Создание Правовой Базы для Развития ИКТ: Пример Законодательства по Э-Подписи в Странах с Развивающейся Рыночной Экономикой

Джеймс К. Демпси*

Введение

Многие развивающиеся страны и страны с переходной экономикой горят желанием участвовать в глобальной экономике, базирующейся на информатизации. Эти страны признают, что законодательство и политика правительства могут играть важную роль либо затормаживая, либо стимулируя развитие информационно-коммуникационных технологий (ИКТ), рост э- экономики, а также создание э-правительства.

Ведение бизнеса и предложение услуг э-правительства на глобальном цифровом пространстве ставит важные вопросы о юридической силе электронных документов и сложные вопросы доверия и удостоверения подлинности. Правительства и эксперты по политике столкнулись с проблемой как обеспечить уверенность и доверие к бизнесу и гражданам, осуществляющим сделки он-лайн. Одно из решений, которое привлекло достаточно большое внимание - это принятие законов об «электронной подписи» или «цифровой подписи»[1]. Во многих странах, политики, стремящиеся стимулировать э-коммерцию и э-правительство, отдают приоритет принятию законов, предназначенных для создания правовой базы для использования и признания электронной и цифровой подписи. За последние 5-7 лет, примерно 50 стран приняли законы или нормативные акты по электронной или цифровой подписи, а другие только рассматривают их.[2] В ряде этих законов предполагается наличие сложных систем «инфраструктуры общих ключей» и «сертифицирующих органов», которые как предполагается, будут заниматься технологией для создания цифровых подписей на основе криптографии. Некоторые включают государственное лицензирование. Некоторые предусматривают, что только подписи, созданные при помощи технологии, утвержденной государством, будут признаваться как имеющие обязательственную силу. Принятие этих законов сопровождалось отчетами, статьями в журналах и газетах предрекающими, что

* Исполнительный директор, Центр Демократии и Технологии, г. Вашингтон, http://www.cdt.org, и Директор по Политике, Глобальная Инициатива по Интернет Политике http://www.internetpolicy.net.

[1] В соответствии с общепринятой конвенцией, в настоящей статье использован термин «электронная подпись» для обозначения любой идентификации сделанной электронными средствами. По данной дефиниции, электронные подписи включают цифровые версии рукописных подписей, биометрические техники, а также строка в эл.почте «От». Термин «цифровая подпись» относится к специфическому виду электронной подписи с использованием асимметричного шифрования, при котором пользователь объявляет открытый криптографический ключ и «подписывает» сообщение закрытым ключом, таким образом, что применение открытого ключа будет подтверждать, что сообщение было «подписано» закрытым ключом, который является единственной парой для того открытого ключа.

[2] Законы многих стран по э-комерции собраны на сайте: http://rechten.kub.nl/simone/ds-lawsu.htm и http://www.mbc.com/ecommerce/legislative.asp.

законодательство по э-подписи произведет коренной перелом в деловой практике и будет стимулировать э-коммерцию.

Одна из целей данной статьи – убедить в том, что роль законодательства по э-подписи на практике значительно меньше, чем это было разрекламировано.[3] Нельзя сказать, что доверие и идентификация не важны для онлайн сферы. Они важны. Технология цифровой подписи и другие идентификационные онлайн системы заслуживают внимания, как в развивающихся странах, так и в развитых. Моя позиция такова, что правовая система может предложить только частичную уверенность, но не может создать полного доверия. Ценность цифровых подписей и иных идентификационных систем проистекает в меньшей степени из юридических норм, чем из самой технологии, выбора сделанного теми, кто использует эту технологию, и способов, с помощью которых бизнес структуры используют ее в своей коммерческой деятельности, поскольку это уже действительно практикуется онлайн.

Вторая тема этой статьи – это то, что зацикливание на электронной подписи при обсуждении э-коммерции и развития ИКТ может создать неправильное представление в отношении приоритетов правовой реформы, которая необходима для поддержки Интернета и э-коммерции. В данной статье приводится мнение, что, акцентирование внимания на законах по электронной подписи, по крайней мере, на слишком раннем этапе, может отвратить от более важных вопросов. Еще хуже выглядит подход, применяющий чрезмерное регулирование электронных подписей, что может замедлить развитие э-комерции.

Третья цель этой статьи – всеусиливающаяся тенденция в странах с развивающейся экономикой разрешить вопросы, связанные с электронными документами и э-подписями. В этом подходе подчеркивается, первое: обеспечение того, что не существует никаких юридических препятствий для принятия электронных документов и, второе, возможность для бизнесменов урегулировать между собой технические стандарты для того, чтобы заключать контракт в электронной форме. Третье, для создания э-правительства, правительства стран могут экспериментировать с идентификационными системами (в том числе, возможно использование цифровой подписи). Но правительства не должны спешить с введением регулятивной системы, целью которой является утверждение технологий или провайдеров услуг по э-комерции.

И последнее, в результате обсуждения законодательных ограничений по электронной подписи были получены достаточно обширные уроки для тех, кто заинтересован в правовых реформах для поддержки роста Интернета как одного из компонентов развития. Первое, здесь подчеркивается важность того, чтобы правовые реформы основывались на тщательном анализе местных нужд и существующей деловой практики, поскольку создается впечатление, что иногда законы по электронной подписи вносятся без предварительной реальной оценки юридических и иных барьеров, препятствующих развитию и использованию ИКТ. Второе, опыт с законодательством по цифровой подписи еще раз подтверждает, что инициативы по правовым реформам, направленные на стимулирование развития ИКТ должны отдавать приоритет основам либерализации телекоммуникаций, устранению барьеров по лицензированию, поддержке предпринимательства, прозрачности, банковскому и валютному законодательству, а

[3] Другие уже также озвучивали эту тему. John Humphrey, et al., Реалии э-коммерции в развивающихся странах, Institute of Development Studies at the University of Sussex and Interdepartmental Programme in Media and Communication of the London School of Economics and Political Science (March 2003), http://www.gapresearch.org/production/Report.pdf; Jane K. Winn, Новый наряд императора: шокирующая правда о цифровой подписи и Интернет коммерции, 37 Idaho L. Rev. 353 (2001).

также улучшению основных транспортных инфраструктур. Если эти вопросы не будут разрешены, э-коммерция не будет процветать, и не имеет значение, какой закон будет принят по э-подписи. В завершение, опыт с законодательством по электронной подписи в развитых, менее развитых странах и странах с переходной экономикой показывает, что закон не в состоянии охватить то, что вне рамок технологии или рыночного пространства.

Необходимость достоверности и доверия в сфере э-комерции и э-управления

Понятно, что появляются вопросы по поводу юридической приемлемости электронных документов и электронных подписей для законодательства многих стран, когда речь идет о контрактах или информации, которые должны в обязательном порядке быть представлены правительству, а также по поводу использования таких формулировок как «письменный» или «оригинал» или «подписанный» - формулировки, которые в течение долгого времени ассоциировались с использовать ли им электронные средства коммуникации при бумажными документами. Коммерческие структуры и частные лица могут сомневаться при совершении сделок или при обращении в госорганы, если они не уверены, что электронное сообщение имеет обязательственную силу. Для того чтобы стимулировать э-комерцию и э-управление, возможно будет необходимо прояснить, что формулировки «письменный», «оригинал» и «подпись», когда они используются в законодательстве или иных нормативных актах относительно заключения контрактов или соответствия требованиям подачи заявлений в госорганы, не исключают использования электронных сообщений.[4]

Однако, есть расхождение между законодательными решениями, которые предлагаются во многих странах, как в более развитых, так и в менее развитых, и необходимостью в достоверности. Проблемы начинаются уже с невозможности отделить достоверность от доверия, и отделить юридические аспекты доверия от неюридических аспектов этого понятия. На самом простом уровне, вопрос насчет достоверности возникает по поводу того, будет ли электронное сообщение соответствовать юридическим требованиям, которые предъявляются к документам «в письменной форме»? Связанные с этим вопросы включают: что является «оригиналом» электронного документа, например, когда доказательственные нормы требуют, чтобы кто-то предоставил «оригинал» документа в качестве доказательства в суд? Это чисто юридические вопросы.

