Суверенитет государств. Юрисдикция государств.

.

Суверенитет государств. Юрисдикция государств

Национальные домены верхнего уровня (CC TLDs) +Интернационализированные домены верхнего уровня (Internationalized TLDs)

- *.РФ, .中國 и др.*

юрисдикция соответствующего государства

Родовые (общие) домены верхнего уровня (Generic TLDs) - *.com, .org, .edu*

юрисдикция США (штат Калифорния)

Суверенитет государств. Юрисдикция государств

Национальные домены верхнего уровня - «идентификация» государства в интернете.

Национальные домены верхнего уровня - критический ресурс государств.

Суверенитет государств. Юрисдикция государств

Первый национальный домен - Соединенные Штаты Америки - . US (1985 г.)

США – является государством фактически не использующим национальный домен верхнего уровня.

В США государственные органы власти используют родовые домены верхнего уровня : Правительство США и соответствующие правительственные органы власти –

. GOV; военные ведомства – . MIL ; образовательные учреждения - .EDU

Суверенитет государств. Юрисдикция государств

Страны с несколькими национальными доменами верхнего уровня:

- Великобритания (.UK, .GB, .EU);
- Российская Федерация (.RU, .SU, .РФ);
- Норвегия (.NO, .SJ, .BV);
- Китай (.CN, .HK, .MO)
- и др.

Суверенитет государств. Юрисдикция государств

Отсутствие национальных доменов верхнего уровня у непризнанных государств

- Абхазия;

-Косово;

- Северный Кипр др.

Суверенитет государств. Юрисдикция государств

Сайт Правительства Косово - http://www.rks-gov.net/
Сайт Президента Северного Кипра размещается в зоне национального домена Евросоюза (.EU) - http://www.kktcb.eu/
Сайт Президента Южной Осетии размещается в зоне национального домена России (.RU) - http://presidentrso.ru/
Сайт Президента Нагорного Карабаха размещается в зоне национального домена Арме

Суверенитет государств. Юрисдикция государств

Наличие национальных доменов верхнего уровня у непризнанных государств:

- Палестина (. PS);

- Западная Сахара (. EH) и др.

Национальные домены верхнего уровня географических территорий - Тайвань (. TW); Гонконг (.HK); Остров Вознесения (. FC); Антарктида (. AQ); Восточный Тимор (. TR)

Суверенитет государств. Юрисдикция государств

Национальные домены верхнего уровня

Государств, прекративших свое существование

- СССР (. SU);
- Судан (.SD);
- Югославия (. YU – прекращен в 2010 г.)

Суверенитет государств. Юрисдикция государств

Статья 1º Настоящий Закон закрепляет принципы, гарантии, права и обязанности использования интернета в Бразилии и предусматривает основополагающие положения деятельности Союза, штатов, Федерального округа и муниципальных образований в данной сфере.

Суверенитет государств. Юрисдикция государств

Основополагающий параграф. Принципы, закрепленные настоящим Законом, не исключают действия иных принципов, установленных в других законах Бразилии, относящихся к данной сфере, а также в международных договорах, одной из сторон которых является Федеративная Республика Бразилия.

Суверенитет государств. Юрисдикция государств

Реализации права каждого на доступ к интернету (статья 4)

Доступ к интернету имеет существенное значение для осуществления прав и обязанностей граждан (статья 7)

Суверенитет государств. Юрисдикция государств

При предоставлении как платного, так и бесплатного соединения с интернетом, также как и передачи, коммутации или маршрутизации, запрещается блокировать, отслеживать, фильтровать или анализировать контент пакетов данных, согласно настоящей статьи.

(Статья 9 §3°)

Суверенитет государств. Юрисдикция государств

Статья 11. В любой деятельности интернет-провайдеров и провайдеров интернет-приложений по сбору, накоплению, сохранению и обработке персональных данных или данных о соединениях, **если хотя бы одно из перечисленных действий осуществляется в пределах государственной территории Бразилии, должно соблюдаться в обязательном порядке право Бразилии**, включая соблюдение права на неприкосновенность частной жизни, права на защиту персональных данных, права на конфиденциальность частных сообщений и журналов регистрации коммуникационных сообщений.

Суверенитет государств. Юрисдикция государств

§1°. Положения статьи 11, применяются к данным, собранным на государственной территории Бразилии, и к контенту коммуникаций, **если хотя бы один из терминалов расположен в Бразилии.**

Суверенитет государств. Юрисдикция государств

§2°. Положения статьи 11, применимы, даже если деятельность юридического лица осуществляется за границей, **однако такое лицо предлагает услуги неограниченному кругу лиц Бразилии, или если, по крайней мере одно из лиц какой-либо хозяйствующей группы, учреждено в Бразилии.**

Суверенитет государств. Юрисдикция государств

§3°. Провайдеры интернет-соединений и интернет-приложений должны предоставлять, в порядке, предусмотренном правилами, информацию, которая позволит удостоверить факт соблюдения ими законодательства Бразилии относительно сбора, накопления, хранения и обработки данных, а также уважительного отношения к конфиденциальности данных и конфиденциальности коммуникаций.

