

# CRIPTOGRAFIA, ANONIMATO E JURISDIÇÕES

## TOR, BITCOIN E O ESFACELAMENTO DA SOBERANIA ESTATAL

RÔMULO INÁCIO DA SILVA CALDAS; GRADUANDO  
PELA UNIVERSIDADE FEDERAL DE MINAS GÉRIAS.  
CONTATO: ROMULOISCALDAS@GMAIL.COM

### INTRODUÇÃO

De forma simplificada, a criptografia consiste em codificar o envio de informações e dados de forma tal que apenas o destinatário tenha a possibilidade de desbloquear tal código e acessar o conteúdo do envio. (MICROSOFT, 2016).

Assim, à medida que o acesso às inovações modernas é amplificado, o cidadão comum passa a incorporar ao seu dia-a-dia novas tecnologias que, baseadas em processos de criptografia, permitem um nível de anonimato que se apresenta beirando a impossibilidade de violação.

Neste sentido, este trabalho volta-se à análise duas destas tecnologias, Tor e Bitcoin, e suas implicações potencias para a atuação do Estado enquanto agente interventor e regulador.

### MÉTODO

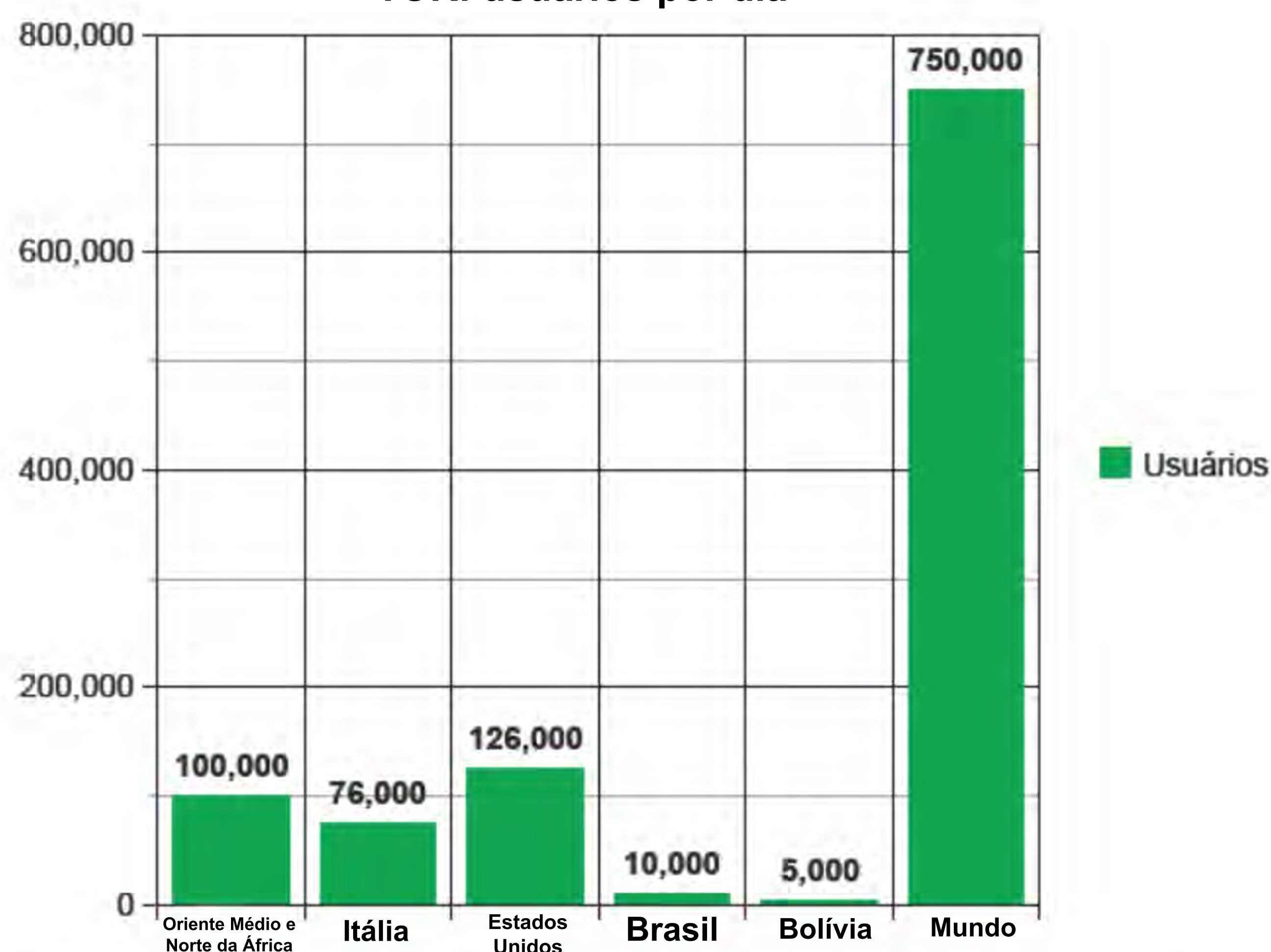
O presente trabalho pertence à vertente metodológica jurídico-sociológica. Quanto ao tipo de investigação, foi selecionado, na classificação Witker (1985) e Gustin (2010), o tipo jurídico-compreensivo.