Более сложная часть вопросов касается того, какие электронные функции могут соответствовать юридическим требованиям к «подписи». Здесь вопрос юридической достоверности совмещен с вопросом доверия на глобальном рыночном пространстве. Разрешение вопросов, связанных с электронной подписью требует полного понимания разнообразных функций, которые выполняет подпись, выполненная чернилами на бумаге.[5] Желание развивать э-комерцию может также оправдать пересмотр той роли, которую играет подпись в контрактах и юридических документах в целом. Выводы в таких исследованиях могут отличаться в странах, где применяется общее право от

[4] См. Анализ международных инициатив по применению электронной подписи, исследование подготовлено для Форума по Интернет праву и политике, сент.2000г. Chris Kuner and Stewart Baker, опубликовано на http://www.ilpf.org/groups/analysis_IEDSII.htm.

[5] См. Jane K. Winn, Новый наряд императора: шокирующая правда о цифровой подписи и Интернет коммерции, 37 Idaho L. Rev. 353 (2001).

стран, где применяется римское право. Тем не менее, в большинстве правовых систем основной юридической функцией «подписи» является – обозначить намерение принять на себя те обязательства, под которыми стоит подпись. Второстепенное значение, подписи может быть ценным материалом при разрешении споров возникших в отношении данного договора. Так, в той мере, в какой подписи являются уникальными и их можно распознать, они могут служить для идентификации и удостоверения личности подписанта. Появление уникальной подписи на листе бумаги может осложнить для подписавшего лица возможность отказаться от подписанного им документа.

Однако, в политических дискуссиях вокруг законов по электронной подписи, вопрос юридической достоверности и вопросы доверия объединены в один. Чтобы принять правовые реформы, приспособленные к реальной практике, очень важно разделить вопрос о том, есть ли уверенность в том, что электронный документ будет иметь юридическую силу и иметь исковую силу, и отдельные вопросы доверия и идентификации. Онлайн коммуникации могут представлять особо острый вопрос доверия и идентификации, но важно признать, что в большинстве своем это не правовые вопросы, которые могут быть разрешены законодательным путем. Например, как получатель электронного сообщения может достоверно знать что лицо, направившее его, является тем самым за кого он себя выдает? Это вопрос идентификации и удостоверения личности. Следующий вопрос – как получатель сообщения, который поверил ему, может избежать того, что мнимый отправитель будет отрицать, что именно он отправил это сообщение? Это вопрос признания («не-отказа»). Также, как можно гарантировать, что сообщение будет прочитано только тем получателем, кому оно направлено, а не тем, кто мог бы перехватить его? Это проблема «конфиденциальности». И последнее, как можно доказать, что сообщение не претерпело изменений или не было как-то по-другому подделано во время передачи или хранения? Это проблема «целостности».

Эти вопросы не уникальны только для электронных сделок, хотя некоторые говорят, что это так. Однако замешательство возникает по поводу этой третьей группы вопросов в сфере э-коммерции, отчасти из-за того, что криптографические технологии, используемые для создания «цифровой подписи», также могут использоваться для увеличения он-лайн доверия перед лицом этих 4 проблем – идентификация и удостоверение личности, признание, конфиденциальность, и целостность. В действительности, цифровые шифровальные технологии, если они надлежаще применены, могут обеспечить гораздо более высокую степень доверия, чем подписи написанные ручкой на бумаге. (Хотя на практике, использовать шифрование для разрешения этих проблем, нелегко). Но компоненты доверия – идентичность, признание, конфиденциальность, и целостность сообщения – в основном не являются юридическими вопросами. Например, шифрование часто используется для установления безопасной связи между веб-сервером и веб-клиентом, таким как, например персональный компьютер. Такая безопасность защищает конфиденциальность информации (такой как номер кредитки, например) между компьютером потребителя и компьютером компании. Там используются такие же технологии, которые могут использоваться и для цифровых подписей, но конфиденциальность данных во время передачи не будет иметь значения для юридической силы данной сделки. Конфиденциальность просто не является юридическим требованием для контракта. Тоже самое, с юридической точки зрения , не является необходимым, чтобы человек подтверждал свою личность для того, чтобы заключать контракт (хотя с практической точки зрения это может быть очень важно). Признание также не является юридическим требованием для заключения контракта.[6] И если целостность документа можно поставить под вопрос, целостность в основном является практическим вопросом, который также применим и к бумажным документам. Это разделение функций

[6] Id.

электронной подписи между теми, которые являются юридическим требованием для заключения договоров и теми, которые просто придают уверенности вне зависимости от юридических требований – слишком часто упускаются из виду при обсуждении э-комерции. Также упускается из виду разница между вопросами достоверности, которые могут быть разрешены путем принятия определенных нормативных актов и вопросами доверия, которые могут быть разрешены посредством технологии независимо от нормативной базы.

ПРАВОВЙ КОНТЕКСТ ДЛЯ РАЗВИТИЯ ЭЛЕКТРОННОЙ КОММЕРЦИИ И ИКТ

Некоторые другие вопросы также часто упускаются при обсуждении электронной коммерции: например, тот факт, что законодательство по электронной подписи не является самым важным реформированием политики, необходимым для поддержки развития электронной коммерции и ИКТ.[7] Самый лучший в мире закон по электронной подписи не сможет заставить процветать электронную коммерцию, если не проводится реформирование в других правовых сферах. И наоборот, э-коммерция сможет процветать без закона по э-подписи, если предпринимаются другие правовые реформы. Вероятно, не будет преувеличением сказать, что уже доказано, что законы по э-подписи в основном не связаны с развитием э-комерции.[8] В наиболее развитых странах с наиболее устойчивой э-коммерцией, последняя начала свое развитие до того как были приняты законы по э-подписи.[9] Подтверждено практикой, что законы по э-подписи в основном несущественны для применения э-подписей, поскольку в реальном мире больше всего э-подписи применяются в закрытых системах, там, где законы не применяются.

По сравнению с законодательством по э-подписи, есть другие реформы, которые гораздо более важны при создании законодательной и регулятивной среды для э-коммерции.[10] Первая и самая главная среди них, это, скорее всего, реформа в сфере

[7] Появился и более реалистичный подход, например, в отчете UNCTAD за 2001г по э-комерции и развитию, в котором говориться что ограничительные регулятивные нормы, такие как контроль за протоколами обмена, защита монополий телекомов, ограничительная торговая практика, ограничения шифрования и запрещение Интернет телефонии, больше заботят предпринимателей в менее развитых странах чем наличие или отсутствие закона по э-комерции. Стр.195.

[8] Например, в США, где контракты в основном регулируются законами штата, штат Юта был первым в котором принят закон по э-подписи. Закон штата Юта дает юридическую силу подписям созданным на основе асимметричной криптосистемы с использованием пар открытых и закрытых ключей. Закон, называющийся Акт штата Юта по цифровой подписи, был подписан губернатором Юты в марте 1995 и в него вносились поправки в течение 1996г законодательной сессией Юты. Нет свидетельств того что компании или частные лица в юте стали использовать э-коммерцию быстрее или больше чем в каком-либо другом штате.

[9] Например, на федеральном уровне США приняли закон по э-подписи в 2000г, но к тому моменту объем розничной э-торговли составил уже 29 млрд. долл. в год (это конечно малая толика от общих розничных продаж в США, но все же значительное свидетельство того что покупатели и продавцы вышли на онлайн рынок не нуждаясь в законе по э-подписи). Amazon.com , онлайн книжный магазин, был создан в 1995, вышел в народ в 1997, и заработал 1,8 млрд.долл. за первые 9 месяцев 2000года – т.е. до того как вступил в силу Акт США по э-подписи. Чтобы посмотреть ситуацию в Англии, см. Ian Lynch, закон по э-подписи, помеченный как «отвлекающий маневр» (июль 25, 2000) http://www.vnunet.com/News/1107369.

[10] Выбор между законами по э-подписи и другими законодательными реформами – это не есть ситуация уступок или где выигрываешь в одном и проигрываешь в другом – за исключением когда правительства вынуждены отдавать приоритет своим правовым реформам. Конечно страны могут принять законы по э-подписи, но в то же самое время применить множество других реформ необходимых для развития ИКТ. Моя идея заключается в том что правительства не должны ставить законы по э-подписи впереди других более фундаментальных реформ и что они не должны воспринимать так что они могут рассматривать что процесс реформирования правовой базы для ИКТ уже завершен если они приняли закон по э-подписи.

телекоммуникаций. Для того чтобы осуществлять э-коммерцию требуется доступ в Интернет, но для этого большинству пользователей и в большинстве случаев, необходим доступ к телекоммуникациям. Уже было продемонстрировано, что принятие документов по «либерализации» (т.е., внедрение конкуренции, приватизация государственных операторов связи и создание независимых регуляторов, способных эффективно распределять частоты и стимулировать конкуренцию) будут лучше стимулировать инвестиции, инновации и развитие инфраструктуры, что приведет к более низким тарифам на доступ, и соответственно внесет свой вклад в развитие ИКТ.[11]

Очень важно отметить, что либерализация не означает нерегулирование. Для либерализации телекома необходимо создание независимого регулятора, которой может проводить в жизнь конкуренцию.[12] Более того, либерализация важна, но не достаточна для продвижения широкомасштабного применения систем ИТ и развития э-коммерции. Исследования национальных систем по инновациям и распространению показывают, что инновации и широкое распространение необходимо больше, чем свободная рыночная система; и в этом правительство и другие институты также играют важную роль.

Также важно устранение ненужных юридических барьеров для развертывания нового бизнеса. Предприниматели онлайн и оффлайн должны иметь возможность оформить бизнес и начать работу без больших препятствий в виде обязательного лицензирования. Государственные регуляторы – плохие судьи в отношении того, что будет иметь успех на рынке, а что не будет. Регулирование полезно с точки зрения защиты интересов потребителей, но слишком часто регулятивные требования, оставшиеся со времен командной и подконтрольной экономики, не защищают интересы потребителей или инвесторов, а просто увеличивают стоимость процедуры, предписанной для начала нового бизнеса. Выбор оптимальных налагаемых регулятивных расходов особенно важен для э-коммерции, где скорость, инновации и гибкость часто являются ключевыми детерминантами успешности на рынке.

Чрезвычайно важны также законы по банковской системе. Люди, у которых нет кредитных карточек или доступа к иным средствам безналичного платежа не могут участвовать в э-коммерции. Правила ограничивающие ответственность владельцев карточек или счетов в случае мошенничества вносят свой вклад в увеличение доверия как онлайн так и оффлайн. Во многих развивающихся странах, необходимо бороться с мошенничеством с кредитками при помощи эффективного применения законов. Торговые кредитные счета недоступны предпринимателям во многих развивающихся странах, большей частью из-за множества афер с кредитками, которые совершают пользователи в этих странах.

В смысле доверия, другой важной проблемой является возмещение. Здесь должны быть эффективные средства, обеспечивающие исполнение контрактов любого вида. В большинстве правовых систем, это зависит от системы отправления правосудия,

---

[11] ОЭСР, Понимание цифрового неравенства (2000), стр. 9 («Либерализация телекоммуникационных услуг является чрезвычайно важной для увеличения доступа к линиям связи (фиксированная и мобильная), альтернативных технологий доступа, уменьшения цен, доступа к и использования Интернета.»); Создание динамики развития: заключительный отчет Инициативы по цифровым возможностям (июль 2001), стр. 35; Скотт Уоллстен, Регулирование и использование Интернета в развивающихся странах, AEI-Brookings Joint Center For Regulatory Studies, Related Publication 03-8 (May 2003).

[12] «Либерализация» или «дерегулирование» телекомов относится к приватизации и конкуренции, это не означает упразднение регулирования. Наоборот, дрегулирование телекомов включает применение правил конкурентной борьбы. По «дерегулированию», телекомы регулируются не как часть госистемы а как частные предприятия. Дерегулирование означает смещение фокуса регулирования. с приватизацией и ее неотъемлемой частью конкуренцией, регулирование цен теряет необходимость, и даже нежелательно, но должна применяться практика взаимосвязи и недискриминационного подхода.

которая должна быть независимой и свободной от коррупции и которая должна функционировать без задержек. Даже традиционная рукописная подпись на бумажном контракте будет ненадежной, если контракт может быть не исполнен, когда кто-то знает, что попытки принудительно исполнить его через суд затянуться на годы. Тоже самое, основные элементы защиты прав потребителей проистекают не из законов о подписях, а из процедур возмещения. Те же принципы защиты прав потребителей, которые необходимы для оффлайн, также относятся и к онлайн миру. Например, потребители не купят что-то через Интернет, пока они не будут уверены, что они смогут получить свои деньги назад, в случае, если товар им не доставят.

В заключение, общее наблюдение: можно более эффективно стимулировать э-коммерцию, если устранять формалистические юридические требования, а не переносить их в цифровой контекст. (То же самое справедливо и для э-правительства). Тем не менее, некоторые законодательные проекты по э-подписи в развивающихся странах и странах с переходной экономикой устанавливают правила для онлайн сделок, которые даже жестче, чем те которые применяются к оффлайн сделкам. Страны совершающие переход к рыночной экономике должны использовать появление э-комерции для того, чтобы в целом пересмотреть формалистические юридические требования, которые применяются к коммерции как оффлайн так и онлайн. Многие развитые страны, где процветает э-коммерция, еще до появления Интернета, устранили некоторые формалистические требования к контрактам и иным юридическим сделкам. (Например, в США уже более века, юридическое требование о «подписи» на контракте не требует рукописной подписи.[13]). Развивающиеся страны, которые хотят воспользоваться преимуществами информационной экономики, могли бы пересмотреть старые правила и посмотреть может быть их можно убрать либо упростить в оффлайн контексте, вместо того чтобы просто пытаться найти для них онлайн эквивалент. Это согласуется с принципом нейтральности сделки: насколько это возможно, сделки в бумажной и электронной форме должны рассматриваться одинаково.

В этом контексте, кто-то может поднять вопрос о необходимости существования и о содержании законодательства по э-подписи. Законодательство по э-подписи может играть особую роль в развивающихся странах, где судебная система не может справиться с новыми вопросами и где другие средства осуществления онлайн сделок, такие как законы о кредитных карточках, отсутствуют. Однако, к процессу принятия законодательства по э-подписи нужно приступать только после проведения полной оценки действующего законодательства – определить на какие вопросы оно отвечает а на какие нет – и четкое понимание того какие функции, как предполагается, будет выполнять э-подпись.

И вместо того, чтобы вводить сложную систему признания цифровых подписей основанных на криптографии, возможно, развивающимся странам лучше послужит инкрементный подход, описанный ниже.

