

VII Fórum da Internet no Brasil

Desafios à coleta extraterritorial de evidências criminais eletrônicas em ambiente de computação em nuvem pública.

Sumário

Informações Básicas	2
Estrutura do Painel	2
Palestrantes	3
Síntese das apresentações e debates	5
Arguições e discussões	7
Consenso	8
Dissenso	8

Informações Básicas

Nesse painel, foram discutidos temas que evidenciam os principais desafios à investigação criminal, trazidos pela computação em nuvem pública, que implementa o estado da arte da mobilidade dos dados, bem como a análise do mesmo, quanto ao uso de criptografia. Assim, quando a evidência eletrônica de crime se encontra armazenada em território estrangeiro, mesmo que em ambiente de computação em nuvem, faz-se necessário estabelecer tratado de assistência judiciária em matéria penal, que tem-se mostrado contraproducente à investigação criminal, devido à burocracia que os casos requerem, sobretudo quando se trata de conteúdo de comunicações.

O painel, no formato de workshop, iniciou-se com a apresentação das regras por parte da organização, sendo, em seguida, apresentados pela proponente os objetivos almejados pela discussão.

As apresentações foram iniciadas com o painalista representante da academia, que trouxe conceitos relativos à computação em nuvem, bem como enfatizou a viabilidade técnica para territorializar os dados. Na sequência, foi abordada a visão do terceiro setor acerca dos conceitos e perspectiva jurídica do tema. O painalista seguinte, representante do setor governamental (Ministério da Justiça), expôs acerca dos desafios à cooperação jurídica internacional em matéria de coleta de prova digital no exterior. Por fim, o representante do setor privado aludiu às tecnologias de armazenamento de dados, enfatizando os desafios trazidos pela criptografia dos dados.

Estrutura do Painel

Proponente:

Nome: Danielle Novaes de Siqueira Valverde

Cidade/Estado: Recife / Pernambuco

Gênero: Feminino

Organização: IPESU

Email: dnsv@cin.ufpe.br

Minibio: Professora no IPESU, Doutora em Ciência da Computação (UFPE) e Mestre em Engenharia de Produção (UFPE). Bacharel em Ciência da Computação e Bacharel em Direito.

Relator:

Nome: George Fragoso de Andrade

Cidade/Estado: Recife / Pernambuco

Gênero: Masculino

Organização: Secretaria de Defesa Social do Estado Pernambuco

Email: george.fragoso@sds.pe.gov.br

Minibio - Mestre em Ciência da Computação com ênfase em banco de dados e reconhecimento de padrões, pela Universidade Federal de Pernambuco em 2011. Bacharel em Direito pela Universidade Cruzeiro do Sul (2014), Graduado em Sistemas de Informação pela Faculdade Integrada do Recife (2005). Lecionou no programa de Pós-graduação da Faculdade Estácio no Curso de Administração de Banco de Dados, em Pós-graduação na FAFIRE em disciplinas nas áreas de Banco de dados, Business Intelligence, Business Analytics, Mineração de Dados e na Universidade de Pernambuco, Faculdade de Administração de Pernambuco, a disciplina Sistema de Informações Gerenciais. Como profissional de segurança pública, atua em atividades de construção e manutenção de sistemas voltados ao apoio a atividade de inteligência de segurança pública.

Palestrantes

Nome: Jorge Cavalcanti Barbosa Fonsêca

Gênero: Masculino

Cidade/Estado: Recife / Pernambuco

Setor: Academia e Comunidade Científica

Organização: Universidade de Pernambuco – UPE

Email: jorge.fonseca@upe.br

Minibio: Doutor em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE). Possui mestrado e graduação em Ciências da Computação também pela UFPE. Atualmente é Professor da Universidade de Pernambuco (UPE). Foi pesquisador ativo no Fórum do Sistema Brasileiro de TV Digital, enquanto coordenador técnico da área de TV Digital no C.E.S.A.R. Colaborou no desenvolvimento de sistemas avançados em parceria com empresas como Motorola, Samsung, HP entre outras. Foi sócio-fundador da TreeyWay Solutions, empresa aprovada no Programa PRIME - Primeira Empresa Inovadora, programa de fomento da FINEP. Tem experiência na área de Ciência da Computação, com ênfase em Sistemas Distribuídos, Contexto, Engenharia de Software e Multimídia.

Nome: Luiza Brandão

Cidade/Estado: Minas Gerais

Gênero: Feminino

Setor: Terceiro Setor

Organização: Instituto de Referência em Internet e Sociedade

Email: luiza@irisbh.com.br

Minibio: Fundadora e Diretora do Instituto de Referência em Internet e Sociedade, é bacharel e mestranda em Direito pela Universidade Federal de Minas Gerais. Fundadora do Grupo de Estudos em Internet, Inovação e Propriedade Intelectual (GNet) e tem experiência na Universidade de Ciências Aplicadas de Schmalkalden (Alemanha) e na Universidade de Genebra (Suíça). Interessa-se pelas áreas de Direito Internacional Privado, Governança da Internet, Jurisdição e direitos fundamentais.

Nome: Kaue Alves Darzi

Cidade/Estado: Brasília / Distrito Federal

Gênero: Masculino

Setor: Órgão Governamental

Organização: Ministério da Justiça

Email:

Minibio: Bacharel em Relações Internacionais, pela UnB, em 2013. Analista do Ministério da Justiça e Chefe de Divisão em Cooperação Jurídica Internacional no Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional.

Nome: Evandro Hora

Cidade/Estado: Recife / Pernambuco

Gênero: Masculino

Setor: Setor Empresarial

Email: evandro@tempest.com.br

Organização: Tempest

Minibio: Professor associado da Pós-Graduação da Universidade Federal de Pernambuco, Sócio-Fundador e Presidente do Conselho de Administração da Tempest Security Intelligence.

Síntese das apresentações e debates

Danielle Novaes

Iniciou agradecendo à organização do Fórum pela oportunidade de proporcionar um ambiente de discussão sobre os desafios às investigações criminais, causados pelo armazenamento no exterior, mas em ambiente de computação em nuvem, de evidências criminais eletrônicas. Em seguida, apresentou o currículo dos painelistas, passando a palavra ao primeiro a se pronunciar, o representante da Academia.

Jorge Fonsêca

- Crime digital e computação forense.
- Cloud Computing e como funciona a arquitetura desta tecnologia.
- Virtualização de máquina, que consiste em ter várias máquinas não necessariamente numa mesma máquina física para garantir disponibilidades.
- Localização de máquinas em nuvem, onde estas máquinas podem estar espalhados em diversos locais territorialmente diferentes.
- Características da Cloud Computing, como o particionamento dos dados.
- Projeto do Google sobre a disponibilidade de internet por meio de balões e no alto mar, reforçando o aspecto da legalidade nestas áreas.
- Passo-a-passo de investigação forense em nuvem.
- Exemplos de como criar máquinas que podem coletar metadados de comunicações em uma máquina na nuvem sob domínio privado que permite analisar estes metadados sem precisar sair do país.
- Computação na Névoa: a nuvem mais próximo do usuário. Conceito expressado pela Cisco desde 2012.
- Evolução da distribuição do processamento e armazenamento dos dados com a IoT.
- Dicotomia da Regulamentação vs. Inovação

Luiza Brandão

- Apresentação do projeto IRIS
- Definição de computação em nuvem sob a ótica do regulamento europeu e do Cybercrime Conventions Cloud Evidence Group (2016)

- Relação entre o fenômeno social e o direito.
- Aspectos relevantes para coleta de evidências nos casos territoriais e extraterritoriais: conteúdo da comunicação, quebra de sigilo, empresas estrangeira que operam globalmente, cumprimento da decisão brasileira e dados no exterior.
- Convenções internacionais, MLATS: Acordos Bilaterais
- Casos da Microsoft entre os USA e a Irlanda e Cloud Act.
- Novas Perspectivas (Desafios e desenhos institucionais)
- Discussão sobre cooperação internacional: Direitos Fundamentais, Coordenação entre os estados e governança global.

Kauê Drazi

- Reforçou que as cooperações foram motivadas pela internacionalização das organizações criminosas.
- Cabe à autoridade central concentração as solicitações de pedidos de ativo (fora de país) ou passivo (dentro do Brasil).
- Abordou sobre como se procedem os pedidos de ativos e passivos para investigação criminal (Fora do País).
- Apresentou os principais atos que são frequentemente solicitados como: ouvida de testemunhas, quebra de sigilo bancário, etc.
- Apresentou os acordos Unilaterais: Palermo (Crime organizado), Viena (Drogas), Merida (Corrupção), Nassau, OCDE.
- Apresentou acordos bilaterais em matéria penal, firmados entre o Governo brasileiro: Canadá, China, Colômbia, Coreia do sul, Cuba, EUA, França, Itália, México, Nigéria, Panamá, Peru, Suíça, Suriname e Ucrânia. Como possibilidade de acréscimo de mais 25 acordos.
- Conceituou os princípios da bilateralidade e o da reciprocidade.
- Explicou como acontece a distribuição do pedido e que qualquer solicitação deve ser encaminhada para cooperacaopenal@mj.gov.br, via formulário ou pelo fone 61 2025 8900.
- Apresentou estatísticas entre tipos de crimes, tipos de diligências, origem dos pedidos ativos por órgão, informações de cumprimento, por estado,
- Reforçou que atualmente há uma demanda de ativos maior que passivos, na ordem de 65% e 35%, respectivamente de 2012 a 2017.

- Crimes mais comuns são contra o patrimônio
- Reforçou que há 3 tipos de requisições (ver na apresentação)
- Apresentou as principais dificuldades: contra os estados unificados. Falta de nexo causal entre o crime e a evidência, destaca-se.

Evandro da Hora

- Reforçou que só existe necessidade de extraterritorialidade devido às redes de computador e como esta tecnologia facilitou a comunicação entre máquinas territorialmente distantes.
- Outro aspecto foi a disponibilidade do dado consultado, mesmo em máquinas diferentes.
- Fez um contrassenso entre o mapa político e mapa da internet.
- Destacou que nenhuma tecnologia foi feita para ser rodada em um único território, abordando o termo: a tecnologia é laica e não exige território.
- Diferenciou os conceitos de metadados e conteúdo a ser obtido como vestígios, sob exemplo de ligações telefônicas.
- No caso de conversa com criptografia: há metadados, mas não há acesso à informação que foi produzida.
- No caso de dados criptografados há uma possibilidade de não se ter acesso aos dados caso sejam seguidas todas as regras de aplicação da segurança, não importando o tipo do arquivo: áudio, vídeo, texto.
- Reforçou um caso entre os EUA e o fundador do PGP. O PGP garante a cifragem dos emails para comunicação.

Arguições e discussões

Inicialmente foi questionado se casos de desrespeito às orientações de comissões da ONU podem interferir nos tratados vigentes de cooperação de acesso dados de forma passiva ou ativa, onde após debate fica óbvio que os fatos de descumprimentos destes tratados ensejam responsabilização do estado em nível internacional, ou seja, abrir mão desses mecanismos pode gerar reflexos indesejados, além de significar abrir mão de uma estrutura de sociedade internacional que vem sendo construída há muito tempo. Logo decisões neste sentido não devem ser precipitadas. Ainda foi reforçado que mesmo após mudanças de governos, o setor responsável pela cooperação jurídica

internacional (DRCI) não foi afetado nem foi alertado acerca de mudança de atuações do órgão.

Outras questões levantadas:

- a relação do tema com a criptografia moderna, a proscricção da criptografia e proscricção de armas, considerando que tratados internacionais já existiam mesmo antes do surgimento da Internet, a exemplo do Tratado de Roma, na década de 1950. Como resposta, referenciou-se que não há a relação direta entre a criptografia e armas e que a solução de cooperação internacional para o combate à corrupção perpassa ao problema técnico, sobretudo se considerar a extrema dificuldade (ou até mesmo a impossibilidade) de vencer uma criptografia forte. Assim, todo o esforço para se conseguir o acesso aos dados, em caso de estarem criptografados, não garante o acesso à informação. Ainda sobre os questionamentos foi identificado que acordos de cooperação existem bem antes da Internet, como exemplo com a Bolívia, do século 19.

- os principais problemas na coleta de evidência criminais eletrônicas com a Europa. Foi respondido que a deficiência na descrição do nexco de causalidade é o principal problema de recusa ao atendimento das requisições endereçadas à Europa. O nexco causal consiste na relação entre o crime, a prova telemática e a importância desta para as investigações vigentes. Ou seja, a quebra de sigilo telemático seja efetiva tem que estar bem fundamentado, justificado e autorizado por mandado judicial.

Consenso

- Necessidade de ampliação da quantidade de acordos de cooperação internacional em matéria penal.
- O uso de criptografia deve ser difundido no âmbito das comunicações pessoais e empresariais.
- Necessidade de mais debates sobre o tema, de forma livre e respeitosa.
- Neutralidade da rede de internet como objetivo de sua criação.

Dissenso

- Não foi obtido consenso de como o governo deve intervir para facilitar a coleta extraterritorial de evidência criminais eletrônicas, armazenadas em *datacenter* de ambiente de computação em nuvem, localizado no exterior, principalmente quando esses dados estão cifrados com criptografia forte.