иметь доступ к цифровым следам и электронным доказательствам, связанным с расследуемым преступлением, или контролировать их.

Это означает, что расследование киберпреступлений часто требует интенсивного международного сотрудничества – как с органами уголовного правосудия из других стран, так и с частными организациями, такими как транснациональные поставщики услуг. Определенные виды киберпреступлений, например программы-вымогатели или компрометация деловой электронной почты, также требуют сочетания финансовых и цифровых расследований.

4.2 ПРОЦЕССУАЛЬНЫЕ ПОЛНОМОЧИЯ И ПОЛНОМОЧИЯ ПО МЕЖДУНАРОДНОМУ СОТРУДНИЧЕСТВУ В ОТНОШЕНИИ КИБЕРПРЕСТУПЛЕНИЙ

Особенности расследования киберпреступлений и других преступлений, связанных с электронными доказательствами, вызывают ряд вопросов, таких как:

- Кто использует/использовал конкретный IP-адрес (статический или динамический) в данный момент времени?
- Кто использует/использовал конкретный адрес электронной почты или псевдоним в

блоге или социальной сети?

- Каковы условия хранения данных о трафике, включая динамические IP-адреса, поставщиками услуг и при каких условиях субъекты уголовного правосудия могут получить такие данные?
- Как получить данные об учетной записи пользователя и/или данные о контенте от международного поставщика услуг, базирующегося за рубежом
- Как получить доступ, изъять и исследовать содержимое электронных сообщений (например, электронной почты или приложений для обмена сообщениями) или данных с различных электронных устройств, в том числе зашифрованных?
- Как отслеживать (онлайн) зашифрованную связь?
- Как обнаружить и отследить онлайн - электронные денежные переводы и транзакции с криптовалютой и ценностями?
- Как конфисковать криптовалюты или другие виртуальные активы?

Хотя расследование киберпреступлений следует тем же процессуальным правилам, что и любое другое уголовное расследование, как это определено в соответствующем национальном законодательстве, получение ответов на эти вопросы может дополнительно потребовать от следователей доступа к определенным процессуальным полномочиям.

Конвенция Совета Европы о киберпреступности 2001 года, также известная как Будапештская конвенция, является первым международным договором о преступлениях, совершаемых через Интернет и другие компьютерные сети.[27] Она открыта для ратификации/присоединения государств, не являющихся членами Совета Европы, и была ратифицирована большим количеством государств в разных регионах, включая большинство государств-участников ОБСЕ. Конвенция предусматривает конкретные полномочия, касающиеся сбора и использования электронных доказательств, а также международного сотрудничества в контексте расследований киберпреступлений. Эти полномочия распространяются как на киберзависимые, так и на киберперступления, а также на любые другие преступления, включающие электронные доказательства.

Конвенция требует от государств-участников интегрировать в свое внутреннее законодательство ряд следственных полномочий в целях уголовных расследований или разбирательств. Это:

- Ускоренное сохранение хранящихся компьютерных данных (Статья 16);
- Ускоренное сохранение и частичное раскрытие данных о трафике (Статья 17);
- Судебный приказ о предоставлении информации (Статья ст. 18);
- Обыск и изъятие хранящихся компьютерных данных (Статья 19);
- Сбор данных о трафике в режиме реального времени (Статья 20);
- Перехват данных контента (Статья 21).

Конвенция также содержит положения, которые составляют основу международного

27 Конвенция о киберпреступности от 23 ноября 2001 г., СДСЕ № 185, вступила в силу 1 июля 2004

сотрудничества в борьбе с киберпреступностью. К ним относятся:

- Спонтанная информация (Статья 26);
- Ускоренное сохранение хранящихся компьютерных данных (Статья 29);
- Ускоренное раскрытие сохраненных данных о трафике (Статья 30);
- Взаимная помощь в отношении доступа к хранящимся компьютерным данным (Статья 31);
- Взаимная помощь в сборе данных о трафике в режиме реального времени (Статья 33);
- Взаимная помощь в отношении перехвата данных контента (Статья 34).

Кроме того, в мае 2022 года Сторонами основной конвенции был открыт для подписания Второй дополнительный протокол к Будапештской конвенции. Он вводит новые процедуры для расширения прямого сотрудничества с поставщиками и организациями в других договаривающихся сторонах, а также для оптимизации международного сотрудничества между органами по раскрытию хранящихся компьютерных данных, в том числе в отношении экстренной взаимопомощи.[28]

Эти полномочия предоставляют специалистам уголовного правосудия важные инструменты для успешного обнаружения, расследования и преследования уголовных преступлений, совершенных с использованием компьютеров. Однако их применение может нарушать права человека и основные свободы. Следователи, использующие эти полномочия, несут ответственность за обеспечение того, чтобы любые ограничения прав человека были основаны на законе, необходимы и соразмерны.

4.3 ГАРАНТИИ ПРАВ ЧЕЛОВЕКА, СВЯЗАННЫЕ С КИБЕРПРЕСТУПНОСТЬЮ

Хотя положения международных и региональных стандартов в области прав человека применяются ко всем уголовным расследованиям, Конвенция Совета Европы по киберпреступности стремится применять их конкретно к расследованиям киберпреступлений и других преступлений, включающих электронные доказательства.

Статья 15 Конвенции требует, чтобы каждая Сторона установила в своем внутреннем законодательстве определенные условия и гарантии, которые должны применяться при использовании процессуальных полномочий Конвенции (см. вставку 2).

Статья 15 не определяет эти гарантии подробно, а вместо этого ссылается на обязательства государств по ЕКПЧ и МПГПП как на источник гарантий. Это гарантирует, что данное положение учитывает существенные различия, существующие в различных правовых нормах относительно способов реализации гарантий.

28 Второй дополнительный протокол к Конвенции о киберпреступности о расширении сотрудничества и раскрытии электронных доказательств, 17 ноября 2021 г., CDCE No. 224.

ВСТАВКА 2 СТАТЬЯ 15 КОНВЕНЦИИ ПО КИБЕРПРЕСТУПНОСТИ– УСЛОВИЯ И ГАРАНТИИ

1. Каждая Сторона обеспечивает, чтобы установление, реализация и применение полномочий и процедур, предусмотренных настоящим Разделом, подчинялись **условиям и гарантиям**, предусмотренным ее внутренним законодательством, которые обеспечивают адекватную защиту прав и свобод человека, включая права, вытекающие из обязательств, которые она взяло на себя в соответствии с Конвенцией Совета Европы о Защите Прав Человека и Основных Свобод 1950 года, Международным пактом Организации Объединенных Наций о Гражданских и Политических правах 1966 года и другими применимыми международными документами по правам человека, и которые должны **включать принцип пропорциональности**.
2. Такие условия и гарантии должны, в зависимости от обстоятельств, с учетом характера соответствующей процедуры или полномочия, среди прочего, **включать судебный или иной независимый надзор, основания, оправдывающие применение, а также ограничение объема и продолжительности таких полномочий или процедуры.**
3. В той мере, в которой это соответствует общественным интересам, в частности разумному отправлению правосудия, каждая Сторона должна учитывать влияние полномочий и процедур, предусмотренных в настоящем разделе, **на права, обязанности и законные интересы третьих сторон.**

Статья 15 выделяет следующие условия и гарантии:

- Принцип пропорциональности;
- Наличие судебного или иного независимого надзора;
- Необходимость указать четкие основания для подачи заявления;
- Ограничение объема и продолжительности полномочий или процедур – в зависимости от полномочий и конкретного случая;
- Необходимость учитывать влияние полномочий на права, обязанности и законные интересы третьих сторон.

На практике это означает, что офицеры, расследующие предполагаемые киберпреступления, должны осознавать влияние, которое их действия оказывают на права, изложенные в международных договорах по правам человека.

Принцип пропорциональности предполагает уравновешивание различных и конкурирующих следственных мер применительно к конкретному расследованию киберпреступлений. Это означает, что вмешательство в права человека должно быть сведено к минимуму и что следователи должны использовать наименее интрузивные средства для достижения своей цели.

Такое уравновешивание возможно только в том случае, если в национальном законодательстве существуют разные – менее и более интрузивные – варианты. Например, существует два возможных способа получить доступ к данным, хранящимся у поставщика услуг. Один из них — использовать охранное обязательство и судебный приказ о предоставлении информации; другой – использовать обыск и изъятие для получения

данных. Как правило, механизм, использующий охранное обязательство и судебный приказ о предоставлении информации менее интрузивный, чем механизм обыска и изъятия, который требует доступа к большему набору данных и обычно проводится на месте. Следователи должны четко обосновать, почему они используют более интрузивный метод расследования, когда доступны менее интрузивные методы.

В любом случае следователи должны предоставить достаточные основания для того, чтобы суд или независимый орган мог санкционировать применение интрузивных следственных мер. Судебные или другие независимые органы должны давать разрешение на использование таких полномочий после тщательной оценки в каждом конкретном случае. В зависимости от тяжести уголовного преступления в соответствии с национальным законодательством могут потребоваться особые условия. Специалисты по уголовному правосудию также должны обеспечить, чтобы интрузивные следственные полномочия не использовались дольше, чем это строго необходимо для эффективного расследования дела.

Кроме того, Второй дополнительный протокол к Будапештской конвенции[29] содержит подробную статью 14 о защите персональных данных. Это положение применяется к новым процессуальным полномочиям, предусмотренным Вторым дополнительным протоколом, и устанавливает обязательства Сторон по обеспечению того, чтобы важные аспекты прав на конфиденциальность и защиту данных, такие как цель и использование, качество и целостность данных, конфиденциальные данные, сохранение данных, автоматизированное принятие решений, безопасность данных и последующий обмен данными – поддерживаются при использовании этих полномочий.

29 Там же.

5

Применение гарантий прав человека при расследовании киберпреступлений

В этой главе рассматриваются элементы, которые следует учитывать специалистам -практикам в области уголовного правосудия, чтобы обеспечить защиту прав человека во время расследований киберпреступлений. Она во многом опирается на рекомендации, содержащиеся в судебной практике ЕСПЧ и СЕС. Это руководство актуально также для Государств, не являющихся членами Совета Европы или ЕС, поскольку оно дает конкретные примеры того, как можно обеспечить уважение прав человека при расследовании киберпреступлений. Некоторые особенно важные решения ЕСПЧ более подробно представлены в Дополнении 2.

5.1 ПРАВО НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Расследование киберпреступлений и других преступлений, связанных с электронными доказательствами, может нарушать право на неприкосновенность частной жизни, если оно:

- Использует персональные данные;
- Включает хранение и обработку данных абонентов, трафике или контенте;
- Вмешивается в конфиденциальность сообщений, например, при перехвате сообщений или данных о трафике;
- Включает тайное наблюдение, например, тайные операции по поимке преступников на онлайн-торговых площадках (Dark Web).

Существует обширная судебная практика ЕСПЧ и СЕС, касающаяся реализации права на неприкосновенность частной жизни.

ОБЪЕМ И ПРИМЕНЕНИЕ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ ПРИ РАССЛЕДОВАНИЯХ КИБЕРПРЕСТУПЛЕНИЙ

В судебной практике ЕСПЧ содержатся подробные указания относительно объема и применения права на неприкосновенность частной жизни в контексте расследований киберпреступлений. В своей прецедентной практике Суд широко определил объем права на частную и семейную жизнь, так что оно распространяется на следующее:

- Защита личной репутации, диффамация (позитивное обязательство государства в отношении обязательства поставщика услуг);
- Защита данных;
- Сбор файлов или данных службами безопасности или другими государственными органами;
- Полицейское наблюдение (в том числе в Интернете и Dark Web[30]);
- Полномочия полицейских останавливать и обыскивать;
- Посещения на дому, обыски и выемки документов;

30 Подробнее о судебной практике ЕСПЧ см.: Совет Европы, Руководство по Взаимной Правовой Помощи (Белград, 2013 г.), стр. 101.

- Перехват телекоммуникаций в контексте уголовного расследования;
- Переписка частных лиц, специалистов и компаний;
- Негласное наблюдение за гражданами и организациями;
- Сохранение данных об абонентах и трафике.[31]

Суд также подчеркнул, что право на частную и семейную жизнь налагает на государства как позитивное обязательство (защищать это право), так и негативное обязательство (воздерживаться от вмешательства в это право). Например, в деле К.У. против Финляндии Суд подчеркнул позитивное обязательство государства эффективно расследовать преступления и принять соответствующее законодательство об исключениях из обязательств поставщиков услуг сохранять конфиденциальность данных.[32] Суд подчеркнул, что, хотя свобода выражения мнений и конфиденциальность сообщений являются первоочередными соображениями, они не могут быть абсолютными. Учитывая серьезность дела, Суд постановил, что государство должно было создать правовую основу для совмещения конфиденциальности интернет-услуг с предотвращением беспорядков или преступлений и защитой прав и свобод других лиц.[33]

Как и любое вмешательство в права человека, ограничения права на неприкосновенность частной жизни должны быть предусмотрены законом, необходимы и соразмерны. Судебная практика ЕСПЧ предоставляет указания относительно того, что это означает на практике. Аналогичные принципы применяются к соответствующему положению МПГПП (статья 17).[34]

Что касается **правовой основы**, законодательство, разрешающее использование полномочий, которые вмешиваются в право на частную жизнь, должно быть доступно для тех, кто может быть затронут, и иметь достаточную ясность, чтобы оно давало «лицам адекватное указание на обстоятельства и условия, при которых власти имеют право прибегнуть к мерам, затрагивающим их права, предусмотренные Конвенцией».[35] Это означает, что различные процессуальные полномочия, доступные следователям (например, положения о запросах сохранять или производить данные, обеспечивать сбор данных о трафике в режиме реального времени или осуществлять поиск и изъятие компьютерных данных, объектов или документов) должны быть четко определены в национальном законодательстве.

Что касается **необходимости и соразмерности**, любое вмешательство должно преследовать законную цель – в данном случае расследование конкретного преступления – и ограничиваться тем, что необходимо для достижения этой цели. Это требует рассмотрения вопроса о том, доступны ли менее ограничительные альтернативные меры.

---

31 ЕСПЧ, Руководство по Статье 8 Европейской Конвенции по Правам Человека: Право на уважение частной и семейной жизни, жилища и переписки (Страсбург, 2020 г.); см. также: ЕСПЧ (2023), Информационный бюллетень о Защите Персональных Данных, доступен по адресу https://www.echr.coe.int/Documents/FS_Data_ENG. pdf; ECtHR (2022), Информационный бюллетень о массовой слежке доступен по адресу. https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.

32 ЕСПЧ, К.У. против Финляндии, 2 декабря 2008 г., № 2872/02, § 49.

33 Там же, §§ 48, 49.

34 См. Комитет ООН по Правам Человека, Замечание общего порядка МПГПП № 16: Статья 17, Право на Неприкосновенность Частной Жизни, 23 марта 1988 г., пункты 4, 5.

35 ЕСПЧ, Фернандес Мартинес против Испании [БП], 12 июня 2014 г., № 56030/07, § 117.

Кроме того, законодательство должно содержать адекватные гарантии против произвольного применения и не предоставлять чрезмерную свободу действий должностным лицам, которым поручено его применение. Это означает, что законодательство, устанавливающее процессуальные полномочия для использования при расследовании киберпреступлений, должно:

- Требовать наличия достаточных оснований для оправдания использования отдельных процессуальных полномочий;
- Оговорить, что данная мера подлежит судебному или иному независимому надзору, особенно если она включает в себя особо агрессивные действия, такие как перехват данных контента;
- Установить сроки хранения данных;
- Исключить (или специально защитить) конфиденциальные данные от судебных приказов о предоставлении информации, а также обыска и изъятия.

Примеры применения принципа соразмерности можно найти в делах ЕСПЧ, связанных с перехватом данных контента, что является наиболее интрузивным процессуальным полномочием, изложенным в Конвенции Совета Европы о Киберпреступности. ЕСПЧ постановил, что, в частности, правовые положения, регулирующие перехват сообщений, должны предусматривать адекватные и эффективные гарантии против произвола и риска злоупотреблений, присущих любой системе тайного наблюдения, и определил конкретные условия и гарантии тайного наблюдения за перепиской (см. раздел «Тайное наблюдение при расследовании киберпреступлений» ниже).[36]

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Еще один важный аспект права на неприкосновенность частной жизни касается права на защиту персональных данных, которое закреплено в ряде международных и региональных правовых инструментов (см. вставку 3). Принципы защиты данных должны учитываться при регулировании полномочий полиции, а также при сборе и обработке персональных данных в контексте уголовных расследований. Эти принципы включают в себя:[37]

- **Законность:** персональные данные должны обрабатываться законно либо с согласия субъекта данных, либо на другом законном основании, предусмотренном законодательством о защите данных.
- **Справедливость:** персональные данные должны обрабатываться справедливо, а субъекты данных должны быть проинформированы о риске.
- **Прозрачность:** персональные данные должны обрабатываться прозрачным образом. Субъекты данных должны быть проинформированы о том, как используются их данные.
- **Ограничение цели:** любая обработка персональных данных должна осуществляться

36 ЕСПЧ, Роман Захаров против России [БП], 4 декабря 2015 г., № 47143/06; ЕСПЧ, Брейер против Германии, 30 января 2020 г., № 50001/12; сравните также с решениями СЕС о сохранении данных.

37 Агентство ЕС по Основным Правам и Совет Европы, Справочник по Европейскому Законодательству о Защите Данных (Люксембург, 2018 г.).

для конкретной, четко определенной цели. Любая дополнительная обработка должна быть совместима с первоначальной целью.

- **Минимизация данных:** обработка данных должна быть ограничена тем, что необходимо для достижения законной цели.
- **Точность данных:** контроллеры данных должны обеспечивать точность и актуальность персональных данных, а также принимать меры по удалению или исправлению неточных данных.
- **Ограничение срока хранения:** персональные данные не должны храниться дольше, чем необходимо, и должны быть удалены или анонимизированы, как только они больше не нужны для целей, для которых они были собраны.
- **Безопасность данных (целостность и конфиденциальность):** при обработке персональных данных должны быть приняты соответствующие технические или организационные меры для защиты данных от случайного, несанкционированного или незаконного доступа, использования, изменения, раскрытия, потери, уничтожения или повреждения.
- **Подотчетность:** контроллеры и обработчики данных должны активно и постоянно реализовывать меры по обеспечению и защите данных, а также должны быть в состоянии продемонстрировать соблюдение положений о защите данных.

ВСТАВКА 3 МЕЖДУНАРОДНЫЕ И РЕГИОНАЛЬНЫЕ ПРАВОВЫЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

- **Конвенция Совета Европы о Защите Физических Лиц в отношении Автоматической Обработки Персональных Данных** от 28 января 1981 г., №. 108 (вступила в силу в 1985 г.).
- **Протокол о внесении изменений в Конвенцию Совета Европы о Защите Физических Лиц в отношении Автоматической Обработки Персональных Данных** от 10 октября 2018 г., №. 223 (еще не вступил в силу).
- **Общий Регламент ЕС по Защите Данных:** Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и свободного перемещения таких данных, а также отмены Директивы 95/46/ЕС (вступившей в силу в 2018 году).
- **Директива ЕС по Правоприменению:** Директива (ЕС) 2016/680 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения и расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, а также о свободном перемещении таких данных и об отмене Рамочного Решения Совета 2008/977/JHA (вступившего в силу в 2018 году).

ЕСПЧ уже рассмотрел широкий спектр нарушений права на частную жизнь согласно статье 8 ЕКПЧ в результате хранения, обработки и использования персональных данных. К ним

относятся: использование наблюдения с помощью GPS в уголовных расследованиях;[38] раскрытие идентифицирующей информации правоохранительным органам со стороны поставщиков телекоммуникационных услуг;[39] бессрочное хранение отпечатков пальцев, образцов клеток и профилей ДНК после уголовных разбирательств;[40] так называемое измерение или сбор данных об использовании или трафике;[41] и хранение данных о пользователях предоплаченных SIM-карт.[42]

В деле *Марпер против Соединенного Королевства* ЕСПЧ ясно дал понять, что простое хранение данных, касающихся частной жизни человека, представляет собой вмешательство в право на неприкосновенность частной жизни, закрепленное в Статье 8 ЕКПЧ. Суд постановил, что защита Персональных данных имеет основополагающее значение для осуществления права на уважение частной и семейной жизни. Внутреннее законодательство должно гарантировать предоставление соответствующих гарантий, особенно когда речь идет об автоматической обработке персональных данных. В частности, внутреннее законодательство должно гарантировать, что такие данные актуальны и не чрезмерны по отношению к целям, для которых они сохраняются, и что они хранятся в форме, позволяющей идентифицировать субъектов данных, не дольше, чем это необходимо для цели, для которой хранятся эти данные. Оно также должно предоставить адекватные гарантии того, что сохраненные персональные данные будут эффективно защищены от неправомерного использования.

СОХРАНЕНИЕ И ДОСТУП К ДАННЫМ АБОНЕНТА ИЛИ ТРАФИКА

Вопросом, непосредственно связанным с защитой персональных данных, является сохранение данных. И ЕСПЧ, и СЕС неоднократно рассматривали этот вопрос. В деле *Бенедик против Словении* ЕСПЧ установил нарушение Статьи 8 ЕКПЧ в связи с отсутствием ясности в конституционной базе Словении в отношении правовых условий доступа к данным подписчиков, относящимся к (динамическим) IP-адресам. Было обнаружено, что пользователи средств доступа в Интернет имеют законное ожидание соблюдения конфиденциальности, даже если они сознательно раскрывают свой IP-адрес публике.

В деле *Брейер против Германии* Суд не нашел нарушения Статьи 8 ЕКПЧ, поскольку условия и гарантии немецкого законодательства, регулирующие обязанность поставщиков услуг хранить персональные данные пользователей предоплаченных SIM-карт мобильных телефонов, и условия согласно которому эти данные предоставляются властям по запросу, были ясными и соразмерными. Вынося решение по этому делу, Суд подчеркнул фундаментальную важность права на неприкосновенность частной жизни и необходимость надежных гарантий для предотвращения использования персональных данных в нарушение Статьи 8.

В частности, Суд установил, что сбор имен и адресов заявителей как пользователей

38 ЕСПЧ, Узун против Германии, 2 сентября 2010 г., № 35623/05; ЕСПЧ, Бен Фаиза против Франции, 8 февраля 2018 г. No. 31446/12.

39 ЕСПЧ, К.У. против Финляндии, 2 декабря 2008 г., № 2872/02; ЕСПЧ, Бенедик против Словении, 24 апреля 2018 г., No. 62357/14.

40 40 ЕСПЧ, С. и Марпер против Соединенного Королевства [БП], 4 декабря 2008 г., 30562/04 и 30566/04.

41 ECtHR, *Malone v. the United Kingdom*, 2 August 1984, No. 8691/79; ECtHR, *Copland v. the United Kingdom*, 3 April 2007, No. 62617/00.

42 ECtHR, *Breyer v. Germany*, 30 January 2020, No. 50001/12.

предоплаченных SIM-карт представляет собой ограниченное вмешательство в их права. В рассматриваемом законе предусмотрены дополнительные гарантии, и люди также могут обратиться в независимые органы по надзору за данными для рассмотрения запросов властей о предоставлении данных и при необходимости обратиться за правовой защитой. Таким образом, в данном случае Германия не вышла за пределы своей свободы усмотрения («пределы усмотрения») при применении соответствующего закона, и сбор данных не нарушил права заявителей.

В 2006 году ЕС принял так называемую Директиву о хранении данных, которая регулировала сохранение определенных типов данных о трафике, связанных с использованием телекоммуникационных сетей (телефон, мобильный телефон и данные Интернета) в целях уголовного правосудия.[43] ТДанные о трафике отражают активность пользователя в сети, что позволяет правоохранительным органам, среди прочего, видеть источник и пункт назначения телефонных звонков в сети, данные о местоположении (в сотовой сети), а также IP-адреса пользователей услуг доступа в Интернет. В частности, в отношении киберпреступности важно отметить, что эта Директива не требовала сохранения посещенных веб-сайтов или других данных, связанных с использованием Интернета, а ограничивалась сохранением связи между IP-адресом и абонентскими данными пользователей.

В 2014 году CEC объявил Директиву о Хранении Данных несовместимой со статьями 7 и 8 Хартии Основных Прав ЕС (уважение частной и семейной жизни и защита персональных данных) и, следовательно, недействительной.[44] Суд постановил, что сохранение данных о трафике, предусмотренное Директивой, несовместимо с правом на неприкосновенность частной жизни из-за ее обобщенного характера (она требует сохранения данных пользователей, которые не подозреваются в каком-либо преступлении), отсутствие гарантий против незаконного доступа и использования данных, а также отсутствие ограничения цели (использование должно было бы применяться к тяжким преступлениям, но этому термину не было четкого определения в Директиве).

CEC далее разъяснил свою позицию в нескольких последующих делах, касающихся национального законодательства в государствах-членах ЕС, основанного на Директиве о хранении данных.[45] Суд установил, что эти национальные правовые рамки нарушают права на неприкосновенность частной жизни и защиту данных, поскольку они требуют общее и неизбирательное сохранение данных о трафике и местоположении. Он пояснил, что такое хранение данных допустимо только в том случае, если существует или прогнозируется серьезная угроза национальной безопасности, и если сохранение данных подлежит судебному или иному независимому контролю и осуществляется только в течение ограниченного периода времени. Он также заявил, что законодательство ЕС не исключает

43 *Директива 2006/24/ЕС Европейского Парламента и Совета о Хранении Данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей общественной связи, и внесение поправок в Директиву 2002/58/ЕС, 13 апреля 2006, ОЖЕС L 105/54.*.

44 CEC, Digital Rights Ireland Ltd против Министра Связи, Морских и Природных Ресурсов и Других и Kärntner Landesregierung и Других [БП], 8 апреля 2014 г., присоединился к C-293/12 и C-594/12.

45 CEC, Digital Rights Ireland Ltd против Министра Связи, Морских и Природных Ресурсов и Других и Kärntner Landesregierung и других [GC], 8 апреля 2014 г., присоединился к C-293/12 и C-594/12; Суд ЕС, Tele2 Sverige AB против Post- och telestyrelsen и Государственный Секретарь Министерства Внутренних Дел против Тома Уотсона и других [БП], 21 декабря 2016 г., присоединился к C-203/15 и C-698/15; CEC, Privacy International против Министра Иностранных Дел и по Делам Содружества и других [БП], 6 октября 2020 г., C-623/17; CEC, La Quadrature du Net и другие против Премьер-Министра и других [БП], 6 октября 2020 г., присоединился к C-511/18, C-512/18 и C-520/18; CEC, SpaceNet и Telekom Deutschland GmbH [БП], 27 октября 2022 г., присоединились к C-793/19 и C-794/19.

национального законодательства, которое предусматривает целенаправленное хранение данных о трафик и местоположении в целях обеспечения национальной безопасности, борьбы с тяжкими преступлениями и предотвращения серьезных угроз общественной безопасности, при условии наличия определенных гарантий.[46]

В то же время Суд пояснил, что законодательство ЕС разрешает общее и неизбирательное хранение данных подписчиков, т.е. данных IP-адреса и данных, касающихся гражданской идентичности пользователей, для тех же целей.[47] Необходимость судебного преследования (кибер) преступления и выявления онлайн-пользователей с преступными намерениями считалось перевешивающим вмешательство в право на неприкосновенность частной жизни, вызванное сохранением ограниченных данных об исходных IP-адресах интернет-пользователей. Это открыло возможности для принятия законодательных мер, предусматривающих превентивное сохранение IP-адресов в целях борьбы с преступностью и обеспечения общественной безопасности. Без этих данных использование Интернета может стать полностью анонимным, что будет иметь серьезные последствия для расследования и судебного преследования (кибер) преступлений.

НЕГЛАСНОЕ НАБЛЮДЕНИЕ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Различные явные и скрытые методы сбора информации представляют собой разную степень вмешательства в право на неприкосновенность частной жизни. Некоторые из этих методов, такие как использование специальных методов расследования и других скрытых следственных мер, включая наблюдение за частными помещениями или домами, перехват сообщений, использование тайных агентов и информаторов, а также доступ к банковским счетам и другой конфиденциальной информации, более подробно рассматриваются в руководстве ОБСЕ *«Права человека в ходе контртеррористических расследований»*.[48]

В отличие от целенаправленного наблюдения, которое обычно основывается на предварительном подозрении и требует разрешения суда или исполнительной власти, программы массового наблюдения не позволяют провести индивидуальную оценку соразмерности в каждом конкретном случае до принятия таких мер. Таким образом, они рискуют подорвать саму суть права на неприкосновенность частной жизни. Информация, собранная в оперативных целях, иногда также используется в качестве доказательств в уголовном процессе. Однако первоначальная цель сбора такой информации отличается от цели преследования за киберпреступления или другие преступления, связанные с электронными доказательствами, и зачастую к ее сбору применяются другие правовые правила и условия. Таким образом, при использовании такой информации в уголовном судопроизводстве явно необходима осторожность. Использование оперативной информации, полученной незаконным путем, в уголовном процессе будет противоречить

46 CEC, SpaceNet и Telekom Deutschland GmbH [БП], 27 октября 2022 г., присоединился к C-793/19 и C-794/19.

47 CEC, La Quadrature du Net и Другие против Премьер-Министра и Других [БП], 6 октября 2020 г., присоединился к C-511/18, C-512/18 и C-520/18; CEC, SpaceNet и Telekom Deutschland GmbH [БП], 27 октября 2022 г., присоединились к C-793/19 и C-794/19.

48 См. также БДИПЧ/ОБСЕ, Права Человека в Антитеррористических Расследованиях: Практическое Руководство Для Сотрудников Правоохранительных Органов (Варшава, 2013 г.).

правам человека.
ЕСПЧ установил нарушения Статьи 8 ЕКПЧ в нескольких делах, связанных с режимами тайного наблюдения, включая массовый перехват сообщений и обмен разведданными, например, *Роман Захаров против России*,[49] *Сабо и Висси против Венгрии*,[50] и *Big Brother Watch и Другие против Соединенного Королевства*.[51] Решение по делу *Висси против Венгрии* ясно показало, что судебный надзор за тайным наблюдением имеет особое значение. Независимый судебный орган должен контролировать их использование; орган, непосредственно связанный с исполнительной властью (в данном случае Министр Внутренних Дел), не отвечает этому требованию. В решении также подчеркивается проблема, касающаяся объема мер наблюдения, и считается, что гарантии, предусмотренные законодательством, недостаточно точны, эффективны и всеобъемлющи в отношении назначения, исполнения и потенциального возмещения за нарушенные права в результате таких мер.

В деле *Big Brother Watch и другие против Соединенного Королевства* Суд заявил, что любой режим массового перехвата сообщений должен подлежать «сквозным гарантиям» на национальном уровне, что означает: оценку необходимости и соразмерности принятых мер необходимо производить на каждом этапе процесса; массовый перехват должен подлежать независимому разрешению с самого начала, когда определены объект и объем операции; и что операция должна подлежать надзору и независимому контролю постфактум.[52]

В связанном с этим деле *Centrum För Rättvisa против Швеции* Суд подчеркнул недостатки внутренней правовой базы, которые не были в достаточной степени компенсированы другими гарантиями.[53] К ним относятся: отсутствие четкого правила об уничтожении перехваченных материалов, не содержащих личные данные; отсутствие обязательства учитывать неприкосновенность частной жизни лиц при принятии решения о передаче разведывательных материалов иностранным партнерам; и отсутствие эффективного контроля постфактум, например, возможности для представителей общественности получать обоснованные решения в ответ на запросы относительно массового перехвата сообщений.

Эти случаи предоставляют четкое руководство относительно некоторых мер безопасности, необходимых в контексте тайного наблюдения за коммуникациями. ЕСПЧ указал, что он ожидает установления режима независимого надзора за использованием таких скрытых и интрузивных полномочий, и что чем более независимым является санкционирующий или контролирующий орган, тем больше вероятность того, что санкционирующий и контролирующий режим будет уместным. Действительно, в деле *Класс против Германии* ЕСПЧ отметил, что судебный контроль за процедурой выдачи разрешений обеспечивает «наилучшие гарантии независимой, беспристрастной и надлежащей процедуры»[54] Использование профильных комиссаров и трибуналов на национальном уровне также

49 ЕСПЧ, Роман Захаров против России [БП], 4 декабря 2015 г., № 47143/06.

50 ЕСПЧ, Сабо и Висси против Венгрии, 12 января 2016 г., № 37138/14.

51 ЕСПЧ, Big Brother Watch and Others v. the United Kingdom [БП], 25 мая 2021 г., № 58170/13, 62322/14 и 24960/15.

52 Там же.

53 ЕСПЧ, Centrum För Rättvisa против Швеции [БП], 25 мая 2021 г., № 35252/08.

54 ЕСПЧ, Класс и другие против Германии, 6 сентября 1978 г., № 5029/71.

может удовлетворить требования Статьи 8 ЕКПЧ.

5.2 ПРАВО НА СПРАВЕДЛИВЫЙ СУД

Расследование киберпреступлений включает в себя ряд процессов, связанных с основными элементами права на справедливое судебное разбирательство, в том числе:

- Доступ к данным, хранящимся на электронных устройствах;
- Поддержание целостности изъятых электронных доказательств в контексте поиска, изъятия и управления электронными данными;
- Доступ к доказательствам и их проверка обвиняемыми в отношении изъятых электронных доказательств;
- Исключение или ограничения, налагаемые на поиск конфиденциальных сообщений и информации (например, переписки с адвокатами, медицинских записей или переписки журналистов с их источниками).

Презумпция невиновности тесно связана с правом не свидетельствовать против себя и хранить молчание.[55] Право хранить молчание особенно важно в контексте поиска и расследования электронных данных. Хотя национальное законодательство может налагать (административные) санкции на свидетеля, который не желает предоставить информацию, например пароль для доступа к компьютеру во время обыска электронных устройств, наложение санкций на подозреваемого будет проблематичным, поскольку подозреваемый может ссылаться на свои право хранить молчание. Поэтому важно, чтобы подозреваемый был проинформирован о своих правах, прежде чем его попросят добровольно предоставить пароль или код доступа к компьютеру или другому электронному устройству.[56]

Устройство хранения данных, такое как внутренний или внешний диск компьютера, USB-накопитель или мобильное устройство, может содержать огромное количество данных, которые невозможно найти во время обыска дома. Поэтому их часто приходится изымать и обыскивать на более позднем этапе.[57] Внутреннее законодательство, включая конкретные правила поиска и изъятия (или, точнее, доступа и копирования[58]) электронных доказательств, должно гарантировать сохранение права на эффективную защиту так же, как и в отношении вещественных доказательств. Соответствующие процессуальные положения включают: обязанность конфисковать электронное устройство и создать точную копию; обязанность проинформировать и пригласить подозреваемого и его адвоката на поиск изъятого электронного устройства; и обязанность раскрыть доказательства, полученные защитой. Введение таких процессуальных гарантий помогает обеспечить реализацию на практике принципа равенства процессуальных возможностей сторон в судопроизводстве и

55 ЕСПЧ, Руководство по статье 6 Европейской Конвенции по Правам Человека: Право на справедливое судебное разбирательство (уголовная ответственность) (Страсбург, 2022 г.), п. 197 и 373.

56 *Конвенция о Киберпреступности, 23 ноября 2001 г., СДСЕ № 185, статья 32(b).*

57 Совет Европы, Пояснительный Доклад к Конвенции о Киберпреступности (Будапешт, 2001 г.), § 187.

58 Там же. §§ 137, 191 и 197.

состязательности процедуры, которые являются важными компонентами справедливого судебного разбирательства.

Большой объем данных, задействованных в некоторых расследованиях, также представляет собой проблему с точки зрения раскрытия данных. Важной гарантией является обеспечение того, чтобы защита имела возможность участвовать в установлении критериев, используемых для определения того, какие данные могут иметь отношение к раскрытию.[59] Это особенно важно в случаях, когда данные хранятся в Интернете. Более того, любой отказ в разрешении защите проводить дальнейшие поиски идентифицированных или помеченных данных по делу (например, данных, полученных в результате обыска) поднимает вопрос о предоставлении адекватных возможностей для подготовки защиты.[60] По возможности защита должна быть проинформирована о критериях поиска в отношении больших наборов данных, иметь равный доступ и иметь все возможности для поиска в наборах данных соответствующих (оправдательных) данных. Привилегированный характер общения между адвокатами и их клиентами также следует уважать при поиске электронных доказательств.

Одним словом, право на справедливое судебное разбирательство требует справедливой и сбалансированной процедуры, особенно когда поиск электронных доказательств осуществляется в соответствии с критериями, установленными органами уголовного правосудия. Недопустимо исключать защиту из этого процесса, поэтому должны быть предоставлены адекватные гарантии и возможности найти оправдательные доказательства.

Наконец, концепция «органа суда, созданного на основании закона», вместе с концепциями «независимости» и «беспристрастности» органа суда составляют часть «институциональных требований» Статьи 6 ЕКПЧ. В прецедентном праве ЕСПЧ существует очень тесная взаимосвязь между этими концепциями.[61] Хотя каждая из них служит определенным целям в качестве отдельных гарантий справедливого судебного разбирательства, существует общая нить, проходящая через институциональные требования, поскольку они руководствуются целью поддержания фундаментальных принципов верховенства закона и разделения полномочий.[62]

В деле *Сабо и Висси против Венгрии* ЕСПЧ подтвердил связь между независимостью органа судебного надзора и правом на справедливое судебное разбирательство.[63] Аналогичным образом, СЕС определил надзор за механизмами хранения данных как важную гарантию в своей прецедентной практике.

59 ЕСПЧ, Сигурдур Эйнарссон и другие против Исландии, 4 июня 2019 г., № 39757/15, § 90; см. также ЕСПЧ, Рук против Германии, 25 июля 2019 г., № 1586/15, §§ 67, 722.

60 ЕСПЧ, Сигурдур Эйнарссон и другие против Исландии, 4 июня 2019 г., № 39757/15, § 91; см. также: Совет Европы, Пояснительный Доклад к Конвенции о Киберпреступности. (Будапешт, 2001 г.), § 179.

61 ЕСПЧ, Гудмундур Андри Астрадссон против Исландии [БП], 1 декабря 2020 г., № 26374/18, § 218.

62 Там же, §§ 218, 232, 233; см. также: Совет Европы, Пояснительный доклад к Конвенции о киберпреступности (Будапешт, 2001 г.), § 70.

63 ЕСПЧ, Забо и Висси против Венгрии, 12 января 2016 г., № 37138/14.

5.3 ПРАВО НА СВОБОДУ ВЫРАЖЕНИЯ МНЕНИЯ

ЕСПЧ неоднократно признавал, что контент, созданный пользователями в Интернете, обеспечивает беспрецедентную платформу для осуществления свободы выражения мнений.[64] Суд, однако, также подчеркнул опасность, которую представляет незаконный онлайн-контент, включая детскую порнографию, разжигание ненависти и высказывания, подстрекающие к насилию.[65]

Право на свободу выражения мнения может быть прямо или косвенно затронуто расследованиями киберпреступлений:

- Прямое вмешательство в право на свободу выражения мнений происходит при блокировке или удалении веб-сайтов и закрытии контента из-за его незаконного характера (например, детская порнография, онлайн-торговые площадки с незаконными товарами и услугами, разжигание ненависти);
- Косвенное препятствие свободе слова может иметь место, если поставщиков услуг или интернет-пользователей заставляют подвергать цензуре контент угрозой санкций или уголовного преследования.

Кроме того, следователи должны сбалансировать защиту прав личности (например, диффамация) и необходимость поддержания общественной безопасности с обязательством обеспечивать свободу слова.

БЛОКИРОВКА ДОСТУПА К ИНТЕРНЕТУ

Международные органы по правам человека неоднократно подчеркивали, что санкционированная государством блокировка целых веб-сайтов, IP-адресов, портов или сетевых протоколов является крайней мерой, которая допустима только в качестве крайней меры и при условии соблюдения минимальных процессуальных гарантий.[66] Меры по блокировке веб-сайтов. могут быть совместимы с международными стандартами свободы выражения мнений только в том случае, если они предусмотрены законом, необходимы и соразмерны для защиты законных целей.[67]

В своей прецедентной практике ЕСПЧ подчеркнул, что блокирование доступа к Интернету может находиться в прямом противоречии с пунктом 1 Статьи 10 ЕКПЧ, который гарантирует свободу выражения мнений «независимо от границ».[68] Дело *Булгаков против России* касалось блокировки всего веб-сайта по решению суда из-за наличия незаконных материалов (даже

64 См. ЕСПЧ, Руководство по Статье 10 Европейской Конвенции о Правах Человека, Свобода выражения мнений (Страсбург, 2022 г.), §§ 588–632.

65 ЕСПЧ, Delfi AS против Эстонии [БП], 10 октября 2013 г., № 64569/09, § 110; ЕСПЧ, Аннен против Германии, 20 сентября 2018 г., № 3682/10, § 67.

66 См. Представитель ООН в ОБСЕ по вопросам Свободы СМИ и Других лиц, Совместная Декларация о Свободе Выражения Мнений и «Фейковых Новостях», Дезинформация и Пропаганда, 3 марта 2017 г., FOM.GAL/3/17.

67 См., например, ОБСЕ, Международные Стандарты и Сравнительные Подходы к Свободе Выражения Мнения и Блокированию Террористического и «Экстремистского» Контента в Интернете (Вена, 2018 г.), п. 47; см. также: БДИПЧ/ОБСЕ, Комментарии к Некоторым Правовым Актам, Регулирующим Массовые Коммуникации, Информационные Технологии и Использование Интернета в Узбекистане (Варшава, 2019 г.), п. 86–89.

68 ЕСПЧ, Ахмет Йылдырым против Турции, 18 декабря 2012 г., № 3111/10, § 67.

после того, как эти материалы были удалены). В своем постановлении суд установил, что для приказа о блокировке не было никаких правовых оснований, поскольку законодательство, на котором основывался приказ, не позволяло властям блокировать доступ ко всему веб-сайту. Суд также постановил, что его вывод о незаконности применим, в частности, к продолжающейся блокировке веб-сайта после того, как запрещенный материал был удален.

В отдельном деле *Ченгиз и Другие против Турции*, касающемся блокировки видеохостинга YouTube, ЕСПЧ постановил, что заявители, которые были пользователями сайта, могли законно утверждать, что эта мера затронула их право на получение и распространение информацию или идей. Учитывая уникальные характеристики платформы, ее доступность и, прежде всего, ее потенциальное влияние, а также учитывая, что у заявителей не было альтернатив, Суд установил, что блокировка нарушила их свободу выражения мнений.[69]

ОТВЕТСТВЕННОСТЬ ЗА ОНЛАЙН КОНТЕНТ

Признавая важные преимущества Интернета для осуществления свободы выражения мнений, ЕСПЧ постановил, что ответственность за клеветнические или другие виды незаконных высказываний должна, в принципе, сохраняться и является эффективным средством правовой защиты от нарушений прав личности.[70]

Оценивая в деле *Delfi AS против Эстонии*, вопрос обязан ли владелец новостного интернет-портала удалять комментарии, опубликованные третьей стороной, Суд определил четыре аспекта, имеющие отношение к определению ответственности поставщиков услуг за контент на их платформах:[71]

- Контекст комментариев;
- Меры, примененные компанией-заявителем для предотвращения или удаления клеветнических комментариев;
- Ответственность фактических авторов комментариев как альтернатива ответственности компании-заявителя;
- Последствия внутреннего разбирательства для компании-заявителя.

Применяя эти соображения, Суд постановил, что система уведомления и удаления, если она сопровождается эффективными процедурами, позволяющими быстрое реагирование, может предложить достаточно сбалансированный подход к правам третьих сторон.[72] Поставщики услуг, таким образом, могут полагаться на такую систему без прямой ответственности за пользовательский контент, такой как клеветнические комментарии.[73] Однако Суд также

69 ЕСПЧ, Ченгиз и Другие против Турции, 1 декабря 2015 г., № 48226/10 и 14027/11, §§ 52, 53, 55; см. также: ЕСПЧ, Ахмет Йылдырым против Турции, 18 декабря 2012 г., № 3111/10, §§ 49, 55, об аналогичном деле, касающемся доступа к веб-сайту, размещенному на хостинговой службе Google Sites.

70 ЕСПЧ, Delfi AS против Эстонии [БП], 10 октября 2013 г., № 64569/09, § 110.

71 ЕСПЧ, Delfi AS против Эстонии [БП], 10 октября 2013 г., № 64569/09, §§ 142–143; см. также: ЕСПЧ, Magyar Tartalomszolgáltatók Egyesülete и Index.hu Zrt против Венгрии, 2 февраля 2016 г., № 22947/13, §§ 60 и последующие.

72 ЕСПЧ, Delfi AS против Эстонии [БП], 10 октября 2013 г., № 64569/09, § 159.

73 ЕСПЧ, Magyar Tartalomszolgáltatók Egyesülete и Index.hu Zrt против Венгрии, 2 февраля 2016 г., № 22947/13, § 91; см. также: ЕСПЧ, Рольф Андерс Даниэль Пиль против Швеции, 7 февраля 2017 г., № 74742/14, § 32; ЕСПЧ, Тамиз против Соединенного Королевства, 19 сентября 2017 г., № 3877/14, § 84; ЕСПЧ, Хойнесс против Норвегии, 19 марта 2019 г., № 43624/14, §§ 73–74, касающийся важности своевременной реакции после уведомления о незаконности контента .

подчеркнул, что в таких делах, как *Delfi AS против Эстонии*, где комментарии третьих лиц принимают форму разжигания ненависти и прямых угроз против физической неприкосновенности отдельных лиц, прав и интересов других лиц и общества в целом, это может дать государствам право налагать ответственность на новостные интернет-порталы, если они не принимают меры по удалению явно незаконных комментариев без промедления, даже без уведомления со стороны предполагаемой жертвы или третьих лиц.

ВСТАВКА 4 «СДЕРЖИВАЮЩЕЕ ВЛИЯНИЕ» НА СВОБОДУ ВЫРАЖЕНИЯ

Если, например, видеосайт сталкивается с нечетким законодательством, он может подвергать пользователей чрезмерной цензуре, чтобы избежать проблем с властями. Этот эффект, часто называемый «сдерживающим» эффектом, можно предотвратить, установив четкие правила, а также режимы, ограничивающие ответственность поставщиков услуг в случаях, когда на их платформах без их ведома или разрешения имеется потенциально незаконный контент. Сдерживающее воздействие на свободу выражения мнений может также возникать, если люди будут подвергать себя самоцензуре в результате слежки или из-за страха стать объектом неправомерных подозрений. Это, в свою очередь, часто является результатом расплывчатых или произвольных норм.

БАЛАНС МЕЖДУ ПРАВОМ НА СВОБОДУ ВЫРАЖЕНИЯ МНЕНИЙ, НЕПРИКОСНОВЕННОСТЬЮ ЧАСТНОЙ ЖИЗНИ И ПРЕДУПРЕЖДЕНИЕМ ПРЕСТУПНОСТИ

ЕСПЧ также рассмотрел необходимость уравновесить права на свободу выражения мнений и неприкосновенность частной жизни с обязанностью государств предотвращать и расследовать преступления. В деле *К.У. против Финляндии* суд постановил, что несовместимо со Статьей 8 ЕКПЧ не обязывать поставщика услуг раскрывать личность лица, разыскиваемого за размещение непристойной рекламы о несовершеннолетнем лице на сайте знакомств в Интернете, ссылаясь в этом контексте на потенциальную возможность угрозы физическому и психическому благополучию несовершеннолетнего, а также уязвимость, вызванную его юным возрастом.[74] Суд заявил, что, хотя свобода выражения мнений и конфиденциальность переписки являются первоочередными соображениями и пользователи Интернета должны иметь гарантию того, что их собственная конфиденциальность и свобода выражения мнения будут соблюдаться, такая гарантия не может быть абсолютной. Время от времени она должно уступать другим законным требованиям, таким как предотвращение беспорядков или преступлений или защита прав и свобод других лиц.[75]

Подводя итог, можно сказать, что свобода выражения мнений может быть ограничена

74 ЕСПЧ, К.У. против Финляндии, 2 декабря 2008 г., № 2872/02, § 41.

75 Там же § 49.

только законом. Законодательство должно определять точные правила и условия блокировки и удаления веб-сайтов или контента, а также ограничивать ответственность поставщиков услуг за контент, создаваемый пользователями. Когда полиция предлагает меры в отношении незаконного контента в Интернете, а суд рассматривает их санкционирование, необходимо тщательно оценить влияние на свободу выражения мнения, чтобы избежать чрезмерного вмешательства. Необходимо найти баланс, особенно в отношении свободы средств массовой информации и в случаях клеветы или разжигания ненависти, когда границы между якобы незаконным контентом и выражением мнения, критики или политических взглядов не всегда ясны. Еще одним важным аспектом является сдерживающий эффект, который цензура оказывает на общество (см. вставку 4). Блокировка веб-сайтов должна ограничиваться исключительно криминальным контентом и не должна затрагивать контент, который не является противозаконным.

5.4 ПРАВО НА ЗАЩИТУ СОБСТВЕННОСТИ

Расследования киберпреступлений часто связаны с виртуальными активами, которые могут быть конфискованы как доказательства преступления и/или конфискованы как доходы от преступлений. Наиболее распространенными виртуальными активами в этом контексте являются криптовалюты, которые часто используются в качестве способа оплаты незаконных товаров, предлагаемых на торговых площадках даркнета, или для получения выкупа в случаях программ-вымогателей. Криптовалюты имеют рыночную стоимость и, следовательно, могут рассматриваться как «собственность» в соответствии с международными стандартами.

Использование криптовалют или других виртуальных активов само по себе не является незаконным, даже если оно не регулируется во многих странах. Однако стандарты по борьбе с отмыванием денег Группы разработки финансовых мер борьбы с отмыванием денег (FATF) требуют регулирования определенных аспектов криптовалют, и все большее число стран внедряют правила для поставщиков криптовалютных услуг, например, в отношении создания кошелька, хранения, обмена на фиатную валюту или на другие криптовалюты или виртуальные активы.

Штраф и конфискация обычно рассматриваются ЕСПЧ как контроль за использованием имущества, который должен рассматриваться в соответствии со статьей 1 (2) Протокола № 1 к ЕКПЧ. Суд рассмотрел различные меры, принятые для борьбы с незаконным обогащением в результате полученных преступным путем доходов. Государства имеют широкую свободу усмотрения при реализации политики по борьбе с преступностью, в том числе путем конфискации:

- Имущества, предположительно имеющего незаконное происхождение;[76]
- Имущества, приобретенного на незаконные средства;[77]

76 ЕСПЧ, Раймондо против Италии, 22 февраля 1994 г., No. 12954/87; Риела и другие против Италии, 4 сентября 2001 г., № 52439/99; ЕСПЧ, Аркури и другие против Италии, 5 июля 2001 г., № 52024/99; ЕСПЧ, Гогитидзе и другие против Грузии, 12 мая 2015 г., № 36862/05 о конфискации, применяемой в гражданском судопроизводстве; ЕСПЧ, Бальзамо против Сан-Марино, 8 октября 2019 г., № 20319/17 и 21414/17, касающиеся разбирательства об отмывании денег.

77 ЕСПЧ, Милорад Улемек против Сербии, 2 февраля 2021 г., № 41680/13.

- Доходы от уголовных преступлений;[78]
- Имущество, являвшееся объектом правонарушения;[79]
- Имущество, которое служило или должно было служить для совершения преступления.[80]

Какая сумма может быть изъята полицией и конфискована судом, зависит от национального режима конфискации, который также может применяться к виртуальным активам в отдельном уголовном деле.

ЕСПЧ рассмотрел несколько дел, касающихся соразмерности и надлежащей правовой процедуры в судебном разбирательстве по делу о конфискации. В деле *Тодоров и другие против Болгарии*,[81] Суд постановил, что в четырех из семи заявлений имело место нарушение статьи 1 Протокола 1 к ЕКПЧ. Национальные суды не смогли установить связь между конфискованным имуществом и преступной деятельностью или между стоимостью имущества и разницей между доходами и расходами. Таким образом, решение о конфискации было несоразмерным.

В деле *Бальзамо против Сан-Марино*,[82] Суд признал, что меры по конфискации были соразмерными, даже при отсутствии обвинительного приговора, устанавливающего вину обвиняемого, а также, если он был также наложен на детей в связи с предыдущей судимостью их отца. Для теста на пропорциональность была признана достаточной высокая вероятность незаконного происхождения в сочетании с неспособностью владельца доказать обратное.

Дело *Гогитидзе и Другие против Грузии*[83] касалось назначенной судом меры конфискации имущества, принадлежащего бывшему заместителю Министра внутренних дел. Суд установил, что был установлен справедливый баланс между средствами, использованными для конфискации активов заявителей, и общей заинтересованностью в борьбе с коррупцией на государственной службе. Заявителям не было отказано в разумной возможности изложить свою позицию, и выводы национальных судов не были произвольными.

78 ЕСПЧ, Филлипс против Соединенного Королевства, 5 июля 2001 г., № 41087/98; ЕСПЧ, Уэлч против Соединенного Королевства, 9 февраля 1995 г., № 17440/90; ЕСПЧ, Силицкене против Литвы, 10 апреля 2012 г., № 20496/02; ЕСПЧ, Гогитидзе и другие против Грузии, 12 мая 2015 г., № 36862/05.

79 ЕСПЧ, Агоси против Соединенного Королевства, 24 октября 1986 г., № 9118/80.

80 ЕСПЧ, Андоноски против бывшей югославской Республики Македония, 17 сентября 2015 г., № 14464/11; ЕСПЧ, Тодоров и другие против Болгарии, 13 июля 2021 г., № 50705/11 и еще 6 человек.

81 ЕСПЧ, Тодоров и другие против Болгарии, 13 июля 2021 г., № 50705/11 и 6 других.

82 ECtHR, *Balsamo v. San Marino*, 8 October 2019, No. 20319/17 and 21414/17.

83 ЕСПЧ, Гогитидзе и другие против Грузии, 12 мая 2015 г., № 36862/05.

6

Заключение

Уважение прав человека и верховенства закона является важным аспектом каждого демократического общества, а также может быть условием законности доказательств и справедливости уголовного процесса. Это также влияет на доверие граждан к государственным учреждениям и во многих случаях является предпосылкой для обеспечения международного сотрудничества, которое имеет решающее значение для эффективного расследования киберпреступлений. Поэтому важно, чтобы специалисты по уголовному правосудию знали и понимали стандарты прав человека, применимые к различным этапам и процессам расследования киберпреступлений.

Многие права человека, включая право на неприкосновенность частной жизни, справедливое судебное разбирательство, свободу выражения мнений и защиту собственности, могут быть затронуты в ходе расследований киберпреступлений. Любое вмешательство в права человека, допускающее ограничения в ходе расследования киберпреступлений, должно быть основано на законе, необходимо и соразмерно и преследовать законную цель, например, защиту прав человека жертв или других интересов общества.

Международные и региональные стандарты в области прав человека, а также судебная практика международных судов, таких как ЕСПЧ, служат важным руководством для государств относительно того, как на практике выполнять свои обязательства в области прав человека в отношении расследований киберпреступлений. Это включает в себя принятие внутреннего законодательства, регулирующего использование следственных полномочий в соответствии с международными стандартами и гарантиями прав человека, а также обеспечение того, чтобы практикующие специалисты обладали знаниями и навыками, необходимыми для соблюдения этих стандартов в ходе расследований киберпреступлений.

7

Дополнения

ДОПОЛНЕНИЕ 1 СООТВЕТСТВУЮЩИЕ СТАТЬИ МПГПП И ЕКПЧ

ДОПОЛНЕНИЕ 2 ИЗБРАННАЯ СУДЕБНАЯ ПРАКТИКА ЕСПЧ

ДОПОЛНЕНИЕ 1 СООТВЕТСТВУЮЩИЕ СТАТЬИ МПГПП И ЕКПЧ

ПРАВО НА УВАЖЕНИЕ ЧАСТНОЙ И СЕМЕЙНОЙ ЖИЗНИ

Статья 17 МПГПП

1. Никто не может подвергаться произвольному или незаконному вмешательству в его личную жизнь, семью, жилище или переписку, а также незаконным посягательствам на его честь и репутацию.
2. Каждый имеет право на защиту закона от такого вмешательства или посягательств.

Статья 8 ЕКПЧ

1. Каждый имеет право на уважение его частной и семейной жизни, жилища и корреспонденции.
2. Не допускается вмешательство органов государственной власти в осуществление этого права, за исключением случаев, предусмотренных законом и необходимых в демократическом обществе в интересах национальной и общественной безопасности или экономического благосостояния страны, для предотвращения беспорядков или преступлений, для защиты здоровья и нравственности или для защиты прав и свобод других лиц.

ПРАВО НА СПРАВЕДЛИВЫЙ СУД

Статья 14 МПГПП

1. Все люди равны перед судами и трибуналами. При рассмотрении любого уголовного обвинения против него или его прав и обязанностей в судебном процессе каждый имеет право на справедливое и публичное разбирательство дела компетентным, независимым и беспристрастным судом, созданным на основании закона. Пресса и общественность могут быть отстранены от участия в судебном процессе в течение всего или части судебного разбирательства по соображениям морали, общественного порядка (ordre public) или национальной безопасности в демократическом обществе, или когда это требуется в интересах частной жизни сторон, или в той степени, в которой это строго необходимо, по мнению суда, в особых обстоятельствах, когда гласность нанесла бы ущерб интересам правосудия; Однако любое решение, вынесенное по уголовному делу или иску, должно быть обнародовано, за исключением случаев, когда интересы несовершеннолетних требуют иного или когда разбирательство касается супружеских споров или опеки над детьми.
2. Каждый обвиняемый в совершении уголовного преступления имеет право считаться невиновным, пока его вина не будет доказана в соответствии с законом.
3. При предъявлении ему любого уголовного обвинения каждый имеет право на следующие минимальные гарантии на условиях полного равенства:

a. Быть незамедлительно и подробно информированным на языке, который он понимает, о характере и причине предъявленного ему обвинения;

b. Иметь достаточно времени и возможностей для подготовки своей защиты и общения с адвокатом, которого он сам выбрал;

c. Быть привлечённым к судебной ответственности без неоправданной задержки;

d. Присутствовать в суде и защищать себя лично или через выбранного им самим адвоката; быть информированным, если он не имеет юридической помощи, об этом праве; и иметь назначенную ему юридическую помощь в любом случае, когда того требуют интересы правосудия, и без оплаты с его стороны в любом таком случае, если у него нет достаточных средств для ее оплаты;

e. Допрашивать или обязать допрашивать свидетелей против него и добиваться явки и допроса свидетелей со своей стороны на тех же условиях, что и свидетелей против него;

f. Пользоваться бесплатной помощью переводчика, если он не понимает или не говорит на языке, используемом в суде;

g. Не подвергаться принуждению к даче показаний против себя или к признанию вины.

4. В отношении несовершеннолетних судебный процесс должен проводиться с учетом их возраста и желанием содействовать их реабилитации.

5. Каждый осужденный за преступление имеет право на пересмотр его осуждения и приговора вышестоящей судебной инстанцией в соответствии с законом.

6. Когда лицо окончательным решением было признано виновным в совершении уголовного преступления и впоследствии его осуждение было отменено или оно было помиловано на том основании, что новый или вновь открывшийся факт убедительно свидетельствует о том, что имела место судебная ошибка, справедливости, лицу, понесшему наказание в результате такого осуждения, выплачивается компенсация в соответствии с законом, если не будет доказано, что не раскрытие в срок неизвестного факта полностью или частично произошло по его вине.

7. Никто не подлежит повторному суду или наказанию за преступление, за которое он уже был окончательно осужден или оправдан в соответствии с законом и уголовными процессуальными нормами каждой страны.

Статья 6 ЕКПЧ

1. При рассмотрении своих гражданских прав и обязанностей или предъявлении ему любого уголовного обвинения каждый имеет право на справедливое и публичное разбирательство дела в разумный срок независимым и беспристрастным судом, созданным на основании закона. Приговор оглашается публично, однако пресса и общественность могут быть исключены из судебного процесса в течение всего судебного разбирательства или его части в интересах морали, общественного порядка или национальной безопасности в демократическом обществе, когда интересы несовершеннолетних или защита частной жизни стороны этого требуют, или в той степени, в которой это строго необходимо, по мнению суда, в особых обстоятельствах, когда гласность нанесла бы ущерб интересам справедливости.

2. Каждый обвиняемый в совершении уголовного преступления считается невиновным,

пока его вина не будет доказана в соответствии с законом.

3. Каждый обвиняемый в совершении уголовного преступления имеет следующие минимальные права:
   a. Быть незамедлительно и подробно информированным на языке, который он понимает, о характере и основании предъявленного ему обвинения;
   b. Иметь достаточно времени и возможностей для подготовки своей защиты;
   c. Защищать себя лично или через выбранного им самим адвоката; или, если у него нет достаточных средств для оплаты юридической помощи получать ее бесплатно, когда того требуют интересы правосудия;
   d. Допрашивать или обязать допрашивать свидетелей против него и добиваться явки и допроса свидетелей со своей стороны на тех же условиях, что и свидетелей против него;
   e. Пользоваться бесплатной помощью переводчика, если он не понимает или не говорит на языке, используемом в суде.

СВОБОДА ВЫРАЖЕНИЯ МНЕНИЯ

Статья 19 МПГПП

1. Каждый имеет право беспрепятственно придерживаться своих убеждений.
2. Каждый имеет право на свободу выражения мнения; это право включает свободу искать, получать и распространять информацию и идеи любого рода, независимо от границ, устно, письменно или печатно, в форме искусства или любыми другими средствами по своему выбору.
3. Осуществление прав, предусмотренных пунктом 2 настоящей статьи, влечет за собой особые обязанности и ответственность. Поэтому на него могут распространяться определенные ограничения, но они должны быть только такими, которые предусмотрены законом и необходимы:
   a. Для уважения прав или репутации других лиц;
   b. Для защиты национальной безопасности или общественного порядка (ordre public), здоровья и нравственности населения.

Статья 10 ЕКПЧ

1. Каждый имеет право на свободу выражения мнения. Это право включает свободу придерживаться своих убеждений, а также свободу получать и распространять информацию и идеи без вмешательства со стороны государственных властей и независимо от государственных границ. Эта статья не препятствует Государствам требовать лицензирования предприятий радиовещания, телевидения или кино.
2. Осуществление этих свобод, поскольку оно влечет за собой обязанности и ответственность, может быть сопряжено с такими формальностями, условиями, ограничениями или штрафами, которые предусмотрены законом и необходимы в

демократическом обществе, в интересах национальной безопасности, территориальной целостности или общественной безопасности, для предотвращения беспорядков или преступлений, для защиты здоровья и нравственности, для защиты репутации или прав других, для предотвращения раскрытия информации, полученной конфиденциально, или для поддержания авторитета и беспристрастности судебной власти.

ПРАВО НА ЗАЩИТУ СОБСТВЕННОСТИ

Статья 1 Протокола к ЕКПЧ

1. Каждое физическое или юридическое лицо имеет право беспрепятственно пользоваться своим имуществом. Никто не может быть лишен своего имущества иначе как в общественных интересах и на условиях, предусмотренных законом и общими принципами международного права.
2. Предыдущие положения, однако, никоим образом не ущемляют право государства обеспечивать соблюдение таких законов, которые оно считает необходимыми для контроля за использованием собственности в соответствии с общими интересами или для обеспечения уплаты налогов или других взносов или штрафов.

ДОПОЛНЕНИЕ 2 ИЗБРАННАЯ СУДЕБНАЯ ПРАКТИКА ЕСПЧ

Бенедик против Словении[84]

Дело касалось нарушения права на уважение частной жизни согласно статье 8 ЕКПЧ. В 2006 году словенская полиция получила от швейцарской полиции информацию об обмене файлами, содержащими детскую порнографию, через одноранговый файлообменный сайт. Среди IP-адресов, зафиксированных швейцарской полицией, был некий динамический IP-адрес в Словении. В августе 2006 года словенская полиция без постановления суда потребовала от словенского интернет-провайдера (ISP) раскрыть данные о пользователе, которому в определенное время был присвоен динамический IP-адрес.
Запрос был основан на положении Закона об уголовном судопроизводстве, которое позволяло полиции запросить у поставщика электронной связи информацию о пользователе определенного средства электронной связи, сведения о котором отсутствовали в соответствующем справочнике.

Интернет-провайдер предоставил имя и адрес абонента, относящиеся к соответствующему IP-адресу. Впоследствии, в декабре 2006 года было издано постановление суда, требующее от интернет-провайдера раскрыть как личные данные, так и данные о трафике абонента, связанного с рассматриваемым IP-адресом. На основании полученных данных районный суд в январе 2007 года назначил обыск дома семьи заявителя. В ходе обыска были изъяты компьютеры, содержащие порнографические материалы с участием несовершеннолетних.

В декабре 2008 года заявитель был признан виновным в совершении уголовного преступления, связанного с показом, изготовлением, хранением и распространением порнографических материалов. Его приговорили к восьми месяцам условно с испытательным сроком в два года. В ноябре 2009 года в апелляционном порядке Высший суд Любляны заменил условный приговор заявителя на шестимесячный тюремный срок.

Заявитель безуспешно пытался обратиться в национальные суды, утверждая, что тайна переписки и других средств связи может быть приостановлена только на основании постановления суда, и поэтому любая незаконно полученная информация должна быть исключена в качестве доказательства. Жалоба заявителя касалась первого запроса полиции к Интернет-провайдеру для идентификации пользователя IP-адреса на основании Уголовно-процессуального закона.

В этом отношении Конституционный Суд в феврале 2014 года пришел к выводу, что Конституция также защищает данные трафика, то есть любые данные, обрабатываемые для передачи сообщений в сети электронных коммуникаций. Он посчитал, что IP-адреса были включены в такие данные о трафике и что обычно требуется постановление суда. Однако заявитель, который никоим образом не скрывал IP-адрес, через который он получил доступ к Интернету, сознательно выставил себя на всеобщее обозрение и, таким образом, отказался от законного ожидания соблюдения конфиденциальности. В результате, хотя

84 ЕСПЧ, Бенедик против Словении, 24 апреля 2018 г., № 62357/14; резюмировано в: ЕСПЧ, Информационная Записка о Прецедентной Практике Суда 217.

данные, касающиеся личности пользователя IP-адреса, в принципе защищены Конституцией как конфиденциальность связи, Конституционный суд постановил, что для их раскрытия в деле заявителя не требуется постановления суда.

Когда дело было передано в ЕСПЧ, Суд пришел к выводу, что запрос полиции к интернет-провайдеру и использование информации об абоненте, позволяющей идентифицировать заявителя, составили вмешательство в его права, предусмотренные Статьей 8 ЕКПЧ. Суд отметил, что меры полиции имели определенную основу во внутреннем законодательстве. Поскольку соответствующее законодательство не было последовательным в отношении уровня защиты, обеспечиваемой интересам заявителя в отношении частной жизни, Суд опирался на интерпретацию Конституционного Суда, согласно которой раскрытие информации об абоненте, связанное с определенным динамическим IP-адресом в принципе требует постановления суда, поскольку данные трафика подпадают под защиту Конституции. Что касается позиции Конституционного Суда о том, что заявитель в конкретном деле отказался от законного ожидания соблюдения конфиденциальности, поскольку он никоим образом не скрывал IP-адрес, через который он получил доступ к Интернету, ЕСПЧ не счел это совместимым со сферой применения права на неприкосновенность частной жизни согласно ЕКПЧ. Таким образом, в данном случае было необходимо постановление суда, и ничто во внутреннем законодательстве не препятствовало полиции получить его.

ЕСПЧ нашел законодательство, а именно соответствующие положения Закона об уголовном судопроизводстве (который не содержал конкретных правил относительно связи между динамическим IP-адресом и информацией об абоненте), Закона об электронных коммуникациях (который конкретно регулировал секретность и конфиденциальность электронных сообщений и Конституции (которая требовала постановления суда для любого вмешательства в конфиденциальность связи), не согласовывают уровень защиты, предоставляемой интересам заявителя в отношении частной жизни.

В этом контексте Суд также отметил, что в соответствующее время не существовало постановления, определяющего условия хранения данных, полученных в соответствии с Законом об уголовном судопроизводстве, и что процедура доступа и передачи таких данных не содержала гарантий против злоупотреблений со стороны Государственных чиновников. В рассматриваемое время не существовало независимого надзора за использованием полномочий полицией в отношении получения информации от интернет-провайдеров.

Таким образом, ЕСПЧ пришел к выводу, что закон, на котором основывалась оспариваемая мера, и способ ее применения национальными судами не были ясными и не предлагали достаточных гарантий против произвольного вмешательства в Статью 8 ЕКПЧ. Суд установил, что вмешательство в право заявителя на уважение его частной жизни не было «соответствующим закону», как того требует Статья 8 (2) Конвенции.

После вынесения решения словенская полиция и прокуратура немедленно изменили свою практику. В 2019 году в Закон об уголовном судопроизводстве были внесены поправки, в которых указано, что данные об абонентах можно получить без постановления суда только в том случае, если данные о трафике не анализируются. На практике это означает, что для доступа к данным пользователя конкретного динамического IP-адреса необходимо

постановление суда. Это не тот случай, когда данные абонента включены в договор с поставщиком услуг, например, для номера мобильного телефона или статического IP-адреса.

В июне 2018 года г-н Бенедик подал иск о защите законности в Верховный Суд. В июне 2020 года Верховный Суд удовлетворил ходатайство заявителя о защите законности, отменил окончательное решение и вернул дело в Краньский районный суд на новое рассмотрение. В мае 2021 года Краньский районный суд прекратил уголовное дело в отношении г-на Бенедика после того, как Краньская районная прокуратура отозвала обвинительное заключение.

В заключение следует подчеркнуть, что условие постановления суда о получении пользовательских данных (динамического) IP-адреса вытекает из Конституции Словении и судебной практики Конституционного Суда Словении и не является международным стандартом. Случай также показывает важность права на уважение частной жизни и достаточную юридическую ясность, и адекватную практику в случае вмешательства в права человека. Из-за нарушения ЕКПЧ по данному делу электронные доказательства были исключены и возобновленное уголовное производство было прекращено.

Брейер против Германии[85]

В соответствии с поправками 2004 года к Закону Германии о Телекоммуникациях телекоммуникационные компании были обязаны собирать и хранить личные данные всех своих клиентов, включая пользователей предоплаченных SIM-карт, даже если это не требуется для целей выставления счетов или по другим договорным причинам, а также предоставлять к ним доступ властям по запросу. Клиенты должны были зарегистрировать у своих поставщиков услуг личные данные, такие как имя и адрес, номера телефонов и дату рождения. Они жаловались на хранение своих личных данных как пользователей предоплаченных SIM-карт.

ЕСПЧ постановил, что нарушения Статьи 8 ЕКПЧ (право на уважение частной жизни) не было. Суд установил, что в целом Германия не вышла за пределы своего усмотрения («пределы усмотрения») в выборе средств для достижения законных целей защиты национальной безопасности и борьбы с преступностью, и что хранение личных данных заявителей данные были пропорциональными и «необходимыми в демократическом обществе». Таким образом, нарушения Конвенции не было.

Суд, в частности, счел, что сбор имен и адресов заявителей как пользователей предоплаченных SIM-карт представляет собой ограниченное вмешательство в их права. Однако он отметил, что рассматриваемый закон имеет дополнительные гарантии и что люди могут также обратиться в независимые органы по надзору за данными для рассмотрения запросов властей о предоставлении данных и, при необходимости, добиваться правовой защиты.

85 ЕСПЧ, Брейер против Германии, 30 января 2020 г., № 50001/12; резюмировано в: ЕСПЧ, Информационная Записка о Прецедентной Практике Суда 236.

Что касается использования сохраненных данных, данные могут быть запрошены различными государственными органами без необходимости постановления суда или уведомления заинтересованных лиц. Запросы на получение данных при определенных условиях могут быть автоматизированы и приводить к созданию списков, основанных на простом сходстве (запросы частичных данных) в именах или числах. Такие запросы информации были разрешены, когда это считалось необходимым «для преследования уголовных и административных правонарушений, предотвращения опасности и выполнения разведывательных задач».

В частности, Суд рассмотрел два основных аспекта. Во-первых, было ли необходимо вмешательство в демократическом обществе и соразмерно, включая вопрос предсказуемости и достаточной детализации соответствующих положений. Суд признал, что рассматриваемое хранение было, с общей точки зрения, подходящей реакцией на изменения в коммуникативном поведении и средствах телекоммуникаций:

- Предварительная регистрация абонентов мобильной связи значительно упростила и ускорила расследование правоохранительными органами и тем самым могла бы способствовать эффективному обеспечению правопорядка и предотвращению беспорядков и преступлений.
- Существование возможностей обойти юридические обязательства не может быть основанием для того, чтобы ставить под сомнение их общую полезность и эффективность.
- Помимо отсутствия консенсуса, тот факт, что на карту были поставлены вопросы национальной безопасности, также оправдывал определенную свободу усмотрения.

Второй аспект, рассмотренный Судом, касался вопроса о том, было ли вмешательство в право на частную жизнь соразмерным. В отличие от дел, ранее рассмотренных Судом, рассматриваемое хранение данных не содержало какой-либо сугубо личной информации и не позволяло создавать персональные профили или отслеживать перемещения подписчиков. При этом не хранилось никаких данных об отдельных событиях общения. Таким образом, вмешательство, хотя и не тривиальное, носило весьма ограниченный характер.

Что касается гарантий регистрации и хранения данных как таковых, Суд отметил, что:

- Заявители не утверждали, что это хранение имело какие-либо технические недостатки.
- Продолжительность хранения ограничивалась календарным годом, следующим за годом прекращения договорных отношений; это не казалось чрезмерным, учитывая, что расследование уголовных преступлений может занять некоторое время и превысить срок действия договорных отношений.
- Сохраненные данные были ограничены информацией, необходимой для четкой идентификации соответствующего абонента .
- Автоматизированные запросы в соответствии с Законом о Телекоммуникациях ограничиваются конкретными полномочиями в области правоохранительной деятельности и национальной безопасности. С другой стороны, ручные запросы прямо не перечислены, но определяются на основе задач полномочий (например, предотвращение опасностей, преследование преступлений, обеспечение соблюдения

правил). Этот уровень детализации является адекватным, несмотря на отсутствие подробного перечисления соответствующих полномочий.

Федеральный конституционный суд Германии также рассмотрел вопрос о том, существовали ли достаточные гарантии для возможного доступа к хранимым данным и их использования в будущем, в частности, в отношении следующих аспектов.

- Компетенция на издание запроса информации: тот факт, что действующее законодательство предусматривает, что информация может быть предоставлена только в той мере, в какой она необходима для выполнения обязанностей, уже создает объективно ограничивающий фактор. Это гарантирует, что поиск разрешен только в том случае, если информация, действительно необходимая для выполнения обязанностей, не может быть получена более легким, но столь же эффективно, другим способом. В результате на неконституционном уровне отсутствует требование о том, чтобы правомочные органы были прямо указаны в законе.
- Цель информационных запросов: запрашивающие органы должны были иметь дополнительную правовую основу для получения данных (аналогия системы двойных дверей[86]).
- Объем информационных запросов: поиск ограничивался необходимыми данными в соответствии с общим обязательством удалять любые данные, которые запрашивающему органу власти не требовались, без неоправданной задержки. Кроме того, требование «необходимости» было присуще не только конкретным правовым положениям, являющимся предметом этой жалобы, но также немецкому и европейскому законодательству о защите данных.
- Рассмотрение и контроль информационных запросов: даже если ответственность за законность запроса информации лежала на самих получающих информацию агентствах, Федеральное сетевое агентство считалось компетентным независимо проверять допустимость передачи данных, когда оно видело причины для проверки. Правовое возмещение ущерба при поиске информации также может быть запрошено в соответствии с общими правилами. Учитывая эти возможности рассмотрения, отсутствие уведомления о процедуре поиска информации не вызывает вопросов в соответствии с Конвенцией.

ЕСПЧ подтвердил решение Федерального Конституционного Суда Германии об отсутствии нарушения прав человека и подчеркнул важность правовых ограничений и гарантий в рамках национальной свободы усмотрения для соблюдения принципов соразмерности и необходимости в демократическом обществе. В частности, он установил, что юридическое обязательство поставщиков услуг хранить персональные данные пользователей предоплаченных SIM-карт мобильных телефонов и предоставлять их властям по запросу было соразмерно законным целям защиты национальной безопасности и борьбы с преступностью, а также то, что получение данных властями сопровождалось адекватными гарантиями.

86 Обмен данными происходит посредством поиска и передачи, которые соответствуют друг другу и каждый из которых требует независимой правовой основы. Образно говоря, законодательный орган должен открыть не только дверь для передачи данных, но и дверь для их получения. Только обе правовые основы вместе, которые должны действовать вместе, как двойная дверь, дают право обмениваться персональными данными.

Роман Захаров против России[87]

Заявитель, который был главным редактором издательской компании, возбудил судебное дело против трех операторов мобильной связи, жалуясь на вмешательство в его право на конфиденциальность его телефонных переговоров. Он утверждал, что согласно соответствующему национальному законодательству, операторы мобильной связи установили оборудование, которое позволяло Федеральной службе безопасности перехватывать все телефонные переговоры без предварительного разрешения суда. Он добивался вынесения судебного постановления, предписывающего убрать оборудование и гарантирующего, что доступ к телекоммуникациям будет предоставлен только уполномоченному персоналу.

Национальные суды отклонили иск заявителя, установив, что он не смог доказать, что его телефонные разговоры прослушивались или что операторы мобильной связи передавали защищенную информацию посторонним лицам. Национальные суды также установили, что установка оборудования, о котором он говорил, сама по себе не нарушала конфиденциальность его разговоров.

ЕСПЧ установил, что само существование оспариваемого законодательства о прослушивании мобильных телефонных переговоров само по себе представляет собой вмешательство в осуществление прав заявителя, предусмотренных Статьей 8. Суд рассмотрел несколько аспектов вмешательства в Статью 8:

- **Законность:** Прослушивание мобильных телефонных переговоров основывалось на внутреннем законодательстве и преследовало законные цели защиты национальной и общественной безопасности, предотвращения преступности и защиты экономического благосостояния страны.
- **Доступность:** правовые положения были официально опубликованы и доступны для общественности.
- **Сфера применения мер тайного наблюдения:** характер правонарушений, которые могли послужить основанием для выдачи запроса на перехват, был достаточно ясен. Однако диапазон был слишком широк, и прослушивание могло быть назначено не только в отношении лиц, являвшихся подозреваемыми или обвиняемыми.
- **Продолжительность мер тайного наблюдения:** закон содержал четкие правила о продолжительности и возобновлении прослушивания, но не о прекращении наблюдения.
- **Процедуры, среди прочего, хранения и уничтожения перехваченных данных:** автоматическое хранение в течение шести месяцев явно нерелевантных данных не может считаться оправданным в соответствии со Статьей 8.
- **Разрешение на прослушивание:** прослушивание должно было быть санкционировано судом, но российские судьи не были проинструктированы проверять наличие «обоснованного подозрения» в отношении заинтересованного лица или применять критерии «необходимости» и «соразмерности». Закон не содержал никаких требований относительно содержания запросов или разрешений на прослушивание. В некоторых

87 ЕСПЧ, Роман Захаров против России, 4 декабря 2015 г., № 47143/06; резюмировано в: ЕСПЧ, Информационная Записка о Прецедентной Практике Суда 191.

приказах не упоминалось конкретное лицо, номер телефона или продолжительность наблюдения. В соответствии с внутренним законодательством не существовало обязательства предъявлять поставщику услуг связи судебное разрешение до получения доступа к переговорам.

- **Надзор:** надзорный орган не мог обнаружить прослушивание, осуществленное без надлежащего судебного разрешения, что в сочетании с технической способностью правоохранительных органов напрямую перехватывать сообщения делает меры надзора неэффективными. Надзор со стороны прокуроров был ограничен.
- **Уведомление о прослушивании и доступных средствах правовой защиты:** лица, чьи сообщения были перехвачены, не были уведомлены.

Судебные средства правовой защиты, на которые ссылалось правительство, были доступны только лицам, располагавшим информацией о прослушивании их сообщений. Таким образом, их эффективность была подорвана отсутствием требования об уведомлении лица, подвергшегося прослушиванию, или адекватной возможности запрашивать и получать информацию о прослушивании от властей. Соответственно, российское законодательство не предусматривало эффективных судебных средств защиты от мер тайного наблюдения в случаях, когда против лица, подвергшегося прослушиванию, не было возбуждено уголовное дело.

По сути, положения внутреннего законодательства, регулирующие перехват сообщений, не обеспечивают адекватных и эффективных гарантий против произвола и риска злоупотреблений. Внутреннее законодательство не отвечало требованию «качества закона» и было неспособно ограничить «вмешательство» тем, что «необходимо в демократическом обществе». Своим решением ЕСПЧ установил точные стандарты и тест на соответствие законодательства в случае массовой слежки.

K. У. против Финляндии[88]

В этом деле ЕСПЧ обсудил позитивные обязательства государств-участников в отношении эффективной защиты частной жизни (конфиденциальности) и использования коммуникационных данных в делах, связанных с электронными доказательствами и киберпреступностью. Дело касалось 12-летнего финского мальчика, чьи данные были против его воли переданы на сайт знакомств и с которым захотел сблизиться взрослый человек. Ясно, что такой (сексуальный) подход в то время был незаконным, тем более что преступник оставался анонимным.

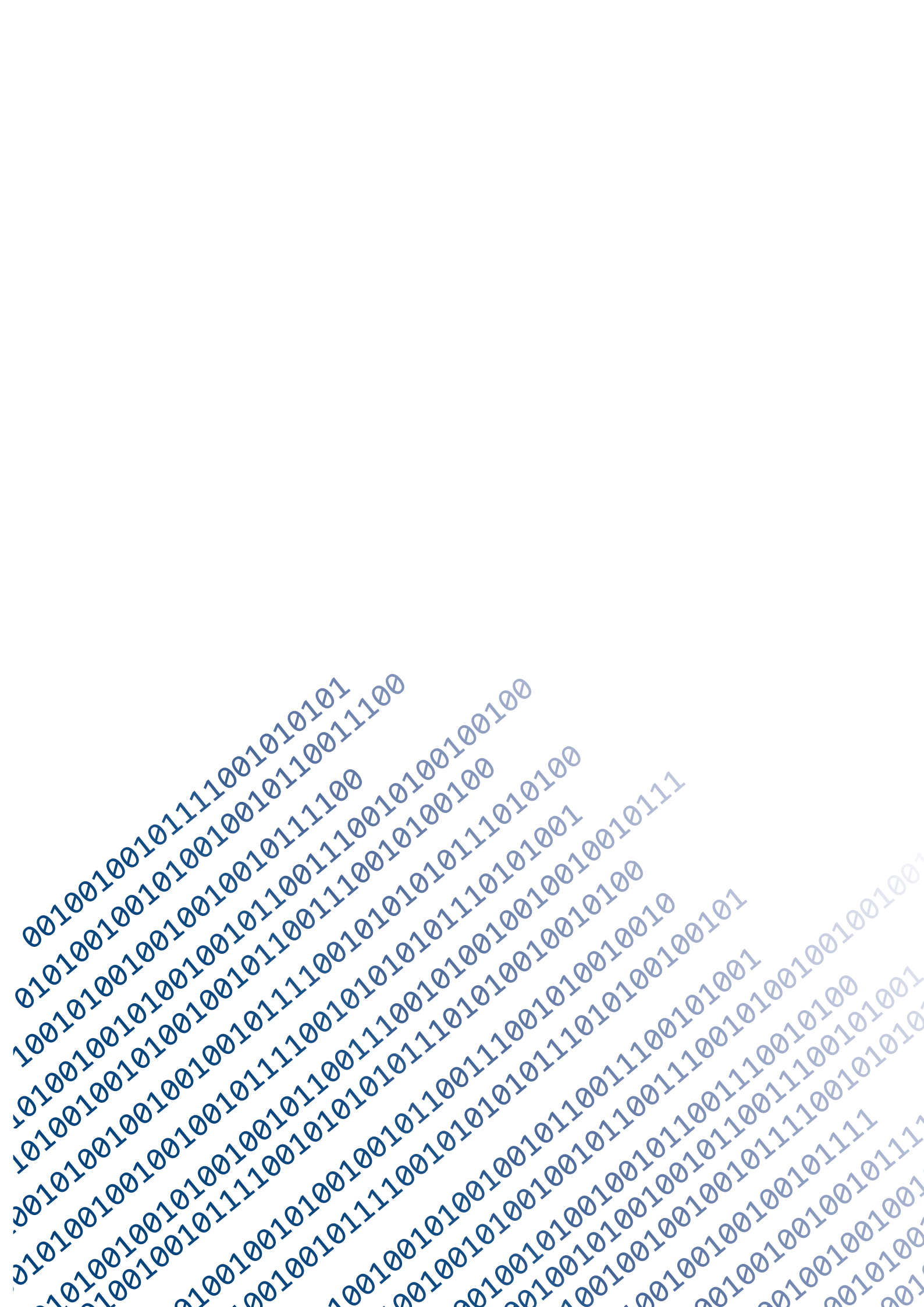
Когда финские власти попытались возбудить дело, им не удалось получить данные о преступнике от поставщика услуг сайта знакомств. В соответствии с финским законодательством поставщик услуг не мог раскрыть личность пользователя по запросу полиции. Суд оценил этот результат и установил, что финский законодатель не принял достаточных мер для разрешения такой ситуации.

88 ЕСПЧ, К.У. против Финляндии, 2 декабря 2008 г., № 2872/02; резюмировано в: ЕСПЧ, Информационная Записка о Прецедентной Практике Суда 114.

Решение гласило: «Суд считает, что практическая и эффективная защита заявителя требует принятия эффективных мер по выявлению и привлечению к ответственности преступника, то есть лица, разместившего рекламу. В данном случае такая защита не была предоставлена. Эффективное расследование никогда не могло быть начато из-за наиважнейшего требования соблюдения конфиденциальности.

Хотя свобода выражения мнений и конфиденциальность сообщений являются первоочередными соображениями, и пользователи телекоммуникаций и Интернет-услуг должны иметь гарантию того, что их собственная неприкосновенность частной жизни и свобода выражения мнений будут уважаться, такая гарантия не может быть абсолютной и должна иногда уступать другим законным императивам, таким как предотвращение беспорядков или преступлений или защита прав и свобод других лиц».

Таким образом, Суд пришел к выводу, что дело К.У. не могло быть эффективно рассмотрено в рамках существующей правовой базы, что привело к нарушению позитивной обязанности государства защищать К.У. от такого типа поведения. Государство не смогло защитить право К.У. на уважение его частной жизни, отдав приоритет требованию соблюдения конфиденциальности над его физическим и моральным благополучием.



ОБСЕ Организация по безопасности и сотрудничеству в Европе