Contribuição Data Privacy Brasil - Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais

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 a neutralidade tecnológica também na regulação de novas tecnologias, como se pode observar nas disposições do Maco 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].

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

---

[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.** . p. 20

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 significativamente interesses e direitos fundamentais dos titulares)***, contudo, não há a presença de nenhum

---

[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

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 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 do EDPB sobre o assunto.

Alguns desses critérios que orientam a avaliação do risco podem ser adotados: 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.