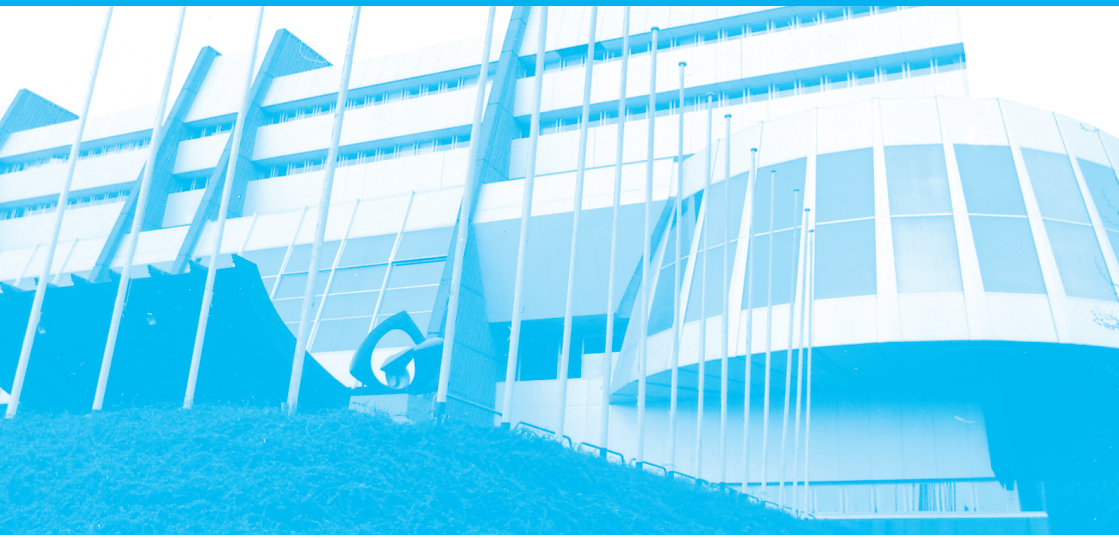
ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В ГРАЖДАНСКОМ И АДМИНИСТРАТИВНОМ СУДОПРОИЗВОДСТВЕ



Юридические инструменты

Руководящие принципы и пояснительный меморандум

Funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В ГРАЖДАНСКОМ И АДМИНИСТРАТИВНОМ СУДОПРОИЗВОДСТВЕ

Руководящие принципы
Комитета министров
Совета Европы
30 января 2019
и пояснительный меморандум

Совета Европы

English edition:

Electronic evidence in civil and administrative proceedings (Guidelines and explanatory memorandum)
ISBN 978-92-871-8929-5

Cover design and layout:
Documents and Publications Production Department (SPDP), Council of Europe

Council of Europe
F-67075 Strasbourg Cedex
http://book.coe.int

Printed at the Council of Europe

Содержание

Руководящие принципы

Комитета министров Совета Европы относительно использования электронных доказательств в гражданском и административном судопроизводстве

(Принято Комитетом министров 30 января 2019 года на 1335-м заседании постоянных представителей министров)

Комитет министров,

Принимая во внимание, что целью Совета Европы является достижение большего единства между государствами-членами, в том числе способствуя принятию общих правил и подходов к правовым вопросам;

Учитывая необходимость предоставления судам, другим компетентным органам с судебными функциями, специалистам, в том числе юристам-практикам, и сторонам производства практического руководства по обращению с электронными доказательствами в гражданском и административном судопроизводстве;

Принимая во внимание, что цель настоящих руководящих принципов – обеспечить общую основу, а не унификацию норм национального законодательства государств-членов;

Учитывая необходимость уважения различий правовых систем государств-членов;

Признавая достигнутый государствами-членами прогресс в области цифровизация систем правосудия;

Отмечая при этом факторы, препятствующие эффективному администрированию электронных доказательств в системах правосудия, такие как отсутствие общих стандартов, а также различия и сложность процедур получения доказательств;

Подчеркивая необходимость содействия использованию электронных доказательств в правовых системах и судебной практике;

Признавая необходимость изучения государствами-членами существующих недостатков при использовании электронных доказательств и определения сфер, в которых возможно внедрение или совершенствование принципов и практик использования электронных доказательств;

Отмечая, что настоящие руководящие принципы направлены на предоставление практических решений проблем, существующих в правовом поле и на практике,

Принимает нижеследующие руководящие принципы в качестве практического инструмента для государств-членов, который призван помочь им адаптировать функционирование своих судебных и других механизмов урегулирования споров в целях решения вопросов, возникающих в связи с использованием электронных доказательств в гражданском и административном судопроизводстве, и призывает их к широкому распространению этих руководящих принципов с целью их применения лицами, ответствен- ными или иным образом связанными с использованием электронных доказательств.

Цель и область применения

Настоящие руководящие принципы охватывают следующие вопросы:

- получение устных показаний с помощью средств дистанционной связи;
- использование электронных доказательств;
- сбор, изъятие и передача доказательств;
- значимость;
- достоверность;
- хранение и обеспечение сохранности;
- архивирование;
- повышение уровня осведомленности, мониторинг, профессиональная подготовка и обучение.

Не следует толковать настоящие руководящие принципы как предписывающие конкретную доказательственную ценность тем или иным видам электронных доказательств. Руководящие принципы следует применять только в той степени, в которой они не противоречат национальному законодательству.

Цель руководящих принципов – облегчить использование и администрирование электронных доказательств в рамках правовых систем и судебной практики.

Определения

В контексте настоящих руководящих принципов:

Электронное доказательство

«Электронное доказательство» означает любое доказательство, полученное на основе данных, содержащихся на каком-либо устройстве или созданных им, при этом функционирование такого устройства зависит от программного обеспечения или данных, хранящихся или переданных посредством компьютерной системы или сети.

Метаданные

«Метаданные» – электронная информация о других электронных данных, которая позволяет идентифицировать, установить источник или проследить историю доказательства, а также соответствующие даты и время.

Услуги удостоверяющего центра

«Услуги удостоверяющего центра» означают электронные услуги, включающие:

а. создание, верификацию и валидацию электронных подписей, электронных печатей или электронных меток времени, услугу электронной доставки заказных писем, создание, верификацию и валидацию сертификатов, касающихся этих услуг; или

б. создание, верификацию и валидацию сертификатов для аутентификации на веб-сайтах; или

в. обеспечение сохранности электронных подписей, печатей или сертификатов, связанных с такими услугами.

