Tomada de Subsídios 2/2021 da Autoridade Nacional de Proteção de Dados

Contribuições do IRIS sobre incidentes de segurança

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

Tomada de Subsídios 2/2021 da Autoridade Nacional de Proteção de Dados

Contribuições do IRIS sobre incidentes de segurança

AUTORIA
Gustavo Ramos Rodrigues
Odelio Porto Júnior
Luiza Couto Chaves Brandão
Victor Barbieri Rodrigues Vieira

PROJETO GRÁFICO, CAPA E DIAGRAMAÇÃO
Felipe Duarte

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

APRESENTAÇÃO

Para contribuir com o maior alcance possível das contribuições oferecidas à Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, o IRIS torna públicas as respostas oferecidas à Tomada de Subsídios nº 2/2021 referente a incidentes de segurança que envolvem dados pessoais. Conforme a missão do Instituto, buscamos nutrir o debate público a partir da perspectiva acadêmica e baseada em referências, tanto da experiência internacional quanto de uma perspectiva multidisciplinar.

Entendemos, por fim, que a consolidação de um sistema nacional de proteção de dados ainda apresenta muitos desafios no contexto brasileiro, mas acreditamos que a colaboração de diferentes setores, bem como a fundamentação consistente das diretrizes da ANPD guardam grande potencial para a garantia dos direitos e liberdades dos titulares de dados pessoais. O amadurecimento das discussões é bem-vindo e consideramos que esta contribuição não esgota, necessariamente, o tema. Esperamos, na verdade, que sirvam para o avanço das discussões e da representatividade de diversos setores na consolidação regulatória da proteção de dados pessoais no Brasil. A seguir, encontram-se a apresentação e as questões elaboradas pela ANPD na Tomada de Subsídios nº 2/2021 e as respectivas reflexões oferecidas pelo IRIS.

Belo Horizonte, 24 de março de 2021.

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

TOMADA DE SUBSÍDIOS Nº 2 /2021

1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?

Há diversos fatores que corroboram para a relevância de um incidente de segurança que afete dados pessoais. A seguir, procura-se apresentar razões pelas quais **a relevância do risco ou dano deve ser presumida** para fins de responsabilidade dos agentes de tratamento de dados pessoais.

Conforme será exposto em mais detalhes a seguir, um incidente de proteção de dados pessoais repercute em responsabilidade objetiva por parte do agente de tratamento, por se tratar de um risco inerente à própria atividade de tratamento de dados pessoais. Dessa forma, a própria ocorrência de um incidente implica na quebra do dever de zelo pela informação em questão, o que atrai uma responsabilidade que se apoia tanto no parágrafo único do art. 927 do Código Civil quanto no art. 46 da própria LGPD; e, no caso de consumidores, no art. 6º, VI do CDC.

Além disso, observa-se, diversas vezes, a dificuldade – ou impossibilidade – de se estabelecer um nexo causal entre o incidente ocorrido e as repercussões danosas do evento. Esse fenômeno também é conhecido como "prova diabólica" no direito civil. Essa barreira informacional torna potencialmente nebulosa a avaliação do incidente pelos agentes de tratamento, decorrente tanto de uma dificuldade de análise de precedentes quanto da baixa previsibilidade – e constatação – das consequências diretas desse incidente.

Acrescente-se a isso o fato de que, uma vez substanciado, o dano decorrente de um incidente de proteção de dados é irreversível: quando as medidas de contingenciamento não são suficientes para impedir a consumação do dano, o que se sucede é inevitável. Isso, por sua vez, se intensifica no meio digital, no qual a constante evolução do estado da arte das tecnologias repercute em uma variedade crescente de modalidades de riscos e danos em um incidente que envolve dados pessoais.

Responsabilidade Objetiva e Direito do Consumidor

Como parte importante dos incidentes de segurança envolve dados pessoais de consumidores, a ANPD deve considerar os debates sobre o conceito de responsabilidade e dano desenvolvidos no direito do consumidor. O regime consumerista de responsabilidade é considerado pela LGPD, no parágrafo único do art. 46 e reforçado pelo comando expresso de diálogo de fontes normativas do art. 64.

O Código de Defesa do Consumidor (arts. 6, VI, e 12 ao 20, Lei nº 8.078) adota como regra a responsabilidade objetiva. Assim, o dever de indenizar fundamenta-se na existência de um nexo causal entre a conduta do responsável (neste caso os agentes de tratamento) e o dano causado ao titular pelo incidente de segurança.

O desenvolvimento da teoria da responsabilidade objetiva (independente de culpa) foi motivado pela necessidade de garantir a proteção de quem sofreu o dano causado; principalmente nos casos em que é a atividade econômica desenvolvida que gera e/ou potencializa as condições para que o risco se concretize em dano.[1] O desenvolvimento de atividades econômicas baseadas em dados pessoais (data

1 BESSA, Leonardo Roscoe.Responsabilidade objetiva no Código de Defesa do Consumidor. **Revista Jurídica da Presidência** Brasília v. 20, nº 120. Fev./Maio 2018 p. 27.Disponível em: <https://bit.ly/3tHrYCR>. Acesso em 21/03/2021.

capitalism[2]) gera incentivos para que os agentes de tratamento busquem ter maior acesso aos dados dos titulares, a fim de extrair informações úteis em termos econômicos. Desse modo, esses agentes de tratamento, ao criarem as condições para o uso dos dados, também geram maiores riscos em relação ao seu eventual uso indevido. Por isso é aplicável a **teoria do risco do direito do consumidor**[3].

Nesse sentido, a responsabilização objetiva, além do seu papel de censurar o causador do dano por meio de incentivo negativo (p. ex. punir agentes que adotam práticas insuficientes de segurança da informação), tem como principal meta garantir uma efetiva reparação à vítima.

Um tratamento de dados pessoais que gere as condições para um incidente de segurança, como práticas de segurança insuficientes por parte do agente, pode ser abarcado pelo "fato do produto ou serviço" (arts. 12 e 14 do CDC). O "fato do produto ou serviço" refere-se aos casos em que o consumidor sofre um dano em decorrência de "defeito" do produto/serviço.[4] Nesse caso, a adoção de medidas inadequadas ou insuficientes de segurança da informação seria considerada um "defeito" do produto/serviço, pela ótica da regulação consumerista, por gerar dano ao consumidor.

Alternativamente, em uma visão mais expansiva da responsabilidade objetiva consumerista, o art. 6º, VI do CDC pode ser entendido como cláusula geral de responsabilidade objetiva.[5] Assim, mesmo que se admitisse que um incidente de segurança da informação não configura "fato do produto ou serviço", a interpretação de que há cláusula geral de responsabilidade objetiva abarca os incidentes de segurança.

