RELATÓRIO – IX FÓRUM DA INTERNET NO BRASIL – FIB 2019

Day Zero Attack e a LGPD: Empresas e Governos estão preparados?

1. INFORMAÇÕES BÁSICAS SOBRE O WORKSHOP

- Título: Day Zero Attack e a LGPD: Empresas e Governos estão preparados?

- Formato: Mesa redonda

- Data: 04/10/2019

- Proponentes e coproponentes:

- KAUNERTH DIREITO DIGITTAL

- **Responsável pelo workshop**

- Nome: Jane Kaunert
- Gênero: feminino
- Data de nascimento: 06/10/1968
- Estado: SP
- Cidade: São Paulo
- E-mail: janne.k@digitalk.adv.br; jkaunert@hotmail.com
- Telefone: (11) 992571720
- Organização: KAUNERTH DIREITO DIGITTAL
- Setor: empresarial

- Coproponente

- Nome: Cristina Mendes Hang
- Gênero: feminino
- Estado: SP
- Cidade: São Paulo
- E-mail: hang@adv.oabsp.org.br; cristina.hang@digitalk.adv.br
- Telefone: (11) 999473884
- Organização: KAUNERTH DIREITO DIGITTAL
- Setor: empresarial

- Membros da mesa

Setor Privado

- Nome: Washington Umpierres de Almeida Junior
- Gênero: masculino
- Estado: São Paulo
- Cidade: São Paulo
- E-mail: wualmeida@gmail.com
- Organização: UTI dos Dados Perícias Digitais e Soluções de Dados Ltda.
- **Presença confirmada**

Terceiro Setor

- Nome: Bruna Martins dos Santos
- Gênero: feminino
- Estado: Distrito Federal
- Cidade: Brasília
- E-mail: brunasantos@codingrights.org
- Organização: Coding Rights
- **Presença confirmada**

Setor Acadêmico (Comunidade Científica)

- Nome: Christian Perrone
- Gênero: Masculino
- Estado: Rio Grande do Sul
- Cidade: Porto Alegre
- E-mail: c.perrone@itsrio.org
- Organização: Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).
- **Presença confirmada**

Setor Governamental (não participou)

1) Nome: Lélio Braga Calhau (**Declinou por compromissos da função)**
   Gênero: masculino
   Estado: Minas Gerais
   Cidade: Belo Horizonte
   E-mail: direitopenal@gmail.com
   Organização: Ministério Público de Minas Gerais.

2) Nome: José Antonio Ziebarth (**Declinou por questões operacionais durante o evento)**
   Gênero: masculino
   Estado: Distrito Federal
   Cidade: Brasília
   E-mail: jose.ziebarth@economia.gov.br
   Organização: Ministério da Economia

- Moderadora

- Nome: Janne Kaunert
- Gênero: feminino
- Estado: São Paulo
- Cidade: São Paulo
- E-mail: janne.k@digitalk.adv.br; jkaunert@hotmail.com
- Organização: KAUNERTH DIREITO DIGITTAL
- **Presença confirmada**

- Relator

- Nome: Carlos Goettenauer
- Gênero: masculino
- Estado: Distrito Federal
- Cidade: Brasília
- E-mail: goette@gmail.com
- Organização: Universidade Corporativa do Banco do Brasil

- Setor: acadêmico
- **Presença confirmada**

2. ESTRUTURAÇÃO DO WORKSHOP

O painel "*Day Zero Attack e a LGPD: Empresas e Governos estão preparados?* " teve como objetivo compreender os ataques dessa natureza e sua abordagem jurídica diante da nova lei geral de proteção de dados brasileira.

Além disso, objetivou-se avaliar em que medida as instituições públicas e privadas estão adequadamente preparadas para lidar com esse tipo de ameaça cibernética, visto, inclusive, o grande número de acidentes de segurança de dados ocorridos nos últimos anos.

As discussões foram extremamente proveitosas e atingiram plenamente os objetivos estipulados, uma vez que foi apresentado um panorama amplo, rico e representativo sobre a questão, demonstrando que apesar da Lei Geral de Proteção de Dados não ser um marco legal de segurança cibernética, ela gera a demanda por maior atenção a esse assunto.

A mesa redonda foi estruturada com base no tema supracitado, a partir do qual cada debatedor contou com 15 minutos para fazer suas considerações e reflexões. A partir de uma composição multissetorial, os membros da mesa trouxeram sua perspectiva sobre o tema. Destaca-se, todavia, a ausência dos participantes vinculados ao setor público, por razões operacionais. Após o discurso dos convidados, abriu-se o espaço para que o público encaminhasse dúvidas, opiniões e provocações, tanto fisicamente, pelo microfone ou em papel, quanto pela internet, na página do IX Fórum do Brasil na Internet.

3. SÍNTESE DOS DEBATES

Após agradecer a equipe do CGI.br e as intérpretes de libras presentes, a moderadora Janne Kaunert introduziu os convidados e passou-lhes a palavra. As discussões foram sistematizadas abaixo:

CONTEÚDO, POSICIONAMENTO OU PROPOSTA	CONSENSO, PONTO A APROFUNDAR OU DISSENSO	OBSERVAÇÕES
Washington de Almeida (Setor Privado)		
A Lei Geral de Proteção de Dados vem tornar ainda mais importante a abordagem dos chamados *day zero attacks*, termo proveniente do inglês, utilizado para descreve a ameaça de vulnerabilidade de segurança desconhecida e para a qual ainda não existe uma correção.	Consenso	Quando essas vulnerabilidades se tornam conhecidas de criminosos digitais, são exploradas para ataques, muitas vezes massivos. Diferentemente das vulnerabilidades conhecidas, os *day zero attacks* não tem solução imediata e já prevista por atualizações dos softwares. Um eventual ataque deve ser respondido pela empresa em conformidade com sua política de segurança de dados. Do contrário, fica exposta uma fragilidade da política ou do próprio sistema de proteção.
Nesse contexto, é importante tentar entender se as empresas e o governo estão prontos para responder a esse tipo de ataque. As ameaças cibernéticas estão disponíveis hoje em vários fóruns de compartilhamento de informações na internet, nos quais os *hackers* dividem experiências e ferramentas para infiltração em sistemas de segurança.	Ponto a aprofundar	Neste mesmo ano, já houve vazamentos de *sites* governamentais em várias esferas, inclusive em famosos vazamentos de dados de aplicativos de conversa envolvendo ministros de Estado. A avaliação da segurança cibernética das empresas também revela várias fragilidades. Ainda, o uso intenso de

A análise mostra que o governo e as empresas sequer estão preparados para os ataques convencionais e não parecem ter condições de responder a *zero days attacks*.		*cookies*, com rastreamento de vários dados dos usuários, que a rigor não podem ser tratados à luz da LGPD, também expõe a segurança dos usuários. Ainda a respeito dos *cookies*, o Tribunal de Justiça da União Europeia já entendeu que a autorização para coleta de dados baseado em uma simples autorização em *checkbox*, não é suficiente para legitimar o rastreamento de usuários na internet.
Algumas ferramentas podem ser utilizadas pelo usuário para compreender os riscos de segurança de navegação na internet. Uma delas é o *Lightbeam*, que mostra quantos *sites* se conectam a um computador quando o usuário acessa um endereço específico. O acesso a um único portal, como o *Google*, gera a execução de centenas de *scripts* e permite o acesso de dezenas de outros sites à máquina do usuários.	Ponto a aprofundar	Existe tentativas de resposta regulatória a esse tipo de fragilidade, como a Política de Governança Digital (Decreto nº 8.638/2016), a Plataforma GovData (Decreto nº 8.789/2016), a Plataforma de Cidadania Digital (decreto nº 8.936/2016), a Estratégia Brasileira para a Transformação Digital (Decreto nº 9.319/2018) e a consulta pública do E-Ciber, que busca produzir um marco normativo sobre segurança cibernética.
Christian Perrone (Comunidade científica e tecnológica)		
A segurança cibernética tem duas dimensões: a vulnerabilidade técnica e vulnerabilidade humana. As pesquisas revelam que o fator humano é imensamente importante e desempenha papel decisivo em casos de vazamentos de dados.	Consenso	Podem ser utilizados incentivos para o comportamento humano, como a entrega de benefícios simples aos usuários em troca de informações que, mais tarde, vão servir para facilitar o ataque à segurança cibernética tanto de governos quanto de empresas. Eventos dessa natureza já aconteceram em vários lugares do mundo.
De onde vem os principais riscos à segurança cibernética? Muitos ataques são realizados por agentes internos às próprias instituições. Os ataques também podem se originar de meios externos, ou seja, de foras das instituições, como é o caso de organizações criminosas que tem esse fim, ou dos ativistas exacerbados, que realizam ataques com o objetivo de chamar atenção a pautas políticas específicas. Os ataques também podem partir de competidores de mercado, em um contexto de espionagem industrial. Também há ataques externos de caráter internacional, inclusive para espionagem, como foi alvo a presidência brasileira há alguns anos.	Consenso	s/o
Qual é a preparação das empresas para os ataques? Soluções tecnológicas, como antivírus e firewall, todas de natureza passiva. Em seguida há formas reativas aos ataques, com a participação de empresas externas no apoio da empresa alvo.	Ponto a aprofundar	As empresas podem ter níveis diferentes conforme suas realidades. Empresas que lidam com poucos dados pessoais naturalmente vão ter menos demanda por segurança cibernéticas e podem viver bem em um nível reativo. Outras empresas, que lidam com grandes volumes de dados pessoais, precisam

Há também a preparação proativa, que estabelece um plano de ação prévio para o caso de ataques cibernéticos, gerando uma cultura organizacional de proteção de dados. No fim, há um nível de segurança progressiva, que busca antecipar os futuros riscos ao sistema de segurança interno da empresa.		necessariamente se colocar em uma posição de segurança progressiva.
A LGPD veio para proteger dados pessoais, mas por consequência gera uma cultura de segurança cibernética. Nesse sentido a lei determina que os agentes de tratamento devem adotar medidas de segurança técnica e administrativa para proteger os dados pessoais, evitando acessos não autorizados e acidentes de vazamento.	Ponto a aprofundar	A autoridade nacional ainda deverá decidir sobre os padrões técnicos mínimos aceitáveis de segurança cibernética. Ademais, as empresas serão obrigadas a notificar a autoridade nacional e os usuários sobre incidentes de segurança. Isso coloca as empresas em uma posição defensiva, diante do risco reputacional no caso de eventual incidente de segurança.
Tipos de solução em face de ataques à segurança cibernética. Primeiro, é possível pensar soluções de natureza técnica, como criptografia de dados, que dificultaria a utilização das informações em caso de incidente de segurança. Em seguida, é possível pensar em como programas de treinamento em segurança da informação. Ainda é possível pensar em soluções de infraestrutura, como a criação de sistemas de proteção ainda mais robustos. Mas a solução mais importante é fomentar uma cultura institucional de proteção de dados, dirigida a redução dos riscos associados ao fator humano.	Consenso	s/o
Bruna (Terceiro Setor)		
Ao tratar o assunto a partir da ótica do terceiro setor, é importante destacar que *hacker* não é necessariamente criminoso.	Consenso	Esse tipo de ponto é importante, especialmente porque os *hackers* muitas vezes prestam inclusive um serviço relevante para a elevação dos padrões de segurança cibernética.
A LGPD não é uma lei de segurança cibernética, mas sim uma lei sobre fluxos de informações, que regula como os atores devem atuar. São campos diferentes, embora muitas vezes se aproximem.	Ponto a aprofundar	Por ora inexiste um marco normativo de segurança cibernética. Entretanto, de certa forma, a LGPD abriu a discussão para a segurança cibernética.
O *zero day attack* é um pouco mais complexo que vazamentos mais simples, porque mesmo a empresa não tem necessariamente como antecipar os riscos a que seus sistemas estão expostos.	Ponto a aprofundar	Já houve ataques de *zero day attacks* que buscaram atacar desde usinas nuclear, até *sites* de comércio eletrônico, como a *Amazon*.
A LGPD trouxe novas regras de segurança cibernética, ainda que não seja uma norma especificamente ligada ao assunto. O governo, contudo, ainda não está adequadamente preparado para lidar com esse cenário, algo que tende a mudar um pouco à medida	Ponto a aprofundar	s/o

que as instituições se adequem à Lei Geral de Proteção de Dados.		
Medidas de segurança à informação não podem ser utilizadas como um escudo para evitar o acesso ao público ao acesso à informação garantido pela Lei de Acesso à Informação, uma ferramenta importante para o exercício da cidadania.	Ponto a aprofundar	A Lei de Acesso à informação foi o primeiro marco legal sobre o tema, inclusive trazendo com ineditismo o conceito de “dados pessoais” no direito brasileiro.
Ainda sob a ótica do terceiro setor, é importante destacar a obrigação de comunicação das empresas no caso de incidentes de segurança, algo que vem ao encontro do dever de transparência no tratamento de dados pessoais.	Consenso	s/o
Regulação de *day zero attack* é complexa em razão da própria natureza dos ataques. Uma solução eventualmente venha a coibir ataques cibernéticos não pode esbarrar no próprio direito à liberdade dos usuários da internet.	Consenso	s/o

Após as apresentações, foi aberta a oportunidade para perguntas. Primeiro, questionou-se sobre incremento de risco à segurança cibernética trazidos pela introdução de novos aparelhos continuamente conectados à internet, no ambiente de *Internet of Things (IoT)*. De modo geral a mesa compreende que o contexto de IoT traz novos desafios, que ainda devem ser depurados no futuro. Contudo, deve-se entender que existe a necessidade de uma proporcionalidade entre o consentimento ao acesso de dados dado pelo usuário e seu tratamento pelas empresas, sob o risco de descumprimento da própria LGPD.