Contribuição Data Privacy Brasil

Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais

Ficha técnica

Associação de Pesquisa Data Privacy Brasil
Direção: Bruno Bioni e Rafael Zanatta
Coordenação Geral de Projetos: Marina Meira e Vinicius Silva

Data Privacy Brasil Ensino
Fundadores: Bruno Bioni e Renato Leite Monteiro
Direção: Bruno Bioni
Coordenação Acadêmica: Pedro Bastos Lobo Martins
Coordenação Comunicação e Marketing: Victor Barcellos

Autoria:
Pedro Bastos Lobo Martins
Pedro Henrique M. Santos

Projeto gráfico e diagramação:
Roberto Junior

Índice

Introdução

No dia 2 de Maio de 2023, a Autoridade Nacional de Proteção de Dados iniciou o processo de consulta pública de uma atividade extremamente importante: a comunicação de incidentes de segurança com dados pessoais. A comunicação de incidentes é crucial na proteção de dados pessoais pois visa proteger os titulares de dados ao mesmo tempo que representam uma postura de prestação de contas pelos agentes de tratamento, o que revela o peso de tal regulamentação.

A consulta pública ficou aberta até o dia 15 de Junho e o Data Privacy Brasil, em sua missão de colaborar para o debate público sobre proteção de dados pessoais, publiciza sua contribuição por meio do presente documento contendo uma sistematização dos principais pontos cobertos em sua participação na consulta que podem ser resumido em três principais pontos: 1 - **Critérios para definição de incidente que possa acarretar risco ou dano relevante aos titulares**; 2 - **Critérios que disparam o dever de comunicação para a ANPD e Titulares de dados afetados** e 3 - **Elementos obrigatórios na comunicação do incidente de segurança**.

Boa leitura!

1. Critérios para definição de incidente que possa acarretar risco ou dano relevante aos titulares

A abordagem adotada pelo artigo em relação aos critérios para a definição de riscos ou danos relevantes é notavelmente restritiva, o que demanda uma avaliação mais aprofundada. Isto pois a redação do artigo induz a uma análise do risco e dano baseado em possibilidades e categorias pré-estabelecidas, em outras palavras, sugerem uma análise em abstrato, a partir do incidente de segurança para fins de comunicação. Por conta disso, a avaliação do que é risco ou dano relevante fica prejudicada e com limitações significativas, uma vez que a utilização de determinados dados é intrinsecamente imprevisível, ainda mais no decorrer do tempo onde novas aplicações e usos podem surgir.

A legislação brasileira adota o princípio da neutralidade tecnológica também na regulação de novas tecnologias, como se pode observar nas disposições do Marco Civil da Internet (lei 12.965/14) e da Lei Geral de Proteção de Dados (lei 13.709/18). Ambas legislações criam regras, deveres e direitos a partir dos criterios de funcionalidade e consequência. A LGPD ao definir o que é um processo de anonimização, por exemplo, não estabelece quais técnicas ou meios devem ser usados para alcançar a anonimização, preocupando-se em definir parâmetros que orientam a análise de se um dado perdeu a possibilidade de ser associado a um indivíduo. Nota-se, ainda, que a LGPD é cautelosa de estabelecer também um critério temporal "III - dado anonimizado: dado relativo a titular que não possa ser identificado, **considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento**;", uma vez que a evolução tecnológica pode permitir novos usos de dados que permitam a reidentificação do titular.

Nesse sentido, o art 5º da proposta de regulamento de comunicação de incidente de segurança com dados pessoais viola o princípio da neutralidade tecnológica estabelecendo, de forma pré-definida, um conjunto específico de dados pessoais que ocasionariam alto risco ao titular de dados em caso de um incidente. Evoluções tecnológicas podem rapidamente permitir novos usos de dados que gerariam um alto risco ao titular. Ainda, abre-se uma disputa para a inclusão e ou exclusão de novos tipos de dados nesse rol que torna mais complexo a atividade regulatória da ANPD e aumenta a insegurança jurídica para os agentes de tratamento e titulares.