Суд

Термин «суд» включает в себя любой компетентный орган с судебными функциями, при исполнении которых он имеет дело с электронными доказательствами.

Основополагающие принципы

Решение о потенциальной доказательственной ценности электронных доказательств принимают суды в соответствии с национальным законодательством.

Электронные доказательства следует оценивать так же, как и другие виды доказательств, в частности, что касается их допустимости, подлинности, точности и целостности.

Результатом использования электронных доказательств не должно стать ухудшение положения сторон или предоставление одной из них несправедливого преимущества.

Руководящие принципы

Получение устных доказательства с помощью средств дистанционной связи

1. Устные доказательства могут быть получены дистанционно с помощью технических средств, если характер доказательства это допускает.

2. При принятии решения о том, может ли устное доказательство быть получено дистанционно, судам следует учесть ряд факторов, в том числе:

- значимость доказательства;
- статус лица, представляющего доказательство;
- безопасность и целостность видеоканала, через который будет транслироваться доказательство;
- затраты и сложности, связанные с обеспечением присутствия соответствующего лица в суде.

3. При получении доказательств дистанционно необходимо обеспечить, чтобы:

а. трансляцию устного доказательства могли видеть и слышать участвующие в судопроизводстве лица, а также представители общественности в случае проведения открытых заседаний; и

б. ллицо, которое дает показания дистанционно, могло видеть и слышать процесс судопроизводства в степени, необходимой для обеспечения справедливости и эффективности судебного процесса.

4. Процедуры и технологии, применяемые для получения доказательств из удаленно, не должны негативно влиять на допустимость такого доказательства и способность суда устанавливать личности соответству- ющих лиц.

5. Независимо от того, происходит ли передача доказательства через открытые или закрытые каналы, следует обеспечить надлежащее качество видеоконференции и шифрование видеосигнала для защиты от перехвата.

Использование электронных доказательств

6. Судам не следует отклонять электронные доказательства и отрицать их юридическую силу исключительно по причине того, что они были собраны и/или предоставлены в электронном виде.

7. В целом, судам не следует отрицать юридическую силу электронных доказательств только потому, что они не содержат усовершенствованную, квалицированную или аналогичным образом защищенную цифровую подпись.

8. Судам необходимо знать и принимать к сведению доказательственную ценность метаданных и возможные последствия их неиспользования.

9. Сторонам следует разрешить предоставлять электронные доказательства в оригинальном электронном виде без необходимости подавать распечатки.

Сбор, изъятие и передача

10. Сбор электронных доказательств следует осуществлять надлежащим и безопасным образом. Предоставлять электронные доказательства суду необходимо с использованием надежных сервисов, например, услуг удостоверяющего центра.

11. Учитывая повышенный риск уничтожения или потери электронных доказательств по сравнению с неэлектронными, государствам-членам следует внедрить процедуры безопасного изъятия и сбора электронных доказательств.

12. Судам необходимо знать и принимать к сведению специфические вопросы, возникающие в связи с изъятием и сбором электронных доказательств за рубежом, в том числе в трансграничном судопроизводстве.

13. Судам необходимо сотрудничать в рамках трансграничного получения доказательств. Суд, получивший запрос, должен сообщить направившему запрос суду обо всех условиях, включая ограничения, при которых суд, получивший запрос, может получить доказательства.

14. Электронные доказательства необходимо собирать, структуриро- вать и администрировать таким образом, который не будет препятствовать их эффективной передаче другим судам, в частности апелляционному суду.

15. Следует содействовать передаче электронных доказательств электронными средствами связи, что будет способствовать повышению эффективности судопроизводства.

16. Системы и устройства, используемые для передачи электронных доказательств, должны сохранять целостность доказательств.

Значимость

17. Судам следует принимать активное участие в администрировании электронных доказательств, в том числе для того, чтобы избежать чрезмерного или спекулятивного представления или истребования электронных доказательств.

18. Суды могут требовать проведения экспертами анализа электронных доказательств, особенно в тех случаях, когда возникают комплексные вопросы доказывания или имеются сомнения относительно манипуляций с электронными доказательствами. Суды принимают решение о достаточности опыта и знаний таких лиц в соответствующей области.

Достоверность

19. При оценке достоверности судам следует учитывать все надлежащие факторы, касающиеся происхождения и подлинности электронных доказательств.

20. Судам необходимо знать и принимать к сведению ценность услуг удостоверяющего центра при определении достоверности электронных доказательств.

21. На усмотрение суда электронные доказательства необходимо принимать в качестве доказательств в степени, допустимой национальным законодательством, за исключением случаев, когда одна из сторон оспаривает подлинность этих доказательств.

22. Принимая во внимание принцип судейского усмотрения, презюмируется достоверность электронных доказательств в мере, допустимой национальным законодательством, при условии, что личность лица, подписавшего документ, может быть подтверждена и обеспечена защита целостности данных, за исключением случаев, когда существуют обоснованные сомнения в обратном.

23. В случае, когда нормы применимого права предусматривает особую защиту для определенных категорий уязвимых лиц, такие нормы имеют преимущественное значение перед настоящими руководящими принципами.

24. В той степени, в которой национальная правовая система содержит соответствующие нормы, когда орган государственной власти передает электронные доказательства независимо от сторон, такие доказательства считаются убедительными с точки зрения их содержания до тех пор, пока не будет доказано обратное.

Хранение и обеспечение сохранности

25. Электронные доказательства следует хранить таким образом, который обеспечивает сохранение читабельности, доступности, целостности, подлинности, достоверности и, когда это применимо, конфиденциальности и тайны.

26. Электронные доказательства следует хранить вместе со стандартизированными метаданными, что обеспечит ясность и понятность контекста их создания.

27. Необходимо обеспечить гарантию читабельности и доступности электронных доказательств с течением времени, учитывая развитие информационных технологий.

Архивирование

28. Судам необходимо архивировать электронные доказательства в соответствии с требованиями национального законодательства. Электронные архивы должны соответствовать требованиям безопасности и гарантировать целостность, подлинность, конфиденциальность и качество данных, а также обеспечивать сохранение тайны.

29. Архивированием электронных доказательств должны заниматься квалифицированные специалисты.