Desse modo, recomenda-se que ANPD parta do princípio de que determinadas atividades de tratamento de dados pessoais, por sua própria natureza, acabam por gerar um maior risco e potencial de tratamento indevido, principalmente em relação a incidentes de segurança da informação. A LGPD, ao ser uma regulação fortemente principiológica que impõe aos agentes a obrigação de analisar e mitigar adequadamente os riscos do tratamento, deve ser interpretada em conjunto com CDC, a fim de garantir a reparação e mitigação de danos (ver resposta 13 desta Tomada de Subsídios).

2 "Data capitalism is, at its core, a system in which the commoditization of our data enables a redistribution of power in the information age. If communica-tion and information are historically a key source of power (Castells, 2007), data capitalism results in a distribution of power that is asymmetrical and weighted toward the actors who have access and the capability to make sense of data." WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business & Society**, Vol. 58(I). 2019. p. 23. Disponível em: <https://bit.ly/3cSsWW5>. Acesso em: 21/03/2021.

3 "Na verdade, o CDC adotou expressamente a ideia da teoria do risco-proveito, aquele que gera a responsabilidade sem culpa justamente por trazer benefícios ou vantagens. Em outras palavras, aquele que expõe aos riscos outras pessoas, determinadas ou não, por dele tirar um benefício, direto ou não, deve arcar com as consequências da situação de agravamento. Uma dessas decorrências é justamente a responsabilidade objetiva e solidária dos agentes envolvidos com a prestação ou fornecimento." TARTUCE, Flávio; e NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**. São Paulo: Editora Forense. 5ª edição. 2016.p. 119.

4 "Por outra via, no fato ou defeito – seja também do produto ou serviço –, há outras decorrências [para além do defeito/vício do produto e/ou serviço em si], como é o caso de outros danos materiais, de danos morais e dos danos estéticos (prejuízos extrínsecos) [gerados ao consumidor]." *Ibid.* pp 125 e 126.

5 "O regime da responsabilidade objetiva do CDC deve aplicar-se, de conseguinte, a todas as hipóteses de relação de consumo quando surgir a questão do dever de indenizar o consumidor pelos danos por ele experimentados. Isto porque o fundamento da indenização integral do consumidor, constante do art. 6º, VI, do CDC, é o risco da atividade, que encerra em si o princípio da responsabilidade objetiva praticamente integra".De acordo com Nelson Nery Júnior (1992, p. 58), conforme citado por Bessa (2018, p. 29-30).

Método da Ponderação na Responsabilidade Civil e Grau do Dano

Conforme já explorado acima, a discussão sobre a conceituação e verificação do dano é uma tema fundamental no campo jurídico da responsabilidade civil. Com a expansão dos danos considerados ressarcíveis na esfera da responsabilidade civil, busca-se criar novos métodos de verificação do dano, principalmente para demandas relacionadas à responsabilidade objetiva, aos danos extrapatrimoniais e coletivos.

Desse modo, Anderson Schreiber sugere que seja aplicado o método da ponderação constitucional, de forma adaptada, para verificação do dano. Para o autor, este método seria importante pois o novo cenário da responsabilidade civil envolve, em grande parte dos casos, interesses igualmente tutelados pelo ordenamento jurídico (p. ex. privacidade *vs* desenvolvimento tecnológico):

> "Tal análise comparativa entre interesse lesado e interesse lesivo exige recurso ao método da ponderação, cujas potencialidades ainda permanecem pouco exploradas fora do âmbito constitucional. A identificação de condições de prevalência em cada caso particular, a partir do exame do ordenamento jurídico, permite, a um só tempo, um reconhecimento de ressarcibilidade limitada ao caso concreto e controle normativo da fundamentação das decisões que acolhem ou rejeitam as demandas de indenização"[6]

A partir das considerações sobre dano no direito civil, parece-nos útil que a ANPD utilize um método de ponderação semelhante para verificar o **grau do dano** sofrido a partir de um incidente de segurança da informação. A premissa é que determinados incidentes, por suas próprias características, intrinsecamente causam danos aos titulares afetados (p. ex. cópia e disponibilização ilícita de dados pessoais/vazamento), conforme exposto na definição de danos extrapatrimoniais.

Desse modo, o método da ponderação constitucional pode ser utilizado pela ANPD como base para elaboração do seu próprio método de análise de danos aos titulares afetados por um incidente de segurança.

Presunção de Relevância e critérios para determinação de exceções

Por todos os motivos elencados, a ocorrência de um incidente repercute em dano *in re ipsa* ao titular de dados. Dessa forma, **deve-se presumir relevante qualquer risco ou dano decorrente de um incidente de segurança relativo a dados pessoais**, exceto quando os agentes de tratamento puderem demonstrar a existência de medidas para assegurar que do incidente não resulte prejuízo aos direitos e liberdades dos titulares afetados.

Ademais, importa mencionar que a presunção de relevância do risco ou dano constitui uma recomendação de boas práticas por parte dos agentes de tratamento. Nesse sentido, o potencial para uma avaliação demasiadamente branda do ocorrido é reduzido, impactando diretamente na probabilidade de subnotificação de incidentes perante a ANPD e os próprios titulares de dados pessoais. Uma postura preventiva dos agentes de tratamento pode, dessa forma, evitar subsequentes responsabilizações por descumprimento dos enunciados da LGPD.

Uma vez que a constatação de "risco ou dano relevante" resulta em obrigação de notificação à ANPD, o conceito opera como equivalente funcional ao que o legislador europeu nomeou como "risco" no Regulamento Geral sobre a Proteção de Dados

6 SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil** - Da Erosão dos Filtros da Reparação à Diluição dos Danos. São Paulo: Editora Atlas. 3ª Edição. 2011. p. 252.

(RGPD) da União Europeia.[7] Na referida norma, o responsável pelo tratamento é compelido a notificar todos os incidentes, a menos que o ocorrido "não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares" (art. 33, 1). **A presunção de relevância do risco e a obrigação de notificar que dela sucede são regra, portanto.** Dadas as similaridades entre o desenho da lei brasileira e do regulamento europeu, entendemos que a adoção de um entendimento análogo favorece maior interoperabilidade entre os sistemas regulatórios, o que beneficia sua observância pelo agente de tratamento.

A análise não se esgota na presunção de relevância, contudo. Além de meio de salvaguarda ao titular de dados e incentivo à adoção de medidas de segurança efetivas, também devem ser consideradas eventuais exceções à regra de relevância presumida do incidente.

Como regra geral, só é razoável entender que o incidente referente a dados pessoais não acarretará prejuízo aos direitos e liberdades dos titulares quando da existência de medidas técnicas e organizacionais capazes de impedir a concretização do referido prejuízo. Assim sendo, e em conformidade com os princípios de responsabilização e de prestação de contas afirmados no art. 6, inciso X da LGPD, o afastamento da presunção de relevância deve estar condicionado à demonstração da existência e da eficácia de tais medidas pelo agente.

Ainda, o enquadramento de um caso concreto nessa exceção deve estar condicionado a uma avaliação de risco informada por uma miríade de fatores. Com base nas orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (p. 25-28) elaboradas pelo Grupo de Trabalho do Artigo 29º para a Proteção de Dados da União Europeia, destacamos os seguintes critérios:

- *Atributos da segurança comprometidos*: o incidente afetou a confidencialidade, a integridade, a disponibilidade ou a não-repudiabilidade dos dados? Incidentes podem comprometer apenas um ou múltiplos atributos e os prejuízos suscetíveis de resultar podem variar amplamente em função deles. Por exemplo, a depender do caso concreto, o comprometimento exclusivo da confidencialidade dos dados médicos de alguém pode ser mais suscetível de resultar em prejuízo reputacional e psicológico, enquanto uma violação que atinja exclusivamente sua disponibilidade ou integridade pode ser mais suscetível de afetar negativamente a possibilidade de recepção de tratamento adequado em uma emergência.

- *Natureza, volumetria e vulnerabilidade dos dados*: Dados de saúde, dados financeiros e dados referentes a documentos de identificação merecem especial atenção pois sua natureza implica que seu comprometimento pode resultar em prejuízo por si mesmos. Outras categorias de dados podem ser associadas a níveis mais elevados de risco por sua própria natureza, como dados de educação, endereços e registros de localização. Além disso, quanto

7 "[...] por risquificação da proteção de dados pessoais entende-se esse processo de reformatação jurídica a partir da ampliação da tutela coletiva e sua imbricação com a autoridade independente de proteção de dados pessoais, a disseminação de instrumentos regulatórios *ex ante* e o uso intensivo de metodologias de gestão de risco e calibragem entre riscos, inovações e imunidades – um processo de "negociação coletiva" (TUBARO e CASILLI, 2018) que supera a tradicional concepção bilateral entre sujeito de direito e aquele que processa dados pessoais pessoais." ZANATA, Rafael A. F. Artigos Selecionados REDE 2017 **I Encontro da Rede de Pesquisa em Governança da Internet Rio de Janeiro.** 14/11/ 2017.p. 184. Acesso em: 24/03/2021. Disponível em: <https://bit.ly/2Ps3ApT>

mais categorias de dados forem comprometidas, maior sua probabilidade de resultar em prejuízo, pois a vulnerabilidade do titular vitimizado pelo incidente aumenta proporcionalmente às possibilidades de combinação e análise agregada dos dados. Em adição às categorias, portanto, deve-se considerar a quantidade de registros afetados e suas possibilidades de combinação.

- *Facilidade de identificação dos titulares*: Deve-se considerar o quão facilmente o titular afetado pelo incidente poderá ser identificado por um terceiro que obtenha acesso aos dados. Essa avaliação deve considerar tanto os dados afetados em si quanto as circunstâncias do incidente, por exemplo, se os dados podem ser combinados a outros que estejam publicamente disponíveis.

- *Severidade e probabilidade de concretização do prejuízo*: Incidentes podem tornar os titulares suscetíveis a consequências de ordens extraordinariamente severas, incluindo roubo ou fraude de identidade, perdas financeiras, prejuízos reputacionais, sofrimentos psíquicos e danos à incolumidade física. A avaliação de risco ou dano decorrente de um incidente deve considerar tanto a severidade do prejuízo potencial quanto sua probabilidade de concretização. No contexto de uma violação de confidencialidade, um fator a ser considerado na análise de severidade é o nível de confiança do agente de tratamento na parte que obteve acesso indevido aos dados. Se foram enviados por engano ao departamento errado de uma organização, por exemplo, o agente pode ter um grau maior de confiança na possibilidade de eliminação dos dados por parte do destinatário. Se, por outro lado, o agente entender provável que um ator malicioso, a exemplo de um criminoso cibernético, obteve acesso às informações, ele deve presumir uma maior probabilidade de concretização de prejuízo ao titular. Ademais, todo risco ou dano cujo prejuízo potencial apresentar elevada severidade ou elevada probabilidade de concretização deve receber a qualificação imediata de "risco ou dano relevante grave", que detalharemos na resposta seguinte e que implica na obrigação de notificação ao titular.

- *Características especiais dos titulares*: É preciso considerar se o incidente afeta categorias que já se encontram em vulnerabilidade social, como crianças, idosos, mulheres, pessoas LGBT+, pessoas negras e indígenas, refugiados, pessoas de religiões de matriz africana, pessoas com deficiência, entre outros. Um incidente que resulte na exposição não-consentida de imagens íntimas provavelmente terá repercussões mais severas sobre as mulheres e pessoas trans afetadas do que sobre homens cisgêneros em virtude das dinâmicas de violência física, social e simbólica que incidem sobre tais sujeitos. Uma violação da integridade dos dados do histórico profissional de pessoas negras pode ser mais provável de prejudicá-las num processo seletivo em virtude da discriminação racial que permeia o mercado de trabalho. Similarmente, a divulgação da lista de nomes dos usuários de um aplicativo de encontros poderá ter impactos mais severos se o aplicativo for voltado a sujeitos do segmento LGBT, podendo resultar na publicização forçosa de sua identidade sexual e/ou de gênero.

- *Características especiais dos agentes*: a natureza das atividades de tratamento conduzidas pelo agente afetam desde os dados afetados, até a probabilidade

do incidente decorrer de um ataque malicioso, bem como as consequências específicas. Um órgão público que trata informações de elevada delicadeza, como um tribunal alvejado por um ataque de *ransomware* ou um Ministério que teve seu banco de dados vazado, tenderão a provocar consequências mais severas para os titulares na ocasião de um incidente.

Em síntese, **recomendamos que a relevância do "risco ou dano" decorrente de incidente de segurança que afete dados pessoais seja presumida, exceto quando os agentes de tratamento puderem demonstrar a existência de medidas capazes de assegurar que do incidente não sucederá prejuízo aos direitos ou liberdades dos titulares**.

Por fim, a eventual demonstração de que as medidas tomadas pelo agente efetivamente justificam a **desconsideração da relevância do risco ou dano é de responsabilidade do agente de tratamento, em conformidade com o princípio da responsabilização e prestação de contas da LGPD.** Recomendamos, nesse sentido, que a identificação de negligência, imprudência ou imperícia na avaliação inicial importem na determinação e/ou agravamento de eventuais sanções administrativas, posto que prejudicam as diligências referentes ao incidente e podem agravar os riscos aos direitos e liberdades do titular.

2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?

Como indicado na resposta anterior, recomenda-se a adição do qualificador grave para certas categorias de risco ou dano relevante. Tal conceito é análogo ao de "elevado risco" positivado no Art. 34, parágrafo 1, do RGPD e que culmina na obrigação de notificação aos titulares afetados. O risco ou dano relevante deve ser considerado grave nas seguintes hipóteses:

1. O incidente afetou dados sensíveis, nos termos do art. 5º, inciso II da LGPD;

2. O prejuízo potencial é altamente provável de concretização;

3. O prejuízo potencial é altamente severo, caso se concretize. Prejuízos altamente severos podem incluir roubo ou fraude de identidade, perdas financeiras, prejuízos reputacionais, sofrimento psíquico e danos à incolumidade física.

A primeira hipótese se fundamenta na distinção estabelecida pelo próprio legislador entre os níveis de proteção aplicáveis a dados pessoais em geral e aqueles reservados a certas categorias de informações pessoais - os dados sensíveis. Em razão da própria natureza, seu comprometimento é tanto mais suscetível de resultar em prejuízo aos direitos e liberdades quanto tais prejuízos podem ser mais severos, razão pela qual se encontram sujeitas a um regime protetivo substancialmente mais rígido. O universo de bases legais para seu tratamento é mais restrito, por exemplo.

A seu tempo, as hipóteses 2 e 3 se alicerçam na necessidade de assegurar a tomada de medidas de mitigação pelo titular, a exemplo de pedidos de bloqueio de cartão de crédito ou mudanças de senha. Desse modo, operam como remédios funcionais a incidentes dos quais resulta grave risco, seja por sua probabilidade ou severidade, aos direitos e liberdades dos titulares.

Quanto à instituição de uma categoria de "risco ou dano baixo", a desaconselhamos veementemente. Dado que a avaliação de risco é realizada inicialmente pelos agentes no momento em que tomam ciência do incidente e importa sobretudo na obrigação de notificar, tal categoria poderia ser instrumentalizada para evadir tal obrigação, para evitar danos reputacionais, custos operacionais de uma investigação forense completa e/ou eventuais sanções. Pelas mesmas razões, **a desconsideração da relevância do risco ou dano deve ser excepcional**.

Ainda, essa preocupação é reforçada pela consideração das especificidades do ambiente regulatório e cultural brasileiro: enquanto o RGPD entrou em vigor nem um contexto já regulado pela Diretiva 96/45/CE, nossa política nacional de proteção de dados ainda se encontra em estágio embrionário, com a entrada em vigor da LGPD bastante recente e sua observância amplamente encarada pelo setor regulado como um fardo regulatório adicional.

Nesse contexto de desconhecimento e subvalorização dos princípios e normas de proteção de dados, uma obrigação ampla de notificar incidentes pode favorecer a construção de uma cultura de proteção de dados ao incentivar os agentes de tratamento à tomada de medidas técnicas e organizacionais para garantir a segurança dos dados tratados, de modo a evitar os custos reputacionais da notificação pela redução efetiva dos riscos. Isso pode incentivar, inclusive, a valorização do investimento na segurança dos dados pessoais como um diferencial competitivo no setor privado.

3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?

Ainda que já seja estabelecida a diferença conceitual entre "risco"e "dano", consideramos que para fins de regulação da matéria específica de que trata o art. 48 a ANPD tem o condão de equipará-los, em razão das particularidades representadas por incidentes de segurança para a efetivação de um sistema de proteção aos dados pessoais.

Para fins do art. 48, risco ou dano relevante devem ser entendidos como sinônimos na medida em que neles deve se enquadrar qualquer situação decorrente de incidente que afete os dados dos titulares em que os agentes de tratamento não são capazes de demonstrar que medidas capazes de assegurar que do incidente não resulte prejuízo aos direitos e liberdades dos titulares afetados foram tomadas.

Desse modo, os conceitos de "risco ou dano relevante" e "risco ou dano relevante grave" passam a operar como equivalentes funcionais aos conceitos de "risco" e "risco elevado" do RGPD. Essa equiparação facilita a preparação dos diversos agentes a partir do conhecimento já produzido em anos de debate e consolidado em uma série de documentos de referência, além de sinalizar internacionalmente pela busca de interoperabilidade entre os sistemas legais e de harmonização dos diferentes cenários a partir de pontos comuns.

Ademais, a equiparação dos termos risco e dano para os fins do art. 48 encontra justificação teórica se examinamos os métodos de avaliação desenvolvidos no campo jurídico da responsabilidade civil. Quanto a este ponto, atenção especial deve ser dada aos casos que envolvam consumidores.

É de simples constatação que um incidente de segurança pode causar aos titulares danos patrimoniais, extrapatrimoniais/morais e coletivos. A partir disso, a questão do dano extrapatrimonial deve ser melhor analisada quanto a sua definição e comprovação.

Para Schreiber, a definição de dano extrapatrimonial pode ser traduzida como a lesão a um interesse merecedor de tutela, tendo o réu[8] agido de forma a trazer risco aos interesses do afetado que são tutelados juridicamente (p. ex. direitos da personalidade, privacidade, proteção dos dados pessoais, etc).[9] Assim, verifica-se que o dano extrapatrimonial pode ser intrínseco a determinadas atividades de um agente. Nesse sentido, o Superior Tribunal de Justiça (STJ) se manifesta:

> "Como se trata de algo imaterial ou ideal, a prova do dano moral não pode ser feita através dos mesmos meios utilizados para a comprovação do dano material. Por outras palavras, o dano moral está ínsito na ilicitude do ato praticado, decorre da gravidade do ilícito em si, sendo desnecessária sua efetiva demonstração, ou seja, como já sublinhado: o dano moral existe *in re ipsa*".[10]

Com base na definição de dano extrapatrimonial elencada acima, podemos analisar brevemente como ela se aplicaria a um caso hipotético de incidente de segurança. Suponhamos que uma base de dados pessoais (nome, filiação, endereço, RG, CPF, conta bancária, dependentes, empréstimos feitos, profissão) de uma empresa de empréstimo foi acessada sem autorização por terceiros. Verificou-se que uma cópia dos dados foi extraída e que a empresa não adotava práticas de segurança adequadas e proporcionais. Contudo, não foi possível confirmar se esses dados foram postos à venda ou mesmo se foram utilizados ilicitamente (p. ex. fraudes), entre o período de tempo da notificação do incidente e a conclusão das investigações.

Pela definição de dano extrapatrimonial elencada acima, o próprio ato de violação da segurança das informações configura um dano, porque viola interesses dos titulares tutelados juridicamente como, por exemplo, o direito à privacidade e à autodeterminação informativa. Ademais, as circunstâncias do caso (invasão e cópia deliberadas das informações) levam ao entendimento de que é alto o suficiente o risco de que os dados possam ser usados ilicitamente. Isso impõe uma situação de incerteza aos titulares e gera a necessidade de adotarem precauções adicionais (p. ex. verificar regularmente sua nota de crédito, modificação de senhas, contratação não autorizada de serviços, retificação de dados) por período longo ou até mesmo indeterminado. Acerca desse último ponto, destaca-se ainda, que os riscos tendem a crescer conforme novas técnicas e formas de análise e exploração dos dados são desenvolvidas e se tornam disponíveis a atores maliciosos.

Em síntese**, ao serem expostos a uma situação de maior risco, há constatação de dano aos titulares pelas novas necessidades impostas de precaução e verificação constantes para detectar e mitigar eventual uso indevido de seus dados**. Esse raciocínio aplica-se especialmente aos casos em que não seja fácil: i) verificar tecnicamente como os dados foram afetados (se houve ou não cópia); e ii) se estes foram utilizados ilicitamente após o incidente.

Por essas razões, conclui-se que o incidente de segurança do qual sucede risco de prejuízo particular, como fraudes de identidade ou danos reputacionais, já configura uma espécie de prejuízo geral aos direitos e liberdades do titular afetado. Tal prejuízo geral se concretiza em três elementos:

8 Utilizaremos o termo "réu" para nos referir aos agentes de tratamento responsáveis por garantir a segurança da informação.

9 SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil** - Da Erosão dos Filtros da Reparação à Diluição dos Danos. São Paulo: Editora Atlas. 3ª Edição. 2011. p. 204.

10 BRASIL. Superior Tribunal de Justiça (1ª Turma). **Recurso Especial 608.918/RS**. 25/05/2004. Disponível em: <https://bit.ly/3tqe3kC>. Acesso em: 18/03/2021.

1. A violação direta à privacidade e à autodeterminação informativa, manifesta na ausência de medidas de segurança eficazes para impedir a concretização dos prejuízos concretos e particulares;

2. A incerteza e aflição impostas aos cidadãos vitimizados pelo incidente, que não podem gozar da segurança mental de saber que seus dados não estão sendo utilizados de forma indevida;

3. A necessidade, decorrente dessa insegurança, de tomar medidas de precaução, mitigação e verificação desses usos indevidos, o que implica em custos de tempo e esforço.

A título comparativo, a definição de risco e dano também tem sido intensamente debatida nos tribunais federais dos Estados Unidos. Apesar das diferenças entre os sistemas jurídicos do *common* e *civil law*, e das especificidades do direito estadunidense, vale mencionar como os conceitos de risco e dano estão sendo analisados naquele contexto, a fim de considerar reflexões produzidas naquele contexto e que podem beneficiar o debate nacional.

Atualmente não há um consenso doutrinário ou jurisprudencial sobre o tema nos EUA. Contudo, alguns tribunais e certos juristas de renome na área de proteção de dados (p. ex. Daniel Solove e Danielle Citron[11]) têm entendido que o risco gerado por um incidente de segurança da informação que afete dados pessoais (*data breach*) também se traduz em dano aos titulares afetados. Este argumento é construído em parte ao se analisar como um número expressivo de incidentes têm afetado as vítimas, principalmente os de violação de confidencialidade. Como os dados violados são geralmente usados para fraudes e roubo de identidade, há um aumento de risco expressivo após o incidente que coloca os titulares em situação pior daquela em que se encontravam anteriormente, o que configura um dano.

As cortes nos EUA identificam em casos de incidente que, normalmente, os titulares afetados acabam sendo forçados a tomar providências para evitar fraudes em seu nome; sofrem de ansiedade gerada pelos riscos de uso indevido; sofrem maior risco de terem impactos negativos em suas notas de crédito, o que afeta sua capacidade de realizar empréstimos (p. ex. comprar um imóvel, abrir um negócio etc.); entre outras consequências. A título ilustrativo, o Departamento de Justiça dos EUA estimou que 26 milhões de residentes nos EUA sofreram roubo de identidade em 2016.[12]

O entendimento que o risco gerado por um incidente de segurança também gera dano aos afetados têm sido adotados pelos tribunais recursais do Sexto, Sétimo e Oitavo Circuitos Federais dos EUA.[13] A lógica do risco como um dano pode ser

11 "In our view, anxiety, and risk, together and alone, deserve recognition as compensable harms. [...] The number of people affected by data breaches continues to rise as companies collect more and more personal data in inadequately secured data reservoirs [38]. Risk and anxiety are injuries in the here and now. Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage. Once victims learn about breaches, they may be chilled from engaging in activities that depend on good credit, like house [...]". SOLOVE, Daniel J.; e CITRON, Danielle Keats. **Risk and Anxiety**: A Theory of Data Breach Harms. GWU Legal Studies Research Paper No. 2017-2. 2017. pp 744-745. Acesso em:24/03/2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638. pp 744-745

12 ESTADOS UNIDOS. HARRELL, Erika. U.S. Department of Justice. Victims of Identity Theft, 2016. Acesso em 24/03/2020. Disponível em: https://bit.ly/31fcv0F

13 Nos EUA, existem três instâncias de Justiça Federal: **(i)** a primeira instância é a "United States District Court"; **(ii)** a segunda instância "United States Court of Appeals", também chamados de "Circuit Courts"; e **(iii)** a última instância referente a "Supreme Court of the United States"

exemplificada por um julgado do 7º Circuito, relacionado a um caso de invasão de sistema de um restaurante onde dados cadastrais e de cartão de crédito de clientes foram obtidos ilicitamente:

> "O aumento do risco de haver cobranças fraudulentas e de haver roubo de identidade decorre do fato de seus dados terem sido roubados. As lesões alegadas são concretas o suficiente para garantir sua legitimidade processual. [...] É plausível inferir um risco substancial de dano originado do incidente de segurança [data breach], porque um dos principais incentivos dos hackers é '*mais cedo ou mais tarde [] fazer cobranças fraudulentas ou roubar as identidades dos consumidores afetados*'"[14] (tradução nossa)

Adicionalmente, os tribunais que compõem esses circuitos têm entendido como dano: (**i**) os gastos com serviço de monitoramento contra fraudes; e (**ii**) os demais custos incorridos na tentativa de remediar o incidente (p. ex. tempo gasto com cancelamento de cartões de crédito, com a verificação de compras suspeitas, fechamento e abertura de novas contas bancárias)[15].

Desse modo, percebe-se como a interpretação jurídica de incidentes de segurança da informação tem sido um desafio para diversos ordenamentos, trazendo questões semelhantes - como em relação a definição de dano e risco - e produzindo, até mesmo, entendimentos similares sobre o tema.

Assim sendo, entende-se razoável equiparar risco e dano para os fins da matéria tratada pelo art. 48. da LGPD.

4. O que deve ser considerado na avaliação dos riscos do incidente?

A avaliação de risco deve considerar os critérios indicados na resposta à pergunta 1. Adicionalmente, recomenda-se a consideração de critérios utilizados por outras autoridades nacionais de proteção de dados, a exemplo da Comissão de Privacidade do Canadá[16]. Também deve ser levado em conta o histórico de violações já analisadas pela ANPD – considerada a evolução do estado da arte em metodologias de gestão de incidentes de segurança –, a fim de preservar a consistência de suas decisões e criar previsibilidade para o cenário regulatório de proteção de dados no país.

5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?

Quanto às informações listadas na lei, indicamos que a ANPD detalhe as informações contempladas pelos incisos do §1º do art. 48, de forma que: a descrição

14 "the increased risk of fraudulent charges and identity theft they face because their data has already been stolen. These alleged injuries are concrete enough to support a lawsuit. P.F. Chang's acknowledges that it experienced a data breach in June of 2014. It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is "sooner or later [] to make fraudulent charges or assume those consumers' identities[.]". ESTADOS UNIDOS. United States Court of Appeals for the 7th Circuit. Lewert v. P.F. Chang's China Bistro, Inc, No. 14-3700. 2016. p.6. Acesso em: 24/03/2021. Disponível em: https://bit.ly/31giPVO.

15 DOWTY, Megal. Life is Short, Go to Court: Establishing Article III Standing in Data Breach Cases. Southern California Law Review, Vol. 90, nº 3. março de 2017. p.687. Disponível em: https://bit.ly/3rkEt5G. Acesso em: 19/02/2019.

16 CANADÁ. Escritório da Comissão de Privacidade do Canadá. **What you need to know about mandatory reporting of breaches of security safeguards**. Outubro, 2018. Disponível em: <https://bit.ly/2P2qLYd>. Acesso em: 23/03/20201.

e natureza dos dados (inciso I) contemple a indicação de categorias de registros tratados, se são relativos à saúde, registros escolares, financeiros, etc., por exemplo; as informações sobre os titulares (inciso II) incluam categorias de titulares afetados e indiquem se há segmentos sociais vulneráveis afetados, conforme recomenda o Grupo de Trabalho sobre o Artigo 29[17]; as informações sobre riscos relacionados ao incidente (inciso IV) indiquem se algum tipo de prejuízo específico é suscetível de ocorrer, como fraude no cartão de crédito, a partir dos registros e titulares afetados.

Além disso, consideramos que os controladores **devem notificar à ANPD o nome e o contato do encarregado (caso a organização o tenha) ou outro ponto de contato por meio do qual informações possam ser obtidas**. Essa recomendação é análoga à previsão contida no art. 33, parágrafo 3 do RGPD da UE. Adicionalmente, **devem informar data e hora aproximadas do incidente, bem como do momento em que o agente de tratamento tomou ciência dele**. A inclusão dessas informações visa facilitar as diligências relativas ao incidente e a avaliação das medidas de contingência tomadas pelo agente em resposta.

6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)

A regra geral para notificação de um incidente de segurança deve ser em prazo mais rápido possível, ou seja, não pode haver demora injustificada. Importante apontar que isso deve se aplicar tanto à comunicação do incidente quanto à ação por parte da própria ANPD. Nesse sentido, recomenda-se a formulação de um regime de comunicação emergencial para incidentes de alta gravidade, que deve operar inclusive durante feriados e finais de semana.

Além disso, recomenda-se que a ANPD estabeleça prazos conforme a gravidade do incidente de segurança. Assim, **quanto maior o risco aos titulares de dados, mais rápida deve ser a notificação**. O parâmetro de 72h como limite para notificação, a exemplo do que considera o RGPD também parece se aplicar de forma adequada ao cenário brasileiro.

O termo inicial do prazo deve ser quando o responsável pelo tratamento tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais. Da mesma forma, a notificação não deve ser realizada apenas ao final da investigação sobre o incidente ou depois de tomadas as medidas de segurança. Isso porque a avaliação completa pelo agente poderá ser realizada em paralelo às medidas estabelecidas pela ANPD, que deverá acompanhar a progressão da investigação.

7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?

A regra geral para notificação de um incidente de segurança deve ser em prazo mais rápido possível, ou seja, não pode haver demora injustificada. A ANPD deve estabelecer prazos conforme a gravidade do incidente de segurança. Assim, quanto maior o risco aos titulares de dados, mais rápida deve ser a notificação, observado o limite de 72h, como se sugere aplicar à ANPD.

17 WP29 - **Guidelines on Personal data breach notification under Regulation 2016/679.** 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em 23/03/2021, p. 15.

Além das informações definidas pelo §1º do art. 48 da LGPD, a notificação aos titulares deve incluir **os dados pessoais tratados pelo agente que não foram afetados pelo incidente e incluir canal de comunicação[18] para atendimento aos titulares.** Isso considera a necessidade de que a população em geral faça parte da construção de uma cultura de proteção de dados pessoais que o Brasil procura alcançar. A inclusão dessa informação pode contribuir ainda para evitar repercussões desproporcionais ou equivocadas ao incidente.

Entre as informações listadas, vale destacar a orientação de auxiliar os titulares em relação a quais medidas eles podem tomar para se proteger do incidente.

8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?

A comunicação pode se dar por múltiplas formas, que incluem o envio individual de mensagens diretas ou a exibição de faixas ou notificações em sites ou plataformas de elevada visibilidade[19]. Deve ser dada preferência aos meios mais ágeis de comunicação aos titulares. Nesse sentido, meios de comunicação impressos e comunicação postal podem ser utilizados na impossibilidade do titular ser alcançado por outras vias. A depender do caso, múltiplos meios podem se fazer necessários.

O conteúdo das notificações deve estar escrito de forma acessível e compreensível aos titulares, o que exige linguagem nítida e uso da língua portuguesa.

No caso de mensagens diretas, estas podem ser feitas por e-mail, SMS ou plataformas de mensageria e devem ser realizadas de forma específica, ou seja, não podem ser enviadas junto de outras informações (ex: atualizações comuns, boletins informativos, etc).

Não seriam consideradas notificações adequadas, por exemplo, emissões de comunicados de imprensa ou publicações em blogs empresariais de baixa visibilidade.

9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?

Cabe salientar que a comunicação, ainda que por etapas, é a regra geral para que a ANPD possa validar o juízo de relevância do incidente e tomar as providências que garantam a efetiva proteção dos dados pessoais. Essa obrigação dos agentes deve ser afastada apenas quando o agente puder demonstrar que foram adotadas, preventiva ou reativamente, medidas técnicas e/ou organizacionais capazes de assegurar que o prejuízo potencial resultante do incidente não se concretizará.

Isso pode ser aplicável, a depender do caso, quando os dados afetados pelo incidente já eram considerados públicos ou quando, com base em padrões técnicos, seja possível assegurar que a disponibilidade e integridade dos dados

18 ESTADOS UNIDOS. Federal Trade Commission. **Data Breach Response:** A Guide for Business. 2019. Disponível em: https://bit.ly/3rdPhCV. Acesso em: 20/03/2021.

19 WP29 - **Guidelines on Personal data breach notification under Regulation 2016/679.** 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em 23/03/2021. p.22.

não foram afetadas, ainda que o outro atributo de segurança da informação, a confidencialidade, tenha sido comprometido. Este é o caso, por exemplo, de violações de confidencialidade de dados tornados ininteligíveis de forma segura (com criptografia forte, por exemplo, cuja chave criptográfica não foi comprometida) e existem cópias seguras dos dados. Mesmo assim, se houver comprometimento posterior de tais padrões de segurança, fica o agente obrigado a notificar a ANPD.

A exceção baseada na robustez das práticas de segurança da informação pode representar, igualmente, incentivos para a utilização de sistemas cada vez mais protetivos e reforçar a importância da adoção de medidas técnicas adequadas ao tratamento dos dados pessoais.

10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?

Com base no exposto previamente, identificamos três cenários em que é razoável desobrigar o agente de tratamento do dever de notificação ao titular.

O primeiro deles corresponde à inexistência de risco ou dano grave ao titular. Essa inexistência é constatada pela demonstração, por parte dos agentes de tratamento, de que o incidente não atingiu dados sensíveis e de que o prejuízo potencial que dele sucede é improvável de se concretizar e pouco severo, caso se concretize. O insucesso em demonstrar a ocorrência de qualquer um desses três requisitos deve ser suficiente para o enquadramento do risco ou dano resultante do incidente como grave e acionamento da obrigação de notificação aos titulares.

O segundo cenário corresponde mais a um afastamento temporário ou parcial da obrigação de notificação. Ele diz respeito à recepção, pelos agentes, de orientações expressas para não notificar os titulares por parte da ANPD. Isto pode ocorrer no contexto de violações que atinjam dados relevantes para investigações criminais ainda em curso, por exemplo, em que pese a necessidade de verificação da aplicabilidade da LGPD no caso concreto. Nesses casos, a ANPD deve justificar suas orientações à luz dos riscos que a realização da notificação pode gerar para a condução das investigações e com base em padrões técnicos bem definidos. Alternativamente, a ANPD pode orientar o agente a realizar uma notificação parcial que exclua as informações que não possam ser compartilhadas naquele momento, porém comunique o titular das demais. Em todos os casos, tão logo cesse o risco decorrente da realização de notificação completa, a obrigação de notificar se torna aplicável novamente e os agentes deverão observá-la. Recomenda-se que a ANPD delimite rigorosamente as hipóteses em que tais orientações poderão ser emitidas.

Por fim, o terceiro cenário se refere à incapacidade operacional do agente para o cumprimento do dever de notificação ao titular. Esse seria o caso, por exemplo, de violações à disponibilidade e/ou à integridade dos dados que comprometam o conhecimento do agente sobre a identidade dos titulares afetados. Um incêndio que provocou a destruição de documentos físicos contendo dados pessoais dos quais não havia cópias pode ter precisamente tais repercussões, que tornam efetivamente impossível a operacionalização da notificação individualizada. Assim como no segundo caso, o afastamento da obrigação de notificação deve ser apenas parcial, de modo que o agente reste compelido a notificar os titulares presumidos por outros meios cabíveis, como publicações em sites e/ou plataformas de elevada visibilidade. A notificação, nesses casos, deve informar quais categorias de titulares o agente presume terem sido afetadas – por exemplo, pessoas nascidas em uma cidade particular entre as datas x e y.

11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)

Recomenda-se a realização da análise da gravidade de incidentes com base em metodologias já consolidadas para gestão de riscos em organizações. Algumas dessas metodologias cuja observância é recomendável serão enumeradas na resposta ao tópico 12.

Critérios específicos para essa análise podem incluir, por exemplo:

- O contexto da atividade de tratamento de dados, observada a natureza dos dados envolvidos no incidente, sua vulnerabilidade e potencialidade para repercutir em eventos danosos para titulares de dados;
- A sensibilidade dos dados envolvidos no incidente;
- A facilidade de identificação dos titulares de dados a partir das informações envolvidas no incidente em questão;
- As circunstâncias do incidente, por exemplo, se os dados foram comprometidos de forma dolosa;
- A probabilidade de que o incidente repercutirá em uso não autorizado dos dados comprometidos;
- A adoção ou não de medidas de contingenciamento reativas, pelos agentes de tratamento, de forma que as consequências do incidente sejam anuladas, cessadas ou, ao menos, minimizadas;
- O número de titulares cujos dados foram envolvidos no incidente em questão;
- Características específicas ligadas ao titular de dados, por exemplo, quando dados de crianças ou de grupos de indivíduos vulneráveis estão envolvidos no incidente;
- Entre outros.

12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?

Existem diversas metodologias para análise de incidentes de segurança, de modo que sugerimos que a ANPD se apoie no estado da arte relativo à segurança da informação e incidentes de segurança.

A título de exemplo do que já foi introduzido para o cenário brasileiro, a ABNT NBR ISO/IEC 27001 – relativa a técnicas de segurança em sistemas de gestão de segurança da informação – remete à ISO/IEC TR 13335-3 sobre metodologias para análise e avaliação de risco. Na mesma linha encontra-se a ISO/IEC 27005:2011, que foi criada para substituir a ISO/IEC TR 13335-3. Ambas foram validadas e possuem relevância internacional para gestão de riscos em atividades de tratamento de dados pessoais.

Adicionalmente, como a família de padrões ISO 27000 refere-se especificamente ao ambiente de tecnologia da informação em uma organização, pode-se citar também a ISO/IEC 31000:2018, para gestão de riscos de natureza mais geral.

Além disso, as recomendações da ENISA[20], embora publicadas no ano de 2013, ainda representam um bom referencial para a constituição de uma metodologia de análise da gravidade de incidentes de segurança. Essa metodologia considera como fatores principais o contexto do tratamento de dados (tipo de dado afetado, por exemplo), a facilidade de identificação dos titulares e as circunstâncias do incidente (atributos de segurança afetados e existência de dolo na violação).

Essas são possíveis fontes de metodologia que, integradas e aplicadas no que é pertinente ao sistema brasileiro de proteção de dados pessoais, podem auxiliar a definição da metodologia própria da ANPD, a partir dos parâmetros oferecidos nesta Tomada de Subsídios.

13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?

Sugestões de Providências

Considerando a finalidade de prevenção e mitigação de danos, seguem algumas sugestões de providências.

- Definição de uma política/plano de resposta a incidentes de segurança da informação.
- Estabelecimento de políticas de segurança com previsão de realização de treinamentos regulares com os colaboradores.
- Notificar os demais agentes de tratamento que possam ter sido afetados, a fim de que eles possam tomar providências adequadas de mitigação do incidente.
- Estabelecimento de canal de contato específico para os titulares afetados por um incidente.
- Aconselhar os titulares afetados sobre quais medidas adicionais eles podem adotar para mitigar/impedir os riscos e danos (p. ex. troca de senha; verificar se houve transações suspeitas, etc).
- Fornecer seguro contra fraudes para os titulares afetados.

Em relação às providências exigidas pela ANPD, é recomendável que ela estabeleça um prazo de adoção de medidas para o agente. Nesse sentido, deve-se exigir que o agente comprove à ANPD que adotou as medidas necessárias após transcorrido o prazo (p. ex. através de envio de documentos comprobatórios, como no caso de políticas internas, contratação de serviços de consultoria, etc).

Manutenção dos Registros de Incidentes

Uma prática que deve ser exigida dos agentes de tratamento - e que deve ser verificada pela ANPD após a ocorrência de um incidente - é a manutenção de registros dos incidentes de segurança que afetam dados pessoais. Esses registros

20 ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches**: working document, v1.0, december 2013. Heráclitón: Enisa, 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em: 23/03/2021.

também devem conter, necessariamente, casos nos quais os agentes concluíram que não seria necessário uma notificação à ANPD e/ou titulares.

Essa exigência é inferida da própria LGPD, pelo princípio da responsabilização e prestação de contas (art. 6, X), e pela própria lógica do mecanismo de notificação de incidentes relevantes.

Considerando que a LGPD estabelece que somente incidentes relevantes devem ser notificados, a primeira análise de risco será realizada pelo próprio agente de tratamento. Assim, ocorrerão casos em que um incidente, a princípio, foi considerado como não relevante para fins de notificação, mas que desenvolvimentos futuros levem a constatação de que, na verdade, o incidente causou riscos ou danos consideráveis aos titulares envolvidos (p. ex. resultados mais precisos de uma investigação). Ainda, pode haver casos em que a materialização de parte do risco/dano ocorre somente após o incidente.

Citamos como exemplo, um caso hipotético em que uma empresa X constatou invasão ao seu banco de dados por agente externo, contudo, não foi possível confirmar se houve ou não exfiltração dos dados pessoais. Após o incidente, houve reportagem midiática sobre a venda ilegal de banco de dados que teria como possível origem a empresa X. Em situações semelhantes a essa, a ANPD deve verificar se as análises de risco realizadas pela empresa X foram feitas de forma adequada, a fim de confirmar se a decisão do agente de não informar estava baseada em uma análise de risco/dano consistente com a LGPD e com as informações disponíveis no momento.

Ou seja, considerando a natureza complexa que caracteriza parte dos incidentes de segurança da informação e as dificuldades forenses de uma investigação, um *assessment* inicial pode não constatar os riscos e danos relevantes que justificariam uma notificação, mas que podem ser descobertos ou vir a se materializar posteriormente. Assim, a exigência de manutenção de registros de incidentes de segurança da informação que afetam dados pessoais, **independentemente da gravidade**, é um incentivo para que os agentes não realizem análises inadequadas e negligentes para não terem de realizar uma notificação.

Sob viés comparativo, a manutenção de registros de incidentes de segurança da informação é exigida no RGDP (art. 33, (5)), o qual estabelece que qualquer incidente de segurança que afete dados pessoais deve ser registrado pelo agente de tratamento; principalmente em relação aos fatos, os efeitos gerados e as ações de resposta/mitigação tomadas. A legislação de proteção de dados do Canadá também exige que os responsáveis pelo tratamento mantenham registros de todos os incidentes de segurança da informação que afetam dados pessoais; os quais podem ser requisitados pela agência reguladora.[21]

21 Artigos 10.3(1) e (2), Division 1.1. CANADÁ. **Personal Information Protection and Electronic Documents Act**. 2000. Disponível em: <https://bit.ly/2QgeZto>. Acesso em: 20/03/2021.

REFERÊNCIAS

BESSA, Leonardo Roscoe.Responsabilidade objetiva no Código de Defesa do Consumidor. **Revista Jurídica da Presidência** Brasília v. 20, nº 120. Fev./Maio 2018 p. 27.Disponível em: <https://bit.ly/3tHrYCR>. Acesso em 21/03/2021.

BRASIL. **Lei nº 12.414**, de 9 de junho de 2011 (Lei do Cadastro Positivo). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 24/03/2021.

BRASIL. Superior Tribunal de Justiça (1ª Turma). **Recurso Especial 608.918/RS. 25/05/2004.** Acesso em: 18/03/2021. Disponível em: <https://bit.ly/3tqe3kC>

CANADÁ. **Personal Information Protection and Electronic Documents Ac**t. 2000. Disponível em: <https://bit.ly/2QgeZto>. Acesso em: 20/03/2021.

CANADÁ. Escritório da Comissão de Privacidade do Canadá**. What you need to know about mandatory reporting of breaches of security safeguards**. Outubro, 2018. Disponível em: <https://bit.ly/2P2qLYd>. Acesso em: 23/03/20201.

DOWTY, Megal. Life is Short, Go to Court: Establishing Article III Standing in Data Breach Cases. **Southern California Law Review**, Vol. 90, nº 3. março de 2017. p.687. Disponível em: https://bit.ly/3rkEt5G. Acesso em: 19/02/2019.

EDPD. **European Data Protection Board's Guidelines 01/2021 on Examples Regarding Data Breach Notification.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf>. Acesso em: 24/03/2021.

ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches**: working document, v1.0, december 2013. Heráclitón: Enisa, 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em: 23/03/2021.

ESTADOS UNIDOS. HARRELL, Erika. U.S. **Department of Justice**. Victims of Identity Theft, 2016. Acesso em 24/03/2020. Disponível em: <https://bit.ly/31fcv0F>

ESTADOS UNIDOS. Federal Trade Commission. **Data Breach Response:** A Guide for Business. 2019. Disponível em: <https://bit.ly/3rdPhCV>. Acesso em: 20/03/2021.

ESTADOS UNIDOS. **United States Court of Appeals for the 7th Circuit**. Lewert v. P.F. Chang's China Bistro, Inc, No. 14-3700. 2016. p.6. Acesso em: 24/03/2021. Disponível em: <https://bit.ly/31giPVO>.

ICO. **ICO Guide to the General Data Protection Regulation - Personal Data breaches**. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whendowe>. Acesso em: 24/03/2021.

ISO. **ISO IEC 27005:2008** - Information Technology - Information Security Risk Management.

SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil** - Da Erosão dos Filtros da Reparação à Diluição dos Danos. São Paulo: Editora Atlas. 3ª Edição. 2011. p. 204.

SOLOVE, Daniel J.; e CITRON, Danielle Keats. **Risk and Anxiety**: A Theory of Data Breach Harms. GWU Legal Studies Research Paper No. 2017-2. 2017. pp 744-745. Acesso em:24/03/2021. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638>.

TARTUCE, Flávio; e NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**. São Paulo: Editora Forense. 5ª edição. 2016.

WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business & Society**, Vol. 58(I). 2019. p. 23. Disponível em: <https://bit.ly/3cSsWW5>. Acesso em: 21/03/2021.

WP29 - Guidelines on Personal data breach notification under Regulation 2016/679. 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em: 24/03/2021.

ZANATTA, Rafael A. F. Artigos Selecionados REDE 2017 **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro. 14/11/ 2017.p. 184. Disponível em: <https://bit.ly/2Ps3ApT> . Acesso em: 24/03/2021.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE