Организация Объединенных Наций A/CN.9/WG.IV/WP.153

Генеральная Ассамблея

Distr.: Limited
6 September 2018
Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Пятьдесят седьмая сессия
Вена, 19–23 ноября 2018 года

Правовые вопросы, связанные с управлением идентификационными данными и удостоверительными услугами

Записка Секретариата

Содержание

V.18-05870 (R) 190918 260918

I. Введение

1. В целях содействия дальнейшему обсуждению в настоящей записке освещаются отдельные аспекты некоторых тем, определенных Рабочей группой как имеющие отношение к рассмотрению ею правовых вопросов, связанных с управлением идентификационными данными («УИД») и удостоверительными услугами (A/CN.9/936, пункт 58). В частности, в ней преследуется цель обратить внимание на основные проблемы и предложить возможные пути их решения и не предполагается ограничивать возможности рассмотрения, при необходимости, дополнительных тем или рассмотрения нескольких тем одновременно. В рабочем документе A/CN.9/WG.IV/WP.154 освещаются некоторые аспекты других тем, определенных Рабочей группой как имеющие отношение к рассматриваемым ею правовым вопросам, связанным с УИД и удостоверительными услугами.

2. Справочная информация о деятельности Рабочей группы по правовым вопросам, связанным с УИД и удостоверительными услугами, изложена в пунктах 6–17 рабочего документа A/CN.9/WG.IV/WP.152. Перечень дополнительных документов, имеющих отношение к этой теме, содержится в пункте 18 рабочего документа A/CN.9/WG.IV/WP.152.

II. Актуальные вопросы будущей работы, связанной с правовыми аспектами управления идентификационными данными и удостоверительными услугами

A. Сфера охвата работы

3. В соответствии с рекомендацией Рабочей группы Комиссия просила Рабочую группу провести работу по правовым вопросам, связанным с УИД и удостоверительными услугами, в целях подготовки текста, призванного содействовать трансграничному признанию УИД и удостоверительных услуг. Просьба Комиссии изложена в достаточно широких формулировках для того, чтобы охватить дополнительные аспекты правового режима УИД и удостоверительных услуг, помимо тех, которые уже были определены (см. пункт 1 выше).

4. Юридические механизмы трансграничного признания УИД и удостоверительных услуг являются одним из основополагающих компонентов правовой среды, способствующей развитию цифровой экономики, тогда как их отсутствие может привести к увеличению «цифрового разрыва». Так, Рабочая группа, возможно, пожелает рассмотреть свою деятельность в более широком контексте решения проблемы «цифрового разрыва».

5. В этой связи Рабочая группа, возможно, пожелает рассмотреть вопрос о том, может ли отсутствие национальной правовой базы, позволяющей использовать УИД и удостоверительные услуги, являться преградой для трансграничного юридического признания УИД и удостоверительных услуг. В этом случае Рабочая группа, возможно, пожелает определить правовые положения, которые необходимо будет включить в национальное законодательство, чтобы в полной мере обеспечить трансграничное юридическое признание УИД и удостоверительных услуг, и обсудить тип правового текста (например, международный договор, типовой закон или и то, и другое), который наиболее подходил бы для достижения этой цели.

6. Кроме того, независимо от иностранных элементов, трансграничное юридическое признание идентичности имеет общие черты с юридическим признанием идентичности в различных системах УИД. Поэтому Рабочая группа, возможно, пожелает рассмотреть вопрос о целесообразности обсуждения механизма, обеспечивающего юридическое признание в различных системах

управления идентификационными данными, с учетом, в надлежащих случаях, иностранных элементов. В таком случае результатом деятельности Рабочей группы могли бы стать руководящие указания в отношении УИД как на национальном, так и на международном уровне.

1. Основополагающая идентичность в сопоставлении с транзакционной идентичностью

7. Рабочая группа, возможно, пожелает вновь обратить внимание на то, что было предложено разграничить первичное и вторичное определения идентичности (A/CN.9/WG.IV/WP.149, пункт 29).

8. Первичное определение идентичности, или основополагающая идентичность, означает присвоение идентификационных данных в том контексте, в котором создается объект, в момент его создания. Таким образом, основополагающая идентичность является, как правило, уникальной и незаменимой. К примерам первичного определения идентичности относятся в частности: регистрация актов гражданского состояния и внесение важнейших статистических записей физического лица органами власти; включение юридического лица в соответствующий реестр компетентным органом, например, в реестр коммерческих корпораций; и присвоение цифровому объекту идентификатора цифрового объекта.

9. Вторичное определение идентичности, или транзакционная идентичность, означает использование идентификационных данных для выполнения конкретной функции (например, для заключения договора; выдачи банкоматом денежных средств; выдачи справки публичным органом).

10. Хотя основополагающая идентичность как таковая зачастую может и не использоваться в коммерческих сделках, ею могут воспользоваться поставщики идентификационных данных для определения транзакционной идентичности. Например, в соответствии с положениями ЮНСИТРАЛ об электронных подписях требуется идентификация подписавшего лица. В некоторых случаях надежная идентификация подписавшего лица может осуществляться на основе использования идентификационных учетных данных и процесса аутентификации, определяющего идентичность исходя из основополагающих идентификационных учетных данных. Таким образом, трансграничное юридическое признание основополагающей идентичности и такое признание в системах управления идентификационными данными может быть полезным или даже необходимым.

2. Охватываемые объекты

11. Рабочая группа предварительно обсудила виды объектов, имеющих отношение к своей работе (A/CN.9/936, пункты 63–65), иными словами объекты, к которым будут применяться результаты своей деятельности. В целом такими объектами были признаны физические и юридические лица, участвующие в торговле, в том числе международной. Во внимание могут быть приняты также объекты, не являющиеся отдельными юридическими лицами, но причастные к коммерческой деятельности. Например, в наименее развитых странах торговцы, осуществляющие свою деятельность в неформальном секторе, могут использовать в качестве основного способа идентификации мобильные идентификационные данные.

12. Участие публичных объектов может быть оправдано с учетом важности для международной торговли некоторых деловых отношений между предприятиями и правительствами и между правительствами, в частности трансграничных механизмов «единого окна» для таможенных операций. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, возникают ли в связи с участием публичных структур в операциях в сфере УИД или доверительных услуг особые вопросы, принимая во внимание, в частности, применение принципов технологической нейтральности (см. пункты 38–40 ниже), автономии сторон (см. пункты 41–47 ниже) и соразмерности средств электронной идентификации для выполняемой функции (см. пункт 46 ниже).

13. Были высказаны разные мнения по вопросу о том, относится ли к сфере охвата этой работы идентификация материальных и цифровых объектов. Согласно одному мнению, материальные и цифровые объекты следует исключить, поскольку они не обладают правосубъектностью и сами по себе не могут быть привлечены к ответственности. В то же время было высказано мнение о том, что такая идентификация не требует наличия признака самостоятельного юридического лица или установления ответственности для идентифицированного объекта (A/CN.9/936, пункт 64).

14. Другая точка зрения заключалась в том, что вопрос об идентификации объектов мог бы быть рассмотрен после изучения Рабочей группой вопроса об идентификации лиц (A/CN.9/936, пункт 65). В этой связи следует отметить, что в контексте модели «интернет вещей» объекты являются одним из основных источников больших данных и что для этой модели особое значение имеет надежное присвоение данных. Например, все более широкое распространение получает использование медицинских приборов, удаленно отслеживающих состояние пациента в ходе повседневной деятельности. При этом важнейшее значение имеет обеспечение присвоения автоматически созданной этими приборами информации именно тем пациентам, к которым она относится. Аналогичным образом необходимо отслеживать лекарственные препараты не только на момент их приема, но также на протяжении всего производственного цикла с целью обеспечить надлежащую идентификацию лекарственного препарата, а также гарантировать его происхождение и состав. Также крайне важно обеспечить надежную идентификацию самого лекарственного препарата и содержащихся в нем веществ.

B. Определения

15. Рабочая группа, возможно, пожелает обратиться к документу A/CN.9/WG.IV/WP.150, содержащему перечень терминов и понятий, имеющих отношение к управлению идентификационными данными и удостоверительным услугам, которые могли бы быть полезными в ходе обсуждения этой темы. Этот перечень не препятствует дальнейшему обсуждению Рабочей группой определений соответствующих терминов по мере продвижения работы.

16. Что касается УИД, то в ходе обсуждения Рабочей группой вопросов, затрагиваемых в настоящей записке, особенно полезными могут быть следующие определения, содержащиеся в документе A/CN.9/WG.IV/WP.150.

17. «Идентичность» или «идентификационные данные» (identity) означают a) информацию о конкретном субъекте в форме одного или нескольких атрибутов, позволяющих субъекту быть в достаточной степени отличимым в определенном контексте; b) набор относящихся к тому или иному лицу атрибутов, которые однозначно характеризуют это лицо в данном контексте (A/CN.9/WG.IV/WP.150, пункт 31).

18. Рабочая группа, возможно, пожелает рассмотреть взаимосвязь между этими определениями и понятиями основополагающей идентичности и транзакционной идентичности (см. пункты 7–10 выше), а также значение этих понятий для своей будущей работы. В этой связи Рабочая группа, возможно, пожелает разъяснить, является ли уникальность атрибутом основополагающей идентичности.

19. «Управление идентификационными данными» (identity management) означает набор приемов, позволяющих управлять процессами идентификации, аутентификации и авторизации физических и юридических лиц, устройств и других субъектов в онлайновом режиме (A/CN.9/WG.IV/WP.150, пункт 35).

20. «Система идентификации» (identity system) означает онлайновую систему для управления идентификационными данными, которая регулируется набором системных правил (именуемых также структурой доверия) и в которой

физические лица, организации, службы и устройства могут доверять друг другу, поскольку авторитетные источники устанавливают и удостоверяют подлинность их идентификационных данных (A/CN.9/WG.IV/WP.150, пункт 38).

21. «Операция с идентификационными данными» (identity transaction) означает любую операцию с двумя или более участниками, которая включает установление, проверку, выдачу, утверждение, аннулирование, передачу или использование идентификационной информации (A/CN.9/WG.IV/WP.150, пункт 39).

22. Рабочая группа, возможно, пожелает воспользоваться понятиями «управление идентификационными данными», «система идентификации» и «операции с идентификационными данными», чтобы разобраться в вопросе о том, следует ли ей в ходе работы по теме юридического признания УИД вести речь о системах идентификации, об операциях с идентификационными данными или же о том и другом (см. пункты 57–59 ниже).

23. «Уровень обеспечения доверия» (level of assurance) означает установление степени уверенности в процессах идентификации и аутентификации — т.е. a) степени уверенности в процессе проверки, используемой для установления идентичности объекта, которому были выданы учетные данные, и b) степени уверенности в том, что объект, использующий учетные данные, является тем самым объектом, которому были выданы учетные данные. Уровень обеспечения доверия отражает надежность используемых методов, процессов и технологий (A/CN.9/WG.IV/WP.150, пункт 42).

24. В ходе обсуждения этой темы Рабочая группа, возможно, пожелает сослаться на определение «уровень обеспечения доверия» (см. пункты 10–19 документа A/CN.9/WG.IV/WP.154). При этом Рабочая группа, возможно, пожелает также принять во внимание следующее определение «уровня гарантии» (assurance level): «уровень доверия к связи между тем или иным объектом и представленной информацией идентичности» (A/CN.9/WG.IV/WP.150, пункт 12), а также примечание к этому определению, в котором поясняется, что понятия «гарантия определения идентичности» (identity assurance) и «гарантия обеспечения аутентификации» (authentication assurance) могут рассматриваться как отдельные компоненты общего понятия «уровень обеспечения доверия» (level of assurance).

C. Общие принципы

25. Рабочая группа определила следующие общие принципы как относящиеся к своей работе по правовым аспектам УИД и удостоверительных услуг: недискриминация в отношении использования электронных средств; функциональная эквивалентность; технологическая нейтральность; и автономия сторон (A/CN.9/936, пункт 67).

