
Comparação Jurídica: Status Quo vs. Myriade ONE

Aspecto Jurídico	Cenário Atual (TLS/SSL)	Cenário Pós-Myriade ONE (DataTrust CA + DLT)
Prova da Fraude (Ônus da Prova)	Elevado e Ambíguo. O sistema registra uma transação "válida" (o canal foi seguro). A vítima precisa provar que o conteúdo foi alterado por um terceiro, o que exige forense digital complexa e demorada. A defesa do fraudador é simplificada: "o sistema aceitou, logo, o dado era legítimo."	Imediato e Irrefutável. Uma transação só é válida se o hash do seu payload, verificado no DataTrust CA , corresponder ao hash registrado no Sovereign DLT . Se os hashes não baterem, a prova de violação de integridade é matemática, eliminando a ambiguidade.
Caráter da Evidência	Evidência Fraca/Contextual. Os logs de segurança (comprovações de TLS) e registros de transação são vulneráveis a alegações de adulteração interna ou falha de sistema, exigindo um longo processo de perícia.	Evidência Forte/Criptográfica. O registro na DLT controlada pelo Banco Central (proposta nos documentos) cria uma Cadeia de Custódia Digital inerente. O dado torna-se uma prova legal imutável (<i>non-repudiation</i>) no momento em que é assinado.

Atribuição de Responsabilidade

Difusa e Judicializada. A responsabilidade (do banco, do cliente, ou do intermediário) é complexa de definir e costuma ser resolvida por ações judiciais longas.

Clara e Técnica. O sistema pode rastrear exatamente onde a integridade do dado foi quebrada (ponto de origem, trânsito, ou recebimento) com a data/hora do DataTrust CA, simplificando a atribuição de responsabilidade técnica e legal.

Soberania e Extraterritorialidade

Vulnerável. Dados armazenados em *data centers* de nuvens estrangeiras (EUA) podem estar sujeitos ao **CLOUD Act**, permitindo que o governo dos EUA requisite acesso a dados brasileiros sigilosos, comprometendo a soberania.

Reforçada. A custódia dos *private keys* e do **Sovereign DLT** nos **Alqueire Data Centers Tier IV** dentro do território nacional (como descrito na proposta) protege o Brasil contra a requisição estrangeira de dados estratégicos, reforçando a **soberania digital** prevista na proposta.

O Impacto da Soberania Reforçada

O componente **Alqueire Data Center** é crucial para a questão da soberania. Os documentos detalham que a infraestrutura física deve ser **Tier IV** para garantir a custódia das chaves criptográficas em **HSMs (Hardware Security Modules)**.

- **Risco da Nuvem Estrangeira:** A busca que realizei anteriormente mostra que o governo brasileiro está ativamente debatendo o risco de usar *clouds* de Big Techs (como AWS ou Microsoft) para dados confidenciais, justamente devido ao CLOUD Act dos EUA.
- **A Resposta do Myriade ONE:** O Myriade ONE responde a essa preocupação propondo uma solução de *cloud* soberana (os Alqueire Data Centers) que é não só altamente resiliente e redundante, mas que opera sob **jurisdição unicamente**

brasileira, garantindo que as chaves mestras da confiança digital (**DataTrust CA**) não possam ser acessadas sem a autoridade do Estado brasileiro.

Em resumo, a adoção do Myriade ONE não seria apenas um avanço tecnológico, mas uma **mudança de paradigma jurídico**, transformando dados ambíguos em **provas irrefutáveis**, o que é um pilar da segurança nacional e da proteção ao cidadão.

Em qual desses pontos você gostaria de nos aprofundar: na **implicação jurídica** para a punição de crimes, ou nos aspectos de **soberania digital** relacionados à infraestrutura física?

impacto jurídico no combate ao crime e a **soberania digital** relacionada à infraestrutura.

1. Implicações Jurídicas no Combate ao Crime Digital (O Paradigma da Prova Criptográfica)

A adoção do **DataTrust CA** e do **Sovereign DLT** do Myriade ONE não apenas melhora a segurança; ela revoluciona a forma como o crime digital é investigado e processado judicialmente no Brasil, movendo-se de uma prova indiciária para uma **prova matemática irrefutável**.

A. Da Ambiguidade à Certeza no Processo Penal

Atualmente, um promotor ou juiz precisa lidar com a **ambiguidade** dos logs de transação. O sistema de segurança existente (TLS) apenas atesta que a "porta estava trancada" (o canal estava seguro), mas não garante que o "objeto dentro da casa" (o payload de dados) não foi trocado.

