COMENTÁRIOS DA BRASSCOM À TOMADA DE SUBSÍDIOS PARA REGULAMENTAÇÃO DO DEVER DE COMUNICAÇÃO SOBRE INCIDENTES DE SEGURANÇA

Brasília (DF), 22 de março de 2021

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, entidade que congrega algumas das mais dinâmicas e inovadoras empresas de Tecnologia da Informação e Comunicação (TIC) alinhadas com a Era Digital, que prestam serviços de TIC, desenvolvem e licenciam software, fabricam e comercializam hardware, disponibilizam redes sociais ou plataformas variadas; ou ainda prestam serviços telecomunicações, tem como Propósito trabalhar em prol de um Brasil Digital, Conectado e Inovador por meio da propositura e defesa de políticas públicas, com especial enfoque no emprego, na diversidade e a educação, bem como, na inovação.

Neste mister, a Brasscom parabeniza a Autoridade Nacional de Proteção de Dados (ANPD) por lançar esta Tomada de Subsídios para discutir a regulamentação sobre o dever de comunicação de incidentes de segurança, nos termos do artigo 48, parágrafo 1º da LGPD.

Consideramos fundamental essa iniciativa de abrir espaço para que todas as partes interessadas possam apresentar considerações e permitir que a futura regulamentação atinja seus objetivos de forma equilibrada e eficiente. Neste sentido, a Brasscom, respeitosamente, vem apresentar suas considerações abaixo dispostos nos seguintes tópicos:

Sumário

Brasscom - Associação das Empresas de Tecnologia da Informação e Comunicação e Tecnologias Digitais
Rua Funchal 263, conj. 142, Vila Olímpia, São Paulo, SP, CEP 04551-060
SHN, Qd. 1, Bl. A, Edifício Le Quartier, Sala 615 Brasília/DF

1. A COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

A LGPD, em seu artigo 48, prevê a necessidade de comunicação pelo controlador à ANPD e ao titular dos dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Para evitar eventuais confusões de conceitos, sugerimos que a ANPD estabeleça de forma clara a diferença entre o termo "incidente de segurança" do termo "incidente de segurança com dados pessoais". Apresentamos abaixo nossas sugestões de definições para ambos os conceitos, usando como referência a ISO 27035-1:2016[1]:

> *"Um incidente de segurança é qualquer evento adverso identificado que pode prejudicar os ativos de uma organização ou comprometer suas operações.*
>
> *Um incidente de segurança com dados pessoais é qualquer evento adverso, identificado e confirmado ou ~~sob suspeita~~, relacionado à violação na segurança de dados pessoais, ~~tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita~~" (grifo nosso).*

Essa clara dissociação entre os conceitos auxiliará as organizações a efetivamente compreender a qualificação legal para a comunicação à autoridade, ou seja, realizá-la apenas quando for identificado e confirmado que o incidente de segurança com dados pessoais acarretará risco ou dano relevante aos titulares. E para que o controlador possa chegar a essa determinação, é fundamental que ele faça um exercício de gestão de risco quando da estruturação do seu processo de tratamento de dados pessoais.

O objetivo da LGPD é a proteção dos titulares dos dados pessoais e não a proteção dos dados em si. Desse modo, o exercício de gestão de risco e de aplicação dos princípios fixados na lei deve ser norteado pelo objetivo de proteção do titular do dado. Dito de outra forma, eventual incidente de segurança que não tenha qualquer potencial de gerar riscos ou prejuízos ao titular do dado não deveria para fins do arcabouço normativo da LGPD, ensejar uma movimentação de comunicação e/ou ações sob a óptica da lei (sem se falar, aqui, em possíveis adoções de medidas de mitigação de risco de segurança da informação propriamente dita).

[1] Organização Internacional de Normalização, ISO 27035-1:2016. Disponível em: https://www.iso.org/standard/60803.html.

Dessa forma, será explicado a seguir a lógica por trás da gestão de risco com o objetivo de promover a avaliação dos norteadores que devem ser adotados para determinar as regras de comunicação de incidentes de segurança para a ANPD.

2. A PREMISSA DE GESTÃO DE RISCO

A premissa de gestão de risco traz sua inspiração nas práticas já corriqueiras de segurança da informação e se concretiza no processo sistemático de identificação, avaliação, tratamento e monitoramento de riscos e eventuais danos, com o objetivo de minimizar ou até mesmo eliminar a possibilidade de impactos negativos sobre objetivo pretendidos, caso alguns dos riscos avaliados venham a se concretizar. Portanto, o gerenciamento de riscos visa reduzir ao mínimo possível os impactos dos riscos sobre a própria organização e terceiros, com a adoção de melhores práticas de infraestrutura, políticas e metodologias, tendo em mente a tecnologia disponível; o custo de implementação; a natureza, escopo, contexto e finalidade das atividades de processamento do controlador de dados; e a probabilidade e magnitude dos riscos envolvidos[2].

Não menos importante, o gerenciamento de riscos é (i) uma ferramenta eficaz a fim de garantir um alto nível de proteção dos direitos e liberdades individuais; (ii) permite que as organizações dediquem seus esforços onde os impactos são mais significativos e mitiguem esses riscos e (iii) promove a inovação, na medida em que permite que as organizações adotem as medidas de proteção de dados necessárias para minimizar o impacto aos indivíduos de suas operações de tratamento nos limites do necessário[3].

Conforme o entendimento do Grupo de Trabalho do Artigo 29[4], grupo europeu independente que lidava com questões relacionadas a proteção de dados[5] antes da entrada em vigor da GDPR, os riscos estão relacionados de acordo com o potencial impacto negativo sobre os direitos e liberdades individuais, e devem ser determinados levando em consideração critérios objetivos.

> Considerando a ampla variedade de tratamento de dados realizados por diferentes tipos de organizações, é importante manter uma flexibilidade em torno da metodologia de análise de risco de modo que as especificidades de cada organização e da natureza dos dados que ela trata possam ser ponderados como parte desse processo de avaliação. Nesse sentido, sugerimos que a ANPD procure adotar - ainda que em caráter orientativo e não normativo - os principais critérios a serem utilizados pelos agentes de tratamento nesse exercício, auxiliando dessa forma agentes menos familiarizados com a proteção de dados e trazendo mais segurança jurídica para o conjunto dos agentes. Tendo em vista a experiência internacional sobre o tema sugerimos que tais critérios incluam as seguintes temáticas:
>
> (i) O tipo de violação *(por exemplo, dependendo do cenário, uma violação da confidencialidade pode ter um impacto maior do que se os dados forem simplesmente perdidos ou apagados);*
>
> (ii) A natureza e sensibilidade dos dados pessoais *(quanto mais sensíveis os dados, maior será o risco de dano para os titulares afetados. De todo modo, aspectos como*

[2] Centre for Information Policy Leadership. The Role of Risk Management in Data Protection, 2014. Disponível em: https://bit.ly/2NZnvMB.
[3] Centre for Information Policy Leadership. Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 2016. Disponível em: https://bit.ly/3ulsNNf.
[4] Article 29 Data Protection Working Party. Statement on the role of a risk-based approach in data protection legal frameworks, 2014. Disponível em: https://bit.ly/2PtgWT3
[5] Função hoje desempenhada pelo European Data Protection Board.

se outros dados pessoais do titular já estavam disponíveis quando o incidente ocorreu também devem ser considerados);

(iii) Facilidade de identificação dos indivíduos;

(iv) Gravidade das consequências para os indivíduos *(por exemplo, as violações em que haja provas de agentes maliciosos que tenham acesso aos dados pessoais podem indicar um risco mais elevado do que as violações em que os dados sejam divulgados por acidente);* e

(v) Características especiais do indivíduo afetado *(por exemplo, dados relativos a crianças/outros indivíduos vulneráveis podem levar à classificação do incidente como de maior risco)*.

Um aspecto adicional importante quando se fala da questão de gestão de risco refere-se ao volume de titulares afetados por um determinado incidente. Nesse particular, entendemos importante destacar que não necessariamente um volume maior de titulares afetados implique em um maior risco aos titulares pois será fundamental se considerar os outros fatores envolvidos no caso concreto, tais como a natureza do dado objeto do incidente, o contexto, dentre outros. Em suas orientações, portanto, recomendamos que a ANPD esclareça que o volume de titulares impactados como um critério para avaliar o risco/dano do incidente não deve ser o aspecto primário a ser considerado, e sim um fator em conjunto com tantos outros para permitir uma avaliação precisa da maior ou menor gravidade da situação. Isso é importante pois o número de usuários afetados não necessariamente indicará um aumento na probabilidade de danos que um indivíduo possa sofrer em razão de um incidente de segurança.

É importante que a ANPD compreenda que o fato de ter havido uma violação não significa necessariamente que as medidas de segurança técnicas e organizacionais implementadas pelos agentes de tratamento tenham sido insuficientes. Em outras palavras, um incidente de segurança não deve ser considerado um indicador incontestável de proteção insuficiente dos dados pessoais ou de que uma empresa agiu de forma "irrazoável" ou inadequada. Cada incidente e as medidas de segurança implementadas têm de ser considerados com base em suas próprias peculiaridades.

Como se pode observar, essa premissa vai além do mero cumprimento das exigências legais. Vai ao cerne do que as organizações responsáveis procuram alcançar, como implementar as medidas de proteção de dados e como demonstrar que estão em conformidade com a lei[6]. Temos, portanto, uma premissa importante no arcabouço de proteção de dados pessoais: não se presume que incidentes não irão ocorrer; espera-se, sim, que as empresas tenham adotado todas as medidas razoáveis para evitar que tais incidentes de fato representem um risco ou levem a um dano aos titulares dos dados pessoais.

Cumpre ressaltar que a Autoridade não deverá, no exercício de sua competência legal, decidir no caso concreto se houve ou não risco ou dano ao titular no caso de um incidente de segurança. Para garantir uma maior segurança jurídica, parece-nos recomendável que normativo específico sobre o tema venha a deixar claro tal entendimento decorrente da própria LGPD.

3. CONCEITO DE RISCO E DANO

[6] Centre for Information Policy Leadership. A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 2014. Disponível em: https://bit.ly/3e1Rnm6.

O conceito de risco e dano para o titular dos dados são conceitos próximos mas essencialmente distintos. Podemos interpretar o risco para o titular dos dados como uma definição mais ampla do que a definição de dano efetivo; o que sugere que o dano "potencial" também seria compreendido pela primeira definição, portanto, a definição de "risco" pode ser entendida como "risco de dano". Tanto o "risco" como o "dano" apontam para uma certa gravidade do impacto do incidente sobre os titulares dos dados, sendo identificados antes de serem levantados os requisitos de notificação.

Isto é semelhante a outras jurisdições onde vimos os termos "risco" e "dano" serem utilizados de forma bastante intercambiável. A ANPD poderia procurar tratar o termo "dano" de forma semelhante. Por exemplo:

- No GDPR[7], a notificação de violações aos titulares dos dados afetados deve ser realizada quando uma violação é "suscetível de resultar num elevado risco para os direitos e liberdades das pessoas naturais";

- Na Lei de Privacidade da Austrália[8], a notificação de violações aos titulares dos dados afetados deve ser realizada quando uma "uma pessoa razoável concluir que o [incidente] poderia resultar em sérios danos a qualquer um dos indivíduos aos quais as informações se referem";

- Na Lei de Privacidade da Nova Zelândia[9], a notificação de violações aos titulares dos dados afetados deve ser realizada para qualquer violação de privacidade que seja "razoável acreditar que tenha causado danos sérios a um indivíduo ou indivíduos afetados ou que seja provável que o faça"; e

- Na Lei de Privacidade do Canadá[10], a notificação de violações aos titulares dos dados afetados deve ser realizada quando a violação cria "um risco real de danos significativos para os indivíduos afetados".

Comparativamente a estes fatores desencadeadores de notificação, o Artigo 48 da LGPD estabelece que: "o responsável pelo tratamento deve informar a Autoridade Nacional de Proteção de Dados e o titular dos dados sobre a ocorrência de incidentes de segurança que possam implicar riscos ou danos relevantes para os titulares dos dados".

Tal como nas outras quatro jurisdições acima enumeradas, o Brasil parece ter uma abordagem comum na identificação de um requisito de "probabilidade" ("poderia") paralelamente a um requisito de "gravidade" ("risco ou dano relevante"). Diante disso, entendemos que a ANPD deveria, em um exercício de harmonia e interoperabilidade com os arcabouços existentes, adotar o conceito de “risco” que siga a experiência sedimentada no GDPR e, por outro lado, o conceito de “dano” e fixado nas legislações da Austrália, Nova Zelândia e Canadá quanto ao “risco relevante [de dano]” ou dano” da LGPD. Certamente, tal diferenciação clara dos conceitos facilitará o entendimento de que o “risco” está relacionado quanto a probabilidade de ocorrência de um dano, enquanto o “dano” está relacionado ao impacto negativo de um dano já materializado.

Tal construção interpretativa se assemelha aquela já consolidada na doutrina brasileira no que tange a conceituação de tais figuras no direito civil pátrio.

[7] GDPR. Disponível em: https://bit.ly/3lupdlq.
[8] Privacy Act 1988. Disponível em: https://bit.ly/3cNqgZN.
[9] New Zealand Privacy Act. Disponível em: https://bit.ly/3tFy6eL.
[10] Personal Information Protection and Electronic Documents Act. Disponível em: https://bit.ly/2QomwGL.

4. MODELOS DE FRAMEWORKS

Neste momento de amadurecimento da sociedade brasileira a uma nova cultura de proteção de dados pessoais é ideal para a ANPD exercer sua competência educacional sobre a temática, promovendo a disseminação da cultura de proteção de dados pessoais e trabalhando para a elaboração de guias para auxiliar no processo de adequação de organizações, apontando os agentes de tratamento para modelos de framework de risco existentes e respeitados, garantindo que as organizações estejam gerenciando o risco adequadamente, fazendo referência às melhores práticas e padrões internacionais de gestão de risco, como alguns modelos a seguir:

4.1. NORMAS ISO

O modelo padrão adotado pela norma ISO 31000:2018[11], publicada pela Organização Internacional de Normalização, apresenta um conjunto de diretrizes para a gestão de riscos enfrentados pelas organizações. A aplicação dessas diretrizes pode ser personalizada para qualquer organização e seu contexto, seja, por exemplo, sobre riscos regulatórios, trabalhista, ambientais, segurança da informação ou jurídicos. Tal norma oferece uma abordagem comum para gerenciar qualquer tipo de risco e não é específica para determinada indústria ou setor e, dessa forma, um modelo como a ISO 31000, na medida em que aborda o risco sob a ótica corporativa, poderá também ser ajustada para que as organizações apliquem a norma sob a gestão de risco ao titular de dados.

Nessa mesma linha, a ISO 27001:2013[12], integra um conjunto de políticas, procedimentos e processos que formam o Sistema de Gestão da Segurança e Informação, uma estrutura central que permite às organizações adotar uma consistência para os seus exercícios de gestão de risco e segurança da informação. Esse padrão indica em linhas gerais quais medidas e ferramentas uma organização deve adotar, alinhado com as melhores práticas internacionais, sem apresentar uma lista taxativa.

A ISO 27005:2018[13], por sua vez, dá sustentação aos conceitos aplicados da ISO 27001, formando a espinha dorsal do projeto de conformidade, delineando como as organizações podem identificar os perigos de segurança da informação que enfrentam, priorizar suas maiores ameaças e selecionar um curso de ação apropriado. Este processo revela quando é apropriado realizar a criptografia de dados, por exemplo, bem como onde as organizações devem reforçar seus processos organizacionais ou outras defesas técnicas e também contém passos que as organizações podem tomar para lidar com a resiliência cibernética, o que as ajudará a proteger processos comerciais críticos.

4.2. NIST PRIVACY FRAMEWORK

O NIST *Privacy Framework*, desenvolvido pelo *US National Institute of Standards and Technology's*, elaborado em colaboração com uma série de organizações, oferece um conjunto de ferramentas para viabilizar uma estratégia de privacidade para as organizações que desejam

[11] International Organization for Standardization.. ISO 31000:2018 Risk management — Guidelines, 2018. Disponível em: https://bit.ly/3bTKdPE.
[12] International Organization for Standardization. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, 2013. Disponível em: https://bit.ly/3rVkrzT.
[13] International Organization for Standardization. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018. Disponível em: https://bit.ly/3qPlP5L.

aprimorar sua forma de utilizar a proteger os dados pessoais; também oferece detalhadamente explicações sobre conceitos de gerenciamento de risco[14].

O NIST não se trata necessariamente de uma lei ou regulação do setor, mas sim uma ferramenta de uso voluntário que pode ajudar as organizações a melhor gerenciarem seus produtos e serviços que afetem indivíduos, a melhor forma de como comunicar suas práticas relacionadas à privacidade, assim como demonstrar o cumprimento de leis que possam afetá-las, como por exemplo o Regulamento Geral sobre a Proteção de Dados (GDPR).

Tendo em vista a natureza global das cadeias de valores em inúmeros setores econômicos, recomendamos a ANPD que ofereça flexibilidade para que as organizações adotem as melhores práticas já internacionalmente disseminadas, escolhendo aquela que mais se aproximar do negócio da empresa, a volumetria e a natureza dos dados coletados.

4.3. METODOLOGIA DA ENISA (2013)[15]

No contexto de DANO e RISCO, acreditamos que a metodologia sugerida pela Agência da União Europeia para a Cibersegurança possa ser uma referência para a ANPD e um guia para os controladores, pois nela são levados em consideração alguns critérios ao avaliar a gravidade de uma violação de dados pessoais como:

- Contexto de processamento de dados: aborda o tipo de dados violados, juntamente com uma série de fatores vinculados ao contexto geral de processamento;

- Facilidade de identificação: determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação; e

- Circunstâncias de violação: que avalia as circunstâncias específicas da violação, que estão relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida.

As recomendações incorporadas nesses diversos *framework* de segurança da informação devem ser consideradas não só na sistematização dos processos de gestão de risco mas também como balizadores para a avaliação de situações de incidente de segurança. Notamos que a metodologia ao fim da avaliação preliminar considera outros dois parâmetros que podem atenuar ou acentuar a gravidade de suposta violação, tais como a quantidade de pessoas atingidas e a ininteligibilidade.

As metodologias acima listadas são construídas com um caráter voluntário, não sendo obrigatórias para as organizações, mas sendo consideradas melhores práticas internacionais e comumente disseminadas como o estado da arte em segurança da informação. Entendemos que a ANPD deverá em seus guias orientativos estimular que frameworks dessa natureza sejam efetivamente utilizados pelas organizações como uma forma de atendimento das obrigações fixadas no artigo 46 da LGPD.

5. PRAZO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

[14] National Institute of Standards and Technology. NIST Privacy Framework: a tool for improving privacy through enterprise risk management, 2020. Disponível em: https://bit.ly/3kliRP8.
[15] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013.

O artigo 48 da LGPD indica que a comunicação sobre o incidente de segurança deverá ser comunicada tanto para o titular dos dados pessoais quanto para a ANPD em prazo razoável a ser definido pela autoridade. Enquanto a regulamentação ainda se encontra pendente, o site da ANPD recomenda que a comunicação seja realizada no prazo de 2 dias úteis, contados a partir da data do conhecimento do incidente[16].

Entendemos que o formulário atualmente disponível no site da ANPD foi desenvolvido em caráter transitório para auxiliar a sociedade em um momento em que inúmeros incidentes de segurança vêm sendo revelados e a ANPD ainda não teve a oportunidade de desenvolver instrumento normativo próprio sobre o tema.

Nesse sentido, aproveitamos para apresentar alguns exemplos do cenário internacional no que diz respeito a esse tipo de comunicação para explorar alguns caminhos que deverão ser examinados pela ANPD como referência para a adoção do normativo pátrio.

5.1. EUROPA - Regulamento Geral sobre a Proteção de Dados (GDPR)

O Regulamento Geral sobre a Proteção de Dados (GDPR)[17], no seu artigo 33 indica que, no caso de um incidente de dados pessoais, os controladores de dados devem notificar a autoridade de supervisão competente sem demora indevida e, quando possível, em até 72 horas após terem tomado conhecimento do incidente, a menos que este não resulte em risco para os direitos e liberdades dos indivíduos. Quando a notificação à autoridade de supervisão não for feita dentro de 72 horas, ela deverá ser acompanhada dos motivos do atraso. De acordo com um estudo realizado pela DLA Piper[18], de 25 de maio de 2018 a 27 de janeiro de 2020, houve um total de 160.921 violações de dados pessoais notificadas por organizações às autoridades de supervisão de proteção de dados dentro da União Europeia.

5.2. ESTADOS UNIDOS

O modelo norte-americano de proteção de dados pessoais é bastante distinto daquele adotado no Brasil e nas demais jurisdições inspiradas na estrutura europeia. Ainda assim, vale observar o caminho adotado por alguns estados americanos no sentido de editar normativas específicas justamente para estabelecer critérios relativos à comunicação de incidentes de segurança.

Alguns estados americanos adotam um modelo pelo qual se fixa um patamar mínimo de titulares afetados para gerar a obrigação de comunicação do incidente de segurança ao órgão competente, como no caso do estado do Colorado[19], Delaware[20] e Illinois[21], onde, ocorrendo um incidente de segurança que afete 500 ou mais indivíduos residentes desses estados, a organização deverá notificar o escritório do respectivo procurador-geral. Vale lembrar que a sistemática da legislação americana é estruturada de uma maneira diferente do Brasil.

Para incidentes de segurança envolvendo dados pessoais sensíveis de saúde, um exemplo notável é o do *Health Insurance Portability and Accountability Act* (HIPAA)[22], lei federal que apresenta um conjunto de normas para a proteção de dados voltado a organizações de saúde norte-americanas, que adota dois caminhos: (i) se o incidente afetar 500 ou mais

[16] Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD. GOV.BR, 2021. Disponível em: https://bit.ly/203VkMH.
[17] Regulamento Geral sobre a Proteção de Dados. Disponível em: https://bit.ly/3rPsu0Y.
[18] DLA Piper. GDPR data breach survey, 2020. Disponível em: https://bit.ly/3bC6yRt.
[19] Colo. Rev. Stat. § 6-1-716.
[20] Del. Code tit. 6, § 12B-101 et seq.
[21] 815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25.
[22] Health Insurance Portability and Accountability Act. Disponível em: https://bit.ly/3l7DMeH.

indivíduos, a organização deverá notificar a Secretaria do Departamento de Saúde e de Serviços Humanos dos Estados Unidos sem atraso injustificado e em nenhum caso depois de 60 dias corridos a partir da descoberta do incidente; ou (ii) se a incidente afetar menos de 500 indivíduos, a organização deverá notificar a Secretaria dentro de 60 dias a partir do final do ano-calendário em que foi descoberta.

Esse modelo setorial nos EUA traz uma referência bastante interessante no sentido de poder ajudar a gerenciar o fluxo de incidentes de segurança envolvendo dados pessoais sensíveis de saúde encaminhados à ANPD, estabelecendo um montante de referência de titulares afetados para se aplicar a obrigação de comunicação. Tal número, se adotado para dados pessoais sensíveis de saúde, precisará considerar o tamanho da população brasileira bem como a natureza transversal da obrigação, não sendo fixada para um único setor econômico.

Nessa estrutura, os incidentes de segurança de menor impacto não deverão ser desconsiderados mas sim compilados em uma única comunicação ao final do período de 12 meses, permitindo assim a autoridade ter um conhecimento da maturidade de segurança e proteção de dados pessoais sensíveis de saúde do país, acompanhar o amadurecimento individual das organizações e estabelecer um fluxo de informações e obrigações menos oneroso e mais eficiente tanto para as organizações que tratam dados pessoais sensíveis de saúde quanto para à ANPD.

5.3. AUSTRÁLIA - *Australian Privacy Act*

O *Australian Privacy Act*[23], lei de proteção de dados australiana, exige que as organizações realizem uma avaliação sobre o risco efetivo do incidente dentro de 30 dias após terem tomado conhecimento de que possa ter havido uma violação, devendo notificar a autoridade australiana e os titulares de dados pessoais afetados após a confirmação de que o incidente apresenta um risco de danos graves para os indivíduos afetados, a causa ou fonte, o tipo de dado pessoal que foi acessado ou divulgado, e o número de indivíduos que estavam em risco de danos graves como resultado do incidente.

5.4. CANADÁ - *Personal Information Protection and Electronic Documents Act* (PIPEDA)

O *Personal Information Protection and Electronic Documents Act* (PIPEDA)[24], lei de proteção de dados canadense, também exige que o controlador realize a comunicação assim que possível, logo após determinar que um incidente, que represente um risco real de dano significativo ao titular, ocorreu.

Os fatores relevantes elencados para auxiliar a determinar que um incidente apresenta um risco real de dano, de acordo com o PIPEDA são (i) o nível de sensibilidade dos dados pessoais envolvidos no incidente e (ii) a probabilidade de que tais dados tenham sido, estejam sendo ou venham a ser utilizados indevidamente. Já no que se refere ao dano significativo ao titular, os fatores considerados na lei incluem danos corporais, humilhação, danos à reputação, perda de emprego, oportunidades comerciais ou profissionais, perda financeira, roubo de identidade, efeitos negativos no registro de crédito e danos ou perda de propriedade.

[23] Australian Privacy Act. Disponível em: Disponível em: https://bit.ly/2ODkMIN.
[24] Personal Information Protection and Electronic Documents. Disponível em: https://bit.ly/3l9IlQm.

5.5. BRASIL - Considerações para a ANPD

Como pode ser observado, cada uma dessas leis, regulamentos e/ou normas setoriais apresentam prazos distintos para a comunicação do incidente de acordo com o grau de maturidade de proteção de dados desses países. O dever de ter que notificar açodadamente, ou seja, em curto espaço de tempo, à ANPD pode acarretar inúmeras notificações de meras ameaças ou de incidentes que, embora confirmados, não geram risco ou dano relevante aos titulares, além de sobrecarregar a autoridade prejudicando sua eficiência nas investigações que realmente merecem sua atenção.

Em meados de 2020, foi publicado um relatório pelo "Grupo de Especialistas Multissetoriais para a Avaliação do GDPR" que identificou que tem havido uma tendência entre as organizações de sobre-notificação de violações de dados, o que resultou em autoridades de proteção de dados locais sendo sobrecarregadas com notificações. Considerando a atual estrutura enxuta da ANPD, este é um ponto de séria preocupação e instamos a regulamentação futura a considerar critérios para que a ANPD se concentre nos casos mais relevantes, em vez de receber todas e quaisquer notificações de incidentes de segurança de dados pessoais.

Há que se considerar que muitas vezes pode haver apenas a mera suspeita de um incidente, que, porém, precisa de mais tempo para ser investigado de modo que haja sua confirmação ou não, dessa forma, a comunicação em duas etapas, a notificação prévia para a ANPD informando a suspeita de um incidente, seguido do prazo após sua confirmação, proporciona fôlego para que as organizações possam envidar seus melhores esforços para uma investigação aprofundada do incidente.

Nesse sentido, com relação aos incidentes que devem ser notificados, a ANPD, seguindo, por exemplo, os moldes da legislação canadense, poderia estabelecer os critérios ali apresentados como balizadores de incidentes de segurança que ensejam um risco ou dano relevante aos titulares, conforme exigido no *caput* artigo 48 da LGPD e, por consequência, indicar que seriam casos efetivos de notificação à ANPD e aos titulares.

Caso o controlador seja informado que é necessário realizar tal notificação, após preencher o questionário, a disponibilização de um formulário simplificado elaborado pela ANPD seria fundamental para permitir uma maior agilidade na submissão da comunicação pelos controladores, o qual deverá solicitar apenas informações objetivas e pertinentes ao incidente de segurança com dados pessoais a ser notificado.

Além disso, considerando que a análise e avaliação de riscos são processos que demandam bastante tempo para serem bem executados, é possível afirmar que o prazo sugerido de 2 dias úteis para notificar um incidente seria bastante oneroso e na prática pouco efetivo, pois muitas vezes o agente de tratamento ainda está procurando entender o que de fato ocorreu.

Nesse sentido, tendo em vista as dificuldades práticas que as empresas enfrentam nos primeiros dias após tomar conhecimento de um incidente de segurança, bem como o volume de incidentes ou suspeitas de incidentes que as organizações enfrentam diariamente, sugerimos uma alternativa faseada para que a comunicação de incidentes seja feita à Autoridade, conforme segue.

A organização que identifica um incidente de segurança deverá, no prazo de 3 dias úteis a contar da tomada de conhecimento concreto do incidente, enviar o que estamos chamando de uma notificação preliminar a ANPD, informando que foi detectado um incidente e que a empresas está trabalhando para identificar se de fato esse incidente afetou dados pessoais e tem o potencial de gerar riscos ou danos aos titulares de dados.

Tal notificação deverá ser feita em um formulário simplificado, permitindo assim a Autoridade monitorar os incidentes existentes e não onerando as organizações enquanto ainda estão buscando entender o ocorrido e adotar as medidas de mitigação necessárias. Uma referência interessante de citar refere-se à ferramenta criada pela Agência Espanhola de Proteção de Dados[25]. Disponibilizada no próprio site da Agência, em espanhol e em inglês, os controladores podem preencher, de forma anônima, um questionário com mais informações a respeito de incidentes de segurança com dados pessoais. A partir das respostas apresentadas, e com base em critérios pré-estabelecidos, a ferramenta indica para o controlador se o incidente deve ser notificado ou não. Sugerimos que a ANPD desenvolva algo no mesmo sentido, entendendo que tal ferramenta será muito útil em auxiliar as organizações a entenderem quais medidas devem ser adotadas.

Uma segunda etapa seria a efetiva comunicação do incidente à Autoridade, decorridos até 30 dias da notificação preliminar, e em um momento em que o controlador pode, de fato, afirmar se há potencial de risco ou dano ao titular do dado. É crucial garantir que as notificações submetidas à ANPD contenham informações precisas e sejam referentes apenas a incidentes relevantes, para evitar um sobrecarregamento do pessoal da autoridade.

Se o prazo for muito curto, conforme sugerido no formulário ora disponibilizado no site, a ANPD corre o risco de ser inundada com muitos incidentes pouco relevantes e não será capaz de se concentrar nos incidentes de maior relevância, causando atrasos desnecessários e prejudicando o bom desempenho da autoridade. O excesso de notificação também gerará um impacto negativo para os titulares, inicialmente alarmando-os indevidamente quanto aos impactos do incidente (e incitando suposições erradas em relação a algumas empresas), além de sujeitá-los a correr o risco de ignorar/perder aqueles incidentes que realmente representariam motivos de preocupação e gerariam a necessidade de tomar medidas.

Em adição ao prazo de 30 dias para a comunicação detalhada do incidente a ANPD, sugerimos que o mesmo prazo seja fixado para a comunicação do incidente aos titulares dos dados pessoais, caso necessária. Importante frisar que a comunicação ao titular dos dados sobre um incidente não deve ser exigida em toda e qualquer ocorrência sob pena de se gerar uma banalização de tais notificações, levando a sintoma similar àquele que se convencionou chamar de fadiga do consentimento. Algo que se faz o tempo muitas vezes deixa com que os titulares considerem com a atenção e seriedade que de fato demandam.

Por fim, gostaríamos de enfatizar que a privacidade, a segurança da informação e a confiança no ambiente digital são preocupações primordiais de nossos associados. A proteção de dados de nossos clientes e de sua privacidade em geral são essenciais para ganhar a confiança dos cidadãos em um mercado tecnológico global. Naturalmente, é de interesse das organizações parte do ecossistema de adotar medidas técnicas e organizacionais para gerenciar e analisar riscos, assim como para mitigá-los. Similarmente, a transparência com a ANPD e os titulares de dados é fundamental para nossos negócios e, portanto, prazos mais extensos para submissão de notificação permitirão com que os controladores tenham informações mais detalhadas sobre os incidentes de segurança que possam causar risco ou dano relevante e, consequentemente, farão com que as notificações sejam mais robustas e esclarecedoras possíveis, destacando todos os seus aspectos de interesse.

6. MECÂNICA DA REGRA DA COMUNICAÇÃO DE INCIDENTES

[25] AEPD. Comunica-Brecha RGPD. Disponível em: https://bit.ly/2P428Kt.

Sugerimos à ANPD que estabeleça algumas exceções à obrigatoriedade da notificação, especialmente em casos nos quais o controlador tenha comprovadamente implementado medidas de segurança apropriadas.

A Lei de Proteção de Dados da Irlanda[26] traz uma estrutura interessante para a implementação de proposta nesse sentido. De acordo com tal arcabouço, o controlador não é obrigado a notificar um incidente de segurança com dados pessoais quando ele tiver implementado medidas de proteção tecnológica e organizacional adequadas que foram aplicadas aos dados pessoais afetados pelo incidente, em particular quando as referidas medidas, incluindo a criptografia, tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-lo, ou até mesmo quando tiver tomado medidas em resposta ao incidente de segurança com dados pessoais que garantem que o elevado risco para os direitos e liberdades do titular em causa decorrente da violação já não é provável de se concretizar.

Desse modo, incidentes que não forem comunicados à ANPD deverão ser devidamente documentados pelas instituições, incluindo relatório de impacto à proteção de dados pessoais, a fim de que seja comprovado o cumprimento dos preceitos da LGPD. Tal prática está de acordo com os padrões globais de privacidade, incluindo o GDPR (Artigo 33).

6.1. CANAIS DE COMUNICAÇÃO TITULAR

Tendo em vista o caráter transversal da LGPD, aplicável a todas as organizações que tratam dados pessoais, independente de seu tamanho ou setor de atuação, entendemos que a normatização da lei deverá ser cuidadosa no sentido de estabelecer critérios flexíveis que possam ser atendidos por entidades dos mais diversos portes e natureza.

No que tange a possível necessidade de comunicação de um incidente de segurança aos titulares de dados atingidos por um incidente de segurança, entendemos que será importante que a norma venha a esclarecer que a organização responsável deverá escolher, de maneira autônoma, a forma pela qual a comunicação deverá ser implementada ao titular do dado.

Uma norma que permita que o meio de comunicação seja escolhido pelo controlador permitirá uma melhor gestão das informações e um melhor atendimento das expectativas dos titulares. Preocupa-nos que uma obrigação muito rígida de comunicação a LGPD poderá levar a experiência similar àquela que se convencionou fadiga de consentimento. Dito de outra forma, tantas serão as comunicações recebidas por um titular que de nada valerão pois serão vistas de maneira banalizada pelo titular de dados pessoais.

Portanto, a comunicação de incidentes de segurança aos titulares deve ser definida pelas próprias empresas e organizações, de modo que seja possível uma avaliação caso a caso, considerando a natureza da atividade da empresa, o contexto da coleta e do próprio incidente de segurança, a natureza dos dados pessoais objeto do incidente, o volume dos dados, dentre outros aspectos. Por exemplo:

(i) Se o número de titulares afetados for inferior a um determinado número, o controlador poderá optar por notificar de forma individualizada.

(ii) Se for muito difícil encontrar as informações de contato de todos os titulares envolvidos, ou se o número de titulares afetados atingir um limite onde seja muito

[26] Irlanda, Data Protection Act 2018. Disponível em: https://bit.ly/3f3wVBM.

trabalhoso notificá-los individualmente, a organização pode optar por criar avisos em seus respectivos sites, ou até mesmo optar pela divulgação do fato em outros meios de comunicação.

6.2. CONTEÚDO DA COMUNICAÇÃO AOS TITULARES IMPACTADOS

Conforme mencionado anteriormente, o artigo 48 da LGPD traz o dever de comunicação de incidentes de seguranças tanto a ANPD como aos titulares dos dados pessoais possivelmente afetados pelo incidente.

Embora a lei não antecipe os contornos e diferenças nessas comunicações, entendemos que o arcabouço normativo a ser editado pela ANPD deverá fazê-lo. O nível de detalhes fornecidos aos titulares dos dados pessoais não deve ser o mesmo que o fornecido à ANPD, e deve ser flexível para atender às necessidades específicas de cada tipo de incidente. Essa mesma abordagem é preceituada no GDPR em seu artigo 34(2)[27] e outras leis de privacidade. Os controladores não devem ser obrigados a revelar todos os detalhes específicos do número de pessoas afetadas para todas as pessoas afetadas, mas, em vez disso, eles devem apenas revelar as categorias de pessoas afetadas (por exemplo, se clientes, funcionários foram afetados etc.); também seria inadequado (e arriscaria futuros incidentes) que os controladores tivessem que compartilhar os mesmos detalhes em torno de suas "medidas técnicas e de segurança" que compartilham com a ANPD.

As organizações estão frequentemente mais bem posicionadas para saber como se comunicar com usuários/titulares de dados e podem ter suas próprias formas de efetuar tais comunicações, respeitando até mesmo o linguajar e estilo de comunicação de cada agente de tratamento com seu público-alvo.

Portanto, sugerimos que a ANPD adote os princípios fixados na LGPD, em especial o de responsabilidade e prestação de contas e permita as organizações flexibilidade para a determinação da melhor forma de atender o dispositivo legal com transparência e responsabilidade.

6.3. FORMULÁRIO DE COMUNICAÇÃO INCIDENTE DE SEGURANÇA

Entendemos que o formulário atualmente disponível no site da ANPD foi desenvolvido em caráter transitório para auxiliar a sociedade em um momento em que inúmeros incidentes de segurança vêm sendo revelados e a ANPD ainda não teve a oportunidade de desenvolver instrumento normativo próprio sobre o tema. De toda forma, gostaríamos de listar alguns pontos problemáticos da versão atual do documento, como uma forma de sugerir que essas questões sejam endereçadas durante a elaboração de futuro formulário definitivo:

1) Exigência de CPF/CNPJ: o formulário atual exige que o notificante apresente um número de CPF ou de CNPJ. Exigir essas informações pode impedir que empresas estrangeiras não estabelecidas no país, mesmo que sujeitas à LGPD, submetam notificações de incidentes de segurança;

2) Operador como comunicante: de acordo com o artigo 48 da LGPD, o controlador é o único agente de tratamento responsável por comunicar quaisquer incidentes de segurança. Sendo assim, entendemos que o operador não pode se configurar como

[27] Art. 34(2) A comunicação ao titular dos dados a que se refere o n. o 1 do presente artigo descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e medidas previstas no artigo 33. o , n. o 3, alíneas b), c) e d).

notificante e, portanto, deve-se presumir que todas as notificações submetidas foram realizadas por controladores.

3) Lista extensa sobre a natureza de dados afetados: no momento da comunicação, o controlador dificilmente terá a visibilidade de todos os tipos de dados pessoais afetados, pois esse levantamento será realizado durante o processo de análise e avaliação de riscos. Portanto, sugerimos que ao perguntar qual a natureza dos dados afetados, tenham apenas duas opções: (i) dados pessoais; e (ii) dados pessoais sensíveis.

4) Medidas de segurança: no momento da notificação, entendemos que seja fundamental que o controlador indique apenas as medidas de segurança que foram ou serão adotadas para mitigar os riscos ou danos atrelados ao incidente de segurança em questão. Isso porque é de nosso entendimento que todas as medidas técnicas e organizacionais de segurança compõem a estrutura de gestão de risco e são, portanto, muito complexas para serem apresentadas exaustivamente em uma notificação.

5) Confidencialidade: a ANPD deve deixar claro que todas as informações fornecidas pelos controladores nos formulários de notificação não serão publicizadas, tendo em mente os possíveis prejuízos em termos de reputação das organizações envolvidas.

7. ELABORAÇÃO DE ORIENTAÇÕES SOBRE INCIDENTES DE SEGURANÇA

Tendo em vista o estágio inicial da adoção da proteção de dados pessoais como direito fundamental e a disseminação da cultura de proteção de dados no país entendemos ser um passo importante e necessário a ANPD divulgar orientações para os agentes de tratamento de dados pessoais e os titulares com relação a definição de critérios para a gestão de risco necessária para a decisão com relação a comunicação de incidente de segurança nos termos da lei.

Um exemplo do que tem sido adotado no cenário internacional é o que recentemente o Comitê Europeu de Proteção de Dados realizou em janeiro de 2021, em que divulgou uma orientação sobre incidentes de segurança[28]. Nele discute-se diversos casos hipotéticos em que são analisadas quais medidas o controlador deveria ter adotado preliminarmente para oferecer o produto e/ou serviço, as medidas de mitigação e a obrigatoriedade de comunicar ou não a autoridade de proteção de dados, baseado na análise de risco ou dano aos titulares de dados.

Seguindo esse mesmo caminho, a Agência da União Europeia para a Cibersegurança (ENISA), centro especializado que promove a cibersegurança na Europa, elaborou, em janeiro de 2018, um guia[29] com o objetivo de orientar as empresas para o tratamento de dados pessoais na implementação do GDPR, no qual o controlador deve avaliar o impacto sobre os direitos e liberdades fundamentais dos titulares, resultantes da possível perda de segurança dos dados pessoais. Quatro níveis de impacto são considerados (Baixo, Médio, Alto, Muito Alto):

- Baixo: Inconvenientes leves que serão superados sem nenhum problema (tempo gasto reinserindo informações, aborrecimentos etc.);

[28] European Data Protection Board. Guidelines 01/2021 on Examples regarding Data Breach Notification, 2021. Disponível em: https://bit.ly/3bSgbuo.
[29] European Union Agency for Cybersecurity. Handbook on Security of Personal Data Processing, 2018. Disponível em: https://bit.ly/3t4rzu4.

- Médio: Inconvenientes razoáveis, que serão superados, apesar de algumas dificuldades (acesso negado a serviços comerciais, falta de compreensão, estresse, custo extra etc.);

- Alto: Inconvenientes expressivos, que serão superados, apesar de sérias dificuldades (dano patrimonial, perda de emprego, perda reputacional, agravamentos da saúde física e mental, nome sujo nos serviços de crédito etc.); e

- Muito alto: Consequências graves e até mesmo irreversíveis (inabilidade para trabalhar, danos físicos ou mentais permanentes ou de longo-prazo, morte etc.).

Por fim, a Agência Espanhola de Proteção de Dados[30] elaborou um guia prático para a gestão e comunicação de incidentes de segurança com objetivo de simplificar a interpretação do GDPR e auxiliar as organizações sobre a importância da gestão, tratamento e solução desses tipos de incidentes, assim como as medidas para sua prevenção, contendo uma (i) lista de mecanismos para detecção e identificação de possíveis violações, (ii) os tipos de violações de acordo com sua gravidades e (iii) um plano de ação de acordo com o número de titulares afetados e os processos que precisam ser levados para a comunicação perante a Agência[31].

Neste sentido, importante que a ANPD adote um guia orientativo para os agentes de tratamento de dados e que possam ser utilizados de referência - no processo de disseminação da cultura de proteção de dados no Brasil - para que organizações fiquem atentas para as medidas técnicas e administrativas que poderão adotar para demonstrar que estão em conformidade com a lei, assim como eventuais exemplos e hipóteses que devem ser olhadas com cautela por potencialmente se configurarem como um incidente de segurança.

Esse guia orientativo de medidas técnicas e administrativas pode ser bastante simples, mas ajudarão as organizações que estão dando seus primeiros passos na mudança de cultura com relação a proteção de dados e segurança da informação, tais como documentação de fluxo de dados, controles de acesso físico e digital, capacitação, treinamento e conscientização de colaboradores; dentre outros.

CONSIDERAÇÕES FINAIS

Esperamos que a visão prática e consequência da experiência de nossos associados com a experiência da implantação da cultura de proteção de dados e a legislação específica sobre esse tema em outras jurisdições ajude a trazer elementos para ajudar o importante papel da ANPD na normatização do tema de incidentes de segurança no Brasil.

Como forma de facilitar a compressão deste documento, apresentamos abaixo, de forma resumida, as recomendações desenvolvidas ao longo do texto para a tomada de subsídios proposta pela ANPD:

(i) Estabelecer, de forma clara, a diferença entre o termo incidente de segurança (evento adverso identificado que pode prejudicar os ativos de uma organização) do termo incidente de segurança com dados pessoais (evento adverso identificado que possa ocasionar risco e/ou dano para os direitos e liberdades do titular dos dados pessoais);

[30] AEPD. Guía para la gestión y notificación de brechas de seguridad. Disponível em: https://bit.ly/3e01DPm.
[31] Como exemplos ilustrativos, o guia apresenta critérios e valores para a criação de um cálculo sobre a classificação separado por: tipo de violação, descrição, origem, gravidade e volume aproximado de afetados.

(ii) Estabelecer os critérios a serem considerados em torno da metodologia da análise de risco para fins de determinação dos incidentes de segurança que deverão efetivamente ser comunicados, que podem incluir: (i) o tipo de violação, (ii) a natureza e sensibilidade dos dados pessoais, (iii) facilidade de identificação dos indivíduos, (iv) gravidade das consequências para os indivíduos e (v) características especiais dos indivíduos afetados;

(iii) Adotar conceitos de risco e dano claros para o contexto específico de incidente de segurança, respeitando o ordenamento jurídico pátrio e se beneficiando das experiências internacionais na temática de proteção de dados pessoais de modo a garantir uma interoperabilidade e harmonia entre os vários arcabouços de proteção de dados existente;

(iv) Estimular a utilização pelos agentes de tratamento de dados de framework globalmente reconhecidos no gerenciamento de risco para servir como uma forma de atendimento das obrigações previstas no artigo 46 da LGPD;

(v) Estabelecer que o prazo de notificação para a ANPD em até 3 dias úteis para que seja feita, na primeira etapa, a notificação preliminar sobre a ocorrência do incidente e, na segunda etapa, a efetiva comunicação do incidente decorridos 30 dias da notificação preliminar, garantindo informações precisas sobre o incidente;

(vi) Estabelecer exceções para a obrigação de notificar a ANPD quando o controlador comprovadamente tenha implementado as medidas de segurança apropriadas e não tiver havido risco ou dano ao titular dos dados;

(vii) Permitir que as organizações tenham flexibilidade sobre quais canais utilizam para comunicar os titulares dos dados pessoais atingidos por um incidente de segurança;

(viii) Esclarecer procedimentos e granularidade distintos para a comunicação sobre incidente de segurança aos titulares dos dados pessoais e à ANPD;

(ix) Ajustar o formulário de comunicação de incidente de segurança disponível no site da ANPD para (i) permitir que empresas estrangeiras submetam notificações à ANPD, (ii) excluir o operador como notificante, em respeito ao artigo 48 da LGPD, (iii) simplificar a lista sobre a natureza de dados afetados, (iv) permitir que o controlador apresente tão somente as medidas adotadas para mitigar os riscos/danos atrelados ao incidente e (v) garantir a confidencialidade do formulário com relação a terceiros;

(x) Elaboração de guias práticos ilustrativos como forma de orientar organizações de todos os tamanhos para que elas possam ter um balizador para o gerenciamento de riscos;

(xi) Elaboração de manuais exemplificativos de incidentes de segurança e elaboração do roteiro do exercício que deverá ser feito pelas organizações para verificar o melhor caminho para o atendimento da legislação.

Tendo em vista o exposto, claro está que os desafios diante da ANPD não são pequenos. Para que a Autoridade tenha uma história de sucesso na implementação da LGPD é fundamental que se tenha em mente que a normatização da LGPD deverá estar sempre pautada pela premissa de gestão de risco estruturante da legislação de proteção de dados no Brasil e em tantas outras jurisdições.

A norma não deverá tirar das organizações a autonomia - e a responsabilidade - de fazer o exercício de risco em cima de sua realidade e daí fixar as maneiras mais apropriadas para, naquele contexto, honrar com os princípios e direitos que emanam da LGPD. É fundamental, portanto, não estabelecer uma lista exaustiva de condutas, eis que fundamental permitir que as organizações, independentemente de seus tamanhos, possam fazer esforços proporcionais aos seus orçamentos e aos riscos atrelados aos seus respectivos modelos de negócio, tendo em mente a natureza, escopo, contexto e finalidade de suas atividades de tratamento, o que, inclusive, incentiva o desenvolvimento tecnológico, a inovação e a proteção aos direitos do titular dos dados pessoais.