Brasília, 09 de agosto de 2021.

RELATÓRIO

TÍTULO E TEMA DO WORKSHOP

Incidentes de Segurança de Dados Pessoais

FORMATO

Painel

PROPONENTES E CO-PROPONENTES

Proponente:

Waldemar Gonçalves Ortunho Junior

Diretor-Presidente da Autoridade Nacional de Proteção de Dados

Setor: Governamental

PALESTRANTES

Palestrantes:

Joacil Basílio Rael

Diretor do Conselho Diretor da Autoridade Nacional de Proteção de Dados, graduado em Ciências Militares pela Academia Militar das Agulhas Negras, Engenheiro de Computação pelo Instituto Militar de Engenharia, Mestre em Sistemas e Computação pelo mesmo Instituto e Doutor em Ciências da Informação pela Universidade de Brasília.

Setor: Governamental

Cristine Hoepers

Gerente Geral do CERT.br/NIC.br. Formada em Ciência da Computação pela UFSC e Doutora em Computação Aplicada pelo INPE.

Setor: Comunidade Científica e Tecnológica.

Luiza Couto Chaves Brandão

Fundadora e Diretora do Instituto de Referência em Internet e Sociedade. Mestre e Bacharel em Direito pela Universidade Federal de Minas Gerais.

Setor: Terceiro Setor

Roberto Gallo

CEO da Kryptus Segurança da Informação S/A e Presidente da Associação Brasileira das Indústrias de Materiais de Defesa

Setor: Empresarial

MODERADORA

Moderadora:

Nairane Farias Rabelo Leitão

Diretora do Conselho Diretor da Autoridade Nacional de Proteção de Dados. Advogada em Privacidade e Proteção de Dados. Bacharel em Direito pela Universidade Federal de Pernambuco.

Setor: Governamental

RELATORA

Relatora:

Mariana Almeida de Sousa Talouki

Coordenadora-Geral de Relações Institucionais e Internacionais na ANPD. Doutora em Direito - com o tema Cibersegurança - pela Faculdade de Direito da Universidade do Porto. Mestre em Direito Constitucional Público pela Universidade de Fortaleza e Bacharel em Direito pela Universidade Federal do Ceará.

Setor: Governamental

OBJETIVOS PROPOSTOS E ATINGIDOS

O Painel intitulado "Incidentes de Segurança de Dados Pessoais" objetivou trazer reflexões sobre o papel dos diferentes atores multissetoriais na prevenção e resposta a incidentes de segurança de dados pessoais. Em um primeiro momento foram apresentadas as diferentes visões dos palestrantes que demonstraram, conforme as suas respectivas áreas de atuação e representatividade, distintas perspectivas acerca da relação entre segurança da informação e proteção de dados pessoais, de forma a alinhar o entendimento da audiência sobre o tema. Os palestrantes do painel apresentaram, portanto, a visão de diferentes grupos de atores – reguladores, entidades de auxílio técnico, agentes regulados e titulares de dados - sobre o tema e refletiram, segundo cada perspectiva, sobre a importância de se convergirem diferentes áreas do conhecimento - jurídica, tecnológica e empresarial.

Nesse diapasão, o tema tratado no painel, “Incidentes de Segurança de Dados Pessoais” teve como objetivos principais a discussão acerca da definição e caracterização desses eventos, a partir de uma abordagem

interdisciplinar que permitisse a reflexão sobre o ecossistema de incidentes, bem como das consequências que irradiam para o Estado, empresas, sociedade civil e demais *stakeholders*. O debate teve, ainda, o condão de descrever sobre o papel da ANPD enquanto órgão central da Administração Pública Federal [ressaltado, em especial, pela Moderação - que ficou a cargo da Diretora Nairane Rabelo - e, ainda, pela Palestrante Luiza Brandão (IRIS)] no tratamento de dados pessoais, além de demonstrar como as demais partes interessadas, incluído os entes regulados e os titulares de dados, podem auxiliar na prevenção e mitigação desses incidentes.