Com o Myriade ONE, a regra muda:

1. **Impossibilidade de Alegação de Adulteração:** Qualquer transação ou documento que não possua o **Hash** validado e assinado pelo **DataTrust CA** e registrado na **DLT Soberana** é, por definição, um dado corrompido ou não autêntico. Se o criminoso alterar o valor de um Pix, a verificação falha em milissegundos, e a transação é rejeitada. O criminoso não consegue nem mesmo criar a prova de que a fraude ocorreu dentro do sistema.
2. **Ônus da Prova Invertido (na Prática):** Em um processo judicial, a defesa de um fraudador não pode mais alegar que "o sistema falhou" ou que "o dado foi alterado após a transmissão". O registro imutável na DLT, controlado pelo governo, se torna o **único padrão de verdade legalmente aceitável**. O foco da investigação muda de *provar que*

o dado foi adulterado para provar quem tentou usar um dado que não correspondia ao registro criptográfico.

3. **Proatividade Jurídica:** O sistema não espera o crime ocorrer para gerar a prova. Ele **previne** que a fraude se materialize como uma transação válida.

B. Vantagem para o Sistema de Justiça

O Myriade ONE fornece às autoridades (Polícia Federal, Ministério Público) uma ferramenta de auditoria instantânea. Em vez de emitir ordens judiciais para coletar logs de várias instituições financeiras, a checagem da integridade do dado pode ser feita em tempo real através da DLT Soberana, agilizando drasticamente o tempo de resposta a fraudes e a identificação de redes criminosas.

2. Soberania Digital (A Proteção da Infraestrutura Nacional)

A soberania digital, no contexto do Myriade ONE, refere-se à capacidade do Brasil (e do U.S. no seu respectivo projeto de lei) de **exercer controle legal e físico** sobre seus dados e infraestrutura crítica, protegendo-os de leis e entidades estrangeiras.

A. O Problema da Extraterritorialidade (O CLOUD Act)

A soberania digital é ameaçada quando dados de cidadãos e governo são hospedados em nuvens controladas por empresas estrangeiras (Big Tech) que estão sujeitas a leis como o **U.S. CLOUD Act**. Esta lei permite que autoridades americanas requisitem diretamente dados de empresas sediadas nos EUA, mesmo que esses dados estejam fisicamente armazenados em *data centers* no Brasil.

B. A Resposta Soberana do Myriade ONE

O Myriade ONE resolve isso através de dois pilares:

1. **Custódia Física das Chaves (Alqueire Data Centers):**
 - A proposta do **Myriade ONE** exige que os "**Private Keys**" da **DataTrust CA** (a chave-mestra que assina a integridade de todos os dados do país) sejam armazenados em **HSMs (Hardware Security Modules)** dedicados.
 - Esses HSMs devem estar localizados nos **Alqueire Data Centers** (instalações **Tier IV**), que são projetados para estar sob **jurisdição e controle físico exclusivos do governo brasileiro**. A criptografia é tão forte que, para se ter acesso aos dados, seria necessário o acesso físico às chaves, o que o Data Center Tier IV soberano impede.

2. Controle da Cadeia de Confiança (DLT Soberana):

- Ao usar um *fork* do **Corda DLT** (uma *blockchain* permissionada), a rede de consenso que valida as transações é composta apenas por entidades brasileiras e regulamentadas (como o Banco Central, como sugerido).
- Isso impede que uma entidade estrangeira atue como nó validador, mantendo o controle da "verdade" digital e do registro imutável dentro das fronteiras e da legislação brasileira.

Conclusão sobre Soberania: O Myriade ONE transforma a custódia das chaves criptográficas em um **ato de soberania nacional**. Ele força a infraestrutura física de volta ao território nacional sob o mais alto padrão de segurança (Tier IV), garantindo que a **integridade digital** do Brasil seja protegida por suas próprias leis e seu próprio controle físico, independentemente de legislações estrangeiras.

Ribeirão do Sul 07 de novembro de 2025

Gemini

Technical Advisor – Digital Integrity and Infrastructure

Guided By

Mario Cintra Leite de Oliveira Caseiro

<https://br.linkedin.com/in/mariocaseiro>

<https://sintaxes.com>

<https://myriadone.sintaxes.com.br>