(Примечание переводчика: «инкрементный» - постепенно разрастающийся, расширяющийся)

ДОСТОИНСТВА И ОГРАНИЧЕНИЯ МЕЖДУНАРОДНЫХ МОДЕЛЕЙ

Как было сказано выше, юридические и технические вопросы, поставленные э-коммерцией и э-правительством, возникают на нескольких уровнях. На простой вопрос о том может ли быть признано, что электронное сообщение не имеет юридической силы как «письменное» сообщение, можно ответить просто. Отдельный вопрос о том, какие электронные техники будут приниматься в качестве юридического эквивалента рукописной подписи, ставит более сложные вопросы, которые в какой-то степени

[13] То же самое верно и для Англии. Николас Бом, Нужен ли нам новый закон по цифровой подписи? http://www.fipr.org/publications/newsig.html

зависят от требований определенной правовой системы (наиболее примечательна, разница между системами общего права и римского прав). Наиболее сложный вопрос в э-комерции ил э-правительстве как с юридической, так и с технической точки зрения – это как человек может удостоверить свою личность онлайн.

Пытаясь найти ответы на некоторые из этих вопросов, в том числе наиболее сложный вопрос о том, как незнакомые люди достоверно могут установить личность онлайн, международные юристы-эксперты и юридические организации разработали модельные законы. Один из них – Модельный закон по электронной коммерции, разработанный в 1996г. Комиссией ООН по международному торговому законодательству (ЮНСИТРАЛ). В нем рекомендуется, чтобы в формулировках законов было четко определено, что какой-либо документ не может быть признан не имеющим юридической силы «в письменной форме» или «оригинала» только на том основании, что он в электронной форме. В нем также разграничены стадии заключения электронного контракта, и рассматриваются такие понятия как оферта и акцепт в электронном контексте. ЮНСИТРАЛ также издал отдельный модельный закон, в котором рассматривается более сложный вопрос о том, какая электронная функция может удовлетворять юридическому требованию к подписи: Модельный закон ЮНСИТРАЛ об электронной подписи от 2001г («ЮНСИТРАЛ Модель по Э-подписи»). В том же направлении, в 1999 г Европейский Союз принял директиву, в которой рассматривается вопрос «общественной среды» для электронных подписей («Директива Евросоюза по э-подписи»).[14]

Эти модели основываются на нескольких принципах одинаковой релевантности как для более развитых стран, так и для развивающихся и переходных стран. Первое, они отражают исходное условие, что э-коммерция будет процветать наилучшим образом, если частному сектору разрешат разрабатывать решения, продиктованные конкуренцией и рыночным выбором. Соответственно, международные модели осуждают любую интервенцию государства, которая может ограничить развитие рынка услуг электронной подписи. В частности, в этих модельных документах осуждается система, по которой организации, предоставляющие услуги э-подписи для э-коммерции, обязаны сначала получить от государства лицензию. Директива ЕС специально запрещает государствам-членам применять обязательное лицензирование. Во-вторых, в модельных законах подчеркивается принцип «технологической нейтральности» - что национальные законы об э-подписи не должны признавать эксклюзивно какую-либо отдельную технологию для создания э-подписи.[15]

Однако, по ряду причин, абсолютно ясно, что смысл, заложенный в этих международных моделях, был неправильно истолкован в развивающихся странах и странах с переходной экономикой. Во многих развивающихся и переходных странах уже приняты или предлагаются законы по э-подписи, слишком регулятивные, отвергающие гибкость потенциальной организации, которая необходима для э-комерции.[16] Отчасти, это возможно из-за того, что на международные модели

[14] Модельный закон по э-коммерции ЮНСИТРАЛ (1996), 16 дек. 1996, http://www.uncitral.org/en-index.htm Модельный закон по э-подписи ЮНСИТРАЛ (2001), 5 июля. 2001 http://www.uncitral.org/en-index.htm; Директива Европарламента 1999\93\ЕС о Рамках сообщества для э-подписей, http://europa.eu.int/ISPO/ecommerce/legal/digital.html

[15] Например, в Директиве ЕС «электронная подпись» определена без отсылки к какой-либо определенной технологии. Она включает недискриминционную статью (Ст.5 п. 2) и общую формулировку подчеркивающую важность открытого подхода с учетом «быстрого развития технологий и глобального характера Интернета».

[16] Например, Российский закон по э-подписи, который вступил в силу в январе 2002, устанавливает шифрование как единственный метод посредством которого, в соответствии с российским законодательством, может быть создана электронная цифровая подпись имеющая юридическую силу. При разработке этого законопроекта были преднамеренно опущены иные аналоги личной подписи и

оказывает влияние неоправданная, крикливая реклама вокруг э-подписи. К тому же, это может иметь место из-за того, что их технологическая нейтральность не позволяет обеспечить адекватной достоверности в развивающихся странах, поэтому эти страны переходят к более регулятивной системе. Международные модели оставляют много вопросов, которые должны разрешаться либо судебными, либо регулятивными органами, либо саморегулируемыми отраслевыми органами, которые будут устанавливать стандарты. Хотя во многих развивающихся странах нет судебной системы, способной практически и юридически давать толкование какого-либо общего закона для каждого конкретного случая, и нет компетентных саморегулирующих и регулятивных институтов. Возможно, частью проблемы является неправильное руководство со стороны донорских организаций или международных консультантов. А также во всем мире у политиков есть склонность хватать то, что лежит под рукой: а это модельный закон по э-подписи, а не о либерализации телекома или законы о защите прав потребителей или кредитных картах, поэтому политики и начинают с э-подписей.

Но возможно самая важная причина, почему модельный закон об э-подписи ЮНСИТРАЛ и директива ЕС могут вводить в заблуждение развивающиеся страны заключается в том, что, хотя они позволяют использовать любую технологию для э-подписи, они в то же время обращают особое внимание на технологию, которая может разрешить самый трудный вопрос в э-комерции – вступление в сделку двух сторон, которые являются незнакомыми друг для друга. В них прописаны процедуры для наиболее надежной формы э-подписи, в том числе создание провайдеров сертификационных услуг, которые ручаются за данные по созданию подписи физического или юридического лица, так что данные по созданию подписи могут быть привязаны исключительно к данному лицу и никому другому. Однако, проблема электронной сделки между незнакомыми лицами, не может быть решена законодательной санкцией; препятствия в основном технологические и экономические. Более важно, в настоящее время, как показывает практика, что большинство э-сделок совершаются не между незнакомыми лицами, которые впервые встретились онлайн, но больше между торговыми партнерами которые сначала установили отношения традиционным способом, при личном общении.[17] Таким образом, значительная часть э-комерции может осуществляться, никогда не обращаясь к разрешению проблемы сделок между прежде незнакомыми лицами. Для развивающихся стран – это неправильная отправная точка в построении правовой среды для э-комерции и развития ИКТ.

РЕАЛИСТИЧНЫЙ ПОДХОД К Э-КОММЕРЦИИ

исключено использование иных технологий для создания электронной цифровой подписи. Baker & MacKenzie, Legal Alert - Electronic Digital Signature Law, January 14, 2002, http://www.bmck.com/ecommerce/Russia-E-Signature-Alert.doc. Аргентинский закон предусматривает создание Федеральной Инфраструктуры по Цифровой Подписи состоящей из Уполномоченного лица по подаче заявок, который будет главой кабинета и будет диктовать нормативные и нотификационные акты в соответствии с законодательством : Консультативная Комиссия по Инфраструктуре Открытых Ключей, расположенная у главы кабинета, которая должна давать рекомендации по техническим аспектам Инфраструктуры Цифровой Подписи; Институт Администратора Цифровой Подписи, ответственный за лицензирование сертификационных органов и контроль за их деятельностью; Лицензированные Сертификационные органы, которые выдают сертификаты и предоставляют иные услуги связанные с цифровыми подписями; и Регистрационные органы, организации ответственные за удостоверение идентификации и иной информации относительно держателя сертификата, полномочия которых делегируются им лицензированными сертификационными органами. См. http://www.pki.gov.ar/English/index.html.

[17] «Наш общий вывод заключается в том, что основной эффект от Б-Б э-комерции – это увеличивать отношения между существующими торговыми партнерами». Джон Хамфри, и др., Реалии э-коммерции с развивающимися странами.

