Организация Объединенных Наций A/CN.9/WG.IV/WP.163

Генеральная Ассамблея

Distr.: Limited
20 February 2020
Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Шестидесятая сессия
Нью-Йорк, 6–9 апреля 2020 года

Проект положений об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг

Представление Всемирного банка

Записка Секретариата

Всемирный банк представил документ для рассмотрения на шестидесятой сессии Рабочей группы. Этот документ воспроизводится в качестве приложения к настоящей записке в том виде, в котором он был получен Секретариатом.

V.20-01484 (R) 110320 130320

Приложение

Замечания Всемирного банка по документу WP.162

Всемирный банк рад представить изложенные ниже замечания по документу A/CN.9/WG.IV/WP.162 «*Проект положений об использовании и трансграничном признании управления идентификационными данными и удостоверительных услуг*» («проект положений») в связи с проведением совещания Рабочей группы в Нью-Йорке 6–9 апреля 2020 года.

I. Общие вводные замечания и соображения

1. Сосредоточенность на УИД: Всемирный банк, как правило, поддерживает работу Рабочей группы IV, особенно в том, что касается управления идентификационными данными («УИД»). Поскольку интерес для Всемирного банка в основном представляют вопросы управления идентификационными данными, приводимые ниже комментарии касаются разделов проекта положений, касающихся управления идентификационными данными.

2. Системы УИД и операции с идентификационными данными: проект положений в основном касается систем УИД и поставщиков услуг УИД, а не операций с идентификационными данными. Ввиду важности операций с идентификационными данными, особенно с точки зрения соблюдения правовых норм и юридического признания, а также с учетом того факта, что электронные операции с идентификационными данными могут проводиться и, как правило, проводятся без использования какой-либо системы УИД или какого-либо поставщика услуг УИД, Рабочей группе следует продолжить рассмотрение возможности обсуждения вопросов, касающихся операций с идентификационными данными.

3. Функции: основное внимание в проекте положений уделяется регулированию систем УИД и поставщиков услуг УИД, и (за исключением статей 5 и 8) в нем практически не учитываются потребности полагающихся сторон, субъектов или других потенциальных участников системы или операции УИД. Например, в проекте положений не рассматривается право полагающейся стороны использовать третью сторону для проверки идентификационных данных в тех случаях, когда законодательство обязывает полагающуюся сторону проверять идентификационные данные. Как и в случае операций с идентификационными данными, Рабочей группе следует рассмотреть возможность уделения более значительного внимания вопросам, затрагивающим другие функции системы УИД, помимо поставщика услуг УИД.

4. Взаимосвязь между системами УИД публичного сектора и частного сектора. Основное внимание в проекте положений уделяется системам УИД частного сектора и поставщикам услуг УИД частного сектора. Как представляется, проект положений не применяется к системам УИД или поставщикам услуг УИД, управляемым публичными органами, например к национальным системам УИД. Соответственно, поскольку многие из национальных систем УИД являются правительственными системами УИД (например, в Индии, Эстонии и т.д.), они выходят за рамки документа, который будет принят на основе проекта положений.

Между тем важно признать, что, вероятно, будет происходить существенное взаимодействие между публичными и частными системами УИД. Например, проект положений, по-видимому, будет применяться в тех случаях, когда то или иное правительственное учреждение будет выступать клиентом (например, полагающейся стороной или субъектом данных) поставщика услуг УИД из частного сектора или полагаться на систему федеративных идентификационных данных частного сектора вместо системы УИД, управляемой правительством. Кроме того, процессы проверки и аутентификации идентификационных данных,

используемые поставщиками услуг УИД из частного сектора, часто основываются на исходных учетных идентификационных данных, выданных правительственными системами, которые часто считаются авторитетными и высоконадежными.

Соответственно, Рабочей группе следует изучить и уточнить характер взаимосвязи между системами УИД публичного и частного секторов, в том числе рассмотреть, в частности, вопрос о том, когда и/или каким образом для систем УИД частного сектора может быть целесообразно использовать исходную информацию об идентификационных данных и процессы аутентификации, предоставляемые правительствами. Это может предусматривать, например, рассмотрение правил, касающихся системы УИД частного сектора:

- использование выданных правительством идентификационных номеров или другой идентификационной информации;
- использование выданных правительством учетных идентификационных данных;
- доступ к государственным базам данных для процессов проверки идентификационных данных и аутентификации; или
- зависимость от информации или процессов, обеспечиваемых правительством, в целом.

5. Удостоверительные системы: в проекте положений не рассматривается роль основанных на договоре правил для отдельных систем УИД, часто называемых удостоверительными системами, системными правилами или правилами схемы (в настоящем документе используется общий термин «удостоверительные системы»), и вопрос о том, как они взаимодействуют с проектом положений[1]. Рабочей группе следует рассмотреть возможность пересмотра проекта положений, чтобы уточнить взаимосвязь между проектом положений и удостоверительными системами УИД, а также вопрос о том, какие проблемы и на каком уровне детализации необходимо рассмотреть в проекте положений в отличие от удостоверительных систем отдельных систем УИД. Например, такие вопросы, как обязанности участников, надежность и уровни доверия, часто рассматриваются в конкретной удостоверительной системе каждой отдельной системы УИД.

Аналогичным образом, Рабочей группе следует рассмотреть возможность обсуждения вопроса о том, в какой степени условия удостоверительной системы могут изменять или отменять условия проекта положений. Например, несмотря на условия проекта положений, касающиеся ответственности, неясно, могут ли стороны выработать свои собственные правила об ответственности в рамках своей собственной удостоверительной системы для конкретных услуг УИД.

6. Опора на правовые модели электронной подписи: структура и подход, принятые в проекте положений, в значительной степени основаны на Типовом законе ЮНСИТРАЛ об электронных подписях и, следовательно, не учитывают тот факт, что вопросы, связанные с подписями, существенно отличаются от вопросов, которые необходимо учитывать при рассмотрении идентификационных данных (хотя идентификационные данные иногда являются составной частью подписи). Поэтому определение имеющего юридическую силу единого электронного эквивалента требованиям в отношении подписи нельзя автоматически применять к требованиям в отношении проверки идентификационных данных.

Частично проблема связана с тем, что законы, требующие подписи, требуют одного и того же (а именно — подписи), тогда как законы, требующие идентификации какого-либо лица, часто предусматривают самые различные требования, которым должен удовлетворять процесс идентификации (в зависимости, например, от того, являются ли идентификационные данные «исходными»

[1] Хотя в статьях 6(c), 6(f), 10(1)(b) и 23(1)(a) проекта положений используется термин «правила, регулирующие работу системы УИД,» этот термин нигде не определяется и не рассматривается подробно.

или же «функциональными»[2], для какой цели требуется идентификация, какие возникают риски и т.д.). Соответственно, хотя относительно легко определить имеющий юридическую силу эквивалент единой концепции подписи, такой же подход не обязательно применим в отношении различных правовых режимов идентификации. Поэтому важно, чтобы Рабочая группа не замыкалась в заранее определенной структуре, вытекающей из законодательства об электронных подписях, а вместо этого провела независимое рассмотрение юридических вопросов, которые необходимо принять во внимание в связи с идентификационными данными.

7. Варианты проверки идентификационных данных: у любой полагающейся стороны есть два варианта проверки идентификационных данных того лица, с которым она имеет дело, т.е. проверяющая сторона может:

- провести проверку идентификационных данных самостоятельно, или
- использовать третью сторону, выступающую поставщиком услуг УИД.

Большинство полагающихся сторон используют первый вариант. Тем не менее, в проекте положений основное внимание уделяется только второму варианту. Рабочая группа, возможно, пожелает рассмотреть вопрос о целесообразности применения в проекте положений более широкого подхода к теме идентификационных данных и рассмотрения вопросов, возникающих в обеих ситуациях.

8. Права полагающейся стороны полагаться: в идеале в проекте положений следует рассмотреть вопросы, касающиеся права полагающейся стороны полагаться. Такое право может включать, например, право полагающейся стороны i) полагаться на идентификационные учетные данные в целом, ii) полагаться на учетные данные третьих сторон для выполнения конкретных требований конкретного закона, налагающего обязанность идентифицировать, и iii) использовать третью сторону, выступающую поставщиком услуг УИД, для выполнения своих юридических обязательств по идентификации какого-либо лица.

9. Права полагающейся стороны использовать третью сторону: в то же время, хотя некоторые законы, которые налагают обязанность идентифицировать, специально разрешают использовать поставщиков услуг, являющихся третьими сторонами (например, положения Закона о защите прав потребителей Калифорнии)[3], многие законы не содержат положений по этому вопросу (или требуют, чтобы полагающиеся стороны проводили идентификацию самостоятельно). Рабочей группе следует рассмотреть также и эти вопросы, касающиеся идентификационных данных.

II. Замечания по конкретным положениям

1. Статья 1. Определения

a) **отсутствующие термины**: ряду терминов, используемых в проекте положений, не дано определения. К числу терминов, которые используются, но не определены, относятся следующие:

- «факторы электронной идентификации»; см. статью 6(d)(i)
- «механизмы электронной идентификации»; см. статьи 6(d)(ii), 8(a), 8(b)
- «управление идентификационными данными»; используется как концепция во всем тексте, но нигде не определяется
- «идентификатор»; см. статью 1(b),

[2] См., например, “Practitioners Guide” (World Bank, 2019) at pages 12 and 13 (inter alia), available at: https://id4d.worldbank.org/guide.

[3] См. California Consumer Privacy Act Regulations at Article 4, Section 999.323(b); available at www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

- «правила, регулирующие работу системы УИД»; см. статьи 6(c), 6(f), 10(b) и 23(a)
    - этот термин может быть предназначен для обозначения удостоверительной системы отдельной системы УИД, хотя, исходя из его существующей формулировки, он может применяться к любому закону или нормативному акту, регулирующему работу системы УИД. Его использование следует уточнить
- «проверка»; — см. статью 6(a)(ii)
    - понятие «проверка», возможно также важно уточнить, поскольку использование этого термина часто приводит к путанице. Например, термин «проверка идентификационных данных» часто используется в одних случаях для обозначения идентификации субъекта данных, а в других случаях для обозначения аутентификации этого субъекта данных. С учетом частотности использования этого термина, его необходимо тщательно уточнить и правильно использовать во всем тексте

b) **аутентификация**: термины «аутентификация» и «электронная идентификация» используются для обозначения, по существу, одного и того же, хотя аутентификация используется в контексте удостоверительных услуг, а электронная идентификация — в контексте услуг УИД. Поскольку эти понятия идентичны, Рабочая группа может рассмотреть возможность использования одного и того же термина в обоих случаях.

c) **электронная идентификация**: замена единого термина «идентификация» терминами «проверка идентификационных данных» и «электронная идентификация» является важным шагом для разъяснения и разграничения двух аспектов процесса идентификации. Однако может возникнуть проблема в связи с тем, что термин «электронная идентификация» описывает весь процесс или что его легко спутать со всем процессом проверки идентификационных данных, выдачи идентификационных учетных данных аутентификации связи между учетными данными и отдельным лицом. Поэтому рекомендуется, чтобы Рабочая группа рассмотрела вопрос о том, можно ли использовать какой-либо термин, альтернативный термину «электронная идентификация».

Кроме того, использование слова «электронный» применительно к этому термину, который предназначен для того, чтобы описать «процесс, используемый для достижения достаточной уверенности в наличии связи между субъектом и идентификационными данными», может создать путаницу в отношении характера процессов, систем и услуг, рассматриваемых в проекте положений. Такая же проблема возникает в связи с определениями терминов «услуги управления идентификационными данными (УИД)» и «система управления идентификационными данными (УИД)», которые требуют, чтобы они обеспечивались «в электронной форме». Описание процесса установления связи в качестве «электронного» или же услуг УИД или систем УИД в качестве систем или услуг «в электронной форме» игнорирует тот факт, что в некоторых случаях весь процесс или его часть могут быть неэлектронными. Например, некоторые функции, такие как функции по проверке идентификационных данных, могут выполняться в неэлектронной форме или основываться на бумажных документах. Поэтому рекомендуется, чтобы Рабочая группа рассмотрела возможность признания того факта, что процессы, системы и услуги, охватываемые проектом положений, вполне могут включать различные неэлектронные элементы.

d) **идентификационные данные**: определение идентификационных данных как набора атрибутов, который позволяет «уникальным образом отличить» [субъекта] [лицо] в определенном контексте, представляется чрезмерно ограничительным. Во многих случаях идентификация используется в целях квалификации, а не установления уникальности. Например, идентификация может

использоваться просто для установления того, относится ли данное лицо к конкретной группе, например, старше ли вы 21 года, являетесь ли вы членом клуба, являетесь ли вы гражданином и т.д. Многие люди, вероятно, будут обладать такими атрибутами, и, следовательно, идентификационные данные не обязательно будут уникальными, однако будут достаточно отличать субъекта данных в соответствующем контексте, в котором требуются такие ограниченные идентификационные данные.