Суверенитет государств. Юрисдикция государств

Основополагающий параграф. Условия договора, которые не соответствуют закрепленному выше порядку, не имеют юридической силы в силу закона, в том числе такие как:

I – нарушение неприкосновенности и конфиденциальности частных коммуникаций, осуществляемых через интернет;

II – **не закрепление в договорах присоединения альтернативной возможности для договаривающейся стороны выбрать Бразильский суд для разрешения споров, возникающих в связи с услугами, оказываемыми в Бразилии.**

Инициативы США: Национальная стратегия идентификации в киберпространстве (2011 г.)

* Основная задача: **повышение надёжности идентификационных данных** и степени **защиты информации**, позволяющей установить **реальную личность пользователя**
* Вследствие разнообразия видов и большого числа учётных записей (паролей, иных видов авторизации) предложено создание «**Экосистемы идентификации**» (Identity Ecosystem) с тремя уровнями (governance layer, management layer, execution layer)
  * Добровольность участия
  * Использование средств обеспечения безопасности данных
  * Совместимость данных из различных систем
  * Экономичность, простота в использовании, доступность для желающих
* Обеспечение возможности информационного обмена **без полной идентификации** участников
* **Допустимость использования различных он-лайновых средств** идентификации, корреляция с данными, накапливаемыми off-line
* Использование персональных данных должно соответствовать **Fair Information Practice Principles**

Неприкосновенность **частной жизни**

* Конституция РФ закрепляет **право на неприкосновенность частной жизни**
  * Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст.23 ч.1)
  * Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст.24 ч.1)
* В отношении персональных данных (например, пользователя интернета) должна обеспечиваться **конфиденциальность информации**
  * Пользователь имеет право на анонимность, на невмешательство, на отсутствие контроля и надзора за его деятельностью (***** см. ниже)
  * Лицо, получившее доступ к информации, идентифицирующего анонимного пользователя, не вправе распространять её
* Право на неприкосновенность частной жизни подлежит осуществлению с учётом признания **прав и законных интересов третьих лиц**
  * (*) В ряде случаев федеральными законами предусмотрены ограничения права на неприкосновенность частной жизни

Ситуация в России:

- ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» (2008)
  - При размещении в сети "Интернет" текстов судебных актов, вынесенных судами общей юрисдикции (…), в целях обеспечения безопасности участников судебного процесса из указанных актов исключаются персональные данные, кроме фамилий и инициалов истца, ответчика (…). **Вместо исключенных персональных данных используются инициалы, псевдонимы или другие обозначения, не позволяющие идентифицировать участников судебного процесса.**
- ФЗ «Об электронной подписи» (2011)
  - Простая электронная подпись
    - Коды, пароли или иные средства, **подтверждающие факт формирования подписи**
  - Неквалифицированная электронная подпись
    - Позволяет **определить лицо, подписавшего электронный документ**
    - Позволяет **обнаружить факт внесения изменений в электронный документ** после подписания
    - Получена в результате **криптографического преобразования информации** с использованием ключа электронной подписи
  - Квалифицированная электронная подпись
    - Неквалифицированная электронная подпись + наличие **квалифицированного сертификата** + использование **аттестованных средств электронной подписи**

Концепция Конвенции об обеспечении международной информационной безопасности (2011 г.)

* Дополнительными факторами, усиливающими опасность (…) угроз {информационной безопасности}, являются:
  * **неопределенность в идентификации** источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц, групп и организаций (…),
  * **различия в национальных законодательствах** и практике формирования безопасной и быстро восстанавливающейся информационной инфраструктуры.
* {К}аждое государство-участник **вправе устанавливать суверенные нормы** и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную ***инфраструктуру, расположенную на территории*** государства-участника или ***иным образом*** находящуюся под его юрисдикцией. Государства-участники ***должны стремиться к гармонизации национальных законодательств***, различия в них не должны создавать барьеры на пути формирования надежной и безопасной информационной среды (…)
* {К}аждое государство-участник должно придерживаться **принципа ответственности за собственное информационное пространство**, в том числе за его безопасность и за содержание размещаемой в нем информации (…)
* В целях организации уголовного процесса государства-участники:
  * (…)
  * принимают законодательные и иные меры, необходимые для того, чтобы гарантировать оперативное предоставление компетентным органам государства-участника или лицу, назначенному этими органами, достаточного количества данных о потоках информации, **которые позволят идентифицировать поставщиков услуг и путь, которым передавалось конкретное сообщение в его информационном пространстве** (…)

Выводы (1)

* Простых решений не просматривается.