Из моделей ЮНСИТРАЛ и ЕС можно выбрать наиболее реалистичный подход, но с несколько другими акцентами. Первое и самое главное, реалистическая правовая база поставила бы во главу угла принцип «автономности стороны», также известный как «деловой выбор» или «свобода контракта». Этот принцип заключается в том, что законом по э-подписи должно разрешаться компаниям и частным лицам, участвующим в э-комерции, достигать договоренности традиционными средствами по их собственной методике заключения электронных контрактов. Так, например, если компания создает онлайн систему закупки для своих поставщиков, она рассматривает как подходящую одну из форм опознавания\удостоверения личности – будет ли это просто идентификационный номер или же криптографическая технология – закон и суды должны обеспечивать соблюдение соглашений, достигнутых внутри этой системы, независимо от того отвечает или нет эта технология специальным техническим стандартам.

Во-вторых, поскольку цель э-комерции лучше достигается через создание среды для конкуренции на рынке, и следует избегать применение государственного лицензирования для э-комерции, как барьера для инноваций, то вероятно э-правительство следует рассматривать отдельно. Для правительства полностью подходит и возможно даже необходимо создание стандартов идентификационной технологии, которая будет использоваться для осуществления сделок с правительством. Для правительства также хорошо было бы создать свою собственную систему э-подписи, и сделать необходимую технологию (или контракт с частной компанией на создание таковой). Но это тоже обычно включает личный контакт, или традиционные средства связи, - создание базы для последующих онлайн операций, устранение необходимости сложных разработок инфраструктуры публичного ключа.

Двух этих элементов по отдельности – бизнес выбор для э-комерции и требования правительства для э-правительства - должно быть достаточно, чтобы охватить довольно большую часть ситуаций, когда э-подписи могут быть полезны в развивающихся странах. Третья категория ситуаций – сделки между незнакомыми лицами – вероятно лучше всего разрешать через принятие законов, регулирующих кредитные карты, дебетовые карты и схемы предоплаты или «кибер-деньги», где самые важные удостоверяющие функции осуществляются в основном между продавцом и компанией, выдавшей кредитную или дебетовую карту или предоставляющую услуги кибер-денег, а не между продавцом и покупателем.

Первый шаг – признание электронных документов как «письменных» и другие правила обмена электронными сообщениями .

Во многих странах закон требует, чтобы контракты или иные документы были в письменной форме и\или подписаны. Другие законы требуют, чтобы сохранялось наличие регистрации. Нормы в отношении доказательств или иные юридические требования могут ссылаться на «оригинал» документа. Возникают вопросы – могут ли электронные документы удовлетворять этим требованиям. В некоторой степени эти проблемы преувеличены, поскольку большинство правовых систем уже справились с телеграммами, телексами и факсами. Но чтобы устранить эти сомнения, в целом, имеет смысл для страны принять какой-то закон, который предусматривает, по крайней мере, что «подпись, контракт либо иной документ не может быть признан не имеющим юридической силы, недействительным или необеспеченным правовой санкцией, только на том основании, что он в электронной форме».[18] В модельном законе ЮНСИТРАЛ по

[18] Это формулировка из законодательства США, Акт по э-подписи в глобальной и национальной коммерции, статья 101(а). Схожая формулировка дается в Директиве ЕС по э-подписи, статья 5.2 которой гласит: «государства участники должны гарантировать что электронная подпись не будет признана не

э-комерции это детально прописано в статьях с 5 по 10. В этом законе не говорится, что любой электронный документ всегда обладает обязательственной силой или что любая электронная подпись всегда действительна. В нем просто говорится, что документ или подпись не могут быть признаны не имеющими юридической силы только на том основании, что он или она в электронной форме. В модельном законе ЮНСИТРАЛ по э-комерции есть также полезные формулировки получения и подтверждения, а также другие правила заключения договоров посредством обмена электронными сообщениями. Для любой страны было бы благоразумно принять эти положения.[19] Они не влекут никакого регулятивного обременения для участников э-комерции.

Второй шаг – принятие бизнес выбора в сделках, основанных на предварительной договоренности достигнутой традиционными средствами.

Более трудный вопрос – какая технология в обмене электронными сообщениями должна соответствовать презумпции достоверности, которая традиционно ассоциируется с рукописной подписью, написанной чернилами на бумажном документе. Но в большом проценте сделок, на этот вопрос можно ответить, придав юридическое признание выбору идентификации и достоверности, который стороны сделали сами. Это принцип «бизнес выбора», «автономности стороны» или «свобода контракта». Это гораздо более важно на практике, чем это может показаться при изучении международных моделей по э-подписи.

Получается так, что в контексте бизнес-бизнесу (Б-Б), проблема доверия между незнакомыми лицами в исключительно онлайн среде возникает редко, поскольку большинство Б-Б коммерсантов не являются друг для друга незнакомыми лицами.[20] Большинство Б-Б коммерсантов, даже в век Интернета, полагаются на личные контакты или иные традиционные средства: проверка кредиток и предыстории (дью дилидженс), чтобы удостовериться в подлинности личности и компетенции партнера.[21] Только после того как личность и доверие были установлены традиционными способами, онлайн сделка осуществляется. Такая онлайн сделка может повлечь, а может, и нет, использование э-подписи созданной на основе криптографии.

имеющей юридической силы и допустимости в качестве доказательства в судебных разбирательствах, только на том основании что ……. она в электронной форме.» Директтва ЕС по э-комерции гласит: «государства участники должны гарантировать что их правовые системы позволяют чтобы контракты заключались посредством электронных средств. В частности, государства участники должны гарантировать что юридические требования к процедурам совершения договоров ни создают препятствий для использования электронных контрактов, ни являются причиной в результате которой такие контракты не будут иметь юридической силы на основании того что они были заключены посредством электронных средств».

[19] См. рекомендации находящегося в Англии Фонда Исследования Информационной Политики (FIPR), http://www.fipr.org/publications/sigdirecon.html.

[20] Руководство по применению модельного закона ЮНСИТРАЛ по е-подписи признает это, устанавливающее в пар. 111 что, «на практике, решения юридических проблем, вытекающих из использования современных средств коммуникации, в основном разрешаются в самом контракте».

[21] Хампфри и его коллеги обнаружили что личные запросы предшествуют э-коммерции. Например, в сельскохозяйственных цепочках поставок, крупные розничные торговцы не заказывают продукцию без проведения обширной проверки помещений поставщика. Джон Хампфри и др., The Reality of E-Commerce with Developing Countries, supra, at p. 27. ранее , стр. 27. как только отношения установлены традиционными способами, компании полностью полагаются на Интернет, поскольку так снижаются их издержки на коммуникацию. 95% исследованных компаний из сектора торговли одеждой, использовали э-почту для размещения и принятия заказов с существующими торговыми партнерами. Многие респонденты этого исследования отмечали, что отношения, основанные на Интернете, не могут заменить личных контактов.

Примером этого может быть онлайн система закупок, которую компания создает для своих поставщиков.[22] Используя традиционные средства, компания выясняет информацию относительно стабильности и профессионализма предполагаемого поставщика. Если компетентность и надежность партнера устраивает компанию, она заключает соглашение с поставщиком традиционным способом (например, контракт с рукописной подписью отправляется по почте или по факсу). Помимо этого стороны определяют средства, которые будут использоваться, чтобы идентифицировать тех поставщиков, которые уполномочены использовать онлайн систему. Компания, использующая такую систему поставок, передаст своим отобранным поставщикам некий идентификатор – это может быть просто пароль и идентификационный номер или криптографическую технологию. В этой ситуации, нет необходимости в государственном регулировании при заключении онлайн соглашений – частная система может быть создана любым способом, который выберет ее владелец. И соглашения с поставщиками, которым предоставлен доступ в эту систему, должны быть обеспечены правовой санкцией в полной мере.