e) **идентификационные учетные данные**: Рабочей группе следует принимать во внимание новые изменения, касающиеся средств передачи информации об идентификационных данных. Хотя идентификационные учетные данные являются типичным средством подтверждения и верификации идентификации, следует отметить, что многие новые системы УИД не используют идентификационные учетные данные как таковые. Таким образом, хотя определение не обязательно является неуместным, следует позаботиться о том, чтобы избежать включения в проект положений предположения о том, что всегда будут использоваться идентификационные учетные данные. Кроме того, следует обратить внимание, что определение охватывает только данные «в электронной форме». Рабочая группа, возможно, пожелает рассмотреть вопрос о том, должен ли проект положений охватывать также традиционные бумажные или личные формы идентификации.

f) **проверка идентификационных данных**: процесс проверки идентификационных данных не должен обеспечивать полного «определения и подтверждения» идентификационных данных субъекта. Иными словами, проверка идентификационных данных, по-видимому, может включать сбор, проверку и/или установление действительности одного или нескольких атрибутов, которые, хотя сами по себе недостаточны для определения и подтверждения идентификационных данных, могут быть использованы другими для подтверждения идентификационных данных. Поэтому Рабочая группа, возможно, пожелает рассмотреть возможность разработки более широкого определения проверки идентификационных данных.

g) **полагающаяся сторона**: исключение определения этого термина и его замена термином «абонент» может быть нецелесообразным. Понятие абонента подразумевает активного участника системы, который связан правилами. Хотя это может включать полагающуюся сторону, заключить соглашение о предоставлении услуг УИД могут и другие лица/организации, включая, например, субъектов. В результате неспособность провести различие между полагающимися сторонами и субъектами (или другими пользователями системы УИД) может привести к путанице в применении правил, изложенных в проекте положений. Рабочей группе предлагается рассмотреть вопрос о сохранении определения термина «полагающаяся сторона», с тем чтобы положения, излагаемые в последующих статьях, соответствующим образом применялись либо к полагающимся сторонам, либо к субъектам.

h) **субъект**: в контексте услуг УИД субъектом является лицо или объект, которые идентифицируются или, по крайней мере, участвуют в процессе проверки идентификационных данных. Исключение ссылки на идентификацию делает данный термин общим и, вероятно, бесполезным.

i) **абонент**: как отмечалось выше, понятие абонента как лица, «которое заключает соглашение о предоставлении услуг УИД или удостоверительных услуг с поставщиком услуг УИД или поставщиком удостоверительных услуг», представляется чрезмерно всеобъемлющим, поскольку оно может охватывать самые различные функции в системе идентификации, а также субъектов. Например, пункт 3 варианта C статьи 12 основывается на предположении о том, что абоненты являются полагающимися сторонами. Между тем, абонентами могут выступать также субъекты или же одна из многих сторон, выполняющих другие функции в системе УИД, и в этом случае положения данного определения будут неуместными.

2. Статья 2. Сфера применения

Рабочей группе следует рассмотреть возможность переоценки сферы применения проекта положений применительно к управлению идентификационными данными. В том виде, в котором статья 2 сформулирована в настоящее время, сфера применения ограничена двумя темами: 1) ***использование систем УИД*** и 2) ***трансграничное признание систем УИД***.

Рабочая группа, возможно, пожелает рассмотреть вопрос о том, должно ли положение о сфере применения охватывать также ***операции УИД***, а также, возможно, содержать ссылку на ***функционирование*** системы УИД и/или ***предоставление*** услуг УИД.

Кроме того, с учетом признания Рабочей группой того, что она не имеет полномочий для разработки правил в отношении правительственных систем УИД (например, общегосударственных систем УИД), Рабочей группе следует рассмотреть возможность пересмотра статьи 2, с тем чтобы уточнить, что она «применяется в отношении… систем УИД ***частного сектора***».

3. Статья 3. Добровольное использование УИД и удостоверительных услуг

В соответствии с пунктом 2 статьи 3 согласие лица на использование системы УИД выводится из его поведения. Между тем, Рабочей группе следует учитывать тот факт, что это неверный вывод в том случае, если идентификационные данные лица были узурпированы — например, когда похититель идентификационных данных использует поддельные учетные данные или же использует подлинные учетные данные, выданные кому-либо другому лицу. В таких случаях лицо, о согласии которого делается вывод, не является лицом, поведение которого принимается во внимание.

4. Статья 4. Толкование

Рабочая группа, возможно, пожелает рассмотреть возможность обеспечения того, чтобы в проекте положений не проводилось различия между моделями системы УИД путем включения концепции **нейтральности системы УИД** (или нейтральности операций с идентификационными данными). Поскольку существует множество различных способов проведения операций с идентификационными данными в режиме онлайн (например, системы одного поставщика идентификационных данных (ПИД), федеративные системы (нескольких ПИД), системы, управляемые пользователем/ориентированные на пользователя, системы-концентраторы, системы ТРР, системы без учетных данных, независимые системы идентификации и т.д.), важно, чтобы проект положений не предусматривал или не предполагал применения какого-либо определенного подхода к процессам идентификации и/или аутентификации или к системе, которая их обеспечивает. Поэтому Рабочей группе следует рассмотреть способы обеспечения того, чтобы проект положений не подразумевал и/или не предусматривал применения какой-либо определенной модели системы.

5. Статья 5. Юридическое признание УИД

Возможно, потребуется провести определенный дополнительный обзор и анализ в отношении пункта (a) статьи 5. В этом положении говорится, что электронная идентификация не может быть лишена юридической силы лишь на том основании, что она осуществляется в электронной форме. Мы предполагаем (но не проверяли этого), что некоторые законы, касающиеся использования идентификационных учетных данных, требуют представления бумажной или другой физической формы, а не электронной формы. Поэтому, чтобы избежать противоречия таким законам, мы рекомендуем провести дополнительный обзор и анализ, чтобы оценить последствия этого положения.

6. Статья 6. Обязанности поставщиков услуг УИД

Уместность универсального подхода: статья 6 устанавливает ряд обязанностей для поставщиков услуг УИД. Перечисленные обязанности представляют собой обязанности, которые соответствуют традиционной модели системы УИД, и они предполагают, что поставщик услуг УИД выполняет или несет ответственность за все функции такой традиционной системы УИД. Тем не менее модели систем УИД подвергаются самым различным изменениям и экспериментам, и вследствие этого возникают опасения, что использование этого перечня обязанностей основано на старой модели, которая может не подходить для более новых систем УИД и/или может необоснованно препятствовать дальнейшим экспериментам. Например, во многих более новых системах УИД за выполнение некоторых функций поставщика услуг УИД, перечисленных в статье 6, могут отвечать различные другие участники (например, поставщики удостоверительных услуг, регистраторы, агенты по подключению, поставщики учетных данных, распорядители, поставщики аутентификационных услуг, концентраторы и т.д.). Учитывая растущее разнообразие моделей систем УИД, Рабочей группе следует рассмотреть вопрос о том, насколько все еще целесообразно предусматривать в проекте положений универсальный набор обязанностей поставщиков услуг УИД.

Источник обязанностей: Рабочая группа, возможно, пожелает также рассмотреть ключевой исходный вопрос. То есть, следует ли излагать в проекте положений обязанности поставщиков услуг УИД частного сектора (или любые другие функции системы УИД) и применять их ко всем системам УИД, или же каждая система УИД частного сектора должна определять такие обязанности в своей собственной основанной на договоре удостоверительной системе. Если обязанности по каждой функции будут включены в применимую удостоверительную систему системы УИД, то это позволит оператору системы и участникам адаптировать такие обязанности с учетом целей и задач конкретной системы УИД, а также применимого законодательства.

Правила, регулирующие работу системы УИД: наконец, следует отметить, что в этом положении содержится ссылка на «правила, регулирующие работу системы УИД», которые не определены. Неясно, например, будет ли такими правилами основанная на договоре удостоверительная система, применяемая к конкретной системе УИД, или же нечто иное.

7. Статья 7. Обязанности поставщиков услуг УИД в случае нарушения безопасности данных

Ответственность за принятие ответных мер в случае нарушения безопасности: в существующей редакции статьи 7, по-видимому, смешиваются понятия систем УИД и поставщиков услуг УИД и предполагается, что система УИД будет находиться под контролем одного поставщика услуг УИД, выполняющего все функции системы УИД. Кроме того, статья 7 возлагает на такого поставщика услуг УИД обязанности во всех случаях, когда происходит «нарушение безопасности» или «утрата целостности» данных, независимо от того, известно ли поставщику услуг УИД о таком нарушении безопасности или несет ли он за него ответственность или обладает ли он над ним контролем. Тем не менее на самом деле в системе УИД могут участвовать несколько сторон, многие из которых могут не нести какой-либо ответственности за сервер/сеть/систему, сотрудников или других лиц или устройства, имеющие отношение к нарушению безопасности, или же не осуществлять над ними контроля.

В соответствии со многими более новыми подходами к системам УИД некоторые из этих функций могут выполняться различными участниками (например, поставщиками удостоверительных услуг, регистраторами, агентами по подключению, поставщиками учетных данных, поставщиками аутентификационных услуг, концентраторами и т.д.). Каждая из этих функций может независимо

являться источником нарушения безопасности, и поставщику услуг УИД может быть даже неизвестно о таком нарушении.

Таким образом, при рассмотрении вопроса о нарушении безопасности данных Рабочей группе следует учитывать *различие между системами УИД и поставщиками услуг УИД* и тот факт, что в одной системе УИД могут участвовать несколько поставщиков услуг УИД (а также многие другие функциональные элементы). Соответственно, первая проблема, вероятно, будет заключаться в определении ответственности за предмет нарушения безопасности и ответственности за выполнение обязанностей по направлению уведомления.

В идеале обязанности по реагированию на нарушение безопасности, предусмотренные в статье 7 (например, по устранению нарушения, отзыву учетных данных, уведомлению властей или уведомлению затронутых субъектов данных и полагающихся сторон), должны возлагаться только на ту сторону, которая фактически пострадала от нарушения или иным образом несет ответственность за, конкретный сервер/сеть/систему, которые были взломаны или скомпрометированы. Например, в случае системы УИД, которая объединяет несколько поставщиков услуг УИД или несколько функций, возможно, целесообразно i) возложить обязанности по устранению нарушения на сторону, которая фактически пострадала от нарушения и в состоянии ограничить последствия и устранить нарушение, и ii) возложить обязанности по уведомлению субъектов на сторону, которая имеет отношения с субъектами.

Системное нарушение безопасности: соответственно, Рабочей группе следует рассмотреть также вопрос о пересмотре статьи 7, чтобы учесть возможность того, что серьезное системное нарушение безопасности в системе УИД с несколькими поставщиками услуг УИД (например, когда скомпрометирован корневой закрытый ключ) может поставить под угрозу всю систему УИД и всех его поставщиков услуг УИД, в зависимости от типа и структуры системы УИД. В этом случае нарушение безопасности может затронуть всех поставщиков услуг УИД, независимо от их ответственности за фактическое нарушение. Поэтому в данном случае, вероятно, потребуется другой тип ответных мер, и все поставщики услуг УИД, вероятно, должны будут взять на себя определенные обязанности по принятию ответных мер, даже если они не несут ответственности за данное нарушение безопасности.

Ответственность за утрату: наконец, обратите внимание, что в пункте 1(b) статьи 7 предусматривается, что поставщик услуг УИД «устраняет такое нарушение или ***утрату***». Хотя, возможно, целесообразно требовать, чтобы поставщик услуг УИД устранял нарушение безопасности (по крайней мере, нарушение, над которым он имеет контроль), Рабочей группе следует рассмотреть вопрос о целесообразности требования о том, чтобы поставщик услуг УИД устранял также «утрату». Утрата может быть значительной, и вопрос о том, должен ли — или в какой степени должен — поставщик услуг УИД отвечать за понесенную утрату, необходимо регулировать в соответствии с применимыми положениями об ответственности, как бы они не были определены.

8. Статья 8. Обязанности абонентов

Функциональные обязанности, подлежащие рассмотрению: в качестве общего замечания следует отметить, что, если в проекте положений будут рассматриваться обязанности участников системы УИД (например, в статьях 6, 7 и 8), то Рабочая группа, возможно, пожелает обсудить вопрос о рассмотрении обязанностей всех участников системы, например, обязанностей агентов по подключению, поставщиков атрибутов, поставщиков услуг УИД, поставщиков услуг по верификации идентификационных данных, пользователей, концентраторов, полагающихся сторон, поставщиков удостоверительных услуг, абонентов и т.д. Это может также оказаться важным для целей распределения ответственности в соответствии со статьей 12 ниже.

Где рассматривать обязанности: кроме того, Рабочая группа, возможно, пожелает рассмотреть вопрос о том, где лучше всего рассмотреть обязанности поставщиков услуг УИД, абонентов и других участников систем УИД. Статьи 6, 7 и 8 проекта положений основаны на универсальном подходе к рассмотрению обязанностей поставщиков и абонентов услуг УИД. Тем не менее с учетом разнообразия систем УИД, возможно, целесообразнее разрешить или предписать каждой системе УИД определить обязанности всех исполнителей ее различных функций в рамках удостоверительной системы, адаптированной к ее конкретной технологии, методологии и цели, а не использовать проект положений для установления универсального подхода ко всем системам УИД. Частично это обусловлено тем, что категории и определения системных функций, а также обязанности участников, выполняющих такие функции, вероятно, будут существенно различаться в зависимости от конкретной системы УИД. Одним из факторов, являющихся причиной таких различий, является цель, для которой создана конкретная система УИД (например, системы для облегчения связи в режиме онлайн в фармацевтической промышленности, такие как система УИД SAFE BioPharma, системы для облегчения обмена научной информацией, такие как система УИД InCommon, используемая университетами, или системы для облегчения связи с правительственными учреждениями, такие как система eIDAS).

Кроме того, как отмечалось выше в отношении статьи 6, модели системы УИД подвергаются самым различным изменениям и экспериментам, что вызывает обеспокоенность по поводу того, что, возможно, нецелесообразно включать стандартный перечень обязанностей, поскольку это может привести к навязыванию устаревшей модели, которая не подходит для многих современных систем УИД и препятствует дальнейшим экспериментам.

Обязанности субъектов/абонентов: статья 8 касается абонентов (т.е. лиц, которые заключают соглашение об услугах УИД). К этой категории, вероятно, относятся многочисленные участники системы УИД, например полагающиеся стороны, отдельные субъекты данных и, возможно, стороны, выполняющие различные другие функции в системе УИД. Эта статья возлагает на абонентов обязанность уведомлять поставщика услуг УИД, если какому-либо абоненту известно, что идентификационные учетные данные или механизмы электронной идентификации соответствующей системы УИД были скомпрометированы, либо ему известно об обстоятельствах, создающих значительный риск того, что они могли быть скомпрометированы.

В случае абонентов, которые являются физическими лицами (например, субъектами данных), это может создавать обременительное и необоснованное требование. Например, могут, вероятно, возникать многочисленные ситуации, когда отдельному абоненту системы УИД может быть известно об обстоятельствах, указывающих на возможную проблему, однако он просто не осознает их значимости. Более того, поскольку эта обязанность, по-видимому, распространяется на всю систему УИД (а не, например, отдельные идентификационные учетные данные, выданные конкретному лицу), это положение, по-видимому, налагает значительное бремя на физических лиц (и в этом отношении на других абонентов системы), которые могут быть осведомлены, но просто не понимать общесистемную значимость определенной информации.

Даже если речь идет об утрате или компрометации личных идентификационных учетных данных какого-либо физического лица, не всегда целесообразно возлагать на это лицо обязанность сообщать об утрате. Как и в случае с похищенными номерами кредитных карт, требование о том, чтобы субъект сообщал об этих событиях, может быть просто нереалистичным или даже неуместным (особенно в случае неискушенных пользователей или нарушений безопасности в Интернете или иным образом, которые они могут быть не в состоянии распознать). В случае же систем УИД, которые не основаны на использовании физических учетных данных, субъект может просто не иметь представления о том, что его учетные данные (например, идентификационный номер) были скомпрометированы.

9. Статья 9. Идентификация [субъекта] [лица] с помощью систем УИД

Целесообразность замещения действующего законодательства: статья 9 в значительной степени основана на положениях Типового закона об электронной подписи и Конвенции Организации Объединённых Наций об использовании электронных сообщений в международных договорах и, как представляется, имеет преимущественную силу по сравнению с действующим законодательством, которое устанавливает уникальные требования в отношении идентификации в конкретных случаях. В законах об электронной подписи такой общий подход по замещению всех других законов о подписи работал хорошо. Тем не менее Рабочая группа, возможно, пожелает оценить, действительно ли это так и в случае идентификации субъекта. В частности, поскольку некоторые законы требуют простой идентификации, а другие содержат весьма конкретные положения относительно порядка и метода идентификации (включая законы о конфиденциальности, законы ЗСК, нотариальное законодательство и т.д.), общее правило о соответствии в результате простого соблюдения стандарта надежности может оказаться нецелесообразным.

Общий процесс идентификации — даже «надежный» процесс, — по-видимому, вряд ли будет удовлетворять различным требованиям об идентификации во всем действующем законодательстве. Кроме того, если стороны коммерческой сделки предъявляют свои собственные требования к идентификации, электронный заменитель, соответствующий общему стандарту «надежности», также может оказаться недостаточным для удовлетворения конкретных или уникальных требований сторон.

Потенциальная коллизия статей: Рабочей группе следует также рассмотреть вопрос о возможной коллизии между пунктом 3 статьи 2 и статьей 9. В пункте 3 статьи 2 признается, что многие действующие законы налагают на стороны из частного сектора различные требования, касающиеся идентификации, и поэтому в данном пункте указывается, что «ничто в настоящем документе не затрагивает юридическое требование о том, чтобы какой-либо [субъект] [лицо] был идентифицирован в соответствии с какой-либо процедурой, определенной или предписанной законом». Тем не менее, универсальный подход, применяемый в статье 9, по-видимому, противоречит этому положению.

Вариант A статьи 9 гласит, что:

> «В тех случаях, когда норма права требует или допускает возможность идентификации [субъекта] [лица], то это норма выполняется в отношении УИД, если для электронной идентификации [субъекта] [лица] используется [надежный [метод] [система УИД]».

Вариант B статьи 9 аналогичен и гласит, что:

> «Субъект может быть идентифицирован с использованием услуг УИД, если для электронной идентификации [субъекта] [лица] используется надежный метод».

Учитывая широкое разнообразие требований в различных законах к процессам идентификации, универсальный подход статьи 9 не представляется осуществимым. Отчасти проблема, по-видимому, заключается в том, что идентификация рассматривается так же, как и электронные подписи. В случае электронной подписи создание электронной подписи в порядке, установленном Типовым законом, будет отвечать положению любого закона, требующему наличия подписи. В то же время это не относится к требованиям в отношении идентификации.

Юридические требования в отношении идентификации кого-либо существенно различаются в зависимости от законодательства, цели, для которой требуется идентификация (исходная или функциональная), и важности вопроса. Например, недавно принятые нормативные акты по применению Закона о защите конфиденциальности данных потребителей в Калифорнии, устанавливают

обширные требования к идентификации, которые должны быть выполнены до того, как личные данные могут быть предоставлены или удалены по требованию лица, претендующего на роль субъекта[4]. Аналогичным образом, множество особых требований к идентификации содержат правила ЗСК финансового сектора. Поэтому Рабочая группа, возможно, пожелает также рассмотреть вопрос о том, целесообразно ли, или при каких обстоятельствах целесообразно, использовать единое универсальное положение о том, что использование надежной системы позволяет выполнить юридическое требование в отношении идентификации.