Relativamente ao conteúdo do Painel, a proposta é que ele fosse composto pelos seguintes pontos principais, sem prejuízo de outros que viessem a ser abordados mediante provocação da plateia:

> Distinção entre os conceitos de segurança da informação, segurança cibernética e proteção de dados;
>
> Análise jurídico-tecnológica da definição de incidentes de segurança, os riscos para a disponibilidade, integridade e confidencialidade da informação e sua relação com o direito à proteção de dados pessoais e os princípios estabelecidos na LGPD;
>
> Correlação entre incidentes de segurança e os conceitos de *data breach* e vazamento de dados - ameaças, riscos, vulnerabilidades, falhas;
>
> Comparativo entre o tratamento de incidentes de segurança conferido pela legislação brasileira, sem prejuízo de outros ecossistemas jurídicos, mas de forma residual;
>
> Fomento por uma cultura de segurança e ciberliteracia como ferramentas de mitigação e prevenção de incidentes;
>
> O papel da ANPD e a regulação a caminho: a desmistificação de alguns pré-conceitos, a objetividade de sua competência;
>
> Políticas públicas relevantes e instituições competentes para o tratamento de incidentes de segurança: A Política Nacional de Segurança da Informação, Estratégia E-Ciber - as competências do GSI e do Ministério da Defesa.

Acerca dos resultados oriundos do workshop, o painel, a partir da discussão sobre os riscos inerentes aos incidentes de segurança, em particular aos titulares de dados pessoais, formas de preveni-los e remediá-los, tanto do ponto de vista individual quanto do institucional, e maneiras adequadas de notificá-los, aos entes reguladores e à sociedade e geral, conduziu a reflexões sobre o risco de naturalização do fenômeno: numa sociedade em

que vazamentos de dados são recorrentes e seus impactos invisíveis, a banalização desses incidentes pode expor titulares de dados a cada vez mais riscos. Há uma maneira de alterar essa perspectiva? Nesse âmbito, foi demonstrado pelos palestrantes:

- A importância e possibilidade de adoção de medidas de segurança (administrativas e técnicas), desde os níveis mais básicos, incluindo qualquer usuário de tecnologia, ressaltando a importância da proteção sob o viés tecnológico;
- Como se devem comparar as medidas e tecnologias de proteção empregadas no Brasil com aquelas utilizadas em outras regiões com legislação relacionada 'a privacidade, em particular no que tange ao Regulamento Europeu (GDPR);
- Quais tipos de tecnologias são as que possuem melhor relação custo-benefício na proteção de dados pessoais pelas empresas;
- Algumas questões e confusões conceituais que giram em torno das definições de incidentes de segurança, a partir de uma desmistificação da ideia de que todo incidente envolve *vazamento ou algum comprometimento de dados*;
- As questões jurídico-normativas relacionadas aos incidentes, incluindo as lacunas nas leis e o destaque para as medidas que estão sendo tomadas por parte da Autoridade Nacional de Proteção de Dados, em especial a oportunidade dada, a partir da tomada de subsídios e da consulta pública, para a participação de diversos *stakeholders* na formulação da regulamentação referente à proteção de dados pessoais e à privacidade.

A intenção foi de que, ao fim do painel, a audiência possa ter obtido uma maior compreensão dos conceitos fundamentais sobre o tema, tais como: incidentes de segurança, vazamentos de dados, confidencialidade, integridade, disponibilidade, etc. Além disso, pretendeu-se identificar estratégias de prevenção e mitigação de incidentes de segurança, do ponto de vista dos agentes regulados, além de apresentar a maneira que reguladores monitoram incidentes de segurança. Por fim, acredita-se que o painel possibilitou uma maior reflexão sobre o papel da sociedade em geral em lidar com o fenômeno dos incidentes de segurança relacionados aos dados pessoais.

METODOLOGIA

A metodologia e as formas de participação desenvolvidas durante o workshop passou por algumas adequações entre a proposta enviada à Administração do FIB e a que fora, de fato, utilizada no momento do Painel.

Inicialmente, cada palestrante seria convidado a apresentar uma exposição inicial sobre o tema, de até 10 minutos, a partir da perspectiva do grupo setorial que representa. Em um segundo momento, o moderador traria perguntas preparadas pelos proponentes para fomentar o debate e também abriria oportunidade para a audiência apresentar suas dúvidas e opiniões. Estimou-se cerca de 30 minutos para essa segunda fase do painel. Por fim, cada panelista teria cerca de 3 minutos para fazer suas considerações finais.

Após algumas reuniões preparatórias entre os panelistas, moderadora e relatora, ficou-se estabelecido dinâmica parecida, mas da seguinte forma: a moderadora iniciou o workshop com uma introdução e relatando algumas das iniciativas por parte da ANPD no que tange aos incidentes de segurança. Em seguida, cada palestrante foi convidado, pela moderadora, a apresentar uma exposição inicial do tema [Joacil Rael (ANPD), Roberto Gallo (Kryptus), Cristine Hoepers (CERT.br) e Luiza Brandão (IRIS), nesta ordem], de 10 minutos, a partir da perspectiva do grupo setorial que representa. Em um segundo momento, a moderadora trouxe perguntas preparadas previamente - em harmonia com os objetivos e conteúdo do workshop, a fim de fomentar o debate, abrindo, em seguida, oportunidade para a audiência suscitar seus questionamentos e opiniões. Por fim, cada panelista teria alguns minutos - por volta de 3 min - para fazer suas considerações finais. A moderadora concluiu, por fim, o workshop.

JUSTIFICATIVA EM RELAÇÃO À GOVERNANÇA DA INTERNET

O tratamento de incidentes de segurança é um tema de extrema relevância para a governança da Internet, uma vez que nossa sociedade amplia cada vez mais suas relações no mundo digital – seja em contextos financeiros, de saúde ou pessoais. Contudo, a carência de conhecimento sobre o assunto pela sociedade em geral e as confusões terminológicas entre os diferentes domínios de conhecimento relevantes acabam criando obstáculos para a proposição de soluções adequadas.

Ao mesmo tempo, é cada vez mais latente que cada parte interessada – sejam reguladores, regulados ou titulares de dados pessoais – tem um papel a cumprir na prevenção e mitigação de incidentes de segurança. Por isso, um debate multissetorial se mostra a maneira mais adequada de agregar as

diferentes perspectivas sobre o tema, sanar dúvidas conceituais e propor soluções colaborativas.

Assim, trazer a discussão para um fórum de governança da Internet, em que diferentes atores se congregam para discutir temas dos mais variados tipos se parece o canal mais adequado para absorver opiniões das mais variadas perspectivas.

RESULTADOS PROPOSTOS E ATINGIDOS

Para além de uma discussão profícua e de perspectivas diferentes, contudo convergentes, foi possível verificar, conforme explanado *supra* (item 7), resultados para além dos esperados. Para além de todos os pontos técnicos e jurídicos abordados e da discussão intensa acerca das nuances acerca dos incidentes de segurança, foi destacada a importância dos vários setores da sociedade - incluindo aí os cidadãos - na cadeia protetiva em termos de novas tecnologias, economia digital, dados pessoais e privacidade.

Ademais, a organização do painel permitiu que os panelistas, moderadora e relatora intensificassem o diálogo até mesmo para além do FIB11, com boas prospecções de prolongamento de troca de experiências e intercâmbio de informações relacionadas ao tema.

Verificou-se, ainda, a intensa participação da assistência, com envio de perguntas de grande utilidade, as quais foram respondidas pelos panelistas, sem prejuízo da complementação com perguntas formulados pela moderação e relatoria, dentre as quais se destacam:

Pergunta	Resposta	Panelista
Sabe-se que cada vez mais os titulares de dados utilizam menos o computador e mais aparelhos móveis no seu dia-a-dia. Essa utilização acaba por desencadear um fluxo de dados considerável que se perfaz no âmbito de aplicativos e para os mais diversos fins (transações bancárias, envio de dados por meio de redes sociais, cadastros em aplicativos de streaming e música,	Embora não se use, há opções de criptografia integradas nesse tipo de dispositivo (*IOS, Windows, Android*) e que, muitas não são utilizados pela falta de cultura. A preocupação com a privacidade deve entrar na vida das pessoas. Quanto aos aplicativos, estes, normalmente, já proporcionam essa segurança. Não é possível adentrar num aplicativo e, por exemplo, inserir a opção porque o código não é do usuário, mas do próprio sistema do aplicativo. Deve-se, contudo, configurar adequadamente o	Joacil Rael

etc.). Como a criptografia pode ser utilizada por indivíduos em suas atividades cotidianas por meio de aparelho de uso móvel (*tablets*, celulares, etc.)? É possível realizar a instalação de ferramentas criptográficas nesses aparelhos? E, ainda, uma ferramenta criptográfica é bastante para proteger os dados pessoais em todos os aplicativos, ou é necessário uma ferramenta específica para cada aplicativo?	aplicativo. Por exemplo: aplicativos bancários. Elementos que devem ser administrados com todo o zelo. Além da senha, precisa-se de uma cifração.	
Sistemas Gerenciadores de Banco de Dados podem cifrar, mas existe uma diferença muito grande de performance. E para as BDs que exigem tempo de resposta mais assertivo? Alguma dica/estratégia?	A criptografia passou de ser uma atividade intensa mais recentemente. Processador tem no seu hardware a criptografia. *TDE (trusted data encryption)*. Impacto de performance e tempo de resposta - é da ordem de 2% a 6%. Há, por outro lado, impacto um pouco maior no processamento da plataforma.	Roberto Gallo
O que as empresas devem cumprir enquanto garantias do serviço que pretendem prestar e cobrar dos, muitas vezes, incautos clientes? Qual o compromisso padrão do negócio?	Pensar nos melhores padrões. Olhar para dados e pensar em termos de formação e prevenção. A LGPD traz alguns aspectos, mas o próprio avanço científico e tecnológico traz o fato de que se devem adotar as melhores práticas. Menciona a minimização de dados - corrida para coletar todos os dados sem a finalidade. Essa cultura de minimização de dados, planejamento, traçar relatórios de impacto e montar uma	Luiza Brandão

	estrutura de governança. Todas essas são obrigações válidas.	

SÍNTESE DOS DEBATES

Síntese dos Debates			
Tipo de Manifestação (Posicionamento ou Proposta)	Conteúdo	Consenso ou Disenso	Pontos a aprofundar
Posicionamento	Enquanto moderadora, a Diretora Nairane ressaltou o papel da ANPD de sancionadora a partir de agosto de 2021, mas que, para além das funções de fiscalização e cominação de multas, a ANPD tem prestado um serviço enquanto educadora, a partir da recomendação de melhores práticas. Mencionou, ainda, problemas relacionados a incidentes de segurança, como a falta de regulamentação, mas destacou o já início das atividades na regulamentação desse tema, como a tomada de subsídios.	Consenso	Muitas contribuições foram recebidas e cabe à ANPD, em breve, colocar à disposição aquelas que servirão de substrato para a norma, bem como a Análise de Impacto Regulatório, mediante Consulta Pública.

Posicionamento	O Diretor Rael, enquanto panelista, ressaltou necessidade de se trabalhar na PREVENÇÃO de incidentes, bem como minimizar as suas consequências danosas. Rael destacou a importância de a sociedade - indivíduos, empresas privadas, administração pública, etc. - conhecer as espécies de medidas preventivas a serem tomadas de forma a evitar ou minimizar danos decorrentes de incidentes de segurança (medidas administrativas, jurídicas e tecnológicas). Nesse quesito, salientou sobre o consenso na ausência de fomento de uma cultura em prol da proteção dos dados pessoais, especialmente no que tange aos	Consenso	Necessidade de se viabilizar um caminho de construção de uma cultura de conhecimento tecnológico simples, a fim de se criar um empoderamento por parte da sociedade na autoproteção de dados.

	aspectos tecnológicos. Rael tratou, ainda, dos seguintes pontos: - ênfase às tecnologias que não representam significativo aumento de custos para organizações e empresas, com destaques às PME´s, sob pena de iniciativas custosas inviabilizarem o negócio; - preocupação com a atualização das versões dos produtos e atualizações; - considerações acerca da criptografia, de firewall, de VPN e de backups como ferramentas apta a redução dos riscos		
Posicionamento	Roberto Gallo, enquanto palestrante, explanou sobre a causa-raiz fundamental de um incidente de segurança, abrangendo os seguintes pontos:	Consenso	As considerações feitas por Roberto Gallo e Joacil Rael convergem em variados âmbitos, em especial no que tange à utilização da criptografia e outras ferramentas de segurança.

	- a perda de dados não implica em uma perda financeira; - a tolerância de risco no Brasil é muito grande se comparada a outros países; - a exemplo do caso *Cambridge Annalytica*, comportamentos aceitáveis em uma determinada época não o são após um determinado tempo; - sobre o contínuo e espantoso recurdescimento de violações de dados, sendo necessário o incremento da automatização da governança de dados, da qualidade de softwares, das áreas de monitoramento. - o conflito de interesse existente entre a área de negócios e as área de segurança e privacidade. Na opinião de Gallo, as áreas de TIC devem estar		Verificou-se, contudo, que o tempo utilizado sobre o tema não foi suficiente para albergar todos os pontos necessários. Verifica-se, portanto, a necessidade do aprofundamento do papel, não apenas de empresários e negócios que realizam o tratamento de dados pessoais, mas também dos indivíduos que, em alguma medida, procedem ao tratamento de dados pessoais ou que são usuários domésticos das tecnologias e que disponibilizam seus dados pessoais ou de outrem quando da utilização dessas novas tecnologias. Talvez o aprofundamento do princípio da subsidiariedade e da necessidade de haver proteção e segurança desde os níveis mais básicos de utilização da rede e do processamento de dados pessoais seja uma perspectiva

	vinculadas das áreas estratégicas e de tomada de decisão de uma determinada entidade; - a importância de tecnologias pontuais ou implementação de tecnologias de prateleiras no combate de incidentes de violação de privacidade.		interessante a ser considerada futuramente.
Posicionamento	Cristine Hoepers, gerente do CERT.br, destacou o seguinte: - boa parte dos problemas de segurança vêm dos projetos ou da implementação dos sistemas; - a importância de cuidar da formação técnica e acadêmica dos profissionais que atuarão nas áreas de segurança. Por essa razão, necessário incutir a cultura de preocupação de segurança e proteção de dados pessoais e	Consenso	Importante o aprofundamento sobre os tipos de reposta no fluxo de tratamento de incidentes e as peculiaridades existente quando tais incidentes, mesmo que residualmente, acarretam ameaças ou prejuízos a dados pessoais e à privacidade dos indivíduos titulares de dados.

	privacidade no corpo docente e discente dos centros acadêmicos; -a importância, ainda, em relação à definição de incidentes de segurança - a cada organização incumbe a competência de definir o que, de fato, é incidente para ela; - todos têm um papel na segurança e na proteção de dados pessoais - o ecossistema é complexo e interdependente.		
Posicionamento	Diferentemente do foco nas áreas de conhecimento mais ligadas à tecnologia, Luiza Brandão, fundadora do Instituto IRIS, focou nas questões jurídicas relacionadas ao tema. Ressaltou os seguintes pontos: - necessidade de integração da parte tecnológica com o		Necessidade de aprofundamento sobre a quebra de confidencialidade e aspectos que devem ser vislumbrado no regime de proteção de dados pátrio. Necessidade de aprofundamento sobre os aspectos que ainda não foram regulamentados pela ANPD.

	Direito, a fim de efetivar a integração da proteção de dados pessoais e a segurança da informação; - importância, ainda, de integrar as diferentes áreas e ciências a fim de produzir soluções factíveis e desenhar modelos de prevenção em incidentes de segurança envolvendo dados pessoais; - destaque ao papel da ANPD enquanto órgão que tem como missão precípua a proteção dos dados pessoais e da privacidade e de fomentar a participação da sociedade na formulação de normas por meio das suas tomadas de subsídio e consultas públicas.		Aprofundamento sobre as diferenças existentes entre as definições de dano relevante e risco relevante.