Признавая что, так осуществляется набольший объем Б-Б э-комерции, в законе по э-комерции или э-подписи должно быть четко обозначено, что контракты, заключенные между сторонами, у которых взаимоотношения именно такого рода, являются юридически обязывающими, даже если они в электронной форме. А «подпись», в каком бы виде стороны не договорились, что она будет (в том числе, просто напечатанное имя или введенный идентификационный номер), должна приниматься как юридически действительная «подпись».

Принцип бизнес-выбора не ограничивается сделками Б-Б. Некоторые сделки бизнес-покупатель (Б-П) основаны на такой же модели. В общем, банковские онлайн услуги доступны покупателям, у кого есть оффлайн счет. Банк и клиент уже удостоверили личности друг друга в той мере, в которой это необходимо для традиционных способов, а также заключили договор с рукописными подписями, поставленными лично в банковском офисе или посредством обмена документами по почте. Даже так называемые «виртуальные банки, у которых нет офисных помещений, не откроют онлайн счет, пока подписанный на бумаге договор, не будет направлен по почте или по факсу в систему банковских онлайн услуг.[23] Поэтому, все онлайн операции между банком и клиентом с использованием системы, которую создал банк и на которую согласился клиент, должны быть признаны юридически обзывающими.

И модельный закон об э-подписи ЮНСИТРАЛ и Директива ЕС включают принцип бизнес-выбора – но он изложен опосредовано или скрыто. В модели ЮНСИТРАЛ говорится, что « Положения настоящего закона могут частично отменяться, либо их действие может варьироваться соглашением, если таковое соглашение имеет юридическую силу в соответствии с действующим законодательством.». Преамбула к директиве ЕС гласит, что «регулятивная база не нужна для электронных подписей, используемых исключительно внутри систем,

[22] «Некоторые виды Б-Б э-комерции, основанной на Интернете, сейчас развиваются, но это частные, эксклюзивные модели, там, где доступ ограничивается фирмами, которые уже интегрированы в цепочки поставки в своем секторе». John Humphrey, et al., The Reality of E-Commerce with Developing Countries, supra, p. 31.

[23] Например, один из лидирующих виртуальных банков в США, Первый Интернет Банк, у которого нет офисов или отделений где клиенты могли бы заключать сделки присутствуя лично, требует чтобы клиенты направляли поручения в бумажном виде по почте или факсу. http://www.firstib.com/apply/personal.html

которые созданы на основе добровольного соглашения по частному праву между определенным кругом участников; …юридическая сила электронных подписей используемых в таких системах и их допустимость в качестве доказательств в ходе судебных разбирательств должна признаваться». (параграф 16.). К сожалению, ни в одной из моделей не предлагаются рекомендуемые юридические формулировки для того, чтобы действительно придать юридическую силу выбору который делают стороны в своих онлайн операциях.

Это важно, что принцип бизнес-выбора применяется к Интернет системам. В некоторых законопроектах, разработанных в развивающихся странах, принцип бизнес-выбора признается только внутри «частных» систем или «корпоративных информационных систем», либо систем, которые не взаимодействуют с сетями общего пользования (СОП). Это слишком узко. Вид коммуникационных сетей не является самым важным определяющим фактором, поскольку многие «частные» или «корпоративные» системы взаимодействуют с СОП, либо даже функционируют внутри них. Значимое условие здесь - является ли эта система для осуществления сделок, ограниченной кругом лиц, обязанных исполнять правила этой системы в соответствии с контрактом, который они подписали традиционным способом.

Третий шаг – государственные стандарты идентификации для э-правительства

Есть одно исключение из принципа, о том, что правительство не должно регулировать технологии, используемые при онлайн идентификации, и это исключение находится в сфере э-правительства. Для стран, в которых обычно применяется жесткая система подтверждения личности для тех, кто осуществляет бизнес с правительством, приемлемо и даже желательно, чтобы правительство ввело стандарты идентификации для тех, кто желает прислать документы в правительство по электронной почте. Однако нет причин требовать, чтобы эти стандарты отвечали техническим стандартам, указанным в директиве ЕС по э-подписи. Правительство само должно решать на каком уровне достаточна идентификация для проведения операций между гражданами и правительством. Как и с применением в э-комерции, самым простым выходом было бы использовать традиционные личные контакты, для того чтобы первоначально установить личность, либо распространить электронные идентификаторы.[24]

Есть несколько способов как правительство может это сделать: правительство может создать свою собственную систему для онлайн идентификации, в которой оно выдает идентификатор (который может быть не более чем пароль). Либо правительство может выдать контракт какой-то частной компании, чтобы она делала это. Наиболее желательно было бы для правительства издать стандарты и утвердить всех частных провайдеров, кто соответствует этим стандартам. Это могло бы стимулировать, чтобы частные предприятия развивали услуги, которые могут использоваться и для э-коммерции. И если технология будет использоваться в частной коммерции, возможно более приемлемо, если правительство не будет контролировать компоненты этой системы.

[24] Например, Дания планирует ввести «государственный сертификат на электронные услуги» , но он не будет соответствовать требованиям директивы ЕС. Однако, по разумению датского правительства это обеспечит достаточную безопасность в большинстве сделок по э-правительству. Э-правительство: датский опыт. Пол Бернт Йенсен, старший советник, министерство науки, технологии и инноваций, Дания, http://www.oio.dk/index.php?o=705d5300e9beb7aa5bdc69ffa88e190a

Хорошую законодательную модель для такого применения э-правительства можно найти в нормативном акте, принятом в штате Иллинойс в США. Основное положение этого документа гласит следующее:

«Если какое-либо положение закона требует или разрешает подачу любой информации, уведомлений, требования или иного документа в государственный орган штата, подача документа, исполненная в электронной форме, должна иметь ту же силу что и подача документа в бумажной форме во всех случаях, когда этот госорган разрешает или согласен на такую подачу в электронной форме, и что такая подача исполнена в соответствии с применяемыми нормами и соглашением.»

***

«Каждый государственный орган имеет право издавать, или заключать контракт на издание, сертификатов для (а) своих сотрудников и агентов и (б) лицам, осуществляющим бизнес или иные сделки с таким государственным органом и предпринимать иные действия связанные с этим, включая создание архивов, а также приостановка и отзыв выданных сертификатов, при условии, что вышеназванное совершено в соответствии со всеми нормами, процедурами и документами установленными Департаментом центральных менеджерских услуг. Департамент центральных менеджерских услуг должен иметь полномочия устанавливать нормы, процедуры и документы, посредством чего государственный орган может выдавать или заключать контракт на выдачу сертификатов.»

Вероятно, это стоящая идея отклонить предложение о том, что должна быть единая система для э-комерции и э-правительства. Есть много преимуществ в создании системы идентификации для правительства отдельной от идентификационной системы для э-комерции. Защита частной информации и безопасность могут быть улучшены, если частные лица и организации будут иметь несколько форм онлайн идентификации, каждый из которых идентифицирует пользователя в разных сферах осуществления операций. Это аналогично тому как имея связку из множества ключей для разных замков, или кошелек с разными кредитками, водительскими правами и паспортом, например, каждый из которых принадлежит одному и тому же человеку, но выполняет функции каждый в своей сфере.

