RELATÓRIO BACKDOOR VIOLAÇÃO OU MITIGAÇÃO DOS PRINCÍPIOS DA SEGURANÇA JURÍDICA E PRIVACIDADE

Título: BACKDOOR: Violação ou Mitigação dos Princípios da Segurança Jurídica e da Privacidade?

Proponente: Leonardo Galli Reis, gênero masculino, Cidade de Londrina, Estado do Paraná; Organização: Solintel; Setor Empresarial;

Co-Proponente: Juliana Guimarães Cornélio, gênero feminino, Cidade de Londrina, Estado do Paraná; Organização: Solintel; Setor Empresarial;

Palestrante: Alexsandra Neves, gênero feminino, Cidade de Londrina, Estado do Paraná; Organização: Solintel; Setor Empresarial;

Palestrante: Willian Prenzler, gênero masculino, Cidade de Londrina, Estado do Paraná; Organização: MOGA Telecomunicações; Setor Empresarial;

Palestrante: Flávia Lefévre Guimarães, gênero feminino, Cisade de São Paulo, Estado de São Paulo; Organização: PROTESTE; 3° Setor;

Palestrante: Tiago Carnelos Caetano, gênero masculino, Cidade de Londrina, Estado do Paraná; Organização: SERCOMTEL; Setor Governamental;

Palestrante: Beatriz Silveira, gênero feminino, Cidade de Belém, Estado do Pará; Organização: Polícia Civil do Estado do Pará; Setor Governamental.

Moderador: Lacier da Costa Dias Junior, gênero masculino, Cidade de Londrina, Estado do Paraná; Organização: Solintel; Setor Empresarial;

Relator: Mariana Palma Vidotti, gênero feminino, Cidade de Londrina, Estado do Paraná; Organização: Solintel; Setor Empresarial;

Conteúdo/ posicionamento	Consenso, ponto a aprofundar	Observações
Backdoor como não sendo a melhor solução	Consenso	Todos os setores entendem que o Backdoor não é mecanismo viável para obtenção de conteúdo que transita em aplicativos ponto a ponto, pois ele acarreta em maior insegurança jurídica e violação de direitos fundamentais. Ainda, todos entendem que é necessário se adotar uma alternativa que possa resguardar tanto a segurança pública como os direitos individuais.
Mecanismo Técnico para obter informações	Ponto a aprofundar	Os debatedores concordam que deve ser encontrada uma ferramenta técnica que não viole os direitos fundamentais, capaz de atender às necessidades das autoridades no momento de uma investigação

RELATÓRIO BACKDOOR VIOLAÇÃO OU MITIGAÇÃO DOS PRINCÍPIOS DA SEGURANÇA JURÍDICA E PRIVACIDADE

Estruturação do workshop

• Objetivos e resultados (propostos e atingidos);

- Encontrar solução para utilização de Backdoor.

- Verificado que a solução seria outra ferramenta técnica que não ferisse os Direitos Fundamentais.

• Metodologia e formas de participação desenvolvidas durante o workshop.

- Pesquisas e entrevistas presenciais e remotas

Síntese do Debate:

Moderador - Lacier: apresentou os membros da mesa e contextualizou o tema, abrindo o workshop com direcionamento de pergunta a Sra. Alexsandra Neves, representante do Setor Empresarial;

Representante Setor Empresarial - Alexsandra: posiciona-se desfavorável a quebra de sigilo arbitrária, ressaltando a importância do sigilo para segredo de negócios e informações de clientes, sendo que o aplicativo ponta-a-ponta é uma evolução tecnológica daquilo que foi o telefone, de forma que informações empresariais sigilosas transitam facilmente pelo aplicativo. Porém, posiciona-se favorável ao backdoor desde que por ordem judicial, em processo de investigação, assim como se dá em outros meios de comunicação, posto que se trata de regra legal clara e expressa e que não prejudica o setor empresarial, podendo se aplicar de forma análoga à comunicação criptografada as formas de fiscalização adotadas na telefonia, por exemplo.