* В силу разнообразия используемых в различных странах и в различных ситуациях мер идентификации (аутентификации, авторизации) в Интернете любые решения, принимаемые на локальном (страновом) уровне могут быть эффективны только на территории данной страны, а попытки распространить такие решения на иные («несвойственные») сферы применения чреваты конфликтами на межгосударственном уровне
  * При этом такие решения могут быть и неэффективными
  * Нарушение принципа технологической нейтральности способно привести к реальной «сегментации» Интернета и может отразиться на стабильности его развития в соответствующих «сегментах»

Выводы (2)

* Введение обязательных мер по «всеобщей идентификации» по «китайскому» (тем более – «северокорейскому») образцу может быть оправдано только при обозначении цели, соразмерной объёму (и обременительности) предлагаемых мер. Без комплексного подхода – в том числе в отношении ограничения доступа к информации, признаваемой «антиобщественной», - такие меры либо бесполезны, либо легко обходимы

* Право на анонимность является составным элементом законного права на неприкосновенность частной жизни и в этом качестве должно безусловно признаваться и уважаться
  * «Абсолютного» права на анонимность быть не должно, можно лишь говорить о степени «относительности» такого права (абсолютная анонимность = абсолютный криминал)
  * Ограничения права на анонимность должны быть соразмерными и установлены законом

Выводы (3)

* Не могут и не должны ограничиваться в «он-лайне» права и свободы, гарантированные для «оф-лайна»
  * Пользователь интернета должен быть уведомлен о своих правах и обязанностях, в том числе о случаях и пределах ограничения его права на анонимность (такое уведомление – обязанность лица, оказывающего услугу в Интернете)
* Случаи и порядок идентификации пользователей, операторов Интернета и владельцев сетевых ресурсов не должны принципиально (в правовом смысле) отличаться от случаев и порядка идентификации лиц, не использующих Интернет
  * В противном случае пользователи и операторы Интернета явным образом дискриминируются
    * Насильно телевизор их всё равно уже невозможно заставить смотреть

Выводы (4)

* Случаи и способы идентификации (аутентификации, авторизации) в Интернете **должны соответствовать характеру тех правовых отношений,** в которых такая идентификация необходима и **учитывать реальную практику** российских и зарубежных интернет-компаний
  * Допустима «неполная» идентификация, достаточная для определённых целей и не являющейся релевантной в других случаях
  * Обязательно соблюдение требований законодательства о защите персональных данных
* С учётом трансграничности Интернета необходимы согласованные меры на международном уровне для **взаимного признания национальных «систем»** идентификации
  * Предложения не должны носить конфронтационный характер и учитывать сложившиеся de facto стандарты и процедуры

Рекомендации 1-2

* (1) Российским органам власти отказаться от идеи введения «обязательной идентификации» в Интернете, что бы при этом не имелось в виду
  * Необходимо определить цели реально необходимой идентификации и сфер применения, в которых подобная идентификация целесообразна
  * Необходим диалог между заинтересованными органами власти, организациями интернет-бизнеса, экспертным сообществом и представителями гражданского общества по техническим и правовым мерам, отвечающим заявленным государством целям идентификации
* (2) Используя опыт работы в Интернете российских и зарубежных компаний, признать возможным использование различных способов и методов идентификации и начать работу по легализации в России «единой авторизации» (OpenID), при необходимости с подключением к этой системе средств аутентификации государственных органов
  * Правоохранительным органам (не только России) следует уделить особое внимание тактике и методике использования систем авторизации в своей деятельности, во взаимодействии с операторами соответствующих сетевых сервисов

Рекомендации 3-4

* (3) Органам власти России, регулирующим отношения в сфере информационных технологий, совместно с соответствующими российскими и зарубежными коммерческими и экспертными компаниями провести НИОКР по внедрению в нашей стране зарекомендовавших себя и перспективных способов идентификации, доказавших высокую эффективность в отдельных (критически важных) сферах применения
  * Распространяемые среди населения программно-аппаратные средства электронной подписи
  * Единые идентификаторы для операторов, предоставляющих услуги доступа к сети Интернет
  * Биометрические средства идентификации
  * Верифицируемые средства создания электронных почтовых адресов и использования защищённых каналов обмена электронными документами с этих адресов (без предоставления и использования средств электронной подписи пользователями)
* (4) Внести в повестку дня международных форумов с участием России вопрос о создании международной «экосистемы» идентификации в Интернете, обеспечивающей взаимное признание {различных видов} идентификаторов пользователей Интернета, операторов Интернет-услуг, владельцев интернет-ресурсов – вне зависимости от их местонахождения
  * Требуется серьёзное изучение американской Стратегии идентификации в киберпространстве в целях допустимости её положений на практике в российских (и иных) реалиях использования Интернета
  * Рассмотрение такого практического для всех стран мира вопроса, как идентификация в Интернете, в неконфронтационном формате, способно благоприятно воздействовать на обеспечение международного мира и безопасности применительно к развитию Интернета

Спасибо за внимание!