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

1. 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.[1]

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.**[2]

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;

---

[1] https://gdpr-text.com/pt/read/recital-86/ , destaque não consta no original

[2] https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf p.21, destaque não consta no original

> 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 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.