Além disso, esse conjunto de dados definido pelo art. 5º já se encontra defasado e não prevê usos de dados que atualmente já são possíveis de ocasionarem dano ou alto risco ao titular em caso de um incidente. Tomemos como exemplo a informação de geolocalização, a qual possibilita uma vasta gama de inferências sobre um usuário, como profissão, laços familiares, hábitos (inclusive de saúde) sem que seja possível delimitar previamente todas as suas potenciais utilizações. Note que nesta categoria de dados pessoais triviais, uma série de outros

dados podem ser extraídos e utilizados com diferentes graus de risco para o titular, incluindo o caso de inferências sensíveis.

De acordo com a atual minuta, um incidente de segurança que envolvesse dados de geolocalização e colocasse em risco algum direito fundamental do titular não geraria o dever de comunicação uma vez que essa categoria de dados não está listada como requisito para o dever de comunicar. Nessa situação a atual regulação pode desproteger titulares em casos onde os riscos a seus direitos são relevantes.

Além de desfavorecer os titulares de dados, essa abordagem restritiva cria uma discrepância no contexto internacional, afastando o Brasil das práticas regulatórias adotadas pelos demais países. Esse é um dos intuitos de uma norma como essa, como consta na Análise de Impacto Regulatório quando ela busca considerar a experiência internacional na construção da proposta de regulamentação[1].

No guia do **European Data Protection Board (EDPB)** sobre o tema, vemos que a análise do risco de um incidente para fins de comunicação tem um direcionamento distinto.

De acordo com o EDPB, a avaliação de risco em situações de incidentes de segurança é diferente do Relatório de Impacto à Proteção de Dados. Isto pois a análise do DPIA é a de um risco em um evento hipotético onde se avalia a probabilidade e os potenciais danos de um incidente de segurança, ou seja, uma análise em abstrato[2].

No caso de um incidente atual, o evento já aconteceu e devem ser consideradas as circunstâncias em específico do incidente junto dos potenciais impactos e possíveis riscos ocasionados por ele[3]. Esse entendimento é o mesmo do guia da Article 29[4] sobre o tema que, inclusive, foi citado no AIR da proposta de nova regulamentação[5].

---

1 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Análise de Impacto Regulatório: construção do modelo regulatório para comunicação e tratamento de incidentes de segurança**. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-publica-sobre-norma-de-comunicacao-de-incidente-de-seguranca-com-dados-pessoais/aircomunicacaodeincidentes.pdf. Acesso em 25/05/2023. p. 32.

2 EUROPEAN DATA PROTECTION BOARD. **Guidelines 9/2022 on personal data breach notification under GDPR**. 2023. Disponível em: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf. Acesso em: 25/05/2022. p. 23-24.

3 Ibid. p. 24.

4 ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679**. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/redirection/document/49827 . Acesso em: 25/05/2022. p. 23-24.

5 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **op.cit.** p. 20.

Uma vez que a análise precisa ser feita a partir das circunstâncias do incidente, os critérios que o EDPB e Article 29 consideram são mais flexíveis na análise de incidentes distintos. São eles: **1)** O tipo de incidente ocorrido; **2)** A natureza, a sensibilidade e o volume de dados pessoais envolvidos; **3)** A facilidade de reidentificação dos titulares dos dados; **4)** A gravidade das consequências para os titulares afetados; **5)** Características especiais dos titulares, como no caso de envolver crianças; **6)** Características especiais do controlador de dados; **7)** O número de pessoas afetadas pela violação. **8)** Elementos gerais[6]. Estes elementos não estão restritos ao EDPB ou ao A29, eles também são mencionados nos guias da AEPD[7], CNIL[8].

Além disso, o artigo em discussão leva a conclusões distintas a certos casos em relação ao cenário internacional. Em um exemplo dado pelo EDPB:

> Um grupo de seguros oferece seguros de automóveis. Para isso, envia regularmente por correio postal apólices de contribuição ajustadas. Além do nome e endereço do segurado, a carta contém o número de registro do veículo sem dígitos mascarados, as taxas de seguro do ano atual e do próximo ano, a quilometragem anual aproximada e a data de nascimento do segurado. Dados de saúde de acordo com o Artigo 9 da GDPR, dados de pagamento (dados bancários), dados econômicos e financeiros não estão incluídos.
>
> As cartas são embaladas por máquinas de envelopamento automatizadas. Devido a um erro mecânico, duas cartas de segurados diferentes são inseridas em um único envelope e enviadas a um segurado por correio. O segurado abre a carta em casa e dá uma olhada em sua carta corretamente entregue, bem como na carta incorretamente entregue de outro segurado[9].

No caso em questão, há o risco ao direito fundamental à privacidade do titular que teve sua carta enviada erroneamente. Isso incide sobre o primeiro critério para a definição de um risco ou dano relevante conforme a proposta de regulamentação (**potencial de afetar significati-**

6 EUROPEAN DATA PROTECTION BOARD. **op.cit.** p.24-26.

7 AGENCIA ESPAÑOLA PROTECCIÓN DATOS. Guía para la notificación de brechas de datos personales. 2021. Disponível em: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf. Acesso em: 25/05/2022.p.17

8 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **op.cit.** p. 26.

9 EUROPEAN DATA PROTECTION BOARD.Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. 2021. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en. Acesso em 20/05/2023. p. 29

vamente interesses e direitos fundamentais dos titulares), contudo, não há a presença de nenhum dos critérios que precisam ser cumulados constantes dos incisos **I, II, III, IV e V** do **art. 5° da proposta**.

Portanto, de acordo com a atual proposta, esse incidente não deflagaria o dever de comunicar. Diferente é a perspectiva do EDPB que entende que este é um caso de comunicação à autoridade, tendo em vista os critérios adotados pela GDPR. Dessa forma, a proposta de regulamentação pode fazer com que casos de incidentes que ofendam os direitos fundamentais dos titulares fiquem sem comunicação.

Por conta disso, manter o art. 5º da proposta com a mesma redação na regulamentação final pode resultar em isolamento e dificuldades no estabelecimento de acordos e cooperação na regulação de questões relacionadas à proteção de dados, indo na contramão do esforço de convergência e interoperabilidade regulatória. Isto é verdadeiro principalmente se considerarmos a transferência internacional de dados, que depende da manutenção de padrões de proteção de dados parecidos ou com o mesmo grau que outros países.

Sugere-se, portanto, que seja adotada uma abordagem procedimental, transferindo a responsabilidade para os agentes de tratamento envolvidos de mensurar o risco com base na concretude do incidente de segurança. Essa abordagem deve se basear exclusivamente em critérios que orientem de forma adequada essa avaliação de risco, levando em consideração a experiência internacional já examinada no próprio AIR e as recomendações recentes do EDPB sobre o assunto.

RECOMENDAÇÃO

Sugere-se que seja adotada uma abordagem procedimental, transferindo a responsabilidade para os agentes de tratamento envolvidos de mensurar o risco com base na concretude do incidente de segurança. Essa abordagem deve se basear em critérios que orientem de forma adequada essa avaliação de risco, levando em consideração a experiência internacional já examinada na própria Análise de Impacto Regulatório realizada e publicada pela ANPD.

Alguns desses critérios que orientam a avaliação do risco: 1) O tipo de incidente ocorrido; 2) A natureza, a sensibilidade e o volume de dados pessoais envolvidos; 3) A facilidade de reidentificação dos titulares dos dados; 4) A gravidade das consequências para os titulares afetados; 5)Características especiais dos titulares, como no caso de envolver crianças; 6) Características especiais do controlador de dados; 7) O número de pessoas afetadas pela violação. 8) Outros elementos do caso concreto.

2. Critérios que disparam o dever de comunicação para a ANPD e Titulares de dados afetados

A partir dos critérios que disparam o dever de notificação de um incidente de segurança envolvendo dados pessoais surge o dever de realizar essa comunicação. De acordo com o art. 48 da LGPD *"O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares"*.

Portanto, não há na LGPD uma distinção explícita entre as situações em que a ANPD deveria ser comunicada e as situações em que os titulares afetados deveriam ser comunicados. Contudo, não há, a princípio, nenhum óbice legal para que a ANPD o faça. Como se verá adiante, ao definir o conteúdo mínimo da comunicação do incidente à autoridade e aos titulares foi feita essa diferenciação (arts. 6º e 9º da minuta de norma proposta).

Isso se dá pois os objetivos que essas comunicações cumprem são distintos. Como reconhecido pelo art. 2º da minuta proposta, o processo de comunicação de um incidente tem propósitos múltiplos, desde a proteção do titular, a efetivação do princípio da responsabilização e prestação de contas, até a promoção da cultura de proteção de dados e fornecer subsídios para que a ANPD realize suas atividades.

Desta forma, pode-se dizer que a comunicação ao titular de dados tem o objetivo primordial de informá-lo a respeito de uma ameaça a seus direitos fundamentais, efetivando o princípio da transparência, e a partir disso possa tomar ações para mitigar esse risco ou dano, contando também com a colaboração do controlador que sofreu o incidente, orientando o titular e oferecendo subsídios para que essa mitigação possa acontecer de forma efetiva.

Por outro lado, a comunicação à autoridade possui objetivos distintos, notadamente, a materialização do princípio da responsabilização e prestação de contas e a criação de uma relação colaborativa entre agente de tratamento e autoridade nacional para lidar com o incidente, mitigando ao máximo seus riscos e levando a uma condução adequada da situação de crise.

Essa colaboração com a ANPD está prevista nos arts. 48 §2º e 3º da LGPD, ao prever que a autoridade deve avaliar a gravidade do incidente e, caso necessário, determine providências adicionais para lidar com o incidente.

O mesmo racional pode ser observado a partir da experiência internacional, em que o Considerando 86 da GDPR orienta que:

> Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, **em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia**.
>
> Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação[10].

Da mesma forma, o European Data Protection Board em seu guia "Guidelines 9/2022 on personal data breach notification under GDPR" orienta a atuação conjunta e prévia entre controlador e autoridade para contactar de forma mais adequada e assertiva os titulares para informá-los a respeito do incidente de segurança:

> Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also **on the appropriate messages to be sent to, and the most appropriate way to contact, individuals**[11].

Adicionalmente, embora a atuação da ANPD se restrinja à legislação de proteção de dados pessoais, e considerando que um incidente de segurança pode afetar outros direitos fundamentais e desencadear também consequências penais, a LGPD atribui à autoridade nacional a competência de se comunicar com outras autoridades e órgãos para garantir uma harmonia entre a LGPD e as demais legislações, conforme estabelecido pelo art. 55-J:

> Art. 55-J. Compete à ANPD:
> XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
> XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
> XXIII - articular-se com as autoridades reguladoras públicas para exercer

10 COMISSÃO EUROPEIA. **Regulamento(UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://gdpr-text.com/pt/read/recital-86/, destaque não consta no original.

11 EUROPEAN DATA PROTECTION BOARD. **op.cit.** p. 21, destaque não consta no original.

suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;

Assim, a notificação à ANPD permite que o incidente de segurança seja lidado em suas múltiplas dimensões, possibilitando uma articulação interinstitucional de forma a melhor mitigar os efeitos do incidente e permitir uma comunicação mais assertiva ao titular, alertando-o sobre os riscos em diferentes frentes em uma única notificação.

Portanto, a diferenciação entre os critérios que disparam o dever de notificar a autoridade e os titulares não só está de acordo com o que é determinado pela LGPD a partir do art. 48 §2º e 3º, as competências da ANPD previstas pelo art. 55-J, como também procedimentaliza de forma adequada as garantias que justificam o dever de notificar cada um destes atores. Ainda, essa diferenciação coloca o cenário brasileiro em maior harmonia com o cenário internacional, efetivando uma convergência regulatória que permite interoperabilidade entre diferentes sistemas normativos e dá maior segurança jurídica aos agentes de tratamento.

Por fim, deve-se considerar que a notificação conjunta entre titulares e autoridade nacional cria um incentivo inadequado aos controladores e pode afetar negativamente os titulares.

Em relação ao comportamento dos controladores, a notificação a todos os titulares afetados pode ser custosa tanto em termos operacionais, mas especialmente do ponto de vista reputacional. Portanto, da forma como a norma está proposta, há um grande risco de subnotificação de incidentes de segurança para a ANPD.

Partindo de um cenário que o controlador não deseja notificar os titulares, uma vez que isso implicaria em uma grande crise reputacional com severos impactos financeiros, resta evidente como a norma proposta incentiva um comportamento de subestimação do risco gerado pelo incidente que afasta ainda mais a presença da ANPD e a possibilidade de uma fiscalização adequada acerca do incidente.

Pela ótica de gerenciamento de risco regulatório por parte do agente de tratamento, uma vez que a notificação é feita apenas à autoridade e não aos titulares, cria-se uma situação de irregularidade conhecida pela ANPD. Há, então, um alto risco que aquela irregularidade seja endereçada pela autoridade reguladora.

Por outro lado, se o agente de tratamento decide não notificar nem a autoridade nem os titulares, há uma menor probabilidade que a situação de irregularidade seja identificada e endereçada pela ANPD.

Com a diferenciação dos critérios de notificação ao titular e a autoridade, exigindo a notificação aos titulares apenas em situações de alto risco, ou seja, situações mais extremas, um incentivo diverso seria criado, e mais adequado aos propósitos da LGPD. Nessa situação, há um incentivo para que o agente de tratamento não opere em irregularidade ao notificar a ANPD de um incidente de segurança que não ocasiona um alto risco aos titulares. Ainda que o agente de tratamento subdimensione o risco e não notifique os titulares, a autoridade estaria

Em suma: no ordenamento criado pela minuta proposta, o subdimensionamento do risco por parte do agente de tratamento leva a uma situação de ausência de notificação, tornando mais difícil a fiscalização e adequação da situação.

Já em um ordenamento que estabeleça critérios distintos para a notificação à autoridade e ao titular, esta última sendo em casos mais graves, o subdimensionamento do risco ainda pode levar a uma situação de notificação à autoridade, que então terá informações suficientes para realizar a avaliação da gravidade do incidente e endereçá-lo de maneira adequada.

Ressalta-se que a criação de incentivos para a notificação de incidentes à autoridade nacional é de suma importância, não só para o correto manejo daquele caso em concreto, mas para que a ANPD tenha dados relevantes e mais próximos da realidade, guiando toda a sua atuação estratégica e permitindo o exercício de competências previstas no art. 55-J que dependem fortemente de uma política pública baseada em dados:

> Art. 55-J. Compete à ANPD:
> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança
> VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
> VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis.

Espera-se ter demonstrado que a não separação dos critérios que criam o dever de notificar a autoridade e os titulares implica em uma leitura reducionista da LGPD, compreendendo-a como uma lei que prevê obrigações burocráticas, e não obrigações procedimentais para garantia dos direitos fundamentais. A correta interpretação do art. 48 da lei é no sentido de

que deve haver uma diferenciação entre o conteúdo e os critérios que disparam o dever de notificar a autoridade e os titulares, por cumprirem propósitos diferentes e procedimentalizarem princípios e garantias diferentes.

RECOMENDAÇÃO

Recomenda-se a diferenciação dos critérios que geram o dever de notificação para a autoridade nacional e para os titulares, considerando que as comunicações cumprem propósitos distintos.

A comunicação à autoridade deve ocorrer sempre que houver risco ou dano relevante, enquanto a comunicação aos titulares deve ocorrer somente quando a gravidade desse risco ou dano for considerada **alta**. Essa avaliação deve ser feita pelo controlador que sofreu o incidente a partir dos parâmetros definidos pela Autoridade.

3. Elementos obrigatórios na comunicação do incidente de segurança

O art. 6° do regulamento proposto define as informações que devem constar na comunicação do incidente à ANPD. Especial atenção deve ser dada às informações constantes nos incisos VII e X da proposta de minuta.

> *Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador,* ***no prazo de três dias úteis****, ressalvada a existência de legislação específica,* ***contados do conhecimento do incidente de segurança****, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:*
> *[...]*
> *VII -* ***a data e a hora do conhecimento do incidente de segurança****;*
> *[...]*
> *X -* ***as informações sobre o operador, quando aplicável****;*

No caso do inciso VII, a exigência das informações acerca da data e hora do conhecimento do incidente são restritivas. Isto pois a ausência de informações acerca das circunstâncias em que o incidente foi conhecido impacta em dois elementos: O marco inicial da contagem do prazo da comunicação (*"a partir do conhecimento"*) constante do art 6° e 9° da proposta e no juízo de gravidade que a ANPD pode fazer para estabelecer medidas adicionais da comunicação aos titulares.

Com relação ao trecho sobre o início do prazo de comunicação, a pergunta ainda sem resposta é: o que torna o agente de tratamento ciente para os efeitos da comunicação?

No guia do EDPB sobre o tema, considera-se que o controlador está ciente ("*aware*") quando ele tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais[12]. Apesar de parecer algo trivial, alguns incidentes de segurança exigirão mais tempo do controlador para que se chegue a essa conclusão.

Nesse sentido, após saber de indícios de um incidente, o controlador pode realizar um breve período de investigação para determinar se ele ocorreu ou não. Durante esse período de investigação, o controlador não pode ser considerado "ciente"[13] e portanto não há início do prazo

12 EUROPEAN DATA PROTECTION BOARD. **op.cit.** p. 11.

13 **Ibid**. p. 12.

para comunicar a autoridadee os titulares. A resposta do EDPB é um caminho para esclarecer melhor a questão no cenário brasileiro.

Com relação ao inc. VII, o requisito de comunicar somente a data e hora do incidente afeta o juízo de gravidade que a autoridade pode tomar. Isto pois existe uma diferença entre um incidente que é percebido internamente a partir de medidas técnicas e administrativas postas em prática por um controlador e um incidente publicamente reconhecido. Certamente o incidente que é reconhecido publicamente e, por exemplo, é exposto midiaticamente pode precisar de medidas adicionais por parte dos controladores para proteger os direitos dos titulares de dados pessoais. Por essa razão, recomendamos incluir as circunstâncias em que o incidente foi conhecido no inciso VII, art 6° da proposta, de forma a permitir que o controlador preste contas acerca do prazo em que está realizando a comunicação e a autoridade tenha mais elementos para avaliar sua tempestividade.

Já com relação ao inciso X do já referido artigo, a problemática está na falta de amplitude da comunicação acerca dos agentes de tratamento que podem estar envolvidos no incidente de segurança. De acordo com o inciso, a comunicação deve conter as informações sobre o operador quando aplicável, contudo, a comunicação não deveria conter a informação de outros controladores e operadores nos casos de compartilhamento de dados?

Novamente, o EDPB oferece soluções nesse sentido. A autoridade recomenda o estabelecimento contratual dos papéis de cada agente de tratamento em situações de incidentes de segurança[14], de forma a contribuir melhor com a comunicação deles. A falta de amplitude na comunicação dos agentes de tratamento envolvidos no incidente de segurança pode vulnerabilizar titulares de dados que estão em outras cadeias de tratamento a qual seus dados são compartilhados.

14 Ibid. p. 13.

RECOMENDAÇÃO

Determinação de critérios expressos acerca de quando um controlador se torna "ciente" para efeitos de contagem de prazos; Aumentar a amplitude dos requisitos de informação à ANPD. Confira a sugestão de mudanças abaixo:

> Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:
> [...]
> VII - a data, a hora e as circunstâncias do conhecimento do incidente de segurança;
> [...]
> X - as informações sobre o operador , quando aplicável, e controladores nos casos de compartilhamento de dados pessoais;