Коллизия этих положений свидетельствует о возникновении проблем при попытке разработать свод норм об идентификации, используя такой же подход, какой ранее использовался в отношении электронных подписей.

Надежность как относительное понятие: кроме того, важно рассмотреть вопрос о том, насколько адекватно в статье 9 признается, что надежность (как и безопасность) является относительным понятием. Надежный метод в одном контексте может быть ненадежным в другом. Например, использование Facebook или Google для проведения электронной идентификации какого-либо лица часто является достаточно надежным методом для получения простого доступа к учетной записи на веб-сайте, однако этого, вероятно, недостаточно для получения доступа к банковскому счету и санкционирования онлайн-перевода средств с этого счета. Поэтому, если предполагается сохранить основанный на надежности подход для получения результата, имеющего юридическую силу, Рабочей группе рекомендуется рассмотреть возможность изменения текста статьи 9, с тем чтобы признать, что «надежный метод» является относительным понятием. Один из возможных подходов заключается в том, чтобы включить нечто подобное понятию «настолько надежный, насколько это необходимо», которое используется в Конвенции Организации Объединенных Наций, т.е. используемый метод либо i) является настолько надежным, насколько это соответствует цели, для которой требуется идентификация, с учетом всех обстоятельств, включая любые соответствующие договоренности; либо ii) является, как было доказано, достаточно надежным.

Различные процессы, имеющие отношение к надежности: поскольку требование надежности применяется только к методу, используемому для электронной идентификации[5], в статье 9, по-видимому, игнорируются также все другие требования к процессу идентификации, которые также могут повлиять на надежность результата, а также методы, которые могут быть использованы для этих процессов. К таким процессам относятся процессы проверки идентификационных данных, процессы подключения, защита учетных данных, процессы аутентификации, процессы электронной идентификации, программное обеспечение, защита данных, сотрудники и т.д. Например, даже если для электронной идентификации какого-либо лица используется объективно надежный метод, это не будет иметь значения, если достаточно надежным не будет также процесс проверки идентификационных данных.

10. Статья 10. Факторы, имеющие значение для определения надежности

В статье 10 указаны только факторы, имеющие отношение к определению надежности «метода… для электронной идентификации»[6], упомянутого в статье 9. Тем не менее в нем не указаны факторы, которые следует оценивать для

[4] См. California Consumer Privacy Act Regulations at Article 4, available at www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

[5] См. пункт (d) статьи 1 проекта положений, в котором электронная идентификация определяется как «процесс, используемый для достижения достаточной уверенности в наличии связи между [субъектом] [лицом] и идентификационными данными».

[6] Определение термина «электронная идентификация», как оно изложено в пункте (d) статьи 1, ограничивается процессом, используемым для достижения достаточной уверенности в наличии связи между субъектом/лицом и идентификационными данными. Оно не охватывает многие другие процессы, которые требуются для системы УИД.

определения надежности любых других ключевых процессов, выполняемых системой УИД, например процесса проверки идентификационных данных.

Статья 10 посвящена следующим четырем категориям факторов:

- соблюдение обязательств по статье 6,
- соответствие «правил, регулирующих работу системы УИД», любым признанным международным стандартам и процедурам, включая систему уровней доверия,
- осуществление надзора или проведение сертификации в отношении системы УИД, и
- наличие «договоренностей между сторонами».

Тем не менее, хотя перечисленные четыре категории факторов охватывают соблюдение правил или стандартов, сертификацию и договоренности между сторонами, они не обязательно устанавливают надежность. Тот факт, что правила и стандарты, сертификация или договоренности существуют и соблюдаются, не обязательно означает, что удовлетворяющая им система УИД является надежной для любого конкретного применения. Поэтому, если Рабочая группа решит указать факторы для определения надежности «метода… для электронной идентификации», она, возможно, пожелает рассмотреть вопрос о том, какие конкретные процессы имеют отношение к надежности (например, процессы проверки идентификационных данных, процессы подключения, защита учетных данных, процессы аутентификации, процессы электронной идентификации, программное обеспечение, защита данных, сотрудники и т.д.), а затем определить, какие правила или стандарты устанавливают надежность в отношении каждого из этих процессов.

Кроме того, как следует из вышеизложенного перечня, существует множество различных процессов, используемых системами УИД, каждый из которых может быть выполнен с использованием одного или нескольких различных «методов», которые могут быть или не быть надежными. Более того, установление того, что «метод… для электронной идентификации» является надежным методом, не обязательно означает, например, что с использованием надежного метода был выполнен процесс проверки идентификационных данных, на который он опирается.

11. Статья 11. Назначение надежных систем УИД

Критерии и компетенция: в статье 11 публичному или частному лицу или ведомству, назначенному государством («**ведомство по вопросам надежности**»), предоставляется право назначать системы УИД, которые считаются надежными. В то же время в статье 11 не устанавливается каких-либо критериев, касающихся компетенции ведомства по вопросам надежности производить такое назначение. Более того, она не содержит указания на процесс, который следует использовать, помимо требования принимать во внимание все соответствующие обстоятельства, включая факторы, перечисленные в статье 10, и общего требования обеспечить соответствие неуказанным «признанным международным стандартам и процедурам, применимым к определению надежности». В результате возникает беспокойство в связи с тем, что неквалифицированные ведомства по вопросам надежности могут оценивать надежность, используя ненадлежащие критерии, и что, следовательно, ненадежные системы УИД могут быть назначены как надежные. Кроме того, назначения надежных систем УИД, вероятно, будут сильно различаться между государствами, даже по одной и той же системе УИД. С учетом важности такого назначения применительно к статье 9 (так как в статье 9 предполагается, что такие назначенные системы УИД используют «надежные методы» и получаемый результат имеет юридическую силу) это может привести к значительным проблемам.

Рабочая группа, возможно, пожелает также рассмотреть вопрос о том, каким образом государство будет назначать такое ведомство по вопросам надежности в качестве компетентного, а также как оно будет обеспечивать, чтобы такое ведомство по вопросам надежности обладало опытом, процессами и ресурсами, необходимыми для назначения «надежных» систем УИД. Должно ли, например, ведомство по вопросам надежности, указанное государством, проходить определенную сертификацию, прежде чем ему будут предоставлены такие полномочия?

Надежность систем или надежность операций: поскольку надежность является относительным понятием, в процессе оценки надежности, вероятно, необходимо будет задавать вопрос «надежна для какой цели?» В связи с этим возникает исходный вопрос о том, следует ли Рабочей группе сосредоточить внимание на надежности систем УИД в целом (независимо от типа операции с идентификационными данными, для которых они используются) или на надежности операций УИД (которые указывают на конкретный контекст, исходя из которого можно судить о надежности).

Надежность систем УИД или надежностью «метода… для электронной идентификации»: основное внимание в статье 11 уделяется надежности «систем УИД», тогда как в статье 9 определяется юридическая сила идентификации на основе надежности «метода... для электронной идентификации». Эти два подхода кажутся несовместимыми, в частности потому, что надежность в отношении метода электронной идентификации является лишь элементом общей надежности функций системы УИД.

Практические вопросы: сосредоточение внимания в статье 11 на роли ведомства по вопросам надежности (и его значении для обеспечения юридической силы, предусмотренной в статье 9) указывает на необходимость создания централизованного организационного механизма для оценки систем УИД в каждом государстве и участия публичных органов по меньшей мере для назначения ведомства по вопросам надежности. Мы призываем Рабочую группу рассмотреть вопрос о практической целесообразности такого подхода.

Кроме того, Рабочая группа, возможно, пожелает рассмотреть вопрос о том, не будет ли необходимость получения преимуществ от назначения надежной системы УИД дискриминировать те системы УИД, которые не в состоянии покрыть расходы на процесс определения надежности. К числу других вопросов, которые Рабочая группа, возможно, пожелает рассмотреть, относятся следующие:

- кого следует уполномочить назначать ведомство по вопросам надежности?
- как определить, является ли ведомство по вопросам надежности квалифицированным и компетентным?
- насколько надежным является назначение надежных систем ведомством по вопросам надежности (поскольку это оценка производится в определенный момент времени)? Как часто его следует повторять?
- должно ли государство заниматься назначением ведомства по вопросам надежности для систем УИД частного сектора или обусловливать определенные юридические последствия получением такого назначения?
- будет ли это иметь в качестве практического результата требование о том, чтобы все системы УИД соответствовали стандартам, установленным государством и/или ведомством по вопросам надёжности (поскольку все захотят получит статус надежной системы), что может стать препятствием на пути дальнейшего развития систем?
- что является «признанным международным стандартом»? Кто обеспечивает признание? Что произойдет, если такой стандарт изменится?

- может ли установление и соблюдение выбранного стандарта потребовать выполнения потенциально дорогостоящих и сложных процедур сертификации?
- как факторы для определения надежных методов (в статье 10) соотносятся с требованиями в отношении определения надежных систем УИД (в статье 11)?

Наконец, поскольку в статье 11 предусматривается назначение систем УИД независимо от местонахождения, Рабочей группе следует рассмотреть вопрос о том, не создаст ли это для систем УИД практическую потребность ходатайствовать о таком назначении в каждом государстве, где ее абоненты будут осуществлять коммерческую деятельность, и не будет ли это препятствовать трансграничным операциям.

12. Статья 12. Ответственность поставщиков услуг УИД

В связи с проектом этой статьи возникает ряд вопросов относительно положений об ответственности, которые Рабочая группа, возможно, пожелает рассмотреть.

Исходное предположение: статья 12 (по крайней мере, варианты B и C), как и статья 6, по-видимому, основана на предположении о том, что ко всем системам идентификации могут применяться одни и те же правила. Тем не менее, с учетом постоянно углубляющихся различий в типах, целях, области применения, функциональных возможностях, методах работы, а также в функциях и обязанностях участников систем УИД, весьма маловероятно, что положения, изложенные в статье 6, или положения об ответственности, изложенные в вариантах B или C статьи 12, будет уместным во всех случаях. Достаточно сопоставить различия между традиционными системами идентификации на основе ИПК, системами идентификации на основе блокчейн, системами идентификации, ориентированными на пользователя, и системами самостоятельной идентификации, чтобы увидеть, что эти положения подходят не во всех случаях. Поскольку системы УИД могут существенно различаться, любое стандартное распределение ответственности может не подходить для всех систем УИД. Поэтому Рабочая группа, возможно, пожелает рассмотреть вопрос о целесообразности универсального подхода к вопросу об ответственности.

Охватываемые функции: статья 12 посвящена ответственности только поставщика услуг УИД. Если Рабочая группа придет к выводу о том, что в этом проекте положений следует рассмотреть вопрос об ответственности, то, возможно, целесообразно рассмотреть вопрос о распределении ответственности между всеми участниками. Это может включать, например, ответственность поставщиков услуг УИД, агентов по подключению, поставщиков атрибутов, поставщиков идентификационных данных, субъектов, пользователей, концентраторов, поставщиков услуг по верификации, поставщиков удостоверительных услуг, полагающихся сторон и т.д. Это важно, поскольку рассмотрение ответственности одного участника системы не позволяет смягчить или устранить ущерб, который может быть нанесен в результате возникновения той или иной проблемы. Такой подход просто переносит такой ущерб на кого-то другого. При определении надлежащего распределения ответственности следует рассмотреть вопрос о том, кто должен надлежащим образом нести ответственность за такой ущерб.

Право на ограничение или отказ от ответственности: Рабочая группа, возможно, пожелает рассмотреть вопрос о том, должен ли поставщик услуг УИД (или другие участники системы) иметь право отказываться от ответственности или ограничивать свою ответственность по договору или другими способами. Вариант A может предусматривать ограничение или отказ от ответственности, по меньшей мере, в пределах, допустимых в соответствии с применимым законодательством. Это положение, по-видимому, основано на признании того, что существует множество других сценариев и типов ответственности, при которых

поставщик услуг УИД или другие участники могут на законных основаниях стремиться отказаться от ответственности или ограничить ответственность, и, по меньшей мере, позволяет учесть возможности ограничения ответственности и варианты отказа от ответственности, предусмотренные в соответствии с применимым законодательством.

Хотя вариант C и обеспечивает ограниченное право на отказ от ответственности, он весьма ограничен по охвату и не допускает применения гибкого подхода. Кроме того, возникает вопрос о том, не запрещают ли положения вариантов B или C в целом поставщику услуг УИД полностью отказываться от ответственности (как это обычно делает правительственный орган).

Кроме того, поскольку варианты B и C ограничивают ответственность поставщика услуг УИД ответственностью за нарушение их обязательств, изложенных в статье 6, возникает вопрос о том, как это ограничение будет действовать в случае похитителя идентификационных данных. Иными словами, если поставщик услуг УИД выдает учетные данные похитителю идентификационных данных или производит его электронную идентификацию, не нарушая положений статьи 6, то кто будет нести ответственность за ущерб? Должна ли нести ущерб жертва хищения идентификационных данных, которая может не осуществлять взаимодействия или контрактов с поставщиком услуг УИД?