30. При необходимости данные следует переносить на новые носители для хранения, чтобы сохранить доступ к электронным доказательствам.

Повышение уровня осведомленности, мониторинг, профессиональная подготовка и обучение

31. Государства-члены должны способствовать повышению уровня осведомленности о преимуществах и ценности электронных доказательств в гражданском и административном судопроизводстве.

32. Государствам-членам необходимо своевременно вносить изменения в технические стандарты, касающиеся электронных доказательств.

33. Все специалисты, сталкивающиеся с электронными доказательствами, должны проходить междисциплинарное обучение об обращении с такого рода доказательствами.

34. Судьи и юристы-практики должны быть в курсе и учитывать развитие информационных технологий, которые могут повлиять на доступность и ценность электронных доказательств.

35. Образовательные программы в области права должны включать модули об электронных доказательствах.

Пояснительный меморандум

Общие комментарии

Зачем нужен новый документ?

1. Суды все чаще обращаются к электронным доказательствам или разрешают сторонам и другим лицам, участвующим в гражданском и административном судопроизводстве, представлять электронные данные.

2. На сегодняшний день существует немного стандартов, применимых к электронным доказательствам на международном, европейском или национальном уровне. В законодательстве и в практиках, применимых к электронным доказательствам, все еще присутствуют существенные пробелы.

3. Цель этих Руководящих принципов относительно использования электронных доказательств состоит не в том, чтобы установить обязательные правовые стандарты, а скорее в том, чтобы служить практическим инструментом для государств-членов Совета Европы в адаптации работы их судебных и других механизмов разрешения споров для решения вопросов, возникающих в связи с электронными доказательствами. В этом смысле Руководящие принципы предназначены для повышения эффективности и качества правосудия.

4. Электронные доказательства во многих отношениях отличаются от других видов доказательств, при этом, при работе с электронными доказательствами в судах и других компетентных органах, выполняющих судебные функции, возникают специфические проблемы. Эти проблемы указывают на необходимость расширения знаний об электронных доказательствах и улучшения обращения с электронными доказательствами в гражданском и административном судопроизводстве.

Метод работы и процесс разработки

5. Вопрос об электронных доказательствах входит в компетенцию Европейского комитета по правовому сотрудничеству (CDCJ), который является межправительственным органом Совета Европы, ответственным за нормотворческую деятельность Совета Европы в области гражданского и административного права.

6. 6. Руководящие принципы были разработаны редакционной группой на основании предложений, внесенных членами и назначенными экспертами CDCJ, и были подготовлены на совещаниях, проведенных в 2018 году. В этих совещаниях также участвовали органы Совета Европы, обладающие опытом и наделенные полномочиями в этой области.

7. Редакционная группа приняла во внимание опыт работы механизмов электронного правосудия, существующих в государствах-членах.

Примеры государств-членов

- Электронная система правосудия («Lietuvos teismų informacinė sistema» («LITEKO»)) была внедрена в **Литве** в 2004 году. LITEKO сокращает количество бумажных дел и позволяет участникам дела представлять все процессуальные документы на веб-странице в Интернете и следить за ходом дела.
- **Хорватия** разрабатывает электронный коммерческий реестр, электронный земельный реестр и интегрированную систему отслеживания случаев («eSpis»). Последнее позволит осуществлять электронную связь между сторонами судебного разбирательства и судом.

Структура и содержание

8. Руководящие принципы являются не только декларацией принципов, но и предлагают практические советы.

Преамбула

9. 9. В преамбуле объясняется, что Руководящие принципы должны приме- няться только в той мере, в которой они не противоречат национальному законодательству. Руководящие принципы не являются обязательным документом. Они не направлены на гармонизацию национальных законодательств государств-членов. Руководящие принципы не должны толковаться как предписывающие конкретную юридическую ценность для определенных электронных доказательств. Они являются достаточно

общими, чтобы подходить для различных правовых систем. Полностью признается разнообразие правовых систем государств-членов.

Цель и область применения

10. Руководящие принципы разработаны для обеспечения решения конкретных проблем, связанных с электронными доказательствами, таких как потенциальная доказательная ценность метаданных, простота фальсификации , искажения и стирания электронных доказательств, а также участие третьей стороны (включая провайдеров услуг удостоверяющего центра при сборе и изъятии электронных доказательств). Руководящие принципы применимы к разрешению споров как в гражданском, так и в административном судопроизводстве.

Примеры государств-членов

В **Словакии** административные органы принимают электронные доказательства, основываясь на общем правиле, согласно которому все, что имеет доказательственную ценность для определения фактического положения дел, может быть представлено в качестве доказательства, если такие доказательства не получены с нарушением закона.

Определения

Электронные доказательства

11. Принимается широкое определение «электронных доказательств» (также называемых «цифровые доказательства»). Они могут иметь форму текста, видео, фото или звукозаписи. Данные могут поступать с разных носителей или методов доступа, таких как мобильные телефоны, веб-страницы, компьютеры или GPS-рекордеры, включая данные, хранящиеся в хранилищах вне собственного контроля стороны. Электронные сообщения (электронная почта) являются типичным примером электронных доказательств, поскольку они являются доказательством, полученным с электронного устройства (компьютера или подобного устройства), и включают в себя соответствующие метаданные (см. определение «метаданных» ниже).

Метаданные

12. «Метаданные» означают данные о других данных. Иногда их называют «цифровой отпечаток» электронных доказательств. Они могут включать в себя важные доказательственные данные, такие как дата и время создания

или изменения файла, документа, или имени автора, а также дату и время отправки данных. Метаданные обычно напрямую недоступны.

Услуги удостоверяющего центра

13. Услуги удостоверяющего центра играют решающую роль в идентификации, аутентификации и безопасности онлайн-транзакций. Определение «услуг удостоверяющего центра» сформулировано в соответствии со статьей 3 (16) Регламента (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года (Регламент eIDAS).

Суд

14. Принято широкое определение «суда», чтобы охватить все органы, наделенные компетенцией разрешать юридические споры между сторонами в гражданском и административном судопроизводстве. Они включают суды, судебные учреждения и административные органы.

Основополагающие принципы

15. Первый принцип поясняет, что, хотя роль экспертов в оценке электронных доказательств важна, суды должны в конечном итоге принять собственное решение о потенциальной доказательной ценности электронных дока-зательств. При этом суды могут быть связаны применимыми законными презумпциями (например, предоставление конкретной доказательной силы для определенного типа электронных доказательств).