Moderador - Lacier: diante do posicionamento do Setor Empresarial, passa a pergunta para os demais setores:

Representante Setor Governamental - Beatriz: Menciona sua participação em investigação em cybercrimes, aponta o caso de pedofilia assistida, no qual o indivíduo paga para assistir vídeo online ao vivo de uma criança sendo abusada, ocorrendo simultaneamente o crime de abuso de menor impúbere e pedofilia online (pornografia infantil). Vem solicitar auxílio para busca de uma solução, pois necessita do acesso à comunicação criptografada para solução de crimes, como o citado e outros crimes de violência online, que consistem em violência moral e psicológica. Levanta a questão do metadado, posicionando que através de metadados é possível identificar a autoria de um crime, porém, muitas vezes são necessários em uma investigação fortes indícios de autoria e a materialidade do crime, que só é possível obtenção através do conteúdo da conversa, ou seja, fluxo de comunicação.

RELATÓRIO BACKDOOR VIOLAÇÃO OU MITIGAÇÃO DOS PRINCÍPIOS DA SEGURANÇA JURÍDICA E PRIVACIDADE

Representante Terceiro Setor - Flávia: posiciona-se pela privacidade de dados, sendo a privacidade e segurança conceitos complementares e não antagônicos. Menciona que mecanismos como backdoor, diante da fragilidade do sistema, facilitam a realização de crimes. Destaca que é necessário se fazer uma análise jurídica do tema, partindo do artigo 5° da Constituição Federal, que garante a inviolabilidade da intimidade, da vida privada, e das comunicações. Menciona a disposição do Marco Civil da internet, o qual disciplina o uso da internet no Brasil com base no princípio da privacidade, bem como depreende que A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Sendo que o provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial. Destaca que o Decreto que regulamenta o Marco Civil (Decreto 8.771/2016) prevê expressamente como mecanismo de segurança o uso de criptografia. Ainda, alerta para uma política de internet das coisas e critica aplicativos e aparelhos que já vem com o backdoor de fábrica, posicionando pela ameaça à privacidade desse padrão. Por fim, faz um comentário sobre a manifestação do Setor Empresarial, dizendo que a interceptação de telecomunicações funciona diferente da interceptação na internet, enquanto a primeira é possível se fazer uma seletividade, na segunda, a partir do momento que se cria uma falha na criptografia, fragiliza-se todo o sistema.

Representante Setor Governamental - Tiago: posiciona que os aplicativos de comunicação ponto-a-ponto são uma evolução daquilo que foi o SMS, e-mail, telefone, entre outras formas de comunicação, sendo que para esses meios já existe quebra de sigilo judicial para acesso à informação. Menciona que o Brasil está passando por uma operação muito grande e que graças a quebra de sigilo se está desvendando muitos crimes. Menciona que o crescente número de usuários de aplicativos ponto-a-ponto, acaba acarretando em um crescente número de usuários mal intencionados, que utilizam esses aplicativos para prática de crimes, de modo que é preciso encontrar um meio para se interceptar tais aplicativos para prevenção de crimes cibernéticos.

Representante Setor Técnico/ Acadêmico - Willian: destaca o contraponto, qual seja a privacidade versus a prevenção de crimes por meio de quebra de sigilo, dessa forma é necessário que o setor técnico consiga conciliar os dois cenários, dar segurança à população e garantir a privacidade. Contudo, pontua que o backdoor não é uma solução viável, diante da fragilidade do sistema. Porém, sugere que é necessário se considerar outras alternativas, que devem ser aprofundadas juntamente com a comunidade técnica mundial e com órgãos governamentais.

Exemplifica com situação análoga que é obrigatoriamente implantado por fabricantes em casos de plataformas de telefonia móvel, plataformas de telefonia fixa e até mesmo na internet para autenticação de clientes, o full interception.