Сделки с незнакомыми лицами

Расширение принципа бизнес-выбора – опять же комбинация традиционных методов с онлайн сделками – служат, для того, чтобы развивать сделки э-комерции между незнакомыми лицами. Продажа книг через Amazon.com может быть примером этому. В этом контексте, поставщик по э-комерции может потребовать от покупателя не больше чем имя, адрес и номер кредитной карточки, чтобы идентифицировать покупателя. Доверие, которое позволяет этому осуществиться, обеспечивается группой договорных отношений, в которые вступают традиционными способами, и законом о кредитных карточках, который определяет ответственность и защиту для всех сторон. Если и продавец, и покупатель не знакомы друг с другом, у обоих из них, и у покупателя и у продавца есть четко определенные взаимоотношения с банком, который выдавал кредитку покупателю – договорные отношения, которые чаще всего устанавливаются традиционными способами с помощью традиционной подписи на контракте. Перед тем как акцептовать сделку, онлайн продавец проверит в банке не была ли эта кредитка украдена, а также могут быть предприняты расследования против мошенничества (попросить адрес для счетов (чтобы гарантировать что он совпадает с адресом, указанным в документе) или номер кода на обратной стороне карточки (чтобы гарантировать, что у пользователя физически есть эта карточка)). Эти меры дают продавцу некоторую уверенность в том, что банк оплатит эту сделку. То же самое, банк,

выдавший кредитку, имеет договорные отношения с покупателем, также заключенные традиционным способом, дающие эмитенту этой кредитной карточки права в отношении покупателя, в том числе право собирать на кредитке счета владельца. И покупатель знает, что если продавец не предоставит ему запрашиваемый товар или услугу, покупатель получит свои деньги назад от банка, а банк имеет право получить свои деньги назад от продавца.

Смысл здесь вот в чем: доверие в отношениях не исходит из электронной подписи – оно проистекает из системы юридических норм (норм применяемых также и в оффлайн мире), которые определяют правоотношения между эмитентами кредитных карточек, владельцами кредитных карточек и поставщиками. (То же самое верно и для правовой системы дебитовых карточек или э-платежей). Мошенничество является проблемой для этой системы, и основные ее участники в поисках лучших способов идентификации. Но даже в развивающихся странах криптографическая идентификация не принята для большинства сделок «незнакомых» лиц, и, тем не менее, в некоторых из них э-комерция процветает.

Конечно, во многих развивающихся странах еще нет схем регулирования для кредитных карточек, дебитовых карточек или иных схожих платежных схем. И даже если правовая база существует, проблема мошенничества создает серьезные препятствия в некоторых развивающихся странах для повсеместного использования кредитных карточек. Онлайн сделки Б-П могут быть недоступны для этих стран. Тем не менее, принятие законов, позволяющих использовать кредитки онлайн или иные виды э-платежей – и создание системы правоприменения, которая будет эффективно бороться с мошенничеством с тем, чтобы финансовые институты принимали риск акцептования сделок с кредитками из развивающейся страны – это шаги которые скорее всего будут более эффективны для удовлетворения требований э-комерции о надежности и доверии, чем было бы принятие закона по э-подписи. Э-подпись может быть составной частью системы для создания доверия в системах кредитных карточек или э-платежей. Но и в этом случае принцип бизнес-выбора опять же может быть применен: где эмитент кредитных карт или провайдер услуг э-платежей будет определять, какую идентификационную технологию использовать, а эмитент кредиток будет заключать контракты со своими клиентами и продавцами традиционными средствами которые устанавливают правила акцепта э-подписи. Закон должен обеспечивать осуществление сделок в соответствии с принципом бизнес-выбора, который регулируется правовыми нормами, которые распределяют риски, связанные с мошенничеством, между эмитентами кредиток (или провайдерами услуг э-пплатежей), покупателями, и поставщиками, и которые также регулируются нормами по защите прав потребителей.[25]

Чисто электронные отношения – конфликт меду достоверностью и технологической нейтральностью

Два принципа описанные выше – бизнес-выбора и стандартов э-правительства – обеспечивают адекватную базу для широкого применения э-комерции и э-правительства. Если страна решит идти дальше и законодательно утвердить стандарты для акцептования э-подписей в отсутствие бизнес-выбора, то она должна очень аккуратно соблюдать баланс между целью достоверности и принципом технологической

[25] Во имя бизнсс-выбора, компаниям не должно быть позволено пренебрегать правилами защиты прав потребителей. Как говорилось выше, развивающимся странам стремящимся поддержать развитие потребительскую э-коммерцию, необходимо принять законы по защите прав потребителей защищающих потребителей при кредитных операциях. В закон по э-подписи которым признается Б-П выбор, должно быть включено положение запрещающее игнорирование защиту прав потребителей.

нейтральности. Создание жесткой бюрократической системы может в действительности задушить развитие рынка.

С одной стороны необходимость достоверности толкает политиков на создание регулятивной системы, которая применяет определенные технологии, что на практике означает применение версии цифровой подписи, которая основана на том, что известно под названием Инфраструктура Открытого Ключа (ИОК).[26] На данный момент, ИОК хотя и не очень широко применяется, но общедоступен, и предлагает самую высокую гарантию идентификации, признания, целостности и конфиденциальности. Тем не менее эволюция технологий электронной и цифровой подписи продолжается. Признавая это , международные модели учитывают принцип «технологической нейтральности» и дают четкое понятие того, что ни одна технология не должна становиться единственным средством создания подписей, имеющих юридическую силу.

В странах с зарождающимся и переходным рынком, абсолютная технологическая нейтральность может ввести в заблуждение. Если правовая система не в состоянии заранее определить те определенные технологии, которые точно будут акцептованы, то вопрос останется на рассмотрение судами в каждом конкретном случае. И потенциальные участники рынка не будут иметь уверенности, которую они хотели бы иметь, перед тем как они заключают онлайн сделку. Пытаясь разрешить этот конфликт, модели и ЮНСИТРАЛ и ЕС директива признают, что регулятивная или саморегулируемая система могла бы отдать приоритет ИОК технологии. ЕС директива предусматривает двухуровневый подход. Она определяет что «современная» электронная подпись будет автоматически признаваться, если она основана на соответствующем сертификате и создана «устройством по созданию защищенной подписи» (Статья 5, п. 1). Хотя и другие технологии могут подходить под критерии ЮНСИТРАЛ и ЕС, нет сомнений, что их писали, имея ввиду именно технологию ИОК.

Поэтому для развивающихся стран не будет неправильным избрать направление политики по разработке системы (либо законодательных стандартов, либо регулятивного определения), которая дает презумпцию юридического признания электронных подписей, созданных на основе ИОК технологий. Однако даже развивающиеся страны должны избегать норм, которые делают ИОК единственным средством создания э-подписей. Законодательно или регулятивно установленное принятие ИОК и только ИОК, будет препятствовать принятию других технологий и тем самым замедлит рост э-комерции. Любые правовые нормы, которые стремятся создать базу для электронной подписи в э-комерции вне сферы бизнес-выбора, должны четко признавать возможные изменения технологий. Статья 6, п.4 модели ЮНСИТРАЛ гласит, что создание законодательно установленных критериев для технологии подписи, которые предполагаются как надежные, не ограничивает возможности для любого лица устанавливать надежность электронной подписи иным способом.[27]

---

[26] Описание ИОК можно найти в Руководстве по применению модельного закона ЮНСИТРАЛ по э-подписи.

[27] В Сингапуре создали двух-уровневую систему. По законодательству Сингапура, цифровые подписи созданные по сертификатам выданным лицензированным сертификационным агентством пользуются преимуществом презумпции доказательства. Без такой презумпции, сторона, которая собирается основывать свои доводы на цифровой подписи, должна предоставить достаточные доказательства, чтобы убедить суд что эта подпись была создана в соответствии с условиями которые делают ее достойной доверия. Имея эту презумпцию, сторона опирающаяся на подпись, просто должна показать что эта подпись была правильна удостоверена, и тогда бремя доказывания возлагается на противную сторону утверждающую обратное. Очень четкое описание сингапурского закона есть на http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/3d122fbf7d5ac170c82568390001fb31?OpenDocument.

Развивающиеся страны имеют понятную заинтересованность в создании общественного доверия бизнесу, который занимается предоставлением услуг э-подписи, таких как сертификаты для подписей, созданных на основе ИОК. Схема государственного лицензирования - один путь обеспечить это доверие, особенно если стандарты внутри индустрии и судебные решения по отдельным делам не являются жизнеспособной альтернативой. Но система лицензирования подвержена таким явлениям как проволочки и фаворитизм. Обязательное государственное лицензирование может помешать развитию конкурентного рынка, если регулятивные требования или бюрократические проволочки будут создавать барьеры для выхода на рынок.