16. Второй принцип гласит, что электронные доказательства не должны находиться ни в более привилегированном, ни в более невыгодном положении по сравнению с другими видами доказательств. В этом отношении суды также должны принять технологически нейтральный подход. Это означает, что следует принимать любую технологию, позволяющую установить подлинность, точность и целостность данных.

> «Хотя статья 6 Конвенции о правах человека гарантирует право на справедливое судебное разбирательство, она не устанавливает каких-либо правил относительно допустимости доказательств или того, как они должны оцениваться, что, следовательно, является прежде всего предметом регулирования национальногоым законодательства и национальных судов» (см. «Гарсия Руиз против Испании» (García Ruiz v. Spain), № 30544/96, параграф 28).

17. Третий принцип относится к равенству сторон и предоставлению равных условий сторонам процесса в отношении электронных доказательств.

Использование электронных доказательств не должно ставить стороны (в гражданском или административном судопроизводстве) в неблагоприятное положение. Например, сторона не должна быть лишена возможности оспаривать подлинность доказательств. Если суд просит сторону представить распе- чатки электронных доказательств, такая сторона не должна быть лишена возможности представить соответствующие метаданные.

Практика ЕСПЧ

«Принцип равенства сторон подразумевает, что каждой стороне должна быть предоставлена разумная возможность представлять свое дело – включая свои доказательства – в условиях, которые не ставят ее в существенно невыгодное положение по отношению к его оппоненту» (См. «Летинчич против Хорватии» (Letinčić v. Croatia), № 7183/11, параграф 48).

Руководящие принципы

Устные доказательства, полученные с помощью средств дистанционной связи

18. Устные доказательства, полученные с помощью средств дистанционной связи, рассматриваются в качестве электронных доказательств для целей этих Руководящих принципов (см. определение «электронных доказательств» выше). Этот раздел Руководящих принципов, однако, не охватывает предварительно записанные устные доказательства. Раздел касается устных показаний в форме видеоконференций (передача синхронизированных изображений и звука в режиме реального времени). Не все устные доказательства могут быть получены с помощью средств дистанционной связи. Следует также учитывать технические устройства. Дистанционное получение доказательств осуществимо с использованием аналоговых или цифровых технических устройств, обеспечивающих передачу данных по электронной связи, в частности двусторонней связи, позволяю- щей передавать изображение и звук в реальном времени. Если показания требуют конфиденциальности, может потребоваться применение мер или технических решений, которые могут ограничить доступ к безопасной коммуникации в разборчивой форме только авторизованным лицам. Устройства, которые могут обеспечить целостность телекоммуникаций, предоставят суду и сторонам адекватную и надлежащую возможность для допроса «удаленного» свидетеля и оспаривания его показаний.

Примеры ЕС и национальных правил

- Статья 10 (4) Регламента Совета (ЕС) № 1206/2001 от 28 мая 2001 года о сотрудничестве между судами государств-членов в получении доказательств по гражданским или коммерческим вопросам предусматривает, что запрашивающий суд может просить запрашиваемый суд использовать коммуникационные технологии, в частности, видеоконференции

- Статья 803 (3) Гражданского процессуального кодекса **Литвы** устанавливает, что «суды Литовской Республики могут просить иностранный суд использовать коммуникационные технологии (такие как видеоконференции) для получения доказательств.

19. Решающими факторами для определения того, следует ли получить устные доказательства посредством дистанционной связи, являются экономические соображения (например, сокращение связанных с ними расходов), практические трудности (например, болезнь, инвалидность свидетеля) и соображения процессуальной эффективности, направленные на то, чтобы избежать чрезмерной длительности разбирательства. Если лицо проживает в другой стране, может быть более целесообразно задавать ему / ей вопросы удаленно. Тот же принцип относится к группе лиц, место жительства которых находится далеко от судебного округа суда, рассматривающего дело. Если лицо является ключевым свидетелем, может быть более целесообразно обеспечить его или ее физическое присутствие в суде для дачи показаний. Другие факторы, которые должны быть рассмотрены судами, включают участие и расходы на переводчиков для слушания. Важно, чтобы судьи, работники судебной системы, в том числе практикующие юристы, и сотрудники суда знали о возможных различиях между показаниями, даваемыми лично и с помощью средств дистанционной связи. Например, при опросе свидетеля дистационно, сложнее наблюдать и интерпретировать его или ее манеру поведения.

20. Руководящие принципы требуют внимания к процессу сбора дистанционных показаний. Это особенно важно в случае доказательств, имеющих фундаментальное значение для разрешения дела, важно обеспечить, чтобы используемая технология позволяла задавать вопросы в ходе дачи показаний (если это предусмотрено правилами процедуры). Это требование едва ли выполнимо, когда передача данных искажается из-за плохой связи или если доступ к техническим средствам ограничен для сторон. Это может дать несправедливое преимущество одной из сторон. Насколько это технически возможно, дистанционные доказательства должны приниматься тем же способом, что и в суде.

21. Используемые методы должны обеспечивать надежную защиту передачи изображения или звука от потери, искажения или несанкционированного раскрытия. Суд может проверить личность любого лица, дающего показания, потребовав от него / нее предоставить соответствующий документ, такой как действительное удостоверение личности, паспорт или водительские права.

22. Все доступные системы связи, как публичные, так и частные, должны обеспечивать как минимум качество видеоконференции и шифрования видеосигнала для защиты от перехвата. Можно получить доказательства через частные средства связи, если это разрешено национальным законодательством, при условии, что используемые решения обеспечивают достаточную техническую безопасность и соблюдение процессуальных гарантий. Частные средства связи в этом контексте означает систему связи, которая не является официальной, правительственной системой, специально созданной для получения доказательств в суде.

Использование электронных доказательств

23. Суды должны осознавать важность электронных данных, представляемых сторонами в качестве доказательств в их первоначальном формате. Если представлена распечатка электронных доказательств, суд может распорядиться, по просьбе стороны или по собственной инициативе, чтобы соответствующее лицо предоставило оригинал электронных доказательств. Примером доказательств, которые могут иметь существенное значение для разрешения рассматриваемого вопроса, если они представлены в оригинальном формате, являются геоданные. Большинство стран мира уже прямо закрепили в своем законодательстве подобное использование электронных доказательств в ходе судебного разбирательства. Пример таких положений можно найти в Регламенте eIDAS.

