1. Informações básicas sobre o workshop

Nome: Para além dos escândalos: dados pessoais e segurança da informação no poder público

Resumo: O workshop analisou a implementação de medidas de segurança da informação no poder público, em especial no contexto do crescente tratamento de dados pessoais dos cidadãos, à luz dos recentes incidentes de segurança que ganharam o noticiário. Representantes dos diversos setores discutiram as condições que possibilitaram tais acontecimentos e as lições que as instituições podem extrair deles, a fim de desenvolver políticas de prevenção e contingência mais efetivas no futuro.

Formato: Painel

Proponente: Gustavo Ramos Rodrigues; Instituto de Referência em Internet e Sociedade; Terceiro setor

Palestrantes:

- Milena Lima; Polícia Civil do Estado do Tocantins; Setor governamental
- Vinicius Serafim; Brownpipe Consultoria; Setor empresarial
- André Ramiro; Instituto de Pesquisa em Direito e Tecnologia do Recife; Terceiro setor
- Isabela Rosal; Laboratório de Políticas Públicas e Internet; Comunidade científica e tecnológica

Moderadora: Ana Bárbara Gomes Pereira; Instituto de Referência em Internet e Sociedade; Terceiro setor

2. Estruturação do workshop

Objetivo e resultados: Em 2020, grandes escândalos envolvendo incidentes de segurança da informação no poder público ganharam o noticiário nacional. Em novembro, o Superior Tribunal de Justiça sofreu um ataque que resultou na cifragem de múltiplas bases de dados. Em seguida, outras cortes foram alvo de invasões em diferentes escalas. Na mesma época, uma falha na segurança dos dados do Ministério da Saúde deixou vulnerável por um mês mais de 16 milhões de dados de brasileiros que já haviam tido diagnóstico ou suspeita de covid-19. Esses incidentes levantaram preocupações sobre como tem sido a implementação das políticas de segurança pelos órgãos públicos, assim como das repercussões potenciais de incidentes futuros sobre o funcionamento das instituições. Ainda, provocaram debates sobre as complexas relações entre segurança da informação e proteção de dados num cenário de crescente coleta e centralização dos dados pessoais dos cidadãos para fins de modernização do serviço público e digitalização do governo. Com o objetivo de constituir um espaço para reflexão sobre os aprendizados institucionais que podem ser desenvolvidos a partir desses acontecimentos, o workshop mobilizou contribuições dos diferentes setores e das cinco regiões, de modo a trazer à tona diferentes perspectivas sobre o tópico. Com a finalidade de orientar o debate, as exposições dos palestrantes buscaram responder às seguintes questões:

Com a finalidade de orientar o debate, as exposições dos palestrantes buscarão responder às seguintes questões:

- Setor governamental: como têm sido as rotinas de tratamento de dados pessoais em órgãos públicos no país, sobretudo dados sensíveis? Há políticas e parâmetros satisfatórios de segurança da informação? E quais os desafios de implementá-los? (há equipe, treinamento?)
- Terceiro setor: quais os riscos e danos que os incidentes de segurança representam para os direitos dos cidadãos? Devemos entender que a ocorrência de incidentes de segurança representa um dano em si mesmo aos direitos dos titulares?
- Setor empresarial: o que os incidentes recentes de segurança da informação nos comunicam sobre as condições com que o setor público brasileiro vem tratando dados pessoais? A modernização digital do país está sendo acompanhada de uma preocupação com segurança da informação? E de políticas efetivas? O que falta para isso?
- Comunidade científica e tecnológica: quais seriam os remédios regulatórios (normativos, judiciais, etc) para que o cenário de incidentes de segurança presente no Brasil possa melhorar? Qual o papel da ANPD em suas diferentes atribuições (normatizadora, repressiva, educacional) nesse contexto?

O workshop avançou na construção de entendimentos coletivos sobre os riscos e as formas mais adequadas de se responder a incidentes de segurança no setor público, bem como sobre quais abordagens normativas e melhores práticas podem favorecer a prevenção desse tipo de incidente. Esses entendimentos foram construídos a partir das contribuições de representantes dos diversos setores e das cinco regiões do Brasil, de modo a trazer uma diversidade de olhares sobre o presente cenário, marcado por grandes escândalos de incidentes de segurança. Nessa seara, os registros das exposições e do diálogo com a audiência se convertem em documentação de referência acerca das reações da sociedade aos recentes escândalos, bem como para indicadores de caminhos potenciais a serem aprofundados em debates futuros, contribuindo para uma cultura de proteção de dados no setor público.

Exposições iniciais:

Milena Lima (Polícia Civil do Estado do Tocantins)

- Reforça que existem três poderes e três esferas, o que implica em elevada complexidade do setor público.
- Existe a parte administrativa e a atividade-fim de segurança pública, a exceção da LGPD deve ser para a atividade-fim, não a atividade-meio. No âmbito administrativo da segurança pública, a LGPD deve ser aplicável.
- Vários entes de segurança vêm indicando encarregados, traçando políticas de privacidade. Muitos entendem que deve haver esse cuidado independentemente da aplicabilidade da LGPD.
- Um desafio é conscientizar o servidor. Já tivemos problemas de vazamentos de dados pessoais e de informações relativas a grandes operações devido a essa falta de cuidado, os quais incluem informações pessoais das pessoas que estão sendo investigadas.

- Bancos de dados de segurança pública vem adotando sistemas com criptografia e autenticação de dois fatores. Para fazer login no sistema policial é preciso ter um aparelho cadastrado e fazer uma segunda autenticação.
- Mesmo adotando todos os meios técnicos, não é possível prevenir um vazamento. Por essa razão, é preciso discutir medidas de mitigação quando ocorrer. A comunicação do vazamento é uma obrigação. O simples vazamento em si já pode gerar uma perspectiva de dano em razão dos crimes que podem ser praticados com os dados.

Vinicius Serafim (Brownpipe Consultoria)

- Incidente não é só vazamento, envolvem comprometimento da disponibilidade dos dados.
- Descompasso entre processos e medidas de segurança preventivas e de mitigação do incidente.
- Ex: Medida de contingência no caso do incidente envolvendo o Superior Tribunal de Justiça foi usar telefones pessoais para comunicar informações comprometidas, o que indica a precariedade da situação.
- Boa parte da preocupação com segurança nos últimos anos vem a reboque da LGPD.
- O Brasil precisa de um centro de prevenção de incidentes similar ao que temos na aeronáutica
- Se não tivermos incentivos robustos para comunicação de incidentes, pode ser que os agentes de tratamento prefiram ocultá-los.
- Decreto 10.448 instituiu a Rede Federal de Gestão de Incidentes Cibernéticos. Ele vem ao encontro dessa necessidade de gerar essa cooperação. É difícil prever seus efeitos, mas ele começa a criar uma estrutura envolvendo a regulação. Esse tipo de ação é positiva.
- Temos cada vez mais complexidade na tecnologia e cada vez menos capacidade humana de lidar com esses aspectos, o que suscita novos desafios.

André Ramiro (Instituto de Pesquisa em Direito e Tecnologia do Recife)

- Há uma verdadeira constante de vulnerabilidades tanto acidentais (decorrentes de falhas e imprevistos) quanto, em certa medida, produzidas pela cultura da esfera pública
- O ecossistema de segurança no campo do poder pública carrega um cenário de muitos vazamentos de dados. Aumento de 500% nos vazamentos de dados entre 2015 e 2021.
- Esse cenário dialoga com medidas de digitalização do setor público que são imaturas ou não dimensionam os riscos efetivamente. Um exemplo é o cadastro base do cidadão. Cabe lembrar o sistema indiano similar, que já expôs dados de dezenas e milhares de indianos em mais de uma ocasião.
- Existe uma cultura de acúmulo de dados pessoais, não de proteção de dados.
- Danos variam muito em razão do órgão e da natureza do incidente, o que torna difícil prever a natureza dos bens jurídicos afetados.
- Caso do Ministério da Saúde afeta dados sensíveis. Caso do STJ pode afetar a locomoção do afetado.

- Não necessariamente existe dano decorrente do incidente diretamente, mas o agente de tratamento ainda assim deve ter o cidadão como centro gravitacional das medidas de segurança
- Dado o acúmulo que o Brasil tem no debate sobre políticas de criptografia, cabe trazer a complexidade de sistemas e dispositivos que se conectam entre si para prover os meios de acesso ao pessoal autorizado e estabelecer esses caminhos necessários de transferência e armazenamento de dados pessoais no serviço público.
- Um celular com acesso representa um ponto em uma superfície de ataque complexa e multifacetada.
- Ferramentas de alto potencial danoso gestadas pelo próprio poder público levantam preocupações. Ente público deve ser pensado não só como parte passiva, mas como parte ativa do ecossistema.

Isabela Rosal (Laboratório de Políticas Públicas e Internet)

- Remédios regulatórios devem focar muito na dimensão preventiva do incidente. Precisamos de instrumentos normativos um pouco mais efetivos que os decretos da PNSI e o da rede de incidentes de segurança cibernética. São remédios fracos.
- Precisamos de instrumentos com participação popular e maturidade técnica.
- Instituir a obrigação da implementação de segurança de dados e que os órgãos tenham planos de governança de dados e de resposta a incidentes de segurança. Devem ser públicos e ter participação social. Titulares e servidores precisam ser conscientizados. Deve haver uma definição nítida de encarregado e de suas funções, inclusive para respostas ao titular.
- Importância de harmonia entre as três esferas e os três poderes.
- O plano deve ser constantemente atualizado e os provedores treinados.
- O papel normatizador e o papel educacional da ANPD são fundamentais no campo da prevenção de incidentes. Construção de leis que definam princípios e novos decretos com respostas mais atuais e padrões mais harmoniosos, inclusive do ponto de vista conceitual. Trazer guias que permitam o entendimento do exercício de direitos dos titulares no setor público.
- Nem necessariamente todos os direitos dos titulares serão exercidos a todos os momentos.
- Atividade repressiva da ANPD demanda fazer revisões sobre a forma de responsabilidade da administração pública. Quando o dano é muito provável, como compatibilizar isso com o sistema de proteção de dados? Quem são os legitimados para representar os titulares em ações coletivas? Dentro do papel repressivo, além das multas (no setor público devem indenizar o titular).
- Deve haver compatibilização da LAI com os requisitos de confidencialidade. Realmente muitos dos decretos existentes hoje em dia trazem a necessidade de coleta excessiva de dados, o que contraria os princípios da necessidade e da finalidade.

Perguntas da audiência

1. Thiago Prates: TCU divulga a lista dos candidatos que receberam auxílio emergencial. Isso é considerado um vazamento de dados?

2. Rodrigo Wilsmann: Sobre a divulgação da lista pelo TCU, não seria o princípio da transparência, por se tratar de dinheiro público?

   Isabela considera que há elementos de transparência que amparam essa divulgação no setor público, como o princípio da transparência e a LAI. Mais orientações sobre como compatibilizar transparência e confidencialidade.

   André reforça que deveria ser absolutamente comprovado o interesse público nesse caso. Acha que é um tratamento potencialmente indevido e desprovido de explicação ao titular dos dados.

3. Natane Santos: Os decretos presidenciais (10.046 e 10.047) preveem a coleta excessiva de dados. Em relação a segurança da informação, quais os riscos do vigilantismo social e a coleta excessiva de dados?

   Isabela considera que esse caráter excessivo reforça a importância da aplicação prática de princípios como necessidade e finalidade. Observa que o setor público já dispõe de muitos dados. Assim, os próprios decretos deveriam abordar a aplicação desses princípios, sobretudo tendo em vista a transparência.

   André o considera excessivamente genérico e mal-sucedido em justificar sua própria necessidade. Observa que o Brasil atual é permeado por políticas tecnoautoritárias que ameaçam os direitos políticos e medidas como essa devem ser enquadradas nesse contexto. Considera que o cadastro base do cidadão ainda não se provou eficaz ou necessário.

   Milena considera que um banco de dados único pode ter maior segurança, pois hoje os dados são distribuídos entre muitos bancos de dados com graus variados de segurança. Assim, um banco único poderia contar com maior investimento em sua segurança. Nesse sentido, a centralização apresenta riscos, mas também oferece benefícios.

4. Rodrigo Silva: É possível que o cenário de LGPD se torna a oportunidade para empresas de Segurança da Informação realizarem “jogadas de marketing” com a divulgação de vazamentos de dados descobertos por eles?

   Vinicius considera que já se observa esse fenômeno e que a comunicação é legítima. Quanto ao uso publicitário, é costumeiro no campo da cibersegurança que se critique o chamado “teatro da segurança” (uso apenas publicitário da segurança). Por outro lado, é legítimo ter iniciativas acadêmicas legítimas de avaliação independente da segurança de sistemas, as quais são importantes para a segurança, caso contrário pode haver efeito inibitório sobre tais pesquisas e notificações. Critica a legislação chinesa que obrigaria vulnerabilidades de segurança a serem comunicadas ao governo primeiro.

   Isabela nota que há um agravante no fato de muitas dessas contratações relacionadas à segurança de software ocorrerem mediante dispensa de licitação, o

que pode gerar efeitos nocivos.

Milena avalia que há criminosos que utilizam da tática de detectar uma vulnerabilidade descoberta e venderem a não-divulgação da falha identificada. Considera que também é preciso se preocupar também com divulgações de dados divulgados ou comercializados por vias legais e ilegais. Comunicação de incidentes deve ser feita de formas ágeis e acessíveis aos cidadãos. Sobre a existência de um órgão centralizador para a comunicação de falhas de segurança, pode ser interessante por representar a possibilidade de evidenciar a boa fé do pesquisador que identificou a vulnerabilidade, o que o protegeria contra eventuais sanções.

André concorda que a exploração de vulnerabilidades nem sempre é realizada de boa fé para fins acadêmicos, há também hoje a exploração comercial sistemática de vulnerabilidades por atores privados e legitimados, os quais por vezes não reportam as vulnerabilidades identificadas. Manter a vulnerabilidade não atualizada pode ocasionar sua exploração eventual quando de sua descoberta por terceiros.

5. Joselma Fernandez: Políticas de tratamento de dados mais eficazes de segurança e transparência nos parece um caminho. Mas, a quem de fato compete a responsabilização nos casos de vazamentos?

   Isabela considera que ainda será necessário definir se haverá indenização dos titulares a partir do orçamento de multas aplicadas ao setor público ou se esses recursos serão direcionados a mecanismos de prevenção de novos incidentes.

   Vinicius compara o tratamento dado hoje à resposta a incidentes com aquele dado à segurança anteriormente: é tratada como uma função secundária de outro setor. Isso suscita preocupações porque a resposta a incidentes costuma ser pouco ágil e precisa, inclusive no setor público. Além disso, chama atenção para as questões de disponibilidade, hoje afetadas por ataques de ransomware, por exemplo, bem como para a irreversibilidade do dano decorrente de vazamentos.

   Milena comenta sobre a nova portaria do CNJ, que determina a instituição de protocolos de prevenção, gerenciamento e investigação de incidentes de segurança, inclusive com determinação de criação de unidades especializadas pelos tribunais, bem como de uma equipe nacional.

6. Thiago Prates: Qual a instituição que homologa os softwares?

   Milena afirma que o Instituto Nacional de Tecnologia da Informação poderia ser, talvez, quem trataria dessa questão, porém não tem certeza. Nota que em outros países busca-se essa centralização, porém há muitas divergências sobre isso. Nota que há controle sobre a exportação de alguns softwares em Israel, por exemplo. Considera difícil ter total controle, pois as autoridades nem sempre sequer tomam conhecimento sobre a tecnologia.

   André menciona a infraestrutura de chaves públicas, que recomenda padrões criptográficos para o ecossistema de inovação brasileiro. Acha delicado falar em um

sistema de homologação de software devido aos impactos sobre a inovação.

7. Lourival Moreira: Na esfera pública, não poderá haver situação onde o atendimento à LGPD irá violar a LAI ou vice-versa? Como harmonizar a transparência com a proteção dos dados e da privacidade em caso conflitante?

   Milena vê uma certa dificuldade na ponderação de interesses. A LAI trabalha com categorias de sigilo e afastamento de sigilo, enquanto a LGPD trabalha com outra lógica. Sobre a publicidade, tem dúvidas sobre até que ponto essa publicidade pode ser compatibilizada com a proteção dos dados. Em alguns casos, o acesso é condicionado a um credenciamento prévio, por exemplo. Em outros, somente algumas autoridades habilitadas têm acesso a essa informação. Esses são instrumentos de cautela potencialmente úteis.

   Isabela concorda com Milena e aponta que a LGPD se tornou muito mobilizada nas justificativas para negativas a pedidos de acesso à informação realizados via LAI.