Ограничения ответственности в варианте C: пункт 3 статьи 12 варианта C основан на предположении о том, что 1) для конкретных операций с идентификационными данными могут быть установлены ограничения в отношении целей или стоимости (хотя в нем не указано, где и как эти ограничения устанавливаются), и 2) что полагающаяся сторона сможет легко получить доступ к информации о таких ограничениях, прежде чем она начнет на что-либо полагаться. Похоже, что это пережиток первоначального подхода, который применялся в некоторых ранних системах ИПК и в соответствии с которым сертификат, выданный сертификационным органом (СО), содержал указание на цель или предельную сумму в долларах, которые полагающаяся сторона должна была оценить, прежде чем на что-либо полагаться. Учитывая широкое разнообразие существующих на сегодняшний день систем УИД, Рабочая группа, возможно, пожелает рассмотреть вопрос о том, является ли ограничение ответственности на основе операций практически применимым. Эту статью, например, можно изменить, чтобы признать, что такие ограничения могут быть предусмотрены в удостоверительной системе поставщика услуг УИД или в договоре с полагающимися сторонами, а не в рамках отдельных операций.

Правительственный интерфейс: наконец, Рабочая группа, возможно, пожелает также рассмотреть вопрос о возможном взаимодействии с правительственными системами УИД. Во многих случаях поставщики услуг УИД полагаются на атрибуты, заверенные третьими сторонами, например, национальными системами УИД или другими правительственными базами данных (такими, как ДАС). Поскольку правительственные системы УИД часто рассматриваются в качестве авторитетного источника данных, хотя они также обычно не несут ответственности за ошибки, следует рассмотреть вопрос об определении того, кто будет нести ущерб в случае ошибок в информации, предоставленной правительством. Таким образом, если предусматривается участие публичных органов, то может потребоваться другой подход.

Мы настоятельно призываем Рабочую группу рассмотреть возможность воздержаться от попыток распределить ответственность, особенно с учетом широкого разнообразия систем, процессов и участников УИД. Если Рабочая группа решит рассмотреть вопрос об ответственности, то мы рекомендуем ссылаться на методы установления ответственности, а не на конкретные стандарты, спецификации или положения об ответственности. Такие методы могут предусматривать, например, ссылку на действующее законодательство (как в варианте A) или ссылку на основанные на договоре удостоверительные системы, которые

применяются системой УИД и с которыми стороны соглашаются на договорной основе.

13. Статья 26. Трансграничное признание УИД и удостоверительных услуг

- Что касается вопроса о трансграничном «признании», то Рабочая группа, возможно, пожелает уточнить ответы на следующие три основных вопроса: признание чего, признание кем и признание с какой целью?

- признание чего? — ответ на этот вопрос, по-видимому, содержится в пункте 1 статьи 26, в котором основное внимание уделяется «системам УИД» и «юридической силе» «систем УИД». Тем не менее неясно, каким образом система УИД может иметь юридическую силу или в чем может состоять юридическая сила системы. Можно предположить, что юридическую силу может иметь решение полагаться на проверку идентификационных данных и/или процессы электронной идентификации, выполняемые системой УИД, однако неясно, каким образом сама система УИД может рассматриваться как имеющая юридическую силу.

Для сравнения — государства признают паспорта, выданные другими государствами на основе стандартов ИКАО. Каждое государство, как предполагается, соглашается с действительностью стандартов ИКАО и может оценивать или не оценивать, соответствует ли система выдачи паспортов каждого другого государства этим стандартам, однако на границе признается «юридическая сила» именно учетных данных, т.е. паспорта, выдаваемого системой каждого государства.

- признание кем? — органом, признающим иностранную систему УИД, по-видимому, будет либо: 1) публичный орган, например правительство или суд, применяющий соответствующую правовую систему (так же, как и при соблюдении юридического требования в отношении проверки идентификационных данных или при определении допустимости доказательства в суде) или 2) полагающаяся сторона (в публичном или частном секторе). В проекте статьи 26 основное внимание, по-видимому уделяется первому варианту, поскольку она содержит ссылку на «юридическую силу» всего того, что подлежит признанию. Более того, второй вариант не требует принятия закона или юридического заключения, поскольку полагающиеся стороны, безусловно, имеют право принимать самостоятельные решения относительно того, будут ли они признавать и/или полагаться на системы УИД или идентификационные данные для целей любой операции, в которой они участвуют.

- признание с какой целью? — если «система УИД» признается законодательством иностранного государства, то что это значит? Концепция системы УИД, имеющей юридическую силу, представляется несколько запутанной. Например, означает ли это, что иностранное государство автоматически признает результаты электронной идентификации, выполненной признанной системой УИД, или это просто означает, что признанной системе УИД разрешается осуществлять коммерческую деятельность в рамках иностранной юрисдикционной системы, однако ее процессы, возможно, потребуется изменить для соблюдения юридических требований, которые иностранная юрисдикционная система предъявляет к своим собственным системам УИД?

Рабочей группе следует рассмотреть возможность уточнения того, что она имеет в виду, заявляя, что система УИД, управляемая за пределами [принимающего государства], имеет ту же юридическую силу в [принимающем государстве], что и система УИД, управляемая в [принимающем государстве].

14. Статья 27. Сотрудничество

Цель статьи 27 не ясна. Как представляется, основное внимание уделяется обмену информацией, опытом и успешными видами практики, что, безусловно, не является нежелательным и в идеале должно поощряться, особенно если такой обмен носит добровольный характер и не требует заключения договоренностей, имеющих обязательную силу для организаций, не участвующих в таком сотрудничестве. В этом случае, однако, не представляется необходимым требовать, чтобы принимающее закон государство назначало организацию, обменивающуюся информацией, в качестве компетентной. Более того, не представляется необходимым сосредотачивать сотрудничество только на трех областях, перечисленных в статье 27.

Если же сотрудничество и обмены являются обязательными или служат основой для юридического признания государством или заключения договоренностей, имеющих обязательную силу для организаций, не участвующих в таком сотрудничестве, это может породить целый ряд проблем, которые, как представляется, требуют дальнейшего обсуждения и разъяснения Рабочей группой.

Обратите также внимание, что статья 27 разрешает (или предписывает) организации или учреждению, назначенному принимающим закон государством в качестве компетентного, сотрудничать «с иностранными организациями». Непонятно, что означает термин «иностранные организации» — например, является ли она иностранной правительственной организацией, является ли она поставщиком услуг УИД, который работает в иностранном государстве, и т.д.? Возможно, такое сотрудничество с «иностранными организациями» должно быть ограничено сотрудничеством с иностранными организациями, которые также назначены иностранным государством в качестве компетентных.