Relatório – 9º Fórum da Internet no Brasil

1. Informações Básicas sobe o Workshop

Título:
Entre investigações e vulnerabilidades: riscos e regulação do hacking governamental no Brasil
Formato: Painel

Proponente:
André Ramiro, IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, terceiro setor
Pedro Amaral, IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, terceiro setor
Marcos César, IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, terceiro setor

Palestrantes:
Carlos Cabral, Tempest, setor privado
Jamila Venturini, Unicamp/LAVITS/Derechos Digitales, comunidade científica e tecnológica
Veridiana Alimonti, Electronic Frontier Foundation, terceiro setor
Tiago Misael de Jesus Martins, Ministério Público Federal, setor público

Moderador:
André Ramiro, IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, terceiro setor

Relator:
Pedro Amaral, IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife, terceiro setor

2. Estruturação do Workshop

a) Objetivos e resultados (propostos e atingidos);
Propostos:

O workshop pretende amadurecer discussão no Brasil, ainda incipiente, sobre a regulação legal e administrativa acerca da contratação e uso efetivo de ferramentas associadas ao “hacking governamental”, aqui incluídas tecnologias de extração massiva de dados de dispositivos apreendidos, bem como a vigilância remota mediante spywares. Também objetivou-se focar no cenário de insegurança cibernética provocada pelo “mercado de vulnerabilidades” incentivado globalmente, pondo em risco não somente a resiliência de sistemas de informação nacionais, como direitos fundamentais de usuários, como a proteção de dados pessoais, a liberdade de expressão ou a presunção de inocência.

Buscou-se abordar ainda os impactos das revelações da ONG Forbidden Stories sobre a utilização do Pegasus em mais de cinquenta países, atingindo mais de mil jornalistas, ativistas e políticos, assim como os problemas da integração ferramentas como as da Cellebrite as técnicas disponíveis em departamentos de investigação de todos os Estados brasileiros, que garantem superações à criptografia forte e acesso irrestrito a dados armazenados. Buscou-se tratar também das bases legais no Código de Processo Penal e no regime brasileiro de proteção de dados pessoais para o hacking governamental e os riscos de uso abusos e arbitrariedades politicamente motivados. O debate, portanto, propõe explorar o contexto sociopolítico e tecnológico em que se inserem e, assim, apontar caminhos e possibilidades regulatórias.

O diálogo foi iniciado entre diferentes stakeholders sobre o estado do uso de ferramentas de hacking operadas por forças de investigação. A partir de um retrato inicial, avançou-se sobre possíveis potencialidades à segurança pública, bem como sobre os riscos à segurança e aos direitos derivados de usos que operam à revelia de garantias que assegurem a proporcionalidade, a necessidade e legalidade dessas medidas. Esperava-se oferecer insumos à políticas públicas que estão na pauta do dia do legislativo brasileiro, a exemplo da Reforma do Código de Processo Penal e da LGPD Penal, assim como avançar com possíveis reformas administrativas que deverão ser observadas por forças policiais na adoção dessas ferramentas.

Resultados alcançados:

No geral, o workshop atendeu aos resultados propostos, na medida em que houve a articulação de pontos específicos a respeito da área de cada palestrante. A partir dos consensos dissensos encontrados em termos de riscos aos direitos humanos e abusos concretos, a maioria dos painelistas apontou como os poderes adquiridos pelo hacking governamental ameaçam diversos do.

b) Justificativa em relação à governança da Internet;

O objeto de discussão se amplia a, pelo menos, duas dimensões geopolíticas: o mercado internacional de ferramentas forenses e de vigilância que encontra representações em diversas localidades e jurisdições, tendo por consumidores organizações governamentais variadas, democráticas e autoritárias; e os desafios dessas operações em responderem a padrões internacionais de direitos humanos, incluindo a proteção à privacidade, à segurança e ao devido processo legal. Não coincidentemente, são fatores que se confundem com questões críticas e transversais à governança global da Internet, como a confiança e a resiliência transfronteiriças ao ecossistema conectado.

Ao passo que o avanço de protocolos de segurança, como a criptografia forte, desenvolvem-se a partir da comunidade tecnológica e são efetivamente implementados por padrão pelo mercado de fabricação de aplicações e dispositivos globalmente, um movimento de contramão é identificado por um nicho que fomenta a exploração de vulnerabilidades nesses mesmos sistemas. Esse fenômeno se insere em um contexto de amplo debate sobre riscos sobre a vigilância operada por setores governamentais, muitas vezes à revelia de ordens judiciais, justificativa ou mesmo da identificação dos agentes. A própria existência de spywares e ferramentas de extração massiva de dados de dispositivos pessoais facilita sua inserção em mercados clandestinos, gerando um cenário de insegurança distribuída e operado por atores maliciosos, sobretudo em países cuja regulação sobre a contratação e uso de ferramentas de hacking seja insuficiente, como no Brasil.