1. Недискриминация в отношении использования электронных средств

26. Принцип недискриминации в отношении использования электронных средств закреплен во многих текстах ЮНСИТРАЛ. В контексте УИД и удостоверительных услуг этот принцип можно было бы сформулировать, в частности, следующим образом[1]:

> Верификация идентичности на основе использования [идентификационных учетных данных] [систем управления идентификационными данными] и удостоверительных услуг не может быть лишена юридической силы, действительности или исковой силы на том лишь основании, что эти

[1] Проекты положений включены только в целях приведения примеров без ущерба для рекомендаций Рабочей группы Комиссии относительно возможной формы ее работы и связанных с этой формой решений Комиссии.

[идентификационные учетные данные] [системы управления идентификационными данными] и удостоверительные услуги имеют электронную форму.

27. В этом проекте положения предлагается выбрать либо «идентификационные учетные данные», либо «системы управления идентификационными данными», исходя из того, о чем следует вести речь — об использовании учетных данных в целях идентификации или же о системе УИД в целом (см. пункты 57–59 ниже).

2. Функциональная эквивалентность

28. В сфере электронной торговли принцип функциональной эквивалентности предусматривает требования, которым должны отвечать электронные запись, метод или процесс для того, чтобы выполнять те же функции, как если бы они были в бумажной форме.

a) УИД

29. Положение о функциональной эквивалентности в отношении УИД можно было бы сформулировать следующим образом:

В тех случаях, когда законодательство требует идентификации объекта или допускает ее, это требование считается выполненным в отношении управления [электронными] [цифровыми] идентификационными данными, если для [верификации [соответствующих] атрибутов объекта] используется надежный метод.

30. Положение о функциональной эквивалентности в отношении идентификации призвано перенести идентификационные требования, применимые к идентификации бумажных документов, в электронную среду. Рабочая группа, возможно, пожелает рассмотреть вопрос о включении слова «[соответствующих]» для указания на то, что для успешной идентификации в режиме онлайн будут необходимы только те атрибуты, которые требуются для идентификации в режиме офлайн. Рабочая группа, возможно, пожелает также уточнить, на какое понятие следует ссылаться — на «электронные идентификационные данные» или же на «цифровые идентификационные данные».

31. Также могут быть подготовлены дополнительные рекомендации в отношении элементов, имеющих значение для определения надежности метода, в частности: a) договорных соглашений, если они допускаются применимым законодательством; b) сертификации третьей стороной и самостоятельной сертификации; и c) соотнесения с уровнями обеспечения доверия. В частности, в связи с упоминанием об использовании «надежного метода» в положении о функциональной эквивалентности, возможно, потребуется использовать метод, обеспечивающий эквивалентный уровень надежности идентификации как в режиме онлайн, так и в режиме офлайн.

32. При обсуждении положения о функциональной эквивалентности в отношении УИД, возможно, было бы полезным сослаться на конкретные случаи использования УИД. В этой связи следует отметить, что идентификация может требоваться для различных целей или функций. Одной из целей является соблюдение нормативных требований. Примером этого требования является применение правила «знай своего клиента» (ЗСК) в финансовом, телекоммуникационном и других коммерческих секторах, а также в области электронных закупок, где правильная идентификация потенциальных поставщиков и клиентов необходима для предотвращения мошенничества и сговора и приведения в исполнение решения о запрещении деятельности.

33. Еще одной целью идентификации является подтверждение действительности коммерческого документа. Например, законодательство, применимое к коносаментам, может требовать идентификации определенных сторон. Об этом говорится в статье 15 Конвенции Организации Объединенных Наций о морской

перевозке грузов (Гамбург, 1978 год) («Гамбургские правила»)[2] и в статье 36 Конвенции Организации Объединенных Наций о договорах полностью или частично морской международной перевозки грузов (Нью-Йорк, 2008 год) («Роттердамские правила»)[3].

34. Кроме того, стороны электронных сделок могут договориться об использовании определенных процедур и методов для точной идентификации друг друга в целях уменьшения рисков и в отсутствие каких-либо законодательных требований на этот счет. Источник такой обязанности идентифицировать себя имеет договорный характер.

35. В случаях, когда идентификация в режиме офлайн, хотя и используется, не является в полной мере удовлетворительной, в целях более эффективного выполнения обязанностей по идентификации может быть принято принципиальное решение относительно перехода на более высокие стандарты идентификации. Рабочая группа, возможно, пожелает рассмотреть взаимосвязь между принятием положения о функциональной эквивалентности и возможным установлением в отношении онлайновой идентификации более строгих требований, нежели требования, применимые в режиме офлайн.

b) Удостоверительные услуги

36. В текстах ЮНСИТРАЛ содержатся положения о функциональной эквивалентности в отношении определенных удостоверительных услуг, а именно в отношении электронных подписей в статье 7 Типового закона ЮНСИТРАЛ об электронной торговле («ТЗЭТ»)[4], статье 6 Типового закона ЮНСИТРАЛ об электронных подписях («ТЗЭП»)[5], статье 9(3) Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах (Нью-Йорк, 2005) («КЭС»)[6] и в статье 9 Типового закона ЮНСИТРАЛ об электронных передаваемых записях[7], и в отношении сохранения и архивирования данных (в статье 10 ТЗЭТ). Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли подготовить конкретные положения для результатов предоставления каждого вида удостоверительных услуг или же в качестве альтернативы можно было бы или следовало бы разработать какое-либо общее положение о функциональной эквивалентности (см. A/CN.9/WG.IV/WP.154, пункт 58).

37. Также Рабочая группа, возможно, пожелает рассмотреть вопрос о том, является ли желательной разработка положения об атрибуции идентификационной информации, или же положения о функциональной эквивалентности будет достаточно, поскольку идентификационная информация будет присваиваться тому же объекту, которому она присваивается в режиме офлайн, и в любом случае она не будет присваиваться поставщику идентификационных услуг. В статье 13 ТЗЭТ содержится пример положения, касающегося атрибуции.

3. Технологическая нейтральность

38. Принцип технологической нейтральности лежит в основе текстов ЮНСИТРАЛ и многих других законодательных положений, касающихся использования электронных сообщений. В контексте УИД и удостоверительных услуг, возможно, потребуется подготовка рекомендаций в отношении минимальных системных требований, в которых будет говориться непосредственно о свойствах системы, а не о конкретных технологиях (A/CN.9/936, пункт 69). Если же будет выбран операционный подход (см. пункты 57–59 ниже), то могут потребоваться рекомендации в отношении минимальных требований к

---

[2] United Nations, Treaty Series, vol. 1695, No. 29215, p. 3.
[3] Резолюция 63/122 Генеральной Ассамблеи, приложение.
[4] Издание Организации Объединенных Наций, в продаже под № R.99.V.4.
[5] Издание Организации Объединенных Наций, в продаже под № R.02.V.8.
[6] United Nations, Treaty Series, vol. 2898.
[7] Издание Организации Объединенных Наций, в продаже под № eISBN 978-92-1-362739-6.

операциям с идентификационными данными, в которых будет говориться уже о свойствах операций. В контексте удостоверительных услуг для соблюдения принципа технологической нейтральности, возможно, потребуется определить конкретные цели, которые преследуются при оказании каждой удостоверительной услуги, без установления обязательства использовать какую-либо конкретную технологию для достижения этих целей.

39. Положение об одинаковом режиме для технологий, методов и систем, связанных с УИД и удостоверительными услугами, можно было бы сформулировать следующим образом:

> Ничто в настоящем [проекте документа] не применяется таким образом, чтобы исключать, ограничивать или лишать юридической силы любые [технологию, метод или систему], используемые для управления идентификационными данными и удостоверительных услуг, которые удовлетворяют требованиям, предусмотренным в настоящем [проекте документа] [, или иным образом отвечают требованиям применимого права].

40. Формулировка «или иным образом отвечают требованиям применимого права», содержащаяся в статье 3 ТЗЭП, предназначена для ряда определенных случаев, когда в другом законодательстве, помимо проекта документа, может предусматриваться использование других требований, отличающихся от изложенных в проекте документа[8].

4. Автономия сторон

41. Принцип автономии сторон означает, в частности, факультативность использования идентификационных и удостоверительных услуг. Этот принцип может в полной мере применяться к коммерческим услугам, однако в контексте доступа к услугам, предоставляемым публичными учреждениями, или взаимодействия с этими учреждениями его применение по принципиальным соображениям может быть ограниченным.

42. Положение о факультативном использовании идентификационных и удостоверительных услуг можно было бы сформулировать следующим образом:

> 1. Ничто в настоящем [проекте документа] не требует от объекта использовать или принимать [идентификационные учетные данные] [системы управления идентификационными данными] и удостоверительные услуги без согласия этого объекта.
>
> 2. Согласие объекта на использование [идентификационных учетных данных] [систем управления идентификационными данными] и удостоверительных услуг может вытекать из поведения этого объекта [и других обстоятельств].
>
> [Пункт 1 не применяется в отношении: ...]

43. В этом проекте положения предлагается выбрать либо «идентификационные учетные данные», либо «системы управления идентификационными данными», исходя из того, о чем следует вести речь — об использовании полномочий в целях идентификации или же о системе управления идентификационными данными в целом (см. пункты 57–59 ниже).

44. Во второй пункт проекта положения включена формулировка «[и других обстоятельств]» с целью охватить случаи, когда объект не способен совершать самостоятельные действия (например, материальный или цифровой объект). В этих случаях согласие необходимо будет получить не от объекта, а от физического или юридического лица, осуществляющего контроль над этим объектом.

---

[8] *Типовой закон ЮНСИТРАЛ об электронных подписях и Руководство по принятию* (издание Организации Объединенных Наций, в продаже под № R.02.V.8), пункт 107.

45. На автономию сторон распространяются ограничения, установленные в законодательстве, подлежащем обязательному применению (A/CN.9/936, пункт 72). Эти ограничения имеют особое значение, поскольку законодательные требования, выполняемые при использовании УИД и удостоверительных услуг, зачастую имеют императивный характер. С учетом вышесказанного для этого принципа предлагается следующая формулировка, основанная на статье 5 ТЗЭП:

> Допускается отход от положений настоящего [проекта документа] или изменение их действия по договоренности, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь силы согласно применимому праву.

46. Применение принципа автономии сторон также обеспечивает свободу выбора тех идентификационных и удостоверительных услуг, которые являются наиболее подходящими для выполнения необходимой сторонам функции (так называемый «принцип соразмерности»). Свобода выбора вида услуг также тесно связана с принципом технологической нейтральности.

47. Принцип автономии сторон призван также способствовать приведению в исполнение договорных соглашений, таких как системные правила УИД и системные правила и структуры удостоверительных услуг. Поэтому системные правила могут иметь особое значение в контексте федерации систем УИД (см. A/CN.9/WG.IV/WP.154, пункт 39). Рабочее определение понятия «идентификационная федерация» означает «группу поставщиков идентификационных данных, полагающихся сторон, субъектов и других лиц, которые соглашаются действовать в рамках сходных программных установок, стандартов и технологий, указанных в системных правилах (или структуре доверия), для того чтобы предоставляемая поставщиками идентификационных данных идентификационная информация по субъекту была понятна полагающимся сторонам и заслуживала их доверия» (A/CN.9/WG.IV/WP.150, пункт 28).

5. Обязательство идентифицировать

48. Согласно еще одному общему принципу, часто встречающемуся в текстах ЮНСИТРАЛ об электронной торговле, не затрагиваются нормы материального права, например, права, обычно применимого к коммерческим сделкам.

49. В контексте УИД и удостоверительных услуг этот принцип означает, что в законодательство в области УИД не следует включать никаких новых обязанностей в отношении идентификации, что в законодательство в области удостоверительных услуг не следует включать никаких новых обязанностей в отношении использования какого-либо конкретного вида удостоверительных услуг и что существующие обязанности остаются неизменными.

50. Соответствующее положение можно было бы сформулировать следующим образом:

> Ничто в настоящем [проекте документа] не устанавливает для стороны требования [верифицировать идентификационные данные другого объекта] [идентифицировать другой объект] или использовать ту или иную удостоверительную услугу.

6. Единообразное толкование

51. В текстах ЮНСИТРАЛ обычно содержится положение, в котором говорится об их равной аутентичности и обязанности единообразного толкования. Это положение призвано обеспечить сохранение единообразия при толковании и применении законодательных текстов.

52. Соответствующее положение можно было бы сформулировать следующим образом:

> 1. При толковании настоящего [проекта документа] надлежит учитывать его международный характер и необходимость содействовать достижению единообразия в его применении, а также соблюдению добросовестности в международной торговле.
>
> 2. Вопросы, относящиеся к предмету регулирования настоящего [проекта документа], которые прямо в нем не разрешены, подлежат разрешению в соответствии с общими принципами, на которых он основан, а при отсутствии таких принципов — в соответствии с правом, применимым в силу норм частного международного права.

53. Ссылка на «право, применимое в силу норм частного международного права» во втором пункте этого проекта положения может быть особенно полезной в трансграничном контексте.

D. Требования и механизмы юридического признания

54. В целом юридическое признание можно понимать как определение требований, которые должны быть удовлетворены для получения правового статуса в той или иной юрисдикционной системе. На национальном уровне для такого юридического признания, возможно, потребуется разработка соответствующих материально-правовых норм.

55. Трансграничное юридическое признание можно понимать как a) предоставление такого же правового статуса в принимающей юрисдикционной системе, который предоставляется в юрисдикционной системе происхождения; b) предоставление такого же правового статуса, который предоставляется в принимающей юрисдикционной системе, независимо от какого бы то ни было иностранного элемента; или c) определение последствий юридического признания в отдельном документе. Кроме того, юридическое признание может иметь взаимный, или зеркальный характер, или же осуществляться в одностороннем порядке. В обоих случаях могут устанавливаться условия для такого признания.

56. Основной рассматриваемой Рабочей группой темой является юридическое признание схем УИД и удостоверительных услуг, которое позволило бы легализовать такие технические возможности, как операционная совместимость идентификационных учетных данных и удостоверительных услуг и использование одних и тех же идентификационных данных и удостоверительных услуг в разных схемах УИД. Как отмечалось выше (пункт 6), трансграничное юридическое признание идентичности имеет общие черты с юридическим признанием идентичности в различных системах УИД, независимо от иностранных элементов.

57. Объектом юридического признания могут быть системы и схемы УИД и удостоверительных услуг. В этом случае могут потребоваться юридические рекомендации в отношении свойств, которыми должны обладать такие системы и схемы для получения юридического признания. Как следствие, юридическое признание могут получить и рабочие процессы этих систем и схем, используемые в ходе операций, иными словами средства электронной идентификации и конкретные удостоверительные услуги.

58. Объектом юридического признания могут быть также операции, осуществляемые с использованием УИД и удостоверительных услуг. В этом случае могут потребоваться юридические рекомендации в отношении условий, которые должны быть выполнены для юридического признания идентификационных учетных данных и верификации идентификационных данных, а также результатов оказания удостоверительных услуг. В существующих текстах ЮНСИТРАЛ об электронной торговле рассматриваются в основном операционные вопросы. Например, в ТЭЭП рассматривается в основном использование электронных

подписей при совершении сделок и лишь частично — свойства систем электронных подписей.

59. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, следует ли ей в своей работе по теме юридического признания сосредоточить внимание на системах и схемах УИД и удостоверительных услуг или на операциях с использованием УИД и удостоверительных услуг, или же охватить и то, и другое.

60 Рабочая группа, возможно, пожелает дополнительно рассмотреть вопрос о том, должна ли ее работа предусматривать только лишь разработку механизма трансграничного юридического признания, или следует также уделить внимание юридическому признанию в различных системах на национальном уровне.

1. УИД

a) Юридическое признание ex ante

61. Один из имеющихся механизмов юридического признания схем УИД предусматривает предварительное составление перечня признанных схем УИД и указание условий для включения в этот перечень. Такой подход, как правило, требует создания централизованного институционального механизма оценки и лицензирования для оценки схем УИД.

62. Такой подход может использоваться также в отношении удостоверительных услуг и позволяет обеспечить ясность и предсказуемость в отношении схем и услуг, которые могут использоваться в различных системах и на трансграничной основе. Вместе с тем при таком подходе юридическое признание могут не получить те схемы и услуги, которые, хотя и используются, в этот перечень не включены. В зависимости от порядка регулирования этот подход может оказаться неспособным реагировать на события столь оперативно, как того может потребовать технический прогресс, что может затруднить внедрение инноваций и привести к введению требований, ориентированных на конкретные технологии.

63. Что касается институционального механизма, необходимого для применения этого подхода, то требуется определить обязательные условия для включения в перечень проводящих оценку учреждений и критерии оценки схем УИД, а также механизмы их обновления, процедуры оценки принимаемых решений и источники финансирования. В зависимости от ряда факторов, в том числе от уже существующих институциональных механизмов, управление такой системой лицензирования может оказаться довольно сложной и дорогостоящей задачей.

64. Более того, централизованная система лицензирования может функционировать более эффективно в сравнительно ограниченных масштабах и в рамках более широких инициатив экономической интеграции, однако на глобальном уровне ее применение может быть затруднено, поскольку может потребоваться активное сотрудничество ее членов.

65. Применение централизованной системы лицензирования на глобальном уровне может потребовать принятия международного договора или иного имеющего такую же обязательную силу международного правового документа. Преимуществами механизма на основе международного договора являются, в частности, предсказуемость и, вероятно, более простое применение для публичных учреждений; недостатки же связаны, в частности, с издержками, сопряженными с созданием и поддержкой функционирования институционального механизма, расходами, которые несут участвующие в нем схемы, и необходимостью заручаться поддержкой достаточного числа государств, схем и пользователей. Механизм на основе международного договора может оказаться особенно уместным для обеспечения финансирования долгосрочных финансовых обязательств, хотя возможно и возмещение расходов за счет пользователей.

66. Принятые в последнее время законы об УИД предусматривают осуществление централизованного надзора для признания правовых последствий применения схем УИД.

67. Единственным законодательным актом, в котором непосредственно рассматриваются трансграничные вопросы, связанные с УИД, является Постановление eIDAS[9]. В частности, статья 6 eIDAS позволяет использовать средства электронной идентификации одного государства — члена ЕС для получения услуг, предоставляемых в режиме онлайн публичным органом в другом государстве-члене, если соблюдены определенные условия. Согласно одному из условий средства электронной идентификации должны относиться к схеме электронной идентификации, о которой уведомлена Европейская комиссия и которая удовлетворяет установленным Европейской комиссией требованиям операционной совместимости. Частью процесса уведомления является проведение экспертного обзора.

68. Другие законы об УИД нацелены на регулирование вопросов УИД, однако трансграничные вопросы в них напрямую не рассматриваются. В этой связи следует отметить, что Постановление eIDAS не затрагивает существующие схемы УИД и призвано обеспечить трансграничное взаимное правовое признание этих схем, тогда как в национальных законах об УИД определяются условия функционирования схем УИД.

69. В законе 2017-20 Бенина содержится раздел, посвященный УИД, в котором рассматриваются уровни гарантии схем электронной идентификации, обязательные условия для направления уведомления о схемах электронной идентификации, нарушениях безопасности, ответственности и операционной совместимости. Эти положения, как правило, основываются на соответствующих положениях, содержащихся в Постановлении eIDAS.

70. В законе об электронном УИД штата Виргиния[10] закреплен механизм, позволяющий не привлекать к ответственности операторов структур доверия в рамках систем идентификации, если они удовлетворят ряд нормативных и законодательных требований (см. A/CN.9/WG.IV/WP.154, пункты 28 и 29). Что касается правовых последствий, то использование идентификационных учетных данных или атрибутов идентификационных данных, соответствующих стандартам, установленным Содружеством Виргинии, условиям договоров и регламентам федераций, удовлетворяет любые требования в отношении коммерчески обоснованного метода защиты или процедуры атрибуции согласно Единообразному закону об электронных операциях и Единообразному закону о компьютерных операциях с информацией[11].

71. В законе № 205-2018 штата Вермонт предусматривается создание нового вида особого коммерческого образования — под названием компании по защите персональной информации — для управления персональной информацией, а именно для предоставления элементов персональной информации об отдельных потребителях третьим сторонам для целей совершения сделок и предоставления услуг сертификации или валидации в отношении персональной информации.

72. Согласно положениям этого закона его цель заключается в том, чтобы компании по защите персональной информации действовали «в наилучших интересах и в целях защиты, и во благо потребителей» (раздел 2451 (3)(B)). В статье 2452 закона № 205-2018 закреплено, что компания по защите персональной

[9] Постановление (EU) № 910/2014 Европейского парламента и Совета от 23 июля 2014 года об электронной идентификации и удостоверительных услугах в отношении электронных операций на внутреннем рынке и отмене Директивы 1999/93/ЕС.

[10] Virginia Electronic Identity Management Act, VA Code §§ 2.2-436–2.2-437 and VA Code §§ 59.1-550–59.1-555.

[11] Единообразный закон об электронных сделках 1999 года и Единообразный закон о компьютерных операциях с информацией 1999 года с поправками, внесенными в 2000 и 2002 годах, являются типовыми законами, подготовленными Национальной конференцией уполномоченных Соединенных Штатов по единообразному законодательству штатов.

информации находится в доверительных отношениях с потребителем при предоставлении услуг по защите персональной информации.

73. Финансовое управление штата Вермонт, уполномоченное осуществлять надзор над компаниями по защите персональной информации, может разработать правила, касающиеся сроков подготовки и содержания отчетов, которые должны будут представлять эти компании. Управление может также принять нормативные положения о защите и сохранности персональной информации и об обмене такой информацией с третьими сторонами.

b) Юридическое признание ex post

74. В качестве альтернативы юридическое признание может осуществляться с помощью механизма, который, как правило, позволяет осуществлять обмен информацией и оценку пригодности для использования схем УИД и удостоверительных услуг только в случае возникновения спора и исходя из заранее определенных критериев. В текстах ЮНСИТРАЛ применение такого подхода выражается, например, в использовании так называемых критериев надежности «ex post facto» (см., например, статью 9(3) КЭС).

75. Преимущество этого подхода заключается в предоставлении сторонам сделки максимальной гибкости в выборе технологий и методов для сторон сделки. Более того, подход не требует создания институционального механизма, что исключает сопряженные с этим расходы, и не должен регулироваться на централизованной основе. С другой стороны, его недостаток заключается в том, что для оценки пригодности схемы УИД или удостоверительной услуги для трансграничного использования необходимо проведение процедур досудебного урегулирования третьей стороной, которые могут также оказаться дорогостоящими и затяжными и поставить стороны в положение неопределенности.

c) Юридическое признание на основе соотнесения с ключевыми параметрами

76. Одно из предложений предусматривает возможность описания систем УИД через соотнесение с ключевыми параметрами с использованием общего шаблона. Юридические требования к такой работе и ее последствия могли бы быть определены принимающей юрисдикционной системой и системой УИД.

77. В целях обеспечения результативности такого описания в процессе работы можно было бы руководствоваться общей характеристикой уровней обеспечения доверия, что, в свою очередь, позволило бы и далее придерживаться принципа технологической нейтральности.

78. Для проведения такой работы не требовалось бы разрешения центрального органа, и она могла бы быть выполнена любой заинтересованной стороной, в том числе частными и коммерческими структурами. Результаты работы по такому соотнесению могли бы быть опубликованы в официальном перечне для открытого распространения.

79. При проведении работы по описанию систем через соотнесение с ключевыми параметрами, необходимо будет принять во внимание ряд параметров, например параметры, определенные в Постановлении (EU) № 2015/1502 Комиссии об имплементации, действующем в рамках Постановления eIDAS. Такими параметрами являются следующие: запись, управление электронными средствами идентификации, аутентификация, управление и организация. Каждый параметр включает в себя несколько составляющих. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, насколько подробные рекомендации потребуются в отношении технических спецификаций и процедур, которых необходимо будет придерживаться в ходе работы по описанию систем через соотнесение с ключевыми параметрами.

80. Наглядно представить, каким образом может быть проведена работа по описанию через соотнесение с ключевыми параметрами, поможет практический пример. Как уже отмечалось, в различных коммерческих секторах широко

применяется правило ЗСК. В зависимости от характера конкретной сделки требования ЗСК обычно удовлетворяются за счет использования полномочий уровня обеспечения доверия «два», или «высокий», или уровня обеспечения доверия «три», или «существенный» (см. описание различных уровней обеспечения доверия в пунктах 13 и 14 документа A/CN.9/WG.IV/WP.154).

81. Такие требования, как правило, не могут быть удовлетворены при использовании идентификационных учетных данных, присвоенных в другой юрисдикционной системе, без официального механизма взаимного юридического признания схем УИД. Соотнесение полномочий с общим описанием уровней обеспечения гарантий позволит установить, удовлетворяют ли идентификационные учетные данные требованиям того уровня обеспечения доверия, который необходим для целей соблюдения правила ЗСК в рамках конкретной сделки.

82. Например, оператор A системы идентификации может представить сертификат, подтверждающий соответствие его схемы электронной идентификации X второму, или высокому, уровню обеспечения доверия и соответствие его схемы электронной идентификации Y третьему, или существенному, уровню, что позволит включить схемы электронной идентификации X и Y в официальный перечень. Юридическое лицо B, желающее вести дела в электронной форме с финансовым учреждением C, может использовать учетные данные, присвоенные схемой электронной идентификации X или схемой электронной идентификации Y, в зависимости от требований к проводимой операции. Финансовое учреждение C может удостовериться в том, что электронные схемы идентификации X и Y включены в официальный перечень и соответствуют конкретным уровням обеспечения доверия, и принять соответствующие учетные данные, присвоенные этими схемами электронной идентификации.

83. Вышеприведенный пример является уместным и в национальном контексте в том случае, если во внутреннем законодательстве напрямую не оговариваются требования в отношении юридического признания и эквивалентности систем электронной идентификации.

84. Предусматриваемый механизм мог бы основываться на двух положениях, регулирующих, соответственно, условия для включения в официальный перечень и последствия включения в такой перечень.

85. Положение об условиях включения в официальный перечень могло бы быть сформулировано следующим образом:

> 1. Поставщики услуг УИД и удостоверительных услуг, которые намерены приступить к оказанию своих услуг, направляют […] [надзорный орган] уведомление о своем намерении вместе с соответствующим сертификатом.
>
> 2. В сертификате указывается, как минимум, следующее:
>
> a) тип заключения об оценке;
>
> b) квалификация проводящего оценку органа;
>
> c) технические спецификации и форматы, используемые для оказания таких услуг, в том числе на основе соотнесения с уровнями обеспечения доверия и стандартами обмена сообщениями.
>
> 3. [Надзорный орган] […] составляет, обновляет и публикует официальные перечни, включая информацию о поставщиках услуг УИД и удостоверительных услуг и предоставляемых ими услугах.

86. Рабочая группа, возможно, пожелает рассмотреть вопрос о том, может ли слово «сертификат» в этом проекте положения охватывать также самосертификацию, которая была бы уместной для услуг, требующих более низкий уровень обеспечения доверия (см. A/CN.9/WG.IV/WP.154, пункты 3–9).

87. В соответствии с проектом положения требуется назначение органа, который будет обеспечивать сохранность и обновление этого официального перечня. В случае, если создан механизм уведомления компетентных национальных органов, таким органом могло бы быть назначено то или иное национальное ведомство.

88. Что касается юридических последствий включения в официальный перечень, то тут некоторые полезные элементы можно было бы извлечь из положений статьи 12 ТЗЭП. Более того, в положение о последствиях юридического признания можно было бы также включить принцип признания иностранных идентификационных и удостоверительных услуг только в том случае, если они соответствуют такому же или более высокому уровню обеспечения доверия, чем требуемый уровень обеспечения доверия в той стране, в которой испрашивается признание (так называемый «принцип взаимности»). Соответствующее положение можно было бы сформулировать следующим образом:

> Идентификационная или удостоверительная услуга, предоставляемая за пределами [принимающего государства] и указанная в официальном перечне, составленном согласно статье ... , обладает такой же юридической силой в [принимающем государстве], какую имеет идентификационная или удостоверительная услуга, предоставляемая в [принимающем государстве] [и отвечающая эквивалентному [уровню обеспечения доверия] […]].

89. Рабочая группа, возможно, пожелает рассмотреть вопрос о необходимости дополнительных рекомендаций в отношении использования процесса описания через соотнесение с ключевыми параметрами и ссылки на понятие уровней обеспечения доверия для определения юридических последствий оказания иностранных идентификационных и удостоверительных услуг. В связи с этим Рабочая группа, возможно, пожелает рассмотреть вопрос о целесообразности использования ссылки на содержащееся в статье 12 ТЗЭП понятие «по существу эквивалентный уровень надежности».

90. В ходе обсуждения Рабочая группа, возможно, пожелает рассмотреть различные примеры использования схем УИД. Поскольку этот вопрос может возникать в рамках как национальных, так и трансграничных операций, Рабочая группа, возможно, пожелает рассмотреть оба сценария. В частности, она, возможно, пожелает рассмотреть часто возникающие сложности, связанные, по всей видимости, с необходимостью соблюдения обязательных требований, которые устанавливаются публичными органами и которые не поддаются простому урегулированию в рамках договорных соглашений. Например, как указывалось выше (пункты 80–83), тот или иной банк может пожелать узнать, какие схемы УИД могут использоваться для удовлетворения требований правила ЗСК.

91. Таким образом, к числу элементов, которые могли бы иметь значение для механизма юридического признания, относятся уведомление и включение в официальный перечень; обязательные требования, в том числе в отношении уровней обеспечения доверия; использование процедур сертификации в целях представления доказательств выполнения требований; центральный надзорный и лицензирующий орган; составление официального перечня.

92. Рабочая группа, возможно, пожелает рассмотреть вопрос о принятии того или иного подхода в отношении механизма юридического признания. При этом она, возможно, пожелает также продолжить обсуждение вопроса о том, должен ли механизм юридического признания применяться только на трансграничной основе или также в контексте различных систем на национальном уровне (см. пункт 60 выше).

2. Удостоверительные услуги

93. Что касается удостоверительных услуг, то уже разработано несколько юридических механизмов для обеспечения юридического признания электронных подписей. В этой связи следует отметить, что согласно одной точке зрения не все электронные подписи являются результатом оказания удостоверительных услуг и таковыми могут считаться только те, которые требуют участия третьей стороны, предоставляющей удостоверительные услуги. Согласно другому мнению все электронные подписи являются результатом оказания удостоверительных услуг. Рабочая группа, возможно, пожелает дать разъяснения по этому вопросу.

94. Что касается текстов ЮНСИТРАЛ, то юридическое признание на национальном уровне обеспечивают положения о функциональной эквивалентности электронных подписей (см. пункт 36 выше).

95. Что касается трансграничного юридического признания, то в статье 12 ТЭП, основанной на подходе «эквивалентность по существу»[12], требуется, чтобы в отношении электронных подписей, обладающих иностранными элементами, не проводилось никакой дискриминации. В статье 9(3) КЭС указаны требования к обеспечению функциональной эквивалентности рукописных и электронных подписей, но не определяется правовой статус подписи как таковой в той юридической системе, в которой испрашивается признание[13].

96. Еще один механизм трансграничного признания электронных подписей основан на заключении специального международного соглашения или, в рамках делегированных полномочий, меморандума о понимании. Например, в статье 14 Постановления eIDAS предусматривается, что удостоверительные услуги, предоставляемые поставщиками, базирующимися за пределами Европейского союза, могут быть признаны в качестве юридически эквивалентных услугам, предоставляемых квалифицированными поставщиками, базирующимися в Европейском союзе, только если они признаются таковыми в соответствии с международным соглашением. В статье 19 Закона об информационных технологиях, принятого в 2008 году в Индии, допускается признание иностранных сертифицирующих органов в следующем порядке:

> «1) С учетом таких условий и ограничений, которые могут быть указаны в нормативных положениях, Контролер с предварительного разрешения центрального правительства и посредством публикации уведомления в официальном вестнике может признавать любой иностранный сертифицирующий орган в качестве «сертифицирующего органа» для целей настоящего Закона.
>
> 2) Если тот или иной сертифицирующий орган признается в соответствии с пунктом 1, то выданный таким сертифицирующим органом сертификат электронной подписи является действительным для целей настоящего Закона.
>
> 3) Если Контролер удостоверяется в том, что тот или иной сертифицирующий орган нарушил какое-либо из условий или ограничений, соблюдение которых позволило ему получить признание согласно пункту 1, то он может [sic] отменить такое признание по причинам, которые должны быть изложены в письменном виде, путем публикации соответствующего уведомления в официальном вестнике».

---

[12] Подробнее об эквивалентности по существу см. в публикации ЮНСИТРАЛ «Содействие укреплению доверия к электронной торговле: правовые вопросы международного использования электронных методов удостоверения подлинности и подписания» (издание Организации Объединенных Наций, в продаже под № R.09.V.4), пункты 158–161.

[13] *Пояснительная записка к Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах* (издание Организации Объединенных Наций, в продаже под № R.07.V.2), пункт 156.

97. Другие методы обеспечения признания электронных подписей в различных системах или на трансграничном уровне базируются на инфраструктуре публичных ключей («ИПК») и предусматривают перекрестное признание и перекрестную сертификацию[14]. Перекрестным признанием называется механизм взаимодействия, при котором полагающаяся сторона, находящаяся в зоне действия ИПК, может использовать удостоверяющую подлинность информацию в зоне действия другой ИПК для удостоверения личности какого-либо субъекта в зоне первой ИПК[15]. Перекрестной сертификацией называется практика признания публичного ключа другого поставщика сертификационных услуг с присвоением ему согласованного уровня доверия, обычно на основании договора[16]. Эти договорные методы могут предусматриваться специальными законодательными положениями. Например, в статье 43 закона 527, принятого в 1999 году в Колумбии, указано следующее:

> Сертификаты цифровых подписей, выданные иностранными сертификационными органами, могут признаваться на тех же условиях, которые предусмотрены законодательством в отношении выдачи сертификатов национальными сертификационными органами, если такие сертификаты признаются уполномоченным национальным сертификационным органом, который гарантирует правильность содержания иностранного сертификата, а также действительность и юридическую силу иностранного сертификата таким же образом, как и собственных сертификатов.

98. Вышеуказанные механизмы функционируют уже в течение некоторого времени, однако пока не позволили в полной мере обеспечить трансграничное признание электронных подписей. ТЗЭП принят ограниченным числом государств и зачастую без статьи 12. Количество участвующих в КЭС государств неуклонно растет, однако оно по-прежнему небольшое. Статутные механизмы взаимного признания являются затратными по времени и ресурсам и используются редко. Механизмы перекрестного признания или перекрестной сертификации на основе ИПК применяются только к тем сертификационным органам, которые договорятся об их использовании, и в том случае, если они не подкрепляются законодательными положениями во всех соответствующих юрисдикционных системах, могут и не удовлетворять обязательным требованиям законодательства.

---

[14] Подробнее о перекрестном признании и перекрестной сертификации см. выше, *Содействие укреплению доверия к электронной торговле*, пункты 165–172.

[15] Там же, *Содействие укреплению доверия к электронной торговле*, пункт 165.

[16] Там же, *Содействие укреплению доверия к электронной торговле*, пункт 169.