Организация Объединенных Наций A/CN.9/WG.IV/WP.145

Генеральная Ассамблея

Distr.: Limited
20 February 2017
Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Пятьдесят пятая сессия
Нью-Йорк, 24-28 апреля 2017 года

Правовые вопросы, связанные с управлением идентификационными данными и удостоверительными услугами

Предложение Соединенных Штатов Америки

Записка Секретариата

Соединенные Штаты Америки представили Секретариату документ для рассмотрения на пятьдесят пятой сессии Рабочей группы. Документ воспроизводится в качестве приложения к настоящей записке в том виде, в каком он был получен Секретариатом.

V.17-01091 (R) 010317 020317

Приложение

I. Введение

На своей пятьдесят четвертой сессии Рабочая группа IV (Электронная торговля) приступила к обсуждению темы управления идентификационными данными (УИД) и удостоверительных услуг. Рабочая группа сделала в предварительном порядке следующие первоначальные выводы:

> «118. После обсуждения Рабочая группа согласилась с тем, что ее будущую работу в области УИД и удостоверительных услуг следует ограничить вопросами использования системы УИД для коммерческих целей и что в ходе этой работы не следует рассматривать вопрос о том, является ли поставщик услуг УИД частным или публичным.
>
> 119. Рабочая группа согласилась также с тем, что в первую очередь следует провести работу по УИД. Кроме того, она согласилась с тем, что особое внимание следует уделить многосторонним идентификационным системам и физическим и юридическим лицам, не исключая при этом возможность рассмотрения в необходимых случаях двусторонних идентификационных систем и физических и цифровых объектов.
>
> 120. Кроме того, было достигнуто согласие о том, что Рабочая группа продолжит свою работу посредством дальнейшего разъяснения целей проекта, уточнения сферы его охвата, выявления применимых общих принципов и разработки необходимых определений».

(A/CN.9/897, пункты 118-120).

Для содействия целенаправленному обсуждению на пятьдесят пятой сессии Рабочей группы и в последующий период делегация Соединенных Штатов Америки подготовила настоящий документ в попытке очертить вопросы, которые могла бы рассмотреть Рабочая группа. Хотя, несомненно, есть много других вопросов, которые необходимо будет рассмотреть Рабочей группе, существует надежда, что приводимый ниже первоначальный перечень можно будет использовать в качестве отправной точки, с тем чтобы задать направленность первоначальному обсуждению и помочь сконцентрировать усилия Рабочей группы. Мы надеемся, что обсуждение этих, а также других вопросов, которые могут быть определены Рабочей группой, сможет указать Секретариату путь при подготовке рабочего документа по УИД.

Мы понимаем, что в межсессионный период эксперты занимались обсуждением соответствующей терминологии в неофициальном порядке. Хотя мы считаем, что в конечном итоге необходимо будет тщательно рассмотреть формулировки определений терминов, которые будут использованы в этом проекте, на данном начальном этапе мы рекомендуем, чтобы Рабочая группа считала использование первоначальных определений просто основой для содействия ее дискуссии. Однако мы признаем, что в конечном итоге может потребоваться достижение договоренности по более детальным юридическим и техническим определениям.

II. Цели и задачи проекта

В качестве отправной точки Рабочая группа, возможно, пожелает рассмотреть общие цели и задачи проекта. В свете первоначального решения сосредоточить внимание на использовании систем УИД для коммерческих целей Рабочая группа, возможно, пожелает рассмотреть, какие из следующих целей и задач могут быть уместны в контексте данного проекта:

- содействие развитию идентификационной экосистемы в частном секторе;
- выявление и устранение правовых барьеров на пути коммерческих операций с идентификационными данными;
- устранение неясностей в отношении применимости существующих правовых норм к коммерческим операциям с идентификационными данными;
- поощрение коммерческого использования цифровых идентификационных учетных данных третьих сторон и укрепление доверия к ним;
- содействие укреплению доверия, необходимого для коммерческих операций с идентификационными данными в режиме онлайн;
- оказание помощи частным сторонам путем создания основы для принятия решений о том, следует ли доверять цифровой идентификационной информации в коммерческих сделках;
- выявление и устранение трансграничных препятствий на пути электронной аутентификации;
- содействие трансграничному признанию цифровой идентификационной информации; и
- содействие укреплению доверия к электронной торговле.

III. Характер предлагаемого рабочего продукта РГ IV

Возможно, целесообразно начать обсуждение вида продукта, который Рабочая группа хотела бы разработать в области управления коммерческими идентификационными данными.

IV. Руководящие принципы

Независимо от конечной формы рабочего продукта, который будет подготовлен Рабочей группой, существует несколько общих принципов, которые Рабочая группа, возможно, пожелает рассмотреть – а в случае необходимости и принять – и которые могут определять ее работу в области УИД. Как и в случае Типового закона об электронной торговле и Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах, такие общие принципы могут быть использованы для определения направленности обсуждений в Рабочей группе. Кроме того, руководящие принципы могут оказаться полезными в прояснении сферы охвата ее работы. Вероятные руководящие принципы, которые, возможно, пожелает рассмотреть Рабочая группа, включают нижеследующие.

A. Источник юридического обязательства производить идентификацию

В качестве отправной точки Рабочая группа, возможно, пожелает рассмотреть, должно ли какое-либо законодательство в сфере УИД предусматривать обязательства идентифицировать участника коммерческой сделки независимо от обязательств, применяемых в результате действия других законодательных актов. Если законодательство в сфере УИД не содержит никакого обязательства идентифицировать участника, юридические требования в отношении идентификации участника коммерческой сделки будут определяться другими действующими законодательными актами, например законами, регулирующими нотариальное оформление, принципом «знай своего клиента», законодательством по борьбе с отмыванием денег или законами, регулирующими доступ к персональным данным. Именно такого подхода придерживалась Рабочая группа в отношении электронных подписей при разработке Типового закона об

электронной торговле и Конвенции Организации Объединенных Наций об использовании электронных сообщений в международных договорах.

B. Автономия сторон

Поскольку системы УИД, как правило, будут регулироваться нормами договорных систем, согласованными участниками таких систем, может быть немаловажным рассмотрение вопроса о том, должен ли – и если да, то в какой степени – тот или иной закон, регулирующий операции в сфере УИД, признавать нормы такой системы и считаться с ними.

Таким образом, Рабочая группа, возможно, пожелает рассмотреть, должен ли принцип автономии сторон применяться к коммерческим идентификационным системам, для того чтобы дать участникам таких систем возможность изменять по договоренности положения любой правовой нормы или определенных правовых норм.

C. Технологическая нейтральность

Для использования в коммерческих сделках может быть разработано и внедрено много различных видов идентификационных систем. В таких системах могут использоваться самые различные технологии. Это может включать простые имена пользователей и пароли или более сложные системы, основанные на стандарте инфраструктуры публичных ключей x.509 или других стандартах, таких как язык разметки подтверждений безопасности (SAML) или «OpenID Connect». Кроме того, в настоящее время разрабатываются системы, использующие новые технологии, такие как «Blockchain».

Поэтому Рабочая группа, возможно, пожелает рассмотреть, следует ли в том или ином рабочем продукте, касающемся УИД, четко указать, что никакие нормы в сфере УИД не должны требовать использования каких-либо конкретных технологий.

Рабочая группа, возможно, пожелает дополнительно рассмотреть, какой подход ЮНСИТРАЛ к вопросу наличия и использования нескольких коммерческих идентификационных систем мог бы быть оптимальным.

Законодательство – помимо того, что конкретно касается УИД, – может, конечно, предусматривать использование сторонами идентификационных систем, отвечающих определенным требованиям. И сами стороны могут настаивать на том, чтобы физические и юридические лица, с которыми они ведут дела, использовали конкретную систему идентификации. Например, коммерческая структура может ограничить доступ к своим услугам пользователями, которые используют одну или несколько конкретных идентификационных систем, членом которых она является.

D. Нейтральность системной модели

В дополнение к многообразию используемых технологий коммерческие идентификационные системы становятся в настоящее время объектом множества экспериментов с применяемыми организационными и коммерческими структурами и подходами. Вероятно, мы можем рассчитывать увидеть в будущем довольно много различных типов идентификационных систем, даже если в них используются одни и те же базовые технологии. Сюда входят механизмы с использованием посредников или узловых центров, модели с одним поставщиком идентификационных данных, модели с одной доверяющей стороной, организационные модели, а также множество других различных подходов.

Соответственно, Рабочая группа, возможно, пожелает рассмотреть, следует ли ей в принципе принимать концепцию нейтральности системной модели – то есть признать, что ни один разработанный конечный продукт не должен быть составлен таким образом, чтобы предполагать или требовать использование какой-либо конкретной коммерческой, организационной или структурной модели системы идентификации, и что он должен быть пригоден для внесения в будущем изменений в концепцию, структуру и коммерческую модель идентификационной системы.

E. Недискриминация

Рабочая группа, возможно, пожелает также рассмотреть вопрос о применимости принципа недискриминации в контексте использования идентификационных систем для коммерческих целей. Согласно этому принципу, например, правовые последствия (например, удовлетворение законного требования об идентификации) и приемлемость электронной идентификации в качестве доказательства в рамках судопроизводства не должны отвергаться лишь на том основании, что такая идентификация была произведена в электронном виде.

F. Взаимосвязь между законодательством в области управления идентификационными данными и законами о защите частной жизни

Коммерческие операции с идентификационными данными, связанные с выдачей или использованием учетных идентификационных данных, часто затрагивают некоторые персональные данные. В таких случаях важное значение может иметь конфиденциальность таких персональных данных.

Законы о неприкосновенности частной жизни обычно касаются защиты персональных данных согласно соответствующим принципам публичного порядка. Поэтому Рабочая группа, возможно, пожелает рассмотреть вопрос о взаимосвязи между этими законами и системами УИД.

G. Взаимосвязь между законодательством в области управления идентификационными данными и законами об обеспечении безопасности данных

Безопасность данных имеет решающее значение для надлежащего осуществления и обеспечения благонадежности операций с идентификационными данными как с точки зрения защиты конфиденциальности персональных данных, задействованных в таких операциях, так и для обеспечения надлежащего функционирования и благонадежности системы передачи учетных данных, в рамках которой совершается такая операция.

Законы о защите данных часто касаются безопасности персональных данных согласно соответствующим принципам публичного порядка. Точно так же и другие законы об обеспечении безопасности данных могут предусматривать то же самое в отношении защиты других аспектов системы передачи сообщений в рамках операций с идентификационными данными. Поэтому Рабочая группа, возможно, пожелает рассмотреть вопрос о взаимосвязи между этими законами и системами УИД.

H. Взаимосвязь между системными правилами, основанными на договоре, и другими законами

Поскольку системы УИД, как правило, регулируются системными правилами, основанными на договоре (т.е. структурой доверия) и согласованными

участниками таких систем, Рабочая группа, возможно, пожелает обсудить взаимосвязь между этими правилами и действующими законами, не имеющими непосредственного отношения к идентификационным данным.

V. Основные темы

A. Юридическое признание

Рабочая группа, возможно, пожелает рассмотреть тему юридического признания идентификационной информации, прошедшей аутентификацию в связи с коммерческой сделкой. В этом контексте Рабочая группа, возможно, пожелает рассмотреть вопросы о том, что представляет собой юридическое признание, какую цель оно преследует и каковы требования для его получения; кто обеспечивает юридическое признание; с какой целью производится юридическое признание; какова взаимосвязь между юридическим признанием и законодательством, предусматривающим ту или иную форму идентификации, как, например, законы, регулирующие нотариальное оформление, принцип «знай своего клиента», законодательство по борьбе с отмыванием денег или законы, регулирующие доступ к персональным данным; и как юридическое признание применяется – если это вообще имеет место – к идентификационным данным юридических лиц, устройств или цифровых объектов.

B. Трансграничное взаимное признание

Концепция взаимного признания имеет важное значение для содействия коммерческому использованию идентификационных учетных данных и укрепления доверия к этим данным как в рамках идентификационных систем, так и за пределами границ юрисдикций.

Существует множество вопросов, которые Рабочая группа, возможно, пожелает рассмотреть в связи с проблемой взаимного признания. Некоторые из наиболее очевидных из них сводятся к следующему: a) должно ли быть предусмотрено требование о признании учетных данных, b) если существует требование о признании учетных данных, кто должен производить такое признание, c) если существует требование о признании учетных данных, учетные данные какой стороны должны подлежать признанию, d) какова цель такого взаимного признания, e) что именно означает «взаимное признание», f) какие характерные элементы (например, уровни обеспечения доверия) должны присутствовать для взаимного признания, g) должны ли быть ограничения в отношении того, когда применяется взаимное признание, и h) следует ли применять взаимное признание к идентификационным данным юридических лиц, устройств или цифровых объектов.

C. Присвоение субъекту идентификационных данных

Присвоение субъекту идентификационных данных (для включения в идентификационные учетные данные) часто является одним из важнейших элементов систем управления идентификационными данными. Основополагающий момент, определяющий этот процесс, заключается в том, когда и при каких обстоятельствах конкретному субъекту присваиваются идентификационные данные, включаемые в учетные данные.

Рабочая группа, возможно, пожелает рассмотреть этот вопрос с двух точек зрения. Во-первых, как поставщик идентификационных данных должен обеспечивать, чтобы информация о субъекте, которую он включает в идентификационные учетные данные, действительно описывала субъекта, поименованного в учетных данных? Во-вторых, в тех случаях, когда используются идентификационные учетные данные, как может доверяющая сторона удосто-

вериться, что информация, содержащаяся в учетных данных, относится к субъекту, предъявившему учетные данные?

D. Доверие к действиям, сообщениям данных или подписям/отнесение их к субъекту

Ключевой вопрос для всех участников идентификационной системы заключается в том, когда и при каких обстоятельствах доверие к идентификационным учетным данным одной из сторон является уместным и обоснованным. Обоснованность доверия одной из сторон может повлиять на целый ряд вопросов, включая случаи, когда полагаются на ошибочные идентификационные учетные данные.

Например, в контексте электронных подписей этот вопрос рассматривался в статье 13 Типового закона об электронной торговле.

E. Распределение ответственности/рисков

Вопросы распределения ответственности и рисков часто приводятся в качестве основных барьеров на пути внедрения коммерческих идентификационных систем. Сюда входят a) опасения поставщиков идентификационных данных и других участников систем идентификации, что риск ответственности, возлагаемый на них в рамках существующего законодательства, является необоснованным или просто слишком большим для того, чтобы они могли начать действовать, а также b) опасения участников идентификационных систем, что законодательство является слишком расплывчатым, двусмысленным или неопределенным для того, чтобы они могли правильно оценить свои риски, связанные с участием.

Рабочая группа, возможно, пожелает рассмотреть, следует ли ей затрагивать вопрос ответственности, и если да, то в связи с какими функциями идентификационных систем и каким образом. Примерами законодательных положений, в которых вопрос ответственности рассматривается в контексте систем УИД, являются Постановление eIDAS Европейского союза и Закон штата Вирджиния об управлении электронными идентификационными данными.

F. Прозрачность

Процессы, процедуры и технологии, используемые поставщиками идентификационных данных для выдачи и подтверждения подлинности идентификационных учетных данных, могут оказывать существенное влияние на обеспечение доверия к какой-либо операции с идентификационными данными, в которой используются эти учетные данные. Поэтому может быть важно, чтобы другие участники системы идентификации понимали, как применяются эти процессы, процедуры и технологии, для того чтобы они могли произвести свою собственную оценку надежности и обоснованности соответствующих операций с идентификационными данными. С этой целью Рабочая группа, возможно, пожелает рассмотреть, обеспечивается ли надлежащий уровень прозрачности со стороны некоторых участников в рамках идентификационной системы. Точно так же Рабочая группа, возможно, пожелает рассмотреть, нужно ли в случае каких-либо сбоев или нарушений в тех или иных процессах, процедурах, технологиях, базах данных или идентификационных учетных данных, которые обеспечиваются одной из сторон в контексте системы идентификации, раскрывать информацию о таком нарушении.

В некоторых случаях требования в отношении прозрачности использовались также в качестве замены нормативных актов, устанавливающих императивный характер определенных процессов, процедур или технологий. Подход,

основанный на прозрачности, позволяет сторонам принимать свои собственные решения относительно благонадежности на основе более полной информации.

G. Благонадежность/уровни обеспечения доверия

Во многих идентификационных системах определены так называемые «уровни обеспечения доверия», для того чтобы помочь участникам решить проблемы, связанные с благонадежностью идентификационных учетных данных и операций с идентификационными данными. Существует несколько уровней обеспечения доверия, и часто они связаны с различной степенью доверия. Например, Европейский союз в своем Постановлении eIDAS определяет три уровня обеспечения доверия (обозначенных как «низкий», «высокий» и «основной»), в то время как в Соединенных Штатах и в других странах используется четыре уровня обеспечения доверия.

Рабочая группа, возможно, пожелает рассмотреть, как лучше всего содействовать укреплению доверия со стороны участников к системе идентификации. Хотя повсеместно используется концепция уровней обеспечения доверия, Рабочая группа, возможно, пожелает также рассмотреть, можно ли для укрепления доверия использовать и другие механизмы, как, например, предписанный уровень прозрачности, сертификация третьей стороной или другие подходы.