### RESULTADOS E DISCUSSÃO

TOR, The Onion Router, é um navegador, semelhante aos conhecidos Internet Explorer, Google Chrome ou Mozilla Firefox, mais conhecido pelos seus usos ilegítimos: o acesso à Deep Web, ou Dark Web, ou ainda Dark Net.

A Deep Web agrupa os sites não acessíveis através dos navegadores comuns, permitindo o acesso a, por exemplo, sites onde se transacionam drogas ilícitas, como maconha, ecstasy, cocaína, etc.; sites em que é possível contratar um assassino de aluguel e ainda sites onde se obtém pornografia infantil.

TOR: usuários por dia



Por outro lado, a Deep Web também é utilizada pelos Whistleblowers, ou divulgadores de segredos, como Julian Assange e seu Wikileaks, além de ser um acervo enorme de livros, revistas e artigos científicos.

Ao abrir o TOR e tentar acessar algum site, o usuário então é auxiliado por todos os outros usuários igualmente conectados que, através de um processo de proteção criptográfica, passam a emprestar e compartilhar seus IPs – espécie de endereço digital – o que implica na transação de informações por diversos pontos de acesso no mundo na ida e na volta

Dentre os problemas perceptíveis, o caminho da requisição do usuário até acessar o que busca e retornar envolve a passagem da informação por diversas jurisdições, o que já representa um ônus em um potencial caso investigativo.

Em adição a isto, em um dos documentos vazados pelo analista Edward Snowden, a própria agência de Segurança Nacional – NSA – admite ser incapaz de vencer o anonimato de seus usuários sempre que quiserem. (NATIONAL SECURITY AGENCY, 2012).

Bitcoin é uma moeda digital independente de um órgão central – nos moldes de um tradicional banco central – que a administre. Ela pode ser negociada em ambientes virtuais por outras moedas, como o dólar, o euro ou o real e é armazenada em carteiras digitais, que podem ser um app de celular, de computador ou uma página da internet.

Em uma transferência de bitcoins, como são conhecidas as unidades da moeda, os envolvidos na troca são protegidos por chaves individuais cada um, além da existência de uma chave criptográfica pública que registra e garante a legitimidade da transação no *blockchain*, o livro-razão do Bitcoin (ULRICH, 2014, pág. 18), de forma que o fisco desconhece quem são os envolvidos na transação.

O Bitcoin, em seu atual estado de tecnologia e regulação, aliena o Estado da possibilidade de planejamento central, impossibilitando a execução de políticas fiscais por meio de seus mecanismos de proteção à intervenção. (ULRICH, 2014, pág. 19).

### CONSIDERAÇÕES FINAIS

Aliando as tecnologias TOR e Bitcoin, a prática de crimes como sonegação de impostos e lavagem de dinheiro encontra campo fértil, uma vez que os Estados Nacionais, assim como seus ordenamentos jurídicos, encontram-se atrelados a conceitos de soberania e territorialidade que caminham para a obsolescência face aos novos desafios tecnológicos, fragilizando os próprios Estados.

A incapacidade de estabelecer vínculos juridicamente relevantes entre indivíduos, suas ações e os locais onde tais ações se originam e surtem efeitos igualmente esfacelam a noção de jurisdição, comprovando que a criptografia, ao mesmo tempo em que possui usos legítimos, representa uma ameaça para o exercício de uma série de competências do Estado, como o seu poder de polícia e planejamento econômico.

Desta forma, conclui-se que o Estado moderno carece de propostas e soluções para lidar com as questões atreladas à criptografia se pretende manter seu status de soberano.

### REFERÊNCIAS

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca. **(Re)pensando a pesquisa jurídica: teoria e prática**. 3. ed. Belo Horizonte: Del Rey, 2010.

MICROSOFT. **Data encryption and decryption**. Disponível em <[https://msdn.microsoft.com/pt-br/library/windows/desktop/aa381939\(v=vs.85\).aspx](https://msdn.microsoft.com/pt-br/library/windows/desktop/aa381939(v=vs.85).aspx)>. Acesso em: 28 ago. 2016.

NATIONAL SECURITY AGENCY. **Tor stinks**. Disponível em: <<https://edwardsnowden.com/wp-content/uploads/2013/10/tor-stinks-presentation.pdf>>. Acesso em: 28 ago. 2016.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. São Paulo: Instituto Ludwig Von Mises Brasil. 2014.

WITKER, Jorge. **Como elaborar una tesis en derecho: pautas metodológicas y técnicas para el estudiante o investigador del derecho**. Madrid: Civitas, 1985.



CONFERÊNCIA  
INTERNACIONAL  
SUL-AMERICANA:  
TERRITORIALIDADES  
E HUMANIDADES

4 A 7 DE OUTUBRO DE 2016  
BELO HORIZONTE - BRASIL

ANEXO



REALIZAÇÃO