Moderador - Lacier: Abre para perguntas

Representante Setor Governamental - Beatriz: abre parêntese para explicar as questões técnicas de um processo de investigação, lembrando que a polícia civil deve trabalhar com a ponderação de direitos humanos, ressaltando que o sistema de interceptação é judicial, de forma que a polícia não consegue realizar esse procedimento sem uma ordem judicial, ao passo que os criminosos fazem, fatos disponíveis na dark web. Ainda, aponta que no passado a Lei 9.296/96 que regulamenta o artigo 5°, inciso XII da CF, mais especificamente o parágrafo único do artigo 1° desta lei, foi questionado no STF, discutindo-se a constitucionalidade da interceptação telemática, decidindo o Supremo pela constitucionalidade da interceptação telemática, desde que se respeite o prazo de 15 dias. Ressalta que a polícia não tem a intenção de monitorar todo e qualquer cidadão, mas sim indivíduos específicos e em casos específicos com forte indícios de crime.

Representante Terceiro Setor - Flávia: Menciona que a Sociedade Civil no processo de elaboração do Marco Civil da Internet debruçou seus esforços para que a quebra de sigilo, entrega de dados, por provedores de conexão e de internet fosse feita somente por ordem judicial, sendo por fim garantido pelo Marco Civil, sendo uma grande vitória para o Direito Brasileiro. Por fim, faz uma crítica sobre a autorização de backdoor de fábrica em dispositivos, que esta autorização ao invés de proteção, traz uma insegurança, pois essa atitude viabiliza a extrema vigilância e incentiva o cometimento de crimes. Posiciona, que as entidades do 3° Setor não é contra as possibilidades que o poder público tenha para viabilizar investigações, mas sim a preocupação está especificamente em relação ao instituto de backdoor, principalmente quando ele vem de fábrica.

Plateia – Sérgio Universidade Federal do ABC Paulista: Questão para o Setor Técnico: se você considera procedente os backdoors instalados em todos os equipamentos de telecom pela Lei Communications Assistance for Law Enforcement Act e questiona se esses dispositivos com backdoor são eficientes para investigação criminal americana, e como é resolvido um trade off - questiona se a mesa acredita em instrumentos de vigilância que eliminam crimes, uma ideia do século XVIII, ou se a mesa considera que existem trade off, que muitas vezes não se resolve o crime e a liberdade de expressão e privacidade.

Representante Setor Técnico/ Acadêmico - Willian: menciona que não teve experiência com o CALEA, menciona que tem conhecimento de algumas técnicas adotadas foras do Brasil que muitas vezes são importadas para cá, como a quadriculação de torres de telefonia móvel, modelo

intrínseco ao governo americano, sendo um aparelho que dá a geolocalização do usuário.

Representante Terceiro Setor - Flávia: faz uma observação que se por um lado o posicionamento anteriormente defendido de que não existe uma contradição entre segurança e privacidade, de outro lado existe contradição entre vigilância e liberdade, sendo tema indiscutível. Posicionando um exemplo dos EUA que tem alta vigilância, mas que isso não impede a ocorrência de crimes.

Representante Setor Governamental - Beatriz: do ponto de vista policial, não há uma proposta de vigilância abusiva ou extremista, mas que se possa se ter acesso a dados em caso de crimes graves e que não tenham outro meio de prova, mediante ordem judicial.

Representante Setor Governamental - Tiago: menciona que o aumento da população, propiciou também um aumento de crimes e que a tecnologia está auxiliando na resolução desses, menciona que o Rio de Janeiro tem 2 centros referências nesse aspecto que possibilita a solução quase que em tempo real da ocorrência, cita como exemplo um crime que aconteceu na praia em que o centro conseguiu se conectar com o policial mais próximo do ocorrido e o agente criminoso foi preso.

Questionamento no youtube: "a ação das autoridades não serve para acabar com os crimes, mas para identificar e colocar na mão da justiça os criminosos".

Plateia: levanta a questão do policeware, arquivo malicioso para policiamento, sendo que em alguns países seu uso foi considerado inconstitucional, mas como o backdoor não parece ser a alternativa mais adequada, questiona se outras alternativas de aplicativos como o policeware podem ser adotados no Brasil, se isso é viável e se não viola direitos fundamentais.

Representante Setor Governamental - Beatriz: explica o conceito do policeware que é um arquivo malicioso aplicado a máquina do investigado, para, por exemplo, fazer uma busca e apreensão de dados, posiciona desfavorável, dizendo que ainda não há mecanismos que garantam que o poder público só fique infiltrado pelo prazo legal de 15 dias, sendo necessário ainda uma evolução legal sobre o assunto.

Representante Terceiro Setor - Flávia: não é contra, desde que aquilo que é previsto no Marco Civil seja cumprido, ou seja, uma ordem judicial, e que ele seja transparente e auditável. Por fim se posiciona que desde que atendidos esses requisitos parece mais justa e proporcional do que o backdoor.

Plateia: ressalta que a privacidade não pode ser abordada em contraposição com a segurança, que na verdade são faces da mesma moeda, solicita qual o posicionamento da mesa na discussão segurança x segurança

como foi o caso da Apple e FBI, pois entende que a criação de vulnerabilidades, mais do que garantir a segurança, cria-se a insegurança, pois nada garante que quem tenha acesso essas vulnerabilidades vá agir com o devido processo legal, cita também o exemplo do wannacry. Por que para garantir a segurança é necessário se minimizar a segurança?

Representante Setor Técnico/ Acadêmico - Willian: ressalta seu posicionamento contrário ao backdoor, qualquer engenharia reversa leva ao ser humano a violar e ter acesso a informações que não aquelas investigadas. Quanto Apple FBI, fica bem claro de que a vulnerabilidade no sistema não é o ideal, inclusive para esfera empresarial, colocando uma marca em contradição, a marca não é mais tão confiável.

Representante Setor Governamental - Beatriz: Destaca que no caso da Apple o FBI no fim não precisou da Apple. Com relação aos direitos humanos, posiciona-se como defensora. Bem como, destaca a importância da diferença de dado e conteúdo, o metadado permite a identificação do sujeito mas somente o conteúdo garante a materialidade do crime. Mais uma vez, destaca que é contra o backdoor, inclusive mencionando a diferença entre backdoor de dispositivo e de aplicativo, mas sendo contrária a ambos, porém solicita uma alternativa viável.

Representante Setor Governamental - Tiago: cita o exemplo da interceptação de correspondência eletrônica, que essa se da unicamente por ordem judicial e que o funcionário dentro do provedor de Telecom responsável por realizar a quebra do sigilo não tem acesso ao conteúdo, assim como qualquer outro funcionário, diretor deste provedor.

Plateia: questiona se é possível criar um software malicioso que se autodestruiria no prazo legal de 15 dias e que fosse auditável.

Representante Setor Governamental - Beatriz e Representante Setor Técnico/ Acadêmico - Willian: concordam que essa alternativa pode ser uma alternativa viável, Willian pontua que mesmo assim é preciso se tomar cuidado, para que se proteja a privacidade e direitos trazidos pelo Marco Civil da Internet.

Plateia: questiona se o problema central não é a falta de investimento de tecnologia e inovação. Também questiona a Beatriz como seria possível casar interesses, mencionando que os crimes não são cometidos online, que a comunicação é online mas que o crime se da em mundo real e não virtual.

Representante Setor Governamental - Beatriz: quando iniciou sua carreira achava que o mundo virtual era paralelo ao mundo real, mas que hoje pensa que o mundo virtual é intrínseco ao mundo real, posto que ao mesmo tempo em que se está realizando presencialmente o workshop, por exemplo, este está sendo transmitido em tempo real pela internet, o que acontece também com crimes, ressalta novamente a violência sexual

infantil online, onde há 2 crimes, violência sexual e pornografia infantil, esse último se dá puramente online.

Representante Terceiro Setor - Flávia: o investimento em tecnologia está profundamente comprometido, que o orçamento do MCTIC representa 50% do orçamento de 2010, ou seja, 07 anos atrás. A proposta é justamente haver mais investimento daquilo que é de interesse público, mas que o Governo, para isso, deve definir prioridades e políticas públicas. Que a política atual de congelamento de investimento nos setores públicos vem trazendo grande prejuízo à sociedade.

Moderador - Lacier: faz colocação que tecnicamente seria possível enxergar um único dispositivo, pois a criptografia se dá no aparelho. E que a fragilidade do whatsapp ficou maior com a modalidade web. Coloca que se for possível, em acordo com o whatsapp e provedor de telecom, clonar o chip para duplicar o aparelho, talvez seria viável.

Plateia: sugere além da autodestruição do software malicioso, é possível se fazer registros de log na máquina, para identificar que não houve abuso na investigação.

Comentário web: acredito que se poderia aproveitar melhor esses criminosos (hakers) para que possam auxiliar o Governo.

Comentário online: muitos aspectos estão dispostos no Marco Civil, mas questiona-se se os dispositivos desse diploma legal estão sendo usados da maneira correta.

Representante Terceiro Setor - Flávia: lembra que o Marco Civil é legislação recentemente aprovada, sendo mais recentemente regulamentada, sendo que o decreto traz um processo de fiscalização e transparência, envolvendo ANATEL, Secretaria Nacional do Direito do Consumidor e o CGI.br. É preciso que esses órgãos se articulem para pôr em prática o que é expresso na lei.

Representante Setor Governamental - Beatriz: menciona que o Marco Civil, em que pese tenha aplicação penal, o Marco Civil não traz o rito, que deve ser regulamentado.

Representante Terceiro Setor - Flávia: Marco Civil é uma lei que traz princípios mas que deve ser colocado em prática.

Plateia: é preciso achar um meio de campo, até onde vai o dever de investigação e até onde vai a privacidade. Lembra caso de assassinado que foi resolvido apenas com metadados.

Comentário web: se a fragilidade não está na criptografia, quem será responsável pela aplicação da lei o administrador do software, o hardware, ou as operadoras.

RELATÓRIO BACKDOOR VIOLAÇÃO OU MITIGAÇÃO DOS PRINCÍPIOS DA SEGURANÇA JURÍDICA E PRIVACIDADE

Representante Setor Técnico/ Acadêmico - Willian: se for feita uma solicitação da informação e não conseguir obter a informação, quem seria responsabilizado? Cita que enquanto operadora era necessário encontrar uma solução, pois era um processo rigoroso dentro da empresa. Questiona se cabe uma coautoria.

Representante Terceiro Setor - Flávia: os provedores de conexão devem guardar os dados por 1 ano e os provedores de aplicação por 6 meses, isto é previsão legal, seu descumprimento é descumprimento de lei. A responsabilidade é do provedor de conexão / aplicação, a depender do caso.

Representante Setor Governamental - Tiago: o operador de conexão tem acesso aos logs de conexão, aos e-mails e não ao conteúdo de aplicativos ponto a ponto.

Representante Terceiro Setor - Flávia: se existe a possibilidade de interceptação seletiva, por ordem judicial, deve ser interceptado, caso a empresa não atenda a ordem judicial poderá haver implicação penal.

Moderador - Lacier: a interceptação depende do whatsapp disponibilizar a chave para que se possa descriptar o conteúdo.

Conselheiro CGI - Sérgio: quando se perde o celular e você compra o outro, você consegue resgatar dados, quem faz isso é o hardware, é complicado de se aplicar, mas funciona como uma criptografia em cima do aparelho. A questão não é a possibilidade ou não de interceptar mas sim a razoabilidade do pedido em ordem judicial. Questiona a interceptação na web, que em geral não se alcança só o investigado mas pessoas que com ele trocam mensagens.

Moderador - Lacier: o mesmo acontece com o grampo telefônico, é um efeito colateral.

Representante Terceiro Setor - Flávia: Decreto que regulamenta o MCI, na questão de solicitação de dados por autoridade pública, é necessário se especificar claramente, é necessário individualizar o que será investigado.

Representante Setor Técnico/ Acadêmico - Willian: o operador deve rejeitar qualquer ordem que esteja fora desses padrões. Aproveita para esclarecer que há uma confusão entre a conta do whatsapp e o SIMCard do smartphone, cita o exemplo do wifi, no qual os dados utilizados não são pelo 4G. levanta a possibilidade da criação de perfis falsos no whatsapp.

Representante Setor Governamental - Beatriz: do ponto de vista da investigação, é necessário se distinguir interceptação da linha, do aparelho e do usuário de um aplicativo, para se direcionar o pedido para alcance de ordem judicial.