Примеры государств-членов

Верховный суд **Хорватии** (Дело № I Kž 696 / 04-7) подтвердил, что SMS-сообщения могут использоваться в качестве доказательств в судебном разбирательстве, поскольку они являются источником информации, равным любому другому письменному содержимому, хранящемуся на другом носителе.

Пример технологии, которая будет специально использована для обеспечения доказательств (Блокчейн).

Блокчейн – это новая технология, которая может повысить доверие к электронным доказательствам и их безопасность. Его можно определить как распределенный реестр, который ссылается на список записей (блоков), которые связаны и защищены криптографией и записаны в децентрализованной одноранговой сети. По своей структуре блокчейн устойчив к изменению данных. После записи данные в любом отдельном блоке не могут быть изменены задним числом без изменения всех последующих блоков, что требует согласованности большинства сетей. Это делает блокчейн подходящим для целей получения доказательств.

В США § 1913 Правил о доказательствах штата Вермонт гласит: (1) Цифровая запись, электронно зарегистрированная в блокчейне, должна быть аутентифицирована в соответствии с Правилом о доказательствах штата Вермонт 902, если она сопровождается письменным заявлением квалифицированного лица, под присягой, с указанием квалификации лица для сертификации и: (a) дата и время, когда запись была введена в блокчейн; (б) дата и время получения записи из блокчейна; (c) запись была сохранена в блокчейне как регулярный вид деятельности; и (d) запись была сделана в ходе регулярно проводимой деятельности как обычная практика.

В Китае Интернет-суд Ханчжоу подтвердил 28 июня 2018 года, что электронные данные, основанные на блокчейне, могут использоваться в качестве доказательств в правовых спорах. Использование сторонней платформы блокчейна, которая является надежной без конфликта интересов, обеспечило правовое основание для доказательства нарушения права интеллектуальной собственности.

24. Для целей положения 7 Руководящих принципов «расширенная электронная подпись» означает электронную подпись, которая соответствует требованиям, изложенным в статье 36 регламента eIDAS, а «квалифицированная электронная подпись» означает расширенную электронную подпись, которая создается устройством для создания квалифицированной электронной подписи, и в основе которой лежит квалифицированный сертификат для электронных подписей.

25. В современной практике большинство электронных данных не имеют каких-либо расширенных или квалифицированных электронных подписей и не защищены каким-либо другим способом. Тем не менее они должны рассматриваться судами как электронное доказательство (в то время как доказательная ценность доказательств может варьироваться в зависимости от конкретного случая), например, с учетом разнообразных услуг удостоверяющего центра, связанных с электронным управлением

документами и идентификацией подписавших сторон, которые доступны по всему миру. Примером является биометрическая подпись, метод получения электронной версии рукописной подписи, когда человек ставит свою электронную подпись на электронном устройстве с помощью специальной ручки и блокнота. В зависимости от применимого законодательства суд может признать такую биометрическую подпись эквивалентной рукописной подписи на бумаге.

26. Метаданные обеспечивают необходимый контекст для оценки доказательств (данных) так же, как почтовая марка предоставляет контекст для оценки обычного (бумажного) письма и его содержания. Электронные доказательства включают метаданные как само собой разумеющееся, и суды должны знать о их потенциальной доказательной ценности. Они могут использоваться для отслеживания и идентификации источника и места назначения сообщения, данных на устройстве, которое генерировало электронные доказательства, даты, времени, продолжительности и типа доказательства. Метаданные могут быть релевантными либо в качестве косвенного доказательства (например, указывая наиболее релевантную версию документа), либо сами по себе могут быть релевантными в качестве прямого доказательства (например, в случае манипулирования с данными файла). Руководящие принципы также касаются потерянных метаданных.

Примеры судебной практики в отношении метаданных в **Ирландии**

Метаданные считались важными для подтверждения происхождения электронных документов / материалов («Когер Инк. и Когер (Дублин) против О'Доннела и других» (Koger Inc. & Koger (Dublin) Ltd v O'Donnell & Others) [2010] IEHC 350).

Ирландские суды постановили, что обязательство раскрывать хранящиеся в электронном виде доказательства включает в себя раскрытие метаданных оригинальных документов, если актуально («Сретав против Craven House Capital PLC» (Sretaw v. Craven House Capital PLC) [2017] IEHC 580; «Гэллпхер против RTE» (Gallagher v RTE) [2017] IEHC 237).

27. Распечатками электронных доказательств можно легко манипулировать, поскольку они не включают в себя метаданные или другие скрытые данные. Это означает, что когда сторона представляет распечатку с экрана веб-браузера, такая распечатка вряд ли может быть признана надежным электронным доказательством или основой для проверки подлинности экспертом. Распечатка – это не что иное, как копия экрана. Его можно очень

просто изменить, поскольку для этого не требуется никаких специальных требований к программному или аппаратному обеспечению.

Примеры государств-членов

Апелляционный суд **Литвы** постановил, что мгновенные снимки экрана компьютера (скриншоты) не заслуживают доверия (дело № e2A-226-516 / 2018, 27 апреля 2018 года).

Сбор, изъятие и передача доказательств

28. Электронные доказательства по самой своей природе хрупки и могут быть изменены, повреждены или уничтожены в результате неправильного обращения или изучения. По этим причинам могут быть приняты особые меры предосторожности для надлежащего сбора доказательств такого типа. Невыполнение этого требования может сделать их непригодными для использования или привести к неточным выводам. В принципе, стороны несут ответственность за надлежащий сбор электронных доказательств в гражданском и административном судопроизводстве. Для разных типов данных могут потребоваться разные методы сбора. Действия, предпринятые для обеспечения безопасности и сбора электронных доказательств, не должны влиять на целостность этих доказательств. В делах особой важности сторонам следует рассмотреть возможность сбора электронных доказательств при поддержке ИТ-специалиста или нотариальных служб. Судьи, работники судебной системы, включая практикующих юристов, должны знать, что данные часто хранятся в сетевых службах. Это касается как облачной вычислительной среды, так и онлайновой доставки услуг.