O debate é emergente e atual, colocando-se como ponto chave para uma discussão multissetorial com alguns dos principais atores da área em atividade no Brasil. A dinâmica sobre a fabricação, contratação e uso dessas ferramentas, portanto, é parte das agendas de cibersegurança e proteção de dados transversais à governança global da Internet, tendo como ênfase, para o debate, o papel do Brasil.

c) Metodologia e formas de participação desenvolvidas durante o Workshop

A proposta do workshop é de mesa redonda, facilitando a troca entre os participantes. O moderador teve 5 minutos iniciais para apresentação da proposta da mesa, contextualização do tema, apresentação dos(as) painelistas e instruções ao público. Contamos com uma pergunta norteadora específica para cada stakeholder e 10 minutos para cada apresentação. A organização proponente mobilizou equipe de comunicação para fazer cobertura da sessão em tempo real nas redes sociais. Assim fazendo, também convidou constantemente o público remoto para interagir tanto na transmissão online como através de posts com hashtags do FIB 12 e das criadas especificamente para a sessão. Paralelamente, a moderação buscou convocar o público presencial para, além da intervenção na última parte da sessão, deixar comentários na transmissão online, listando impressões que poderiam ser lidas pela moderação entre as falas dos(as) painelistas. Durante a sessão, a moderação irá reforçar a possibilidade de interação do público remoto junto à transmissão online. Ao fim, esperava-se instigar o espaço para perguntas da audiência presencial e remota. No entanto, houve um problema técnico para a participação remota de um dos palestrantes, o que atrasou o início da mesa e, consequentemente, impossibilitou a participação do público com perguntas e falas na última etapa.

3. Síntese dos debates

TIPO DE MANIFESTAÇÃO	**CONTEÚDO**	**CONSENSO OU DISSENSO**	**PONTOS A APROFUNDAR**
Proposta: O enquadramento jurídico atual dá conta da questão ou é necessário modernizar a regulação existente para lidar com os riscos surgidos pela uso de ferramentas de hacking por agentes estatais para fins de investigação e inteligência?	Carlos Cabral abordou a estrutura complexa e diversa do mercado de ciberarmas, em termos de atores, usos e táticas. Apontou ainda como esse tema é atravessado justamente pelo mercado de vulnerabilidades, fomentado principalmente pelos Estados, mas também para cibercrimes, e que permitem níveis críticos de intrusão e, consequentemente, de abuso, sendo uma ameaça, na visão dele, para a democracia por permitir um “poder total”.		O risco inerente ao mercado de vulnerabilidades que é estruturado de forma a recompensar muito mais os abusos e mal usos.
Proposta: No Brasil, vemos o uso de tais ferramentas para solucionar crimes de grande comoção, assim como organizações criminosas, mas pode ser usado para proteger os interesses de	Tiago Misael argumentou que a maioria esmagadora dos usos dessas ferramentas é feito de maneira legal, sendo raros os abusos. Por outro lado, a investigação é necessária para resolver colisões entre direitos e ações dos cidadãos e dos funcionarios públicos, ao mesmo tempo em que os crimes dependem cada vez mais dos meios tecnológicos para sua realização.	Misael discorda da mesa ao defender que a investigação não deve ser considerada como ‘hacking’, e que o a lei atual é base suficiente para permitir o uso de malware para fins de investigação.	

governo. Como lidar com essas tensões?			
Proposta: Como articular as questões do devido processo, a integração existente desses expedientes ao ferramental da investigação criminal e a margem de decisão do magistrado para permitir como ultima ratio o uso de malware, ferramentas de alto potencial de risco, para fins de investigação?	Veridiana Alimonti focalizou nos riscos possibilitados pelo hacking governamental, especialmente quando estão na seara das atividades de inteligência, pouco reguladas, que frequentemente envolvem vigilância de opositores, ativistas e até de espionagem entre governos. Nesse sentido, o direito à privacidade protege um conjunto de outros direitos, como direito de opinião e direito à integridade física, entre outros, enquanto a própria atividade de hacking governamental vai de encontro ao dever de prezar pela segurança e prevenção de crimes.	Há um dissenso em relação à Misael quanto à raridade dos abusos.	Os ganhos de poderes pelo Estado e a dificuldade de controlar seu uso.
Proposta: Assim como acontece com os métodos de investigação policial, é necessário atualizar os direitos para fortalecer a democracia num contexto crescentemente mais digital? E como fazê-lo?	Jamila Venturini apontou a centralidade dos principios de legalidade, necessidade e proporcionalidade para avaliar a adequação das políticas de vigilância ao sistema de direitos humanos. Na América Latina, parece haver uma tendência à inadequação, em termos de opacidade e baixo controle externo das práticas de vigilância estatal.	Com exceção de Tiago Misael, os participantes concordam que é necessário avançar na regulação do hacking governamental pelo fato de que entre poderes inéditos aos agentes do Estado.	Os precedentes que devem ser considerados para avançar na regulação do uso de hacking por agentes do Estado.

Devido aos problemas técnicos para conexão do palestrante que participou de maneira remota, que atrasaram mais de 15 minutos o início do painel, e sem a possibilidade de estender o debate para além do horário definido, não houve tempo para perguntas e colocações do público.