Директива ЕС, использующая двухуровневый подход, дает более обширную презумпцию юридической силы сертификата, выданного провайдером, аккредитованным в соответствии с требованиями Директивы. Эта схема, конечно, не является обязательной. Аккредитация, выданная какой-то признанной в этой индустрии группой, поможет легче подтвердить юридическую силу контракта или допустимость документа, но сторона, которая полагается на нелицензированного провайдера может, тем не менее, доказывать, что документ отвечает стандартам установленным в приложении к Директиве. Такой вариант может стать приемлемой моделью для стран с развивающейся экономикой.

Если в странах с развивающимся рынком выберут все же обязательное государственное лицензирование провайдеров услуг э-подписи для э-комерции, регулятивные требования должны быть прозрачными, ограничиваться требованиями необходимыми для защиты общества, и гармонизированы внутри региона с соответствующей ссылкой на международные стандарты. Местные и иностранные компании, а также группы по международным стандартам могут дать направляющую линию и должны стать активными участниками при разработке этих требований.

Ключевой принцип вот такой: любая схема лицензирования должна признавать принцип бизнес-выбора. Если стороны договорились с помощью традиционных средств, что они заключат электронный контракт, не прибегая к услугам лицензированного провайдера, закон должен признавать и обеспечивать правовой санкцией такие контракты.

Однако, даже подпись, созданная по технологии от лицензированного провайдера, имеет право только на опровержимую презумпцию юридической силы. Не имеет значения, на чем страна остановит свой выбор из разнообразия от законодательно утвержденных стандартов до государственного лицензирования, одна из сторон всегда может пытаться доказать, что цифровая подпись не была выполнена надлежащим образом.

Лицензирование отличается от прямого участия правительства в процессе э-подписи. Обе международные модели ясно выступают против участия правительства в выдаче, регистрации, хранении или подтверждении компонентов подписи. Однако некоторые развивающиеся страны отдали прямое, функциональное управление госоргану. Например, Статья 10 закона РФ: исполнительному органу отдается полномочие – получать и удостоверять сертификат до того как пользователь сможет полагаться на этот сертификат, и вести единый реестр удостоверенных сертификатов. Это почти гарантированно приведет к обратным результатам. Бюрократические процедуры могут стать источником ненужных проволочек. Второе, и возможно более важное, доступ правительства к информации о подписях вызывает сомнения в безопасности и защите частной информации, что отрицательно скажется на использовании э-подписей. Негативный эффект от такого подхода может быть смягчен только тем фактом, что люди не будут это использовать.

ЗАКЛЮЧЕНИЕ

В этой статье я попытался рассмотреть вопрос электронной подписи в его истинном контексте, подчеркнув более широкие правовые реформы, которые должны стать приоритетным объектом внимания в странах с развивающейся и переходной экономикой, если они хотят стимулировать рост ИКТ, а также описать реальную и все увеличивающуюся базу для основных элементов законодательства, признающего электронные документы и электронную подпись.

По многим причинам, веским и не очень, правительства отдают приоритет принятию законов об электронной подписи. Я убежден, что данная приоритетность не оправдана. Я попытался включить в контекст те самые истинные вопросы достоверности, доверия и авторизации онлайн, на которые иногда ссылаются, оправдывая принятие законов по э-подписи. Я утверждаю, что есть иные правовые и институциональные реформы, которые намного более приоритетны. Я также утверждаю, что со специальной ссылкой на акцептование электронных документов и признание электронных контрактов, даже относительно умеренные правовые реформы достигнут целей по стимулированию э-комерции и э-правительства.

Попытки развития э-комерции и э-правительства посредством реформирования законодательства относительно юридического признания документов и подписей должны начинаться с оценки того, что необходимо изменить и почему.[28] Законы, предназначенные для развития э-комерции не должны налагать на э-коммерцию бремя большее чем то, которое уже существует в мире бумажных документов. Оценка правовой среды должна ставить вопрос о том, какие конкретно существуют юридические препятствия для э-комерции. Рекомендуется, чтобы развивающиеся страны не выбирали в качестве моделей контракты между незнакомыми друг с другом лицами. Наоборот, развивающиеся страны должны обеспечить поддержку онлайн контрактам между уже состоявшимся торговыми партнерами. В сфере э-комерции есть важные вопросы доверия, которые не могут быть разрешены посредством законодательства. Фактически, подход чрезмерного регулирования законодательства может скорее задушить э-коммерцию, вместо того чтобы стимулировать ее. Лучше всего э-коммерцию будет стимулировать устранение барьеров, а не создание новых.

На основе международных моделей, возможно обрисовать в общих чертах закон об электронном документе для развивающихся стран. Во-первых, когда действующее законодательство требует письменной формы, оригинал, или подпись, должно быть четко определено, что какой-либо документ не может быть признан не имеющим юридической силы только на том основании, что он в электронной форме. Во-вторых, самой логичной реформой, которую можно провести в законодательстве страны для развития законодательства по э-комерции, возможно будет в том, чтобы придать полную юридическую силу контрактам, заключенным в электронной форме между любыми лицами, которые предварительно договорились посредством традиционных средств, заключить сделку в электронной форме, независимо от вида технологии, которую они оговорили для идентификации друг друга в онлайн контексте.

Глобальным компаниям необходима система э-подписей, которой они могут доверять в глобальных масштабах. Обычно, наиболее быстрый способ добиться глобального единообразия – посредством системы контрактов, которые заключаются

[28] « Спускаемые сверху распоряжения правительства развивающие «э-готовность» не будут иметь успеха, пока не будут предприняты большие меры для изучения того как действительно используются интернет-приложения ….. . политики ….. должны поддерживать подход «снизу вверх», который основан на реалистичных оценках возможностей и препятствий в Б-Б э-коммерции…. .» Хапмфри и др. The Reality of E-Commerce with Developing Countries, supra, p. ii.

традиционным способом. Если какая-то развивающаяся страна принимает какой-либо закон, и есть сомнение в том будет ли он обеспечивать правовой санкцией э-подписи, используемые в таких контрактах, то страна создает причину того, что глобальные пользователи э-подписи будут избегать осуществления э-коммерции в этой стране. Другими словами, закон по э-подписи, который не предусматривает бизнес-выбора, на практике может оказаться более вредным для участия в глобальной цифровой экономике, чем отсутствие такого закона вообще.

Для поддержки э-правительства вероятно можно порекомендовать, чтобы те, кто осуществляют онлайн бизнес или осуществляют иные операции с э-правительством, получали идентификатор, выданный этим правительством или выданный провайдером, утвержденным правительством.

Помимо этого, для правительства очень сложно предусмотреть в законодательстве то, что на данный момент технология и рынок еще не создали. Регулятивная система может дать презумпцию юридической силы для некоторых существующих и признанных технологий, таких как PKI . Но если закон дает презумпцию юридической силы для определенных технологий, он также должен предусмотреть принцип нейтральности технологии, разрешающий судам принимать любую технологию, отвечающую объективным критериям. Нужно избегать государственного лицензирования провайдеров услуг. В целом, политика должна приветствовать развитие конкурентного рынка, на котором присутствуют много провайдеров услуг, и применяются различные виды технологий.

Развитие технологий и процедур по электронной подписи будет продолжаться. Развивающиеся страны и страны с переходной экономикой могут играть существенную роль в проводящихся исследованиях, экспериментах и инновациях. Тем временем, реалистичные модели принятия электронных подписей, описанные здесь, могут в наибольшей степени стимулировать применение э-комерции и э-правительства без регулятивного вмешательства.