29. При том, что наблюдается рост знаний и опыта со стороны судей, работников судебной системы, включая практикующих юристов, работающих с доказательствами, конкретные стандарты по-прежнему отсутствуют. Для сбора и изъятия электронных доказательств государствам-членам может потребоваться принятие специальных документов и процедур. Между тем, судьи, работники судебной системы, включая практикующих юристов, должны стремиться обеспечить целостность, конфиденциальность и безопасность таких данных. Это включает в себя сохранение защищенных резервных копий в случае сбоя одного из способов хранения. Необходимо сохранять электронные данные в их оригинальном формате.

30. Хотя использование данных может носить исключительно внутренний характер, становится все более вероятным, что они могут носить трансграничный характер с участием других стран. Примером является местоположение в другой стране инфраструктуры, используемой для

обработки или хранения данных, или местоположение провайдера, который позволяет хранить или обрабатывать данные. Следует поощрять прямое сотрудничество между судами и провайдерами услуг удостоверяющего центра или облачных услуг в международных делах. При работе с электронными доказательствами судьи, работники судебной системы, включая юристов, могут принимать во внимание такие факторы, как место учреждения провайдера услуг, место обработки данных и наличие местных законов, регулирующих доступ к данным.

Пример трансграничной технологии

Совместное использование данных (облака) - это хранение различных частей базы данных на разных серверах, которые могут находиться в разных физических местах. Это стало обычной техникой безопасности. Глобальный характер интернета и растущее использование облачных сервисов все менее предполагают, что доступ к данным носит исключительно внутренний характер.

31. Существуют значительные различия между национальными процессуальными правилами сбора доказательств. Суды, использующие доказательства, полученные за границей, должны учитывать эти различия. При трансграничном получении электронных доказательств рекомендуется, чтобы суды тесно сотрудничали в этом вопросе. Запрашивающий суд должен быть проинформирован о процессуальных правилах, используемых запрашиваемым судом, чтобы адаптировать свою оценку электронных доказательств в соответствующих случаях. В частности, получение доказательств за рубежом не должно приводить к нарушению основных принципов и норм процессуального права, таких как равенство сторон.

32. Эффективность разбирательства повышается, если возможна передача электронных доказательств в другие суды в оригинальном формате, а не их распечатывание и отправка. Переданные электронные данные должны сопровождаться соответсвующими метаданными. Это включает использова- ние дополнительных метаданных, созданных судами, для надлежащего управления данными и их беспрепятственной передачи в другие суды. Структурированные метаданные дают судам контроль над доказатель- ствами. В идеале копия электронного доказательства должна использо- ваться для передачи в другой суд.

33. Передачу электронных доказательств с помощью электронных средств можно стимулировать и упрощать посредством внедрения общих техни- ческих стандартов, форматов файлов и оцифровки внутренних судебных и административных систем. Принимая во внимание более высокий риск уничтожения электронных доказательств, следует внедрить

на национальном уровне проце- дуры, обеспечивающие безопасную передачу электронных доказательств.

34. При передаче доказательств должны приниматься во внимание целостность, сохранность и безопасность данных. Надежные услуги, такие как услуги удостоверяющего центра, могут быть необходимы для обеспечения надлежащей передачи электронных доказательств. Если передача требует конфиденциальности, может потребоваться применение мер или технических решений, таких как шифрование, которые обеспечивают доступ к защищенной связи только уполномоченным лицам.

Значимость

35. Количество доказательств, которые могут потребоваться для доказывания определенного факта, может меняться в зависимости от сложности доказательства. Сторона может легко предоставить ненужные большие объемы электронных данных, что затруднит или сделает невозможным эффективное обращение с ними суда или других участников. Следовательно, активное управление судом электронными доказательствами с целью огра- ничить их предоставление только строгой необходимостью для принятия решения по делу является существенным. При активном управлении дан- ными должен соблюдаться принцип пропорциональности. Каждый запрос о предоставлении электронных доказательств должен рассматриваться по существу, в частности, с точки зрения его полезности для целей доказывания. Стороны должны иметь право оспаривать такие запросы.

36. Судьи, работники судебной системы, в том числе практикующие юристы, должны осознавать возможную потребность в технических знаниях и понимать, где могут потребоваться дальнейшие исследования или дополнительные специальные знания, такие как мнение экспертов. Эксперты должны быть компетентными и иметь достаточную подготовку для выполнения поставленной задачи.

Достоверность

37. Отделение цифровой идентичности от физической может вызвать проблемы, связанные с достоверностью доказательств. Во-первых, суды должны стремиться установить личность автора электронных данных. Если в действующем законодательстве не указан способ установления личности, ее можно определить любым объективным способом, например, с помощью электронной подписи или проверки адреса электронной почты, с которого был отправлен документ.

38. Услуги удостоверяющего центра могут предусматривать технологические механизмы, обеспечивающие достоверность доказательств. Например, сертификаты для электронных подписей, иногда называемые «цифровым идентификатором» лица, могут гарантировать как подлинность, так и целостность данных. Если личность подписавшего лица с электронной подписью сомнительна, суд может потребовать от провайдера услуг, связанных с электронной подписью, сделать заявление в отношении вопросов, по которым он компетентен предоставить доказательства. Метка времени (сертификация времени) может быть одинаково важна для подтверждения целостности электронных данных.

Пример услуг удостоверяющего центра

Метка времени – это механизм, который позволяет доказать целостность данных. Она демонстрирует, что данные существовали в определенный момент и не были изменены. Метка времени придает ценность электронным доказательствам, поскольку включает соответствующие метаданные о моменте их создания.

39. Насколько это допускается действующим законодательством и по усмотрению суда, поощряется и рекомендуется принятие судами в качестве доказательства всех видов электронных доказа- тельств. В случае возникновения спора стороны обычно определяют вопросы, подлежащие разрешению, и, если сторона не ставит вопрос о подлинности электронных доказательств, суду не нужно поднимать этот вопрос по собственной инициативе. Только в том случае, если сторона оспаривает электронное доказательство, от стороны, стремящейся пола- гаться на доказательство, может потребоваться продемонстрировать его подлинность, например, путем предоставления метаданных или получения соответствующего предписания для получения дополнительных данных от других лиц, таких как провайдеры услуг удостоверяющего центра.

40. Конкретная ссылка на усмотрение суда в Руководящих принципах 21 и 22 подчеркивает важную роль усмотрения суда в отношении предмета этих Руководящих принципов.

41. Как и в случае любых других доказательств, сторона в судебном производстве может оспорить доказательства. В таком случае указанная сторона может потребовать у суда исключения доказательств, например, из-за того, что автор данных не может быть надлежащим образом идентифицирован. Надежность электронных данных может быть доказана любым способом, например, квалифицированными электронными подписями или другими подобными методами идентификации и обеспечения целостности

данных. Однако в соответствии с применимым законодательством правовое действие электронных подписей определяется, например, при условии, что только квалифицированная электронная подпись должна иметь эквивалентную юридическую силу рукописной подписи (мокрыми чернилами). Например, применимое законодательство может требовать, чтобы устройства, используемые для генерирования подписей, находились под исключительным контролем подписавшего.

Квалифицированная электронная подпись ЕС

Квалифицированные электронные подписи, обеспечивающие целостность данных, не требуют проведения судом специального анализа технологий, используемых для их создания. Достаточно проверить реестр квалифицированных провайдеров услуг удостоверяющего центра ЕС.

42. Руководящий принцип 23 касается бремени доказывания. Более уязвимые лица, такие как потребители и дети, могут не быть технически и / или экономически способны представить электронные доказательства. В тех случаях, когда существуют благоприятные для них законодательные положения, которые облегчают или отменяют бремя доказывания, эти законодательные положения имеют преимущественную силу над Руководящими принципами. Суды должны играть активную роль в случаях, когда дело касается уязвимых лиц.

43. В зависимости от национальной правовой системы следует уважать доказательную ценность публичных (официальных) электронных систем, которые генерируют электронные доказательства. Например, данные из электронных публичных реестров могут рассматриваться как официальный документ, что приводит к презумпции их достоверности. Электронная запись других судебных процессов может рассматриваться как надежное представление фактов без риска человеческой ошибки (например, если сравнивать ее с содержанием, которое судья диктует для внесения в протокол).

Примеры государств-членов общественных систем удостоверения

Существуют конкретные виды трастовых услуг, предоставляемые на национальном уровне, такие как «Доверенный профиль» (Trusted Profile) (**Польша**), «Электронное архивирование и цифровизация» (Electronic archiving and digitalization) (**Бельгия**), «Долгосрочное сохранение информации / документов» (Information/documents long term preservation), Платформа LEXNET для обмена информацией между судебными органами и широкий спектр юридических операторов (**Испания**).

Хранение и обеспечение сохранности

44. Хранение в значении этих Руководящих принципов относится к продолжительности гражданского или административного судопроизводства. Электронные доказательства могут храниться в судах в течение периода судопроизводства, например, на портативных устройствах (картах памяти), серверах, резервных системах и других местах хранения данных (включая облачную вычислительную среду). Суды должны хранить электронные доказательства в их первоначальном формате (например, не в виде распечаток) в соответствии с действующим законодательством. Также следует принимать во внимание вопросы кибербезопрасности, что означает, что суды должны применять проактивные подходы к защите целостности электронных доказательств от киберугроз, включая повреждение или несанкционированный доступ. Уделив должное внимание вопросам предотвращения угроз, суды могут предотвратить влияние киберугроз на целостность электронных доказательств и снизить общие риски кибербезопасности. Посторонние лица не должны иметь доступа к электронным доказательствам независимо от метода их хранения.

45. Хранящиеся электронные доказательства могут быть связаны со стандартными метаданными, описывающими контекст их создания, а также с существующими связями с другими электронными записями. Внедрение международных стандартов для метаданных обеспечивает уровень согласованности при хранении электронных доказательств. Поскольку создание стандартизированных метаданных может быть трудным и трудоемким, суды могут использовать инструменты, которые могут помочь в создании стандартизированных метаданных.

> Пример решения, используемого для стандартизированных метаданных
>
> Существует ряд инструментов для создания стандартизированных метаданных. Например, инструмент управления метаданными может генерировать файл XML (расширяемый язык разметки), содержащий метаданные, относящиеся к электронному доказательству. Для работы с XML-файлами не требуется сложного программного обеспечения. Этот формат одновременно стандартизированный и достаточно гибкий для применения в различных информационных системах. Это может упростить как хранение, так и поиск электронных доказательств.
>
> В этом отношении должны соблюдаться международные стандарты, применяемые к метаданным, например, опубликованные международными сообществами по стандартизации, такими как ISO (Международная организация по стандартизации).

46. Принцип 27, касающийся обеспечения сохранности электронных доказательств, применим как к хранению, так и к архивированию электронных доказательств, которое происходит после завершения производства. Электронное доказательство должно храниться и архивироваться в первоначальной форме, в которой оно было создано, передано, получено и которая существенно не изменяет данные. Электронные доказательства должны быть доступны в читаемом формате в течение всего времени разбирательства. Целостность электронных доказательств должна поддерживаться на всех этапах

Архивирование

47. Руководящие принципы архивирования охватывают период после разбирательства и касаются Рекомендации (2003) 15 Комитета министров Совета Европы государствам-членам об архивировании электронных документов в юридическом секторе. Национальное законодательство обычно предусматривает сроки хранения и технические условия архивирования. Системы, используемые для архивирования, должны быть безопасными и гарантировать отслеживаемое использование и соблюдение конфиденциальности. Должны быть приняты надлежащие технические и организационные меры для обеспечения защиты электронных доказательств и предотвращения несанкционированного доступа к ним. Электронный носитель данных, если он используется, должен быть снабжен идентификационным сертификатом, содержащим основные данные о нем. Такой носитель должен быть надлежащим образом защищен, особенно от потери данных, вредного воздействия химических веществ, тепла, света, излучения, магнитных или электрических полей и от механических повреждений.

48. Службы архивирования могут проверить, возможно, с помощью электронных подписей или других электронных процедур, что электронные доказательства архивируются квалифицированными специалистами или компетентными организациями и что они не изменяли данные. Как данные об электронных подписях, с которыми были подписаны электронные документы, так и данные для проверки этих подписей, должны быть должным образом заархивированы. Государства-члены должны предоставить организациям в юридическом секторе, наделенным законом обязанностью архивирования, необходимые ресурсы для архивации электронных доказательств.

49. Миграция означает смену носителя для сохранения доступа к электронным доказательствам. Пренебрежение миграцией может привести к нечитаемости данных. Электронные документы могут быть заархивированы путем периодической передачи данных с одного носителя на другой или из одного формата в другой. Миграция также должна применяться к метаданным, касающимся архивных электронных документов. Миграция данных на новый носитель должна происходить регулярно, принимая во внимание, например, ухудшение и износ рассматриваемого носителя и до того, как они устареют из-за технологического развития носителей и оборудования. Переход на новый носитель или формат должен осуществляться, когда это необходимо, с учетом технологического развития.

Пример долгосрочного решения

Данные могут быть перенесены на сетевые устройства, такие как облачная вычислительная среда. Они постоянно совершенствуются за счет технологического развития медиа и оборудования. Облачное архивирование может также обеспечить больший контроль над расходами при оплате только за необходимое пространство.

Пример устаревшего решения

CD или DVD или другие оптические диски становятся нечитаемыми из-за физического или химического износа. Причины этого эффекта варьируются от окисления отражающего слоя до физического истирания и истирания поверхностей или краев диска, включая видимые царапины, до других видов реакций с загрязняющими веществами.

Повышение уровня осведомленности, мониторинг, профессиональная подготовка и обучение

50. 50. Содействие включает в себя широкое распространение этих Руководящих принципов среди судов и юристов, их перевод на местные языки, организацию семинаров и конференций по электронным доказательствам.

51. Пересмотр технических стандартов, касающихся электронных доказательств, может включать, например, новые способы их хранения, обеспечения сохранности и архивирования.

52. Доступ к междисциплинарному обучению работе с электронными доказательствами необходим для судей, работников судебной системы, включая практикующих юристов. Обучение может охватывать конкретные проблемы, возникающие в связи с электронными доказательствами, такие как важность метаданных, важность временных меток и использование

облачной вычислительной среды или блокчейна при сборе и изъятии, необходимость представления электронных доказательств в исходном формате, а не просто отсканированных изображений или распечаток.

53. Осведомленность о более широком цифровом контексте и использовании технологий, таких как облачные вычисления, услуги удостоверяющего центра или блокчейн, важна для судей, специалистов, включая практикующих юристов.

54. Знание материальных и процедурных вопросов в контексте электронных доказательств должно быть неотъемлемой частью юридического образования.

Избранная библиография и другие ресурсы

Рекомендация (2003) 15 Комитета министров Совета Европы государствам-членам об архивации электронных документов в юридическом секторе.

Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds.), *Handling and Exchanging Electronic Evidence across Europe*, Springer 2018;

Forgó N., Hawellek C., Knoke F., Stoklas J., *The Collection of Electronic Evidence in Germany - a Spotlight on Recent Legal Developments and Court Rulings*, in: *New Technology, Big Data and the Law* (ed. Forgó, Fenwick, Corrales), Springer 2017;

Morabito V., *Business Innovation Through Blockchain*. *The B³ Perspective*, Springer International Publishing AG Cham 2017;

Hofmann E., Strewe U., Bosia N., *Supply Chain Finance and Blockchain Technology. The Case of Reverse Securitisation*, Springer Munich 2018;

Singer P., Friedman A., *Cybersecurity and cyberwar: What everyone needs to know*, Oxford, Oxford University Press 2014;

Mason S., *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis*. Report prepared by Stephen Mason assisted by Uwe Rasmussen. Strasbourg, 27 July 2016, CDCJ(2015)14-final;

Albert J., *Study on possible national legal obstacles to full recognition of electronic processing of performance information on construction products (under the construction products regulation), notably within*

the regimes of civil liability and evidentiary value, Final General Report, 30-CE-0517177/00-3630-CE-0517177/00-36;

W. Schünemann, M. Baumann Editors (ed.), Privacy, *Data Protection and Cybersecurity in Europe*, Springer International 2017;

Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR)*. A Practical Guide, Springer International 2017;

Mason S., Seng D. (ed.), *Electronic Evidence, Institute of Advanced Legal Studies for the SAS Humanities Digital Library*, School of Advanced Study, University of London, 2017;

Mason S. (ed.), *International Electronic Evidence*, British Institute of International and Comparative Law, 2008;

Mason S., *Electronic Signatures in Law Institute of Advanced Legal Studies for the SAS Humanities Digital Library*, School of Advanced Study, University of London 2016;

Mason S., *Electronic Disclosure A Casebook for Civil and Criminal Practitioners*, PP Publishing 2015;

Electronic Evidence: Model Policy Guidelines & Legislative Texts, Establishment of Harmonized Policies for the ICT Market in the ACP countries, HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures 2013, https://www.itu.int;

Capriolli E., *Droit international de l'économie numérique*, Paris, Litec, 2007;

Biasiotti M. A., Turchi F., Epifani M., *The EVIDENCE Project: bridging the Gap in the Exchange of Digital Evidence Accross Europe*, SADFE 2015, http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/SADFE-2015-Proceedings.pdf (October 2015).

Руководящие принципы относительно использования электронных доказательств в гражданском и административном судопроизводстве представляют собой практический инструмент для упрощения использования данного вида доказательств в судебных разбирательствах. Их главной задачей является обеспечение помощи государствам-членам Совета Европы в адаптировании механизмов урегулирования споров к применению электронных доказательств в гражданском и административном судопроизводстве, что в свою очередь ведет к повышению эффективности и качества правосудия.

Руководящие принципы касаются получения устных доказательств с помощью средств дистанционной связи, использования электронных доказательств, сбора, изъятия и передачи доказательств, значимости, достоверности, хранения и обеспечения их сохранности, архивирования, повышения уровня осведомленности, мониторинга соответствующих технических стандартов, а также подготовки и обучения.

Они представляют собой первый международный инструмент в данной области.

PREMS 147419

RUS

Совет Европы является ведущей организацией на континенте в области прав человека. В неё входят 47 стран, включая все страны Европейского Союза. Все страны - члены Совета Европы подписали Европейскую конвенцию по правам человека, международный договор, призванный защищать права человека, демократию и верховенство права. Европейский суд по правам человека осуществляет надзор за исполнением Конвенции в государствах-членах.

www.coe.int

The European Union is a unique economic and political partnership between 28 democratic European countries. Its aims are peace, prosperity and freedom for its 500 million citizens – in a fairer, safer world. To make things happen, EU countries set up bodies to run the EU and adopt its legislation. The main ones are the European Parliament (representing the people of Europe), the Council of the European Union (representing national governments) and the European Commission (representing the common EU interest).

http://europa.eu

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE