Os vazamentos de dados de cidadãos na deepweb/darkweb sob a ótica da lgpd.

Lacier Dias - Moderador: Apresentando evento do FIB. Vazamentos da Deepweb sob a ótica da LGPD. Vários palestrantes vão falar sobre os impactos nas pessoas e no país.

Em janeiro, houve um megavazamento de dados: 226 milhões de brasileiros expostos.

Karina Figueiredo – Setor Governamental. Polícia Civil do Pará: Fala sobre a repercussão do vazamento na deepweb. As pessoas não sabem como e onde ocorreu o vazamento. A internet é feita de camadas: a mais comum é a surface e nas mais profundas são a darkweb. Onde fazem tráfico de drogas, de pessoas e exigem conhecimento maior. Já na deepweb, ocorrem a exposição dos dados vazados, como CPF, endereço, número de telefones. A deepweb não passa por investigação rotineira. A polícia é repressiva, quando as pessoas procuram. Observam uma atuação maior da polícia federal, que tem expertise em investigações cibernéticas e são pioneiras em algumas áreas. As polícias civis dos estados têm unidades especializadas em crimes cibernéticos. No Pará, a investigação é voltada aos crimes ocorridos, especialmente em pornografia infantil. A atuação da polícia judiciária é repressiva. Os vazamentos de dados têm relação com a incidência de fraudes. A partir do momento que os criminosos estão em posse dos dados, eles cruzam nomes de banco de dados e conseguem traçar o perfil de vítimas de suas ações. Fraudes têm crescido de forma assustadora, como a clonagem de WhatsApp. Com esses dados, eles podem fazer outras ações como solicitar cartão de crédito, soltar pishings, etc. Em 2020, houve clonagem de 5 milhões de contas de WhatsApp, sendo que o estado de São Paulo liderou esse ranking com 1,2 milhão de vítimas. Esse tipo de crime é o que tem várias formas de aplicar: por ligações, SMS, pesquisas, depois solicitam o código enviado via SMS. Importante ter autenticação em duas etapas. Esse vazamento leva a reflexões: a importância da LGPD e a necessidade de divulgação para as pessoas da importância de prevenir seus dados pessoais. Como o cidadão pode se prevenir se for mais atento.

Alfonso Presti – Setor Governamental – Ministério Público do Estado de São Paulo: As redes sociais são quase uma parte do nosso corpo. Já trabalhou no MP com todo tipo de vazamento que existe. O indivíduo antigamente utilizava CPF de pessoas falecidas. Hoje qualquer um abre uma conta. Quando se fala de fraude, um vazamento já aconteceu, a fraude é a consequência desse vazamento. O vazamento sempre é ligado à área criminosa patrimonial com o mau uso do dado. Esse mau uso pode ser pela incapacidade de gerir esses dados ou criminoso. Empresas privadas e públicas coletam e armazenam esses dados, houve camadas de proteção, que podem ser violadas e gerar vazamentos. Hoje esse vazamento é monetizado. Os dados são moedas de troca com valores, de forma legal. Pede autorização de dados para compartilhar. Quando o dado já chegou na Darkweb ou na Deepweb esse dado já foi mal utilizado. É possível que o vazamento se dê por uso de software de sequestro de banco de dados, como houve com empresas recentemente. A LGPD prevê sanções, mas ainda mal se sabe como usar. A pessoa geralmente não fica sabendo que seus vasos são vazados porque eles são armazenados na Deepweb, que não temos acesso. Antigamente se vendiam dados em ruas de comércio de eletrônicos. Autoridades de justiça ficaram à mercê de atentados com vazamentos. Importante entender que a atuação da PF e do CiberGaeco e a polícia especializada só trabalha por repressão. A forma de reagir é comunicar imediatamente o vazamento de dados para as

autoridades. Judicializar a reconstituição daquele dano e punir quem fez o uso indevido. Procurar os órgãos de defesa do consumidor quando ocorrer os dados. Tem que se criar uma cultura de procurar a polícia. Se não procurar não vai acontecer nada. Não se pode banalizar esses crimes.

Quando o acesso ao banco de dados é por software, é preciso criar sistemas de proteção. O pior é o mau uso político, estigmatizante. Decreto 1046 de 2019, que queria unir o cadastro básico do cidadão. Esse cadastro poderia virar um grande Big Brother, pois coleta dados sensíveis e dá acesso a ABIN e GSI, por exemplo. Esse cadastro procura seus dados e hábitos nas redes, podendo destruir reputações, estigmatizar pessoas. Com o artigo 16, vai permitir ao governo uma informação deletéria que nenhum governo deveria ter. Isso é gravíssimo. E-CPF, certificado A-1.

Flávia Lefevre – Terceiro Setor - Intervozes: Cidadão fica vulnerável para aprender se proteger apenas depois de uma fraude. Lamentável que a LGPD só tenha sido aprovada em 2018 e só entrou em vigor em setembro de 2020. A ANPD não se constituiu quando a lei entrasse em vigor e estivesse minimamente aparelhada para atuar no setor. O estabelecimento da ANPD só foi criado em agosto de 2020 e agora seu regulamento ainda está sob consulta pública. A ANPD ainda não está preparada para lidar com esses processos, mesmo após convênios com outras entidades. Há um vácuo regulatório, a lei precisa ser regulamentada para ser aplicada. Não há definição de procedimentos administrativos para aplicação de multas. O presidente na época vetou que a ANPD fosse uma autarquia independente. Ela ficou na presidência em claro conflito de interesses. Quem vai escolher os representantes será o atual presidente da república que viola os direitos da população. Apesar de as sanções poderem ser autuadas, apenas 4% das empresas estão adequadas à lei. As empresas poderiam estar sendo orientadas pela autarquia, mas ainda não exercem esse papel. A recessão democrática está acontecendo em vários países, não apenas o Brasil. A lei é boa, que ela não se torne algo para ser usado contra nós.

Anna Gardemann – Setor Empresarial – Gadermann e Vidotti Advogados: O que são dados e de que maneira os cidadãos podem se proteger. O setor empresarial enxerga a LGPD como necessária, mas precisa ser trazida para a realidade brasileira. Implantar a LGPD é um processo caro e complexo e as pessoas não têm sequer conhecimento do que são dados pessoais. É necessário ter subsídios para que as empresas pequenas tenham acesso. Necessidade de simetrias que precisam ser olhadas pela ANPD, antes que exijam de pequenas empresas que tenham um sistema de TI que impeça o vazamento. Importante ter apoio na implementação antes das sanções num Estado todo despreparado, interessado em implantar e não sabe como.

Mariana Vidotti - Setor Empresarial – Gadermann e Vidotti Advogados: Regulação da fiscalização pela ANPD que ainda está em fase de consulta pública. A forma como a ANPD vem se propondo a lidar com os dados pessoais vem preocupando que ela não possa ser eficaz. Fiscalização vem sendo pautada pela adoção da sanção educativa e responsiva e não punitiva. Quando se opta pela sanção que não seja pecuniária, precisa considerar a capacidade de mercado da empresa. Se partir do pressuposto que a medida educativa seja aplicada amplamente não estaremos seguros sobre o vazamento de dados

sem simetria, pode trazer conforto às grandes corporações não façam a proteção de forma efetiva.

Ricardo Vieira de Souza – Comunidade Científica – PUC-SP : Agradece o grupo por ter uma boa audiência. Pesquisa sobre o quanto nossos dados são valiosos. Empresas de tecnologia na Bolsa de Valores de Nova Iorque são trilionárias (Google, Amazon, Microsoft, Facebook, etc.). O negócio dessas empresas é tratar nossos dados. Reforçar o problema com o WhatsApp, cujos dados pessoais estão sendo vazados, contas clonadas e pedido de dinheiro para familiares da vítima. Esses dados devem ter sido vazados por alguma grande empresa. Eles conseguem até identificar parentes e solicitam transferências de dinheiro. Eu fui vítima, tentaram pedir dinheiro para minha mãe, mas eu estava do lado dela. Fiz BO e é possível rastrear os criminosos. Parceria entre CERTBR e ANPD é muito saudável. Ainda não existe regulamentação de como proceder em casos como esses. A gente vê diariamente dados de brasileiros estão sendo expostos, inclusive de grandes empresas. Depois que o dado é exposto, o problema é muito grande. A gente precisa prevenir antes de acontecer o vazamento. As empresas precisam fazer o penteste, teste de penetração. Os vazamentos afetam o direito à personalidade. Os processos de compliance precisam ser rigorosos e implantados pelas empresas. Um criminoso com um conjunto de dados afeta as pessoas, porque pode abrir contas, fazer compras. As pessoas leigas não tem como saber que seus dados foram vazados. Os sites que dizem que informam se seus dados foram vazados, não é possível. Há até um inquérito no STF contra esses sites. Infelizmente só vamos saber se fomos vítimas ou não de vazamento se sofrermos um golpe. Esse fórum deve trabalhar para conscientizar as autoridades de que a internet deve ser segura.

Rodada de perguntas e respostas

Leonardo Reis – Relator – Setor Empresarial - Solintel: Tanto a LGPD quanto a Lei de Segurança Cibernética se aplicam a todas as empresas independente do segmento ou porte? Para provedores de internet valem a LGPD e o regulamento de segurança cibernética criado pela Anatel, que abrange a parte técnica e a jurídica. Independente do segmento da empresa, qualquer CNPJ vai ter que cumprir a LGPD e a Resolução de Segurança Cibernética. É importante proteger todos os dados do cidadão.

Karina Figueiredo – Setor Governamental. Polícia Civil do Pará: O que impede a polícia a agir apenas de maneira punitiva mas agir de forma preventiva. A polícia judiciária tem essa função repressiva, mas nada impede que a polícia aja preventivamente. Devido à alta demanda da polícia judiciária, não é possível fazer isso. A polícia militar tem o papel preventivo. Se a polícia entrasse na Deepweb iria encontrar muitas coisas. É possível fazer monitoramento, investigação, infiltrar agentes. Tem um papel do governo verificar como ocorrem os vazamentos e como evitar. Defendo a informação ao cidadão para se prevenir de golpes. Exemplo: as pesquisas do Ministério da Saúde sobre Covid, que solicitam o envio de códigos. Existe autenticação de dois fatores em quase todos os aplicativos.

Alfonso Presti – Setor Governamental – Ministério Público do Estado de São Paulo:. Decreto 1004649, Brasil virando Estônia. O governo brasileiro tem um desejo que todas as pessoas tenham certificação digital. Tamanha diversidade no Brasil, fica mais difícil. Na Estônia e na Dinamarca foram feitos com resultados interessantes. Governo quer

colocar a população do Brasil numa base de dados não só biométrica, como comportamental. Para induzir todos a estarem nessa base, são usados estratagemas como o cadastro do auxílio emergencial. Essa ideia seria boa se houvesse uma autoridade nacional de proteção de dados efetiva e na mão da sociedade civil. Hoje é um governo de direita com viés autoritário, amanhã pode ser um governo de esquerda com viés autoritário. A realidade é que os dados empoderam o poder público. É por isso que as redes sociais estimulam o uso de hashtags, com isso conseguem identificar o comportamento dos usuários.

Flávia Lefevre – Terceiro Setor - Intervozes: Dicas de ações de segurança para cidadãos cada vez mais conectados. Como penalizar os responsáveis de alguma forma. Importante autenticação de dois fatores, dedicar algum tempo em decidir que tipo de cookies determinado site pede autorização de uso. Invista tempo para ler a política de privacidade dessas empresas. Isso é importante para poder restringir o acesso aos dados do cidadão. Mas isso não é suficiente para deixar o cidadão protegido. A atuação preventiva num mundo tecnologicamente complexo e na mão de empresas poderosas. Facebook, Google e WhatsApp, por exemplo, têm só no Brasil, mais de 120 milhões de usuários que utilizam diariamente por mais de 3/4 horas por dia essas redes, precisaria ter atuação preventiva da ANPD em cima para impor o cumprimento de determinadas obrigações. Dizer que essas empresas já atendem à legislação europeia não adianta, já houve vários vazamentos de dados de Facebook, fraudes no WhatsApp. Poder judiciário tem plenas condições de fazer valer a lei, por meio da regulação e princípios para promover coerência e harmonia na aplicação da legislação.

Anna Gardemann – Setor Empresarial – Gadermann e Vidotti Advogados: Qual o papel da LGPD no vazamento de dados na Darkweb? Que hajam dentro das empresas políticas de governança e boas práticas no tratamento de dados para que evitem os vazamentos. Antecipar a prática nas empresas ou nas pessoas físicas. Adequação da LGPD para ter uma responsabilidade pelo estabelecimento de uma cultura de tratamento de dados nas empresas. Existem profissionais que sugerem a adoção de uma cláusula dizendo que a empresa está tratando dados pessoais, mas isso não é o suficiente para proteger o cidadão de um vazamento de dados que vá parar na Darkweb ou na Deepweb. As pessoas precisam entender o que são dados pessoais, por que se coleta. É necessário instituir essas políticas nas empresas, treinar funcionários, para impedir que haja vazamentos.

Mariana Vidotti - Setor Empresarial – Gadermann e Vidotti Advogados: Quais são as consequências para as empresas quando ocorrem esses ataques e vazamentos? A LGPD estabelece várias punições que vão de sansões a multas que podem chegar a 2% do faturamento das empresas limitadas a 50 milhões de reais. Também existe e regulamento de fiscalização da ANPD que trata de uma vertente educativa, gerando uma incerteza de como se dará a aplicação dessas multas e em quais situações serão aplicadas.

Ricardo Vieira de Souza – Comunidade Científica – PUC-SP: Você vê ação efetiva por parte do governo em como corrigir vulnerabilidades no sistema de segurança e impedir a venda dos dados na Darkweb. Existe mecanismo para coibir esses vazamentos. Houve grandes vazamentos de dados nesse ano e a ANPD e a Polícia Federal foram acionadas, mas essas ações correm em segredo de justiça e para não expor os dados dessas

pessoas. Existe a necessidade de aperfeiçoamento das investigações desses crimes. Hoje é muito mais fácil cometer um crime cibernético de dentro de casa e obter vantagens financeiras do que apontar uma arma para alguém e correr um risco de ser pego pela polícia. A criminalidade cibernética vem se aperfeiçoando e pode em algumas vezes ficar impune. A sociedade clama por um aperfeiçoamento das instituições, para saber a origem dos vazamentos, de quais bancos de dados os criminosos se utilizaram. Investir também em tecnologia para e aperfeiçoar seus processos. A legislação tem um instituto muito importante que nesses casos, como se tratam de organizações criminosas, a lei de abrange as organizações criminosas prevê o agente infiltrado. O policial infiltrado se passa por um criminoso e entra nos fóruns que vendem dados clandestinamente na Darkweb e na Deepweb e consegue abranger toda essa teia da organização criminosa. Quem compra os dados está sujeito à pena do crime de receptação.