TOMADA DE SUBSÍDIOS Nº2/2021 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

CONTRIBUIÇÃO DO DATA PRIVACY BRASIL SOBRE INCIDENTES DE SEGURANÇA

/ FICHA TÉCNICA

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

Associação de Pesquisa Data Privacy Brasil
Direção: Bruno Bioni e Rafael Zanatta
Coordenação Geral de Projetos: Mariana Rielli
Coordenação de Incidência: Bruna Santos

/ AUTORES

Bruno Bioni
Rafael Zanatta
Renato Leite Monteiro
Bruna Santos
Helena Secaf
Mariana Rielli
Pedro Martins
Davi Teófilo
Emanuella Halfeld
Gabriela Vergili
Iasmine Favaro
Julia Mendonça
Marina Kitayama
Pedro Saliba
Thaís Aguiar

Projeto Gráfico e Diagramação:
Roberto Junior

/ APRESENTAÇÃO

A Autoridade Nacional de Proteção de Dados (ANPD) recebeu contribuições para a Tomada de Subsídios nº 2/2021 sobre notificação de incidentes de segurança nos termos do art. 48 da LGPD como primeiro passo para a regulamentação da matéria. O Data Privacy Brasil, em sua missão de colaborar para o debate público sobre proteção de dados, submeteu a presente contribuição.

A contribuição foi feita a partir de um trabalho interinstitucional entre a Associação Data Privacy de Pesquisa e a Data Privacy Brasil Ensino. Além das questões estabelecidas pela ANPD, a contribuição seguiu três eixos de análise: 1) O que é um incidente de segurança e o que deflagra o dever de notificação? 2) Como e quando reportar um incidente de segurança? 3) Uma vez reportado qual deve ser o papel dos órgãos reguladores em termos de fiscalização e colaboração em um plano de contenção?

Ressalta-se que esta é a primeira contribuição do Data Privacy Brasil no processo de regulamentação de incidentes de segurança, que, por sua vez, também contou com sua primeira tomada de subsídios. Deste modo, tanto a posição institucional quanto o debate público acerca do tema ainda estão em processo de construção. Espera-se que interpretações e consensos possam surgir a partir deste documento e dos diálogos possibilitados por ele.

EIXO I

O que é um incidente de segurança e o que deflagra o dever de notificação?

Um incidente de segurança de proteção de dados é um evento que ocasiona a violação de algum dos três pilares da segurança da informação, ou de mais de um deles: confidencialidade, integridade e disponibilidade.

O dever de notificação, por sua vez, se apresenta a partir de duas perspectivas: um dever dialógico, tanto com o titular quanto com a Autoridade Nacional de Proteção de Dados, e uma obrigação que promove a adoção de medidas de mitigação para os riscos e/ou danos que podem ser ocasionados. Sendo assim, o dever de notificação é deflagrado pelo risco e/ou dano ocasionado aos titulares.

Por fim, entende-se que o incidente de segurança sempre deflagra um dever. Caso não exista um risco e/ou dano relevante, o agente de tratamento deve ao menos registrar o incidente e a avaliação que levou à considerá-lo irrelevante. Portanto, em uma lógica de regulação assimétrica propõe-se a seguinte escala de obrigações derivadas de um incidente de segurança:

I. SEM RISCO RELEVANTE

O incidente de segurança deve ser anotado nos registros das atividades de tratamento de dados, especialmente o juízo de valor do porquê foi considerado irrelevante;

II. RISCO RELEVANTE

Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e titular e ser ativado um plano de resposta à incidente de segurança;

III. DANO RELEVANTE

Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas também notificar os órgãos reguladores e o titular e o plano de resposta deve ser mais robusto frente ao do item anterior.

/ JUSTIFICATIVA

Inicialmente, é importante um recorte para delimitar o escopo da presente contribuição. Entende-se que o art. 46 da LGPD amplia o conceito de "incidente", não o restringindo apenas a violações de segurança da informação, mas a qualquer ilegalidade no tratamento de dados, na medida em que o referido artigo determinar que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas a proteger dados pessoais de "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Nesse sentido, a contribuição terá sua análise restrita às consequências geradas por incidentes de segurança. Um outro ponto importante é que o incidente de segurança (*security incident*) é um termo guarda-chuva para qualquer evento que comprometa as normas de segurança da informação de uma organização. O CERT.br define incidente de segurança como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores".[1]

Para o contexto da proteção de dados pessoais, deve-se limitar a análise para incidentes de segurança que envolvam dados pessoais. Incidentes de segurança que comprometam o funcionamento de uma máquina agrícola, por exemplo, ou que resultem no compartilhamento não autorizado de material protegido por segredo industrial não devem, a princípio, ser considerados como incidentes de segurança de dados pessoais, fugindo portanto do escopo da contribuição.

Feita essa ressalva, incidentes de segurança de dados pessoais podem ser divididos em três categorias: 1) incidentes de confidencialidade; 2) incidentes de disponibilidade; e 3) incidentes de integridade.[2]

Sendo assim, eventos que ocasionem a violação de algum desses três elementos de segurança da informação, ou de mais de um deles, serão considerados incidentes de segurança de dados pessoais.

A violação de confidencialidade pode se caracterizar quando há tentativa ou uso não autorizado de um sistema, seja utilizando técnicas como varreduras, força bruta SSH, ou mesmo sistemas de engenharia social capazes de fraudar identidades e usuários autorizados a acessar uma base de dados.

A violação de disponibilidade pode se caracterizar quando um dado é deletado permanentemente de forma acidental ou de forma não autorizada. A encriptação não autorizada ou acidental dos dados de forma a torná-los inacessíveis também deve ser considerada uma violação de disponibilidade, como no caso de um *ransomware*, por exemplo.

[1] CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Perguntas frequentes ao CERT.** 2017. Disponível em <https://www.cert.br/docs/certbr-faq.html#6>.

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

A violação de integridade pode se caracterizar quando existe algum tipo de alteração não autorizada com relação aos dados, criando dados inexatos, incompletos ou desatualizados.

Um exemplo de incidente pode ser uma situação em que um sistema que possui uma falha técnica (vulnerabilidade) tem essa falha explorada por um agente malicioso; ou ainda, a referida falha técnica pode permitir que dados sejam inadvertidamente publicados em área pública do sistema que não deveria mostrar aqueles dados.

Ainda, é possível que a disponibilidade seja afetada temporariamente, como no caso de um apagão de energia ou sobrecarga do servidor de armazenamento, por exemplo. Nesse caso, caso esse evento resulte em uma impossibilidade de acessar os dados, será caracterizado um incidente de segurança. Contudo, deve-se avaliar o risco apresentado por essa indisponibilidade. Uma indisponibilidade de acesso a uma aplicação de comércio eletrônico não oferece um risco significativo aos titulares. Por outro lado, a incapacidade de acessar dados de um paciente em um hospital oferece um risco muito maior.

Um último ponto a se considerar na definição de "incidente de segurança de dados pessoais" é se o incidente só é caracterizado quando uma ação comitiva viola algum desses elementos, ou se a mera inobservância de padrões de segurança que assegurem a confidencialidade, disponibilidade e integridade pode ser considerada, por si só, um incidente de segurança de dados pessoais.[3]

> **EXEMPLO:** Um hospital que possui um sistema de controle de acesso falho, permitindo que mais funcionários possuam a credencial e as permissões de "médico" do que o número de médicos empregados pelo hospital. Nesse caso, ainda que não se verifique um evento específico, em que um funcionário não autorizado acessou dados de saúde de pacientes, por exemplo, o risco aos titulares já está caracterizado por não haver um sistema que garanta a confidencialidade dos dados.[4]

Ressalta-se que não há necessariamente uma relação de causalidade entre a inobservância de padrões de segurança e o risco aos titulares. É possível que sistemas não seguros não gerem riscos relevantes para os titulares. Dito de outra forma, a relevância do risco é um elemento constitutivo do que se entende por incidente de segurança notificável. Essa interpretação sistemática entre dos

[3] ALUNGE, Rogers. **Breach of security vs personal data breach: effect on EU data subject notification requirements.** International Data Privacy Law. 2020. Disponível em: <https://doi.org/10.1093/idpl/ipaa021>.

[4] O exemplo citado encontra similaridades com o caso "Hospital do Barreiro", primeira multa aplicada pelo CNPD, Autoridade de Proteção de Dados de Portugal por, dentre outras violações, violar a confidencialidade e integridade dos dados sob seu controle. Disponível em: <https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-10-19-CNPD-Hospital-do-Barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos/>.

caputs dos artigos 44, 49 e 48 da LGPD. Apesar de um evento poder ser considerado um incidente de segurança, este só ganha repercussão jurídica, a ponto de desengatilhar a obrigação de notificação, se causar um risco relevante.

Contudo, isso não significa que um efeito adverso à confidencialidade, integridade e disponibilidade de uma base de dados, ainda que não cause um risco relevante, seja desprovida de qualquer efeito jurídico. Isto porque a negligência em não corrigir uma sucessão de incidentes de segurança sem risco relevante é o que pode assim torná-lo. Por esse motivo, tão importante quanto endereçar as nuances conceituais de um incidente de segurança nortificável, é fixar que cabe ao agente de tratamento de dados guardar registros sobre tais incidentes e, principalmente, acerca do seu juízo de valor acerca da sua (ir)relevância. O objetivo é formar uma trilha auditável dos incidentes de segurança**.**

Trata-se de uma interpretação que decorre da lógica precaucionário da proteção de dados, a partir da exegese do art. 49 da Lei Geral de Proteção de Dados, que traz o dever de "atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares" e nos princípios da prevenção (art. 6º, VIII da LGPD) e da responsabilização e prestação de contas (art. 6º, X).

Por fim, em relação ao dever de notificar, para se estabelecer o que deflagra esse dever, é preciso primeiro entender as razões pelas quais existe o dever de notificação. O principal objetivo da proteção de dados pessoais é a garantia dos direitos fundamentais dos titulares (art. 1º, caput da LGPD). Sendo assim, a notificação de um incidente de segurança deve ser compreendida como uma medida que tem como objetivo último proteger, ou mitigar os danos e/ou riscos ocasionados ao titular.

Ao notificar o titular, permite-se que ele tome as medidas que achar necessárias para resguardar seus direitos. Sejam elas medidas preventivas como a troca de credenciais e senhas, uma maior atenção em relação a e-mails e mensagens possivelmente fraudulentas, sejam também medidas afirmativas de exercício de direitos, seja em sede judicial, administrativa ou extrajudicial.

A notificação à Autoridade Nacional de Proteção de Dados, por outro lado, possui um objetivo objetivo duplo. Primeiro, a Autoridade Nacional pode auxiliar o agente de tratamento na avaliação dos riscos e/ou danos do incidente, e se haveria necessidade de também notificar o titular, além de sugerir medidas de mitigação de danos. Em segundo lugar, essa notificação ao órgão regulador é também uma maneira de demonstrar que o agente de tratamento está tomando as medidas necessárias para mitigar os riscos e cessar a violação.

Portanto, risco e/ou dano aos titulares que surgem a partir de um incidente de segurança de dados pessoais deflagra o dever de notificação. Ressalta-se, contudo mais uma vez, que um mero incidente de segurança, especialmente o juízo acerca do porquê não acarretaria risco relevante, também deve ter repercussão jurídica que é compor os registros das atividades de tratamento de

dados. Seguindo a ideia de uma regulação assimétrica e responsiva, quanto maiores os riscos, maiores os deveres. Há uma escalada na intensidade do conjunto de obrigações que derivam de um incidente de segurança:

I. **sem risco relevante:**
O incidente de segurança deve ser anotado nos registros das atividades de tratamento de dados, especialmente o juízo de valor do porquê foi considerado irrelevante;

II. **risco relevante:**
Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e titular e ser ativado um plano de resposta à incidente de segurança;

III. **dano relevante:**
Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e o titular e o plano de resposta deve ser mais robusto frente ao do item anterior.

Feito esse recorte e essa conceituação inicial, serão abordadas agora questões específicas levantadas pela Autoridade Nacional de Proteção de Dados que se relacionam com o eixo.

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

A relevância de um incidente de segurança se dá na medida em que direitos fundamentais dos titulares são ameaçados, não se limitando apenas ao direito à privacidade em outros direitos dos titulares previstos pela LGPD, mas a todos os direitos constitucionalmente garantidos. Recomenda-se que a ANPD tenha uma abordagem baseada em direitos para a avaliação de relevância de incidentes de segurança.

Ainda, com a constante evolução tecnológica, torna-se impossível prever todos os possíveis usos ilícitos de dados pessoais que podem colocar os titulares em risco. Sendo assim, é mais recomendável que não exista uma lista fixa de critérios de análise, mas sim diretrizes gerais para orientar a avaliação do risco de acordo com o contexto de cada caso. Possíveis critérios para essa avaliação serão melhor descritos na resposta da pergunta 4.

/ JUSTIFICATIVA

Diferentes incidentes de segurança podem ocasionar diferentes riscos e/ou danos aos titulares de dados. Em razão da massificação das atividades de tratamento de dados, um titular pode ter seus direitos e liberdades fundamentais violados das mais variadas formas por um incidente de segurança.

A ideia mais comum que se tem de incidente de segurança é associada ao "vazamento de dados", ou seja, incidentes de confidencialidade que podem violar a privacidade, a intimidade e a autodeterminação do titular, por exemplo. Nesse caso, deve-se ter claro que, embora a exposição não autorizada de dados sensíveis possa ser ainda mais gravosa, mesmo dados a princípio considerados "triviais", e até mesmo dados públicos, podem gerar riscos e danos para os titulares.

> **Exemplo:** A exposição de dados simples, como telefone e e-mail de clientes registrados em uma loja virtual pode dar ensejo a fraudes e golpes.

Por outro lado, a exposição de dados de nome completo e CPF de pessoas que se identificaram para acessar uma clínica de reabilitação de usuários de drogas gera um risco à privacidade e à intimidade muito grande.

Contudo, os riscos aos titulares não se limitam aos direitos tradicionalmente associados à privacidade. A indisponibilidade de dados de um paciente de um hospital pode gerar riscos à saúde e à integridade física do titular, por exemplo. Da mesma forma, a quebra de integridade de dados de um sistema de assistência social pode fazer com que pessoas que necessitam de algum benefício não o recebam.

Por fim, com a constante evolução tecnológica torna-se impossível prever todos os possíveis usos ilícitos de dados pessoais que podem colocar o titular em risco. Sendo assim, é mais recomendável que não exista uma lista fixa de critérios de análise, mas sim diretrizes gerais para orientar a avaliação do risco de acordo com o contexto de cada caso. Possíveis critérios para avaliação dos riscos serão melhor descritos na resposta da pergunta 4.

Sendo assim, a relevância de um incidente de segurança se dá na medida em que direitos fundamentais dos titulares são ameaçados, não se limitando apenas ao direito à privacidade, ou direitos dos titulares previstos pela LGPD, mas a todos os direitos constitucionalmente garantidos. Recomenda-se que a ANPD tenha uma abordagem baseada em direitos para avaliação de relevância de incidentes de segurança.

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

A categorização de risco e/ou dano em baixo, médio e alto é uma boa medida, tanto para avaliar as medidas que devem ser tomadas pelo agente de tratamento para mitigá-los, quanto para fixação de obrigações. Os níveis de risco devem ser distinguidos a partir dos critérios adotados para relevância do risco e/ou dano (conforme respostas das perguntas 1 e 4). Ainda, o risco e/ou dano baixo devem ser considerados como não relevantes, visto que não há que se falar em inexistência de risco.

Ressalta-se, contudo, que mesmo com a adoção de critérios mais objetivos, a avaliação do risco é sempre casuística, independentemente da(s) categoria(s) em que a ocorrência esteja inserida, visto que as particularidades de cada caso podem se mostrar determinantes.

/ JUSTIFICATIVA

Um risco e/ou dano baixo deve ser fixado de forma a não ser relevante. Isso porque toda atividade de tratamento de dados envolve algum grau de risco, bem como qualquer efeito adverso à confidencialidade, integridade e disponibilidade de uma base de dados. Sendo assim, não há de se falar em risco e/ou dano nulo ou inexistente.

Portanto, recomenda-se que riscos e/ou danos sejam considerados baixos à medida em que não causem grandes impactos adversos para direitos e liberdades do titular, representando mero incômodo.

Nesse sentido, os critérios elencados na resposta da pergunta 4 podem servir como um parâmetro para a definição do grau de risco e/ou dano.

Ademais, o grau de risco pode variar também ao longo do tempo, tendo-se em vista as inovações tecnológicas e o estado da arte das medidas de segurança e mitigação de riscos disponíveis no mercado, bem como as tecnologias usadas por invasores para criar novos usos para dados extraídos ilegalmente.

Um exemplo é o roubo ou perda de um computador de uma agência de publicidade com planilhas com dados detalhados de um grande número de titulares de dados, incluindo dados sensíveis. Caso esse computador não possua nenhum mecanismo de segurança, como senha, criptografia e/ou

exigência de credenciais de acesso para a planilha, o risco aos titulares seria alto. Por outro lado, na hipótese de existência de mecanismos de segurança robustos, e sem nenhum indício de que houve um roubo arquitetado com o objetivo de extração de dados, os riscos aos titulares seriam baixos.

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

De forma geral, a principal diferença entre um risco e um dano, no campo da proteção de dados, **é a materialização de alguma violação aos direitos fundamentais**. Um risco representa um potencial de violações, enquanto um dano sugere uma violação em concreto. Contudo, deve-se também ter em mente que a tutela da proteção de dados opera na lógica da inviolabilidade, e em decorrência do princípio da autodeterminação informativa, a mera perda do controle das informações pessoais pode representar um dano na esfera moral.

A distinção entre dano e risco, para o objeto em questão, possui um principal fator de relevância: a calibração das obrigações decorrentes de um incidente de segurança. Nota-se que o risco já é suficiente para deflagrar o dever de notificação. Ainda, quanto maior o grau desse risco, maiores os deveres, não só de notificação, mas também de adoção de medidas de mitigação.

/ JUSTIFICATIVA

Um incidente de segurança pode causar uma série de danos extrapatrimoniais, diante da sensação, por exemplo, de insegurança e receio em face da potencial divulgação indevida dos dados em questão. Em especial no caso de um vazamento de dados sensíveis, o incidente pode constituir também uma violação direta da privacidade e intimidade dos titulares.[5] Já os danos patrimoniais podem acontecer quando terceiros mal-intencionados utilizam os dados para cometimento das mais variadas fraudes, no que se costuma chamar de *identity theft*.

De forma geral, a principal diferença entre um risco e um dano, no campo da proteção de dados, é a materialização de alguma violação aos direitos fundamentais. Um risco representa um potencial de violações, enquanto um dano uma violação em concreto.

[5] GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados.** *In:* BIONI, Bruno *et al* (org.). **Tratado de proteção de dados pessoais**. São Paulo: Forense, 2021. Cap. 17. p. 628-666.

Contudo, a proteção de dados apresenta duas particularidades:

1. Ela opera na lógica da inviolabilidade[6], de forma que uma vez ocorrido o dano, é impossível o retorno ao *status quo ante*.

2. A mera perda de controle de informações pessoais pode representar, por si só, um dano moral, à medida que a autodeterminação informativa do titular é afetada. O efetivo roubo de identidade, por exemplo, representa uma concretização material do dano. Contudo, a impossibilidade de exercer controle sobre as informações pessoais também gera, por si só, um dano, ainda que de outra natureza.

A distinção entre dano e risco, para o objeto em questão, possui um principal fator de relevância: a calibração das obrigações decorrentes de um incidente de segurança. Nota-se, em primeiro lugar, que o risco já é suficiente para deflagrar o dever de notificação. Ainda, quanto maior o grau desse risco, maiores os deveres, não só de notificação, mas também de adoção de medidas de mitigação.

Por outro lado, a configuração de um dano pode ensejar obrigações também na esfera de reparação, não só a título indenizatório dos titulares, mas também no sentido de mitigar a permanência ou agravamento do dano. A título de exemplo, cita-se o caso estadunidense Equifax, em que a Federal Trade Commission (FTC), ao constatar o dano a milhões de titulares, fixou obrigações ainda mais severas, não só de indenização, mas também determinando que a Equifax constituísse um fundo provisório a título cautelar, oferecesse gratuitamente aos titulares afetados um serviço de monitoramento de uso de seus dados [*free credit monitoring*] e serviços gratuitos de restauração de identidade [*Free Identity Restoration Services*] para casos de fraude e roubo de identidade.[7]

Portanto, em uma lógica de regulação assimétrica, se o incidente de segurança chega a apresentar não só um risco, mas um risco e/ou dano, as obrigações de notificação e reparação se tornam ainda mais relevantes. Isso não significa, contudo, que o risco não possa, por si só, ser relevante a ponto de desencadear tais obrigações, conforme aprofundado adiante.

[6] BRASIL. Supremo Tribunal Federal. ***Medida Cautelar na Ação Direta 6.387/DF.*** Medida cautelar contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, que dispõe sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020". Requerente: Conselho Federal da Ordem dos Advogados do Brasil –CFOAB. Relatora: Min. Rosa Weber, 24 de abril de 2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>.

[7] FEDERAL TRADE COMMISSION. ***Equifax Data Breach Settlement: What You Should Know.*** 2019. Disponível em: <https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-settlement-what-you-should-know>.

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

Apresenta-se aqui uma lista de critérios que podem ser considerados na avaliação dos riscos e/ou danos do incidente, para determinar a relevância desse incidente e, seguindo a lógica que vem sendo argumentada até aqui, determinar quais obrigações seriam deflagradas.

Em uma lista não exaustiva, sugere-se os seguintes critérios de avaliação: Volume de dados pessoais; número de titulares possivelmente afetados; natureza dos dados pessoais; perfil dos titulares dos dados; existência de dados pessoais sensíveis; natureza da atividade do controlador; o que levou ao incidente de segurança; motivação do incidente de segurança; possibilidade de identificação dos titulares; consequências para os titulares da indisponibilidade ou quebra de integridade dos dados; possibilidade de reversão do risco e/ou dano ocasionado; possibilidade de agregação dos dados para extrair inferências ou traçar perfil comportamental do titular e, por fim, se a base de dados em questão foi pseudonimizada.

/ JUSTIFICATIVA

Com a massificação do uso de dados para diversas finalidades, a própria atividade de tratamento já é capaz de impactar a vida e desenvolvimento da livre personalidade do indivíduo[8]. No entanto, cabe uma análise pormenorizada a partir de cada incidente de segurança, de modo que os diferentes efeitos adversos sobre os indivíduos sejam levados em consideração.

Nesse sentido, os possíveis riscos e danos podem ser classificados em resultados físicos, materiais e imateriais[9]. Alguns exemplos podem ser roubo de identidade e fraudes diversas, envolvendo, inclusive, perdas financeiras, mas também danos à imagem, reputação pessoal e profissional, entre outros. Ressalta-se que violação à privacidade e à autodeterminação informativa não são meramente abstratas, mas possuem consequências reais nas vidas dos titulares, tanto de ordem emocional quanto material. Isso se torna especialmente mais grave no caso de grupos já vulnerabilizados, ou em situações em que havia uma relação de maior confiança entre o titular e o controlador de dados.

[8] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento.** Rio de Janeiro: Gen Forense, 2019.

[9] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

Nesse sentido, os critérios para avaliação dos riscos do incidente devem partir do seguintes elementos:

- Volume de dados pessoais

- Número de titulares possivelmente afetados

- Natureza dos dados pessoais

  Observação: Ressalta-se que a quebra de confidencialidade de dados públicos, publicamente acessíveis ou tornados manifestamente públicos pelo titular não representa, necessariamente, um menor risco e/ou dano, especialmente se houver cruzamento e/ou combinação desses dados com outros dados que não sejam publicamente acessíveis.

- Perfil dos titulares dos dados

  Exemplo: Titulares em situações de maior vulnerabilidade, como crianças, idosos, pessoas com deficiência podem ser desproporcionalmente afetadas por um incidente de segurança.

- Existência de dados pessoais sensíveis

- Natureza da atividade do controlador

  Exemplo: Uma indisponibilidade dos dados de um hospital é muito mais grave do que uma indisponibilidade de dados em um site de comércio eletrônico.

- O que levou ao incidente de segurança

  Exemplo: Em um ataque *ransomware* em que há uma ameaça por parte dos invasores de violação dos direitos dos titulares pode apresentar um risco muito maior para os titulares de usos futuros desses dados do que uma deleção acidental dos arquivos.

- Motivação do incidente de segurança

  Exemplo: Um incidente de segurança com motivações políticas, que quebra a confidencialidade de dados de ativistas, pode colocar esses titulares em posição ainda mais vulnerável, elevando o grau do risco.

- Possibilidade de identificação dos titulares

- Consequências para os titulares da indisponibilidade ou quebra de integridade dos dados

- Possibilidade de reversão do risco e/ou dano ocasionado

  Exemplo: A quebra de confidencialidade de dados como nome, CPF, impressão digital não pode ser reparada. Por outro lado, dados que podem ser alterados, como um login, ou dados pseudonimizados são passíveis de reparação.

- Possibilidade de agregação dos dados para extrair inferências ou traçar perfil comportamental do titular

- Se a base de dados foi pseudonimizada.

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

A principal hipótese de exceção da obrigação de informar a ANPD a respeito da ocorrência de um incidente de segurança é quando este resultar em um **risco e/ou dano baixo aos titulares de dados**, representando mera inconveniência ou incômodo. Contudo, ainda que não exista a obrigação de notificar, argumenta-se que o dever de registro do incidente e da avaliação feita se mantém.

Por fim, recomenda-se que, em observância ao princípio da prevenção e ao momento inicial de formação de uma cultura de proteção de dados no país, **que os agentes de tratamento, em caso de dúvida do grau de risco e/ou dano, notifiquem a Autoridade Nacional**, para que a ANPD possa oferecer maiores orientações e ajude o agente de tratamento na avaliação do risco e/ou dano, bem como indique possíveis medidas de mitigação.

/ JUSTIFICATIVA

Com fulcro no artigo 48 da LGPD, a notificação à ANPD deve ser feita sempre que o incidente puder resultar em "risco ou dano relevante" aos direitos e liberdades individuais, seja dos titulares de dados ou da coletividade. Nesse sentido, o grau de risco depende de fatores diversos, de modo que as boas práticas e governança do tratamento de dados (arts. 50 e 51, LGPD) têm um papel muito importante para determinar o que deve ou não ser notificado, inclusive sendo parte imprescindível para a justificativa de casos não notificados.[10]

[10] GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados**. *In:* BIONI, Bruno *et al* (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666.

Sendo assim, os incidentes de segurança de dados pessoais que apresentarem riscos e/ou danos considerados "baixos" (conforme argumentado na resposta da pergunta 2), podem ser dispensados da obrigação de notificar a Autoridade Nacional de Proteção de Dados.

Por exemplo, uma hipótese de dispensa da notificação seria o caso da perda de um dispositivo móvel criptografado com segurança, utilizado pelo controlador ou equipe[11]. Isso porque, se a chave de criptografia permanece na posse segura do controlador e esta não é a única cópia dos dados pessoais, então tais dados ficarão inacessíveis para um invasor, o que certamente dificultaria qualquer tipo de violação resultante em riscos ou danos para os direitos e liberdades dos titulares de dados em questão.

Por outro lado, a invasão do banco de dados de um hospital, por exemplo, é uma situação que implica maiores riscos e potencial de dano concretizado para a saúde dos titulares, haja vista que alterações ou exclusões de dados podem comprometer o tratamento adequado ao paciente. Desse modo, inevitavelmente, existe a necessidade de notificação à ANPD.

No entanto, um incidente que tenha como consequência apenas a necessidade dos titulares alterarem uma senha de acesso, por exemplo, pode ser considerado de baixo risco e, portanto, excetuada a obrigação de notificar, uma vez que o risco seria considerado uma mera "inconveniência".[12]

Destacamos também alguns exemplos de boas práticas realizadas por outras autoridades de proteção de dados do mundo:

A. A autoridade de proteção de dados do Reino Unido (*Information Commissioner's Office* – ICO), determina a notificação de incidentes que "coloquem em risco os direitos e liberdades das pessoas", excluindo dessa obrigação os casos nos quais **"não ofereceriam riscos para além da inconveniência"**;[13]

B. A autoridade francesa de proteção de dados (*Commission Nationale de L'informatique et des Libertés* – CNIL), por sua vez, determina que deverão ser notificados à autoridade incidentes que coloquem em risco a "vida privada" dos titulares. A estes deverão ser comunicados os incidentes que representem "risco elevado". **Caso haja dúvida na avaliação da situação, deve-se notificar**

[11] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

[12] LUCIANO, Maria. **Vazamentos de dados na LGPD: em busca do significado de "incidente de segurança"**. Revista do Advogado, São Paulo: AASP, ano 39, n. 144, p.163-225, nov. 2019.

[13] INFORMATION COMMISSIONER'S OFFICE. **Personal data breaches.** Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/>.

a autoridade para que ela determine a necessidade ou não de notificação.[14]

Ressaltamos também a importância da documentação de todos os processos de tomada de decisão, inclusive quando o controlador julgar que não há a necessidade de notificar à Autoridade e nem aos titulares. Tal obrigação de registro se encontra alinhada com os princípios de prevenção e responsabilização e prestação de contas, e o dever geral de registro das atividades de tratamento (art. 37), facilitando, inclusive, a posterior justificativa dos casos que não forem notificados.

Por fim, recomenda-se que, em observância ao princípio da prevenção e ao momento inicial de formação de uma cultura de proteção de dados no país, **que os agentes de tratamento, em caso de dúvida do grau de risco e/ou dano, notifiquem a Autoridade Nacional**, para que a ANPD possa oferecer maiores orientações e ajude o agente de tratamento na avaliação do risco, bem como indique possíveis medidas de mitigação.

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

Em harmonia com o que se argumentou até aqui, bem como os parâmetros internacionais sobre a questão, entende-se que o dever de informar os titulares sobre um incidente de segurança de dados pessoais pode ser excetuado nas seguintes hipóteses: 1) Quando o risco e/ou dano ao titular for baixo. 2) Quando o agente de tratamento tenha aplicado medidas de segurança técnicas e organizacionais que tornam eventual incidente irrelevante para os titulares. 3) Quando, após o incidente, o agente de tratamento tomar medidas de mitigação para garantir que um eventual risco e/ou dano aos titulares não seja mais provável de se concretizar. Por fim, 4) Quando a comunicação individual aos titulares envolver um esforço desproporcional, o controlador poderia fazer a comunicação de forma pública e difusa.

/ JUSTIFICATIVA

O critério primordial para identificar a necessidade ou não de informar um incidente de segurança aos titulares de dados é a probabilidade de resultar em altos riscos para os seus direitos e liberdades individuais. Dessa forma, verificada a gravidade do incidente, a ANPD poderá determinar que o controlador adote algumas providências, como divulgar amplamente o fato em meios de comu-

[14] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Les violations de données personnelles.** 20 jun. 2018. Disponível em: <https://www.cnil.fr/fr/les-violations-de-donnees-personnelles>.

nicação, além de determinar a adoção de medidas para mitigar os possíveis efeitos (art. 48, § 2º da LGPD). Nesse mesmo sentido, ao informar os titulares sobre o ocorrido, os controladores podem fornecer informações e orientações sobre as medidas a serem tomadas, para garantir a proteção em relação às possíveis consequências.[15]

Ocorre que nem todos os incidentes precisam ser informados aos titulares, até para protegê-los de um excesso de notificações desnecessárias. Assim, tratando sobre hipóteses de desnecessidade de notificação, o artigo 34 (3) da GDPR elenca algumas condições e circunstâncias:

A. **Quando o agente de tratamento aplicou medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes da violação**, principalmente medidas que tornam os dados pessoais ininteligíveis, como a criptografia, para qualquer pessoa que não esteja autorizada a acessá-los. O que, dentro de uma perspectiva brasileira, coincide com o disposto no artigo 48 § 3º da LGPD.

B. **Imediatamente após uma violação, o controlador tomou medidas para garantir que o alto risco inicialmente representado para os direitos e liberdades dos indivíduos não seja mais provável de se concretizar e resultar em dano.** Por exemplo, dependendo das circunstâncias do caso, o responsável pelo tratamento pode ter imediatamente identificado e tomado medidas contra o indivíduo ou grupo que acessou os dados pessoais antes que houvesse alguma consequência relevante decorrente do incidente. A devida consideração ainda precisa ser dada às possíveis consequências de qualquer quebra de confidencialidade, mais uma vez, dependendo da natureza dos dados em questão.

C. **Quando a comunicação individual acerca do incidente envolveria um esforço desproporcional.** Nos casos em que, por exemplo, os dados de contato do indivíduo tenham sido perdidos como resultado da violação ou não sejam conhecidos em primeiro lugar. Um exemplo é a inundação de um depósito de um escritório de estatística, resultante na perda dos documentos contendo dados pessoais, que foram armazenados apenas em papel. Em situação semelhante, o controlador deve fazer uma comunicação pública ou tomar medida equivalente, a fim de garantir que as pessoas sejam informadas de forma igualmente eficaz.

[15] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

Nesse mesmo sentido, no parecer 03/2014[16], o qual aborda as notificações em caso de violação, o WP29 explicou que uma violação de confidencialidade de dados pessoais que foram, por exemplo, criptografados com um algoritmo de última geração, ainda assim configura uma violação de dados pessoais, devendo ser notificada à Autoridade. No entanto, se a confidencialidade da chave estiver intacta, ou seja, se a chave não foi comprometida com nenhuma violação de segurança e foi gerada de forma a não ser acessada por qualquer pessoa que não esteja autorizada, então os dados são, em princípio, ininteligíveis. Portanto, é improvável que a violação afete de maneira adversa os indivíduos e, como consequência, não exigiria comunicação aos mesmos.

[16] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2014 on Personal Data Breach Notification.** 2014. Disponível em: <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/03/WP-Opinion-032014.pdf>.

EIXO II

Como e quando reportar um incidente de segurança?

Neste eixo, busca-se responder a perguntas relativas a "como" realizar notificações e comunicações relativas a incidentes de segurança que envolvam dados pessoais. Para pensar em forma e prazo da notificação será de suma importância resgatar o objetivo por trás de se notificar a Autoridade e aos Titulares. Resgatar e entender o objetivo por trás das notificações pode ser útil para apontar caminhos possíveis e esperados, que sempre busquem o objetivo da notificação, assim como o da própria comunicação ao titular, que é o de limitar os riscos e danos decorrentes do incidente.

Nesse sentido, em relação ao prazo de notificação a Autoridade, a combinação entre os fatores - celeridade como regra e tempo razoável para identificação do nível de risco e dano podem servir como parâmetro, visto que a notificação busca munir a Autoridade para uma investigação e mitigação de danos. No caso da comunicação do titular, a finalidade da notificação é alertar sobre os riscos e está relacionada ao fornecimento de informações específicas sobre as etapas que estes devem seguir para se proteger e, caso necessário, buscar mais informações. Dessa forma, por mais que possuam objetivos diferentes, as notificações à Autoridade e ao Titular se assemelham por buscarem sempre limitar os danos decorrentes do incidente. Serão agora endereçadas as questões específicas levantadas pela Autoridade Nacional de Proteção de Dados que se relacionam a esse eixo:

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

CRITÉRIO: O TIPO DE INCIDENTE

Informações que devem ser prestadas:

- tipo do incidente de segurança, conforme divisão tripartite (confidencialidade, integridade, disponibilidade);
- descrição geral do incidente de segurança (ex: caso de hacking, malware, vazamento, etc);
- tipo de incidente de tratamento inadequado (tratamento em desconformidade com a LGPD, mas que não viole algum dos pilares da segurança da informação)

CRITÉRIO: NATUREZA, SENSIBILIDADE E VOLUME DOS DADOS PESSOAIS

- natureza dos dados (tipos de dados pessoais alvos do incidente, tais como dados cadastrais, identificadores únicos, dados financeiros, dados de geolocalização, etc) - art. 48, §1º, I da LGPD;
- sensibilidade dos dados (no caso de haver dados sensíveis, conforme definição da lei, envolvidos no incidente, descrição em destaque);
  - » caso não haja dados sensíveis, criticidade dos tipos de dados, como aqueles protegidos por algum tipo de sigilo regulatório (lei do sigilo bancário) ou que tenha alguma classificação de restrição de circulação (segredo, sigiloso, circulação interna, público)
- volume estimado de dados afetados pelo incidente;
- volume estimado de indivíduos afetados pelo incidente.

CRITÉRIO: CARACTERÍSTICA DOS TITULARES

- as informações sobre os titulares envolvidos (art. 48, §1º, I)
  - » tipos de titulares atingidos (clientes, pacientes, usuários, assinantes, estudantes, trabalhadores etc);
  - » relação dos titulares impactados com o agente, caso haja (clientes, pacientes, usuários, assinantes, estudantes, trabalhadores etc);
  - » presença de titulares impactados que são crianças ou adolescentes e estimativa de volume de indivíduos com essa característica afetados.

CRITÉRIO: SEVERIDADE DAS CONSEQUÊNCIAS PARA OS INDIVÍDUOS

- os riscos relacionados ao incidente (art. 48, §1º, IV)
  - » síntese da conclusão da avaliação de risco realizada previamente pelo agente, com destaque para principais pontos de atenção;
  - » tempo estimado em que os dados pessoais estiveram comprometidos.

OUTRAS INFORMAÇÕES

- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (art. 48, §1º, III);
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 48, §1º, VI);
- dados do controlador (nome, informações de contato, identificação do encarregado ou ponto de contato designado);
- indicação de caráter transfronteiriço do incidente;
- os motivos da demora, no caso de a comunicação não ter sido imediata (art. 48, §1º, V);
- intenção de complementar posteriormente a notificação original, com indicação prévia de quais informações podem estar incompletas ou imprecisas.

/ JUSTIFICATIVA

Ao adentrar no "como" das notificações e comunicações relativas a incidentes de segurança que envolvam dados pessoais, é importante resgatar o próprio objetivo de se notificar a Autoridade competente e/ou comunicar os titulares acerca do ocorrido. O que se almeja com isso? A LGPD é, conhecidamente, uma norma que consagra, junto ao princípio da segurança (art. 6º, VII), também o da prevenção (art. 6º, VIII). Para além dos princípios, todo o desenho da norma aponta para a busca de um equilíbrio entre, de um lado, a razoabilidade na implantação de medidas (técnicas e administrativas) preventivas, isto é, que evitem a concretização de incidentes de segurança, e a mobilização para contenção de incidentes e mitigação de danos diante da sua ocorrência. Se é verdade que a lógica por trás de normas horizontais de proteção de dados é proteger os titulares contra quaisquer usos inadequados de seus dados pessoais, visando evitar os danos de diversas naturezas que eles podem causar, também é verdade que parte substancial dessas normas, e das obrigações que elas geram, dedica-se justamente a lidar com a quase inevitabilidade dos incidentes.

Partindo desse ponto, destaca-se, mais uma vez, a lógica de corregulação e accountability (princípio denominado "responsabilização e prestação de contas" na LGPD) que permeia a LGPD: no caso de incidentes de segurança e do dever de notificação, por exemplo, é responsabilidade dos agentes de tratamento adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Isso se desdobra na previsão de que a dosimetria das sanções

administrativas da lei levará em consideração "adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados" (art. 52, § 1º, VIII). Cabe ao agente, melhor posicionado nesse ecossistema, tanto a adoção de medidas preventivas, quanto a avaliação inicial do risco gerado por um eventual incidente e dos danos que podem recair sobre os titulares. Tal análise é que deflagra, ou não, o dever de notificação. Por outro lado e de forma complementar, cabe à Autoridade Nacional de Proteção de Dados (ANPD) a tarefa de conduzir a sua própria investigação, além de possivelmente determinar medidas específicas que o agente deve tomar para responder ao ocorrido. Um dos objetivos desta notificação (assim como o da própria comunicação ao titular) é o de limitar os danos decorrentes do incidente.

Diante desse quadro, uma forma de sistematizar **quais** informações devem constar em uma notificação à Autoridade competente é partir do conjunto de informações reunido pelo próprio agente de tratamento de dados ao avaliar a gravidade/risco do incidente. Salvo poucas exceções, as informações que alimentaram a análise inicial do agente serão imprescindíveis ao trabalho da Autoridade, seja para identificar eventuais falhas no plano de resposta desenvolvido e determinar medidas adicionais, seja no curso geral da investigação por ela conduzida. Assim, os critérios gerais levados em consideração para a determinação do dever de notificar podem ser o ponto de partida, do qual são extraídas as categorias específicas de informações que devem ser fornecidas. Algumas dessas informações já são exigidas pela própria LGPD, no seu art. 48, mas há outras que não foram descritas pelo legislador, conforme tabela explicativa acima.

Descritas as categorias de informação que devem ser fornecidas à Autoridade por meio de notificação, cabe ressaltar a possibilidade, consagrada no Regulamento europeu, de "faseamento" da notificação, isto é, o fornecimento, em um primeiro momento (vide resposta seguinte) das informações disponíveis a partir da análise de risco que deflagrou o dever de notificação e, constatada a incompletude das informações, ou descobertas outras informações no curso da investigação interna, a possibilidade de complementação da notificação, sempre com o objetivo de munir a Autoridade do máximo de subsídios para atuar diante do incidente. Isso decorre da noção de que a indisponibilidade, em um determinado momento, de informações precisas ou completas sobre um incidente não deve ser um obstáculo para a pronta notificação. A intenção de complementar a notificação com informações adicionais também deve ser objeto da notificação original.

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

Os fatores que devem ser considerados na definição de um prazo razoável são, principalmente, os seguintes: por um lado, um dos objetivos primordiais da notificação é robustecer as medidas de contenção e mitigação dos danos gerados pelo incidente, de forma que a celeridade é um aspecto central; por outro, apenas incidentes que imponham "risco ou dano relevante" geram o dever de notificar, o que pressupõe a existência de um período de avaliação interna do ocorrido e reunião de informações que darão suporte à própria notificação.

A combinação entre os fatores - celeridade como regra e tempo razoável para identificação do nível de risco e dano - sugerem que a abordagem adotada pela GDPR **(72 horas a partir do conhecimento do incidente)** pode ser um ponto de partida interessante. Nesse ponto, importante ressaltar que a referência ao Decreto nº 9.936, de 2019, que regulamenta a Lei do Cadastro Positivo e prevê um prazo de dois dias úteis para notificação à ANPD, embora seja válida por se tratar da única previsão em lei atual sobre a matéria, não deve ser a base da regulamentação pretendida.

/ JUSTIFICATIVA

Observando legislações de outros países que tratam do dever de notificar incidentes de segurança envolvendo dados pessoais, percebe-se que o prazo para a notificação inicial varia de 24 a 72 horas, a partir do conhecimento do agente responsável pela notificação acerca da existência de um incidente. Há também normas que optam por comandos abertos, como "imediatamente", ou "em tempo razoável", como é o caso da LGPD.

Os fatores que devem ser considerados na definição de um prazo razoável são, principalmente, os seguintes: por um lado, um dos objetivos primordiais da notificação é robustecer as medidas de contenção e mitigação dos danos gerados pelo incidente, de forma que a celeridade é um aspecto central; por outro, apenas incidentes que imponham "risco ou dano relevante" geram o dever de notificar, o que pressupõe a existência de um período de avaliação interna do ocorrido e reunião de informações que darão suporte à própria notificação.

Por último, conforme mencionado anteriormente, a eventual incompletude ou imprecisão de certas informações não é óbice para a pronta notificação, na medida em que ela pode ser posteriormente complementada. Dessa forma, o controlador não pode se eximir de notificar o ocorrido sob a justificativa de aguardar a finalização de uma perícia ou outro processo técnico excessivamente prolongado.

A combinação entre os fatores - celeridade como regra e tempo razoável para identificação do nível de risco e dano - sugerem que a abordagem adotada pela GDPR (72 horas a partir do conhecimento do incidente) pode ser um ponto de partida interessante. Nesse ponto, importante ressaltar que a referência ao Decreto nº 9.936, de 2019, que regulamenta a Lei do Cadastro Positivo e prevê um prazo de dois dias úteis para notificação à ANPD, embora seja válida por se tratar da única previsão em lei atual sobre a matéria, não deve ser a base da regulamentação pretendida.

Não foi possível identificar outras legislações, ao redor do mundo, que considerem se tratar de dia útil ou não um fator na delimitação do prazo de notificação. Justamente em razão do potencial gravoso de incidentes de segurança que envolvam dados pessoais, é preferível que o prazo estabelecido se dê em dias corridos, ou até mesmo em horas, a fim de se evitar prolongamentos desnecessários. Por se tratar de situação excepcional, não há justificativa razoável para o condicionamento do prazo a esse fator específico.

Por fim, discorre-se brevemente sobre o elemento "a partir do conhecimento do incidente", ponto de partida para a contagem do prazo para notificação à Autoridade. Diante de previsão semelhante no Regulamento europeu, o antigo Working Party 29 debruçou-se sobre o tema e sugeriu a combinação de dois fatores sobre essa definição: a certeza razoável sobre a ocorrência de um incidente de segurança + a certeza razoável de que tal incidente envolveu o comprometimento, seja qual for o tipo, de dados pessoais. Veja-se, não se trata de ciência sobre os detalhes do incidente, nem mesmo sobre o volume estimado de indivíduos afetados, ou categorias específicas de dados comprometidos. Basta que o controlador tenha uma certeza, baseada em indícios razoáveis, de que um incidente de qualquer natureza ocorreu e que esse incidente envolveu dados pessoais em sua custódia, que é considerado o "conhecimento do incidente". O fator existência de dados pessoais envolvidos é relevante, na medida em que pode ser que haja o alerta muito rápido sobre um incidente, sem que haja certeza razoável, em um momento inicial, de que dados pessoais (e não outros dados, por exemplo) foram comprometidos.

Acerca disso, dois pontos conclusivos: a identificação da existência de um incidente, bem como a análise do risco envolvido e potenciais danos (ambos fatores essenciais tanto para a deflagração do dever de notificar quanto da possibilidade de fazê-lo no prazo adequado) estão diretamente relacionadas a obrigações estabelecidas na LGPD, como a instalação de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais (art. 48) ou os próprios deveres relacionados à governança de dados. Isso evidencia a relação próxima entre os princípios da segurança e da prevenção. Ademais, seja quando se fala de prazo máximo para a primeira notificação, ou mesmo para a determinação do momento em que o agente tem conhecimento do incidente, o mote sempre deve ser de máxima prontidão na tomada de medidas necessárias para o controle do incidente e mitigação dos danos, desde a primeira investigação sobre uma suspeita. Em suma, entendemos que o prazo de 72 horas contados a partir do momento que o controlador toma conhecimento do incidente de segurança que envolve dados pessoais é razoável para atingir os objetivos de proteção da notificação.

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

Em um cenário de incidente tal qual descrito no caput do art. 48 da LGPD, ou seja, aquele que possa acarretar risco ou dano relevante aos titulares, entendemos que a comunicação ao titular deve ocorrer assim que do conhecimento do controlador acerca das circunstâncias de risco em questão e do não cabimento de nenhuma das hipóteses de exceção delineadas nas respostas anteriores, já que se parte do pressuposto de que nem todo incidente necessariamente será reportado aos titulares.

Nesse sentido, o próprio processo de avaliação de riscos aos titulares, ao indicar que este é considerável, serve enquanto critério para se chegar à conclusão preliminar de que um incidente deve ser notificado ou, no caso, comunicado aos titulares. Ademais, o processo já pressupõe a reunião de informações mínimas que permitem ao titular tomar medidas protetivas e mitigatórias do risco ou dano. Diante disso, a comunicação deverá se dar imediatamente a partir da constatação do referido dever.

Entendemos, entretanto, que a comunicação ao titular difere da notificação à Autoridade na medida em que há algumas circunstâncias em que as **próprias medidas tomadas pelo controlador, por exemplo, afastarão o dever de comunicação.** Dessa forma, o dever de comunicação ao titular deve se dar de forma independente do prazo máximo estipulado em relação à notificação da Autoridade, na medida em que há um elemento adicional de análise - a verificação de alguma hipótese de desobrigação da comunicação, inclusive pela adoção de medidas mitigatórias. **A regra, em todos os casos, deve ser que, constatado o dever geral de notificar e afastadas tais hipóteses, a comunicação seja imediata.**

/ JUSTIFICATIVA

Diferentemente da LGPD, a GDPR faz uma diferenciação expressa entre o que seria a obrigação de notificação à Autoridade e a obrigação de comunicação do titular dos dados nos casos de incidentes de segurança. Em relação à Autoridade, a GDPR estipula que a notificação deve ocorrer quando o incidente puder gerar riscos aos direitos e liberdades dos titulares, enquanto a comunicação aos titulares é mandatória apenas quando este risco for elevado.

No caso da Autoridade, a normativa europeia estabelece o prazo de notificação de até 72h após o controlador ter realizado investigação sobre o incidente que o permita concluir que ele representa um risco aos direitos e liberdades individuais. Entretanto, não há previsões temporais específicas quanto ao prazo para a hipótese de comunicação do titular, a única determinação é de que esta deverá ser realizada assim que o controlador tiver conhecimento da situação de alto risco[17]. Considerando que a situação descrita no caput do art. 48 da LGPD descreve um "risco ou dano relevante", o cenário aproxima-se daquele inscrito na previsão do art. 34 da GDPR.

É nesse mesmo sentido que entendemos que, via de regra, no caso de incidentes de segurança, deverá haver a notificação do titular, a não ser quando: (i) o risco e/ou dano ao titular for baixo; ou (ii) quando as medidas de segurança técnicas e organizacionais tornaram o incidente irrelevante para os titulares; ou (iii) quando, após o incidente, as medidas de mitigação garantam que o risco e/ou dano aos titulares não é mais provável de se concretizar; ou (iv) quando a comunicação aos titulares individualmente envolver um esforço desproporcional. Por isso, a notificação do titular, se não desproporcional, cabe sempre que houver uma circunstância de maior risco (não baixo) que não tenha sido dirimida por medidas do controlador.

A caracterização da comunicação sem demora será entendida a partir da avaliação de oportunidade do controlador, em que serão consideradas a natureza e gravidade da violação em si, bem como do nível de risco para os titulares. O Considerando 86, por exemplo, aponta como a avaliação da oportunidade da comunicação deverá ser considerada diferentemente em determinados casos. Quando, por exemplo, o controlador tiver conhecimento da necessidade de mitigar um risco imediato, é necessária a comunicação de pronto. Por outro lado, a comunicação a respeito da necessidade do controlador implementar medidas contra a continuidade da violação ou prevenção de ocorrências semelhantes podem justificar mais tempo para envio. Ainda sobre circunstância que justifiquem a não imediata comunicação do titular, o Considerando 88, do mesmo modo que o art. 3, (5) do regulamento da Comissão Europeia n. 611/2013, indica que a comunicação ao titular dos dados pode ser atrasada por uma autoridade para preservar a integridade de uma investigação sobre as circunstâncias da violação.

Algo importante a ser considerado na avaliação da razoabilidade do tempo de comunicação do titular é a diferença entre os objetivos desta e da notificação à Autoridade. No caso da comunicação do titular, a finalidade é de alerta e está relacionada ao fornecimento de informações específicas sobre as etapas que estes devem seguir para se proteger e, caso necessário, buscar mais informações.[18]

[17] EUROPEAN DATA PROTECTION BOARD. **Guidelines 01/2021 on Exemples regarding Data Breach Notification.** Jan, 2021, p. 06. Ver também: CENTRE FOR INFORMATION POLICY LEADERSHIP. **Comments by the Centre for Information Policy Leadership On the Article 29 Working Party's "Guidelines on personal data breach notification under Regulation 2016/679".** Dec. 2017, p. 11-15.

[18] SOMBRA, Thiago Luís e CASTELLANO, Ana Carolina. **Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva.** Revista do Advogado. AASP, 2019 v. 39 n. 144 nov, p. 168-173.

Como observado, dependendo da natureza da violação e do risco apresentado, a comunicação oportuna ajudará os indivíduos a tomar medidas para se proteger de consequências danosas da violação.

Considerando que um dos objetivos da comunicação é fornecer informações para que o titular possa se proteger e, também, que os aspectos de um processo de investigação podem ser mais morosos que outros, a comunicação não necessariamente deve ser feita de uma só vez, podendo, se adequado, ser dividida em momentos distintos[19]. Se uma parte da investigação é concluída e o controlador percebe que há a necessidade de comunicação do titular, ele deverá fazê-la imediatamente, fornecendo ao indivíduo as orientações possíveis para mitigação do risco ou dano. Conforme novas partes da investigações forem sendo concluídas, novos comunicados, quando cabíveis, devem ser enviados.

Partindo dessa perspectiva, entendemos que mais adequado que colacionar o prazo de comunicação do titular ao prazo de notificação da Autoridade, ou mesmo que afixar um prazo diferente para a comunicação, seria determinar de que ela ocorra logo que o controlador tenha conhecimento (ou informações suficientes para tanto) de que o incidente representa riscos relevantes aos titulares e que também tenha avaliado a inexistência de alguma hipótese de afastamento do dever de comunicação. Nesse sentido, caberá a Autoridade fazer uma avaliação de oportunidade sobre o período da comunicação e sobre a existência de eventuais justificativas para atrasos.

Que informações devem constar dessa comunicação?

Entendemos que as informações mínimas referentes à comunicação do titular devem ser:

- A descrição da natureza dos dados pessoais afetados (§ 1º, I, art. 48 da LGPD);
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (§ 1º, III, art. 48 da LGPD);
- Os riscos relacionados ao incidente; (§ 1º, IV, art. 48 da LGPD);
- Os motivos da demora, no caso de a comunicação não ter sido imediata; (§ 1º, V, art. 48 da LGPD);
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. (§ 1º, VI, art. 48 da LGPD);
- Uma descrição da natureza da violação;
- Informações de contato do responsável pela proteção dos dados e também qual o melhor canal de comunicação para dirimir dúvidas (SAC);
- Possíveis medidas a serem tomadas pelo titular para mitigar riscos, danos e efeitos adversos (como alterar a sua senha);
- A data estimada do incidente.

[19] Commission Regulation (EU) N. 611/2013, (7).

Entendemos, também, que a comunicação do titular deverá tratar exclusivamente do incidente, não podendo incorporar informes de assuntos distintos. Além disso, ressaltamos que a comunicação, nos termos da LGPD, não exime o controlador de cumprir com eventuais previsões de comunicação referentes a outras normativas setoriais eventualmente aplicáveis.

/ JUSTIFICATIVA

Por não diferenciar as hipóteses de notificação da Autoridade e de comunicação do titular, o conteúdo prescrito como mínimo dos informes em ambos os casos é a princípio o mesmo. Apesar de as indicações sobre informações mínimas necessárias aparecem de forma conjunta no texto da Lei, entendemos que, assim como em relação ao prazo de comunicação, deve-se considerar as particularidades acerca de seus objetivos, inclusive no tipo de linguagem utilizada.

Com base em normativas europeias, e observando as particularidades da comunicação ao titular dos dados, entendemos que para além dos pontos já exigidos pelo § 1º do art. 48, ainda é importante que a comunicação ao titular contenha:

I. Uma descrição da natureza da violação (eg. se foi um vazamento, uma encriptação, etc)
II. Informações de contato do responsável pela proteção dos dados e um canal ativo de comunicação
III. Possíveis medidas a serem tomadas pelo titular para mitigar riscos, danos e efeitos adversos.
IV. A data estimada do incidente

Sobre o tópico **(iii)**, é importante observar que as medidas de mitigação de riscos e danos irão variar de acordo com o caso concreto, de modo que não há como predeterminar uma lista de quais medidas a comunicação deve conter. Alguns exemplos nesse sentido, a depender do caso concreto, seriam: a redefinição de senha, aconselhamento de uso de senhas exclusivas, cuidado com e-mails de *phishing* ou atividades fraudulentas em suas contas, atualização de sistemas, criptografia de dados.[20]

Do mesmo modo que alguns requisitos mínimos específicos poderiam ser acrescidos à hipótese de comunicação do titular, ao que parece, nem tudo o que está previsto nos incisos do art. 48 parecem enquadrar-se ao caso da comunicação. O inciso II, que prevê "as informações sobre os titulares envolvidos", não parece que deve ser lido da mesma forma para a Autoridade e para o titular dos dados. Este último não necessariamente precisa das informações de outros envolvidos. Assim, por

[20] INFORMATION COMMISSIONER'S OFFICE. **Personal data breaches.** Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/>.

mais que seja um requisito mínimo da notificação à ANPD, em relação à comunicação, a previsão do inciso II será adequada apenas em determinadas situações concretas.

Além disso, cabe ressaltar que é importante que a notificação seja realizada de maneira transparente e não deve ser enviada com outras informações, tais como atualizações, boletins informativos ou mensagens-padrão. Esse ponto é descrito de maneira expressa no art. 3 (4) do Regulamento da Comissão Europeia n. 611/2013, e é relevante para que de fato o titular dos dados tenha acesso claro ao ocorrido, podendo assim tomar medidas necessárias.

Por fim, destacamos que a comunicação do usuário nos termos da LGPD não exime o controlador de cumprir com requisitos advindos de eventuais regulações setoriais a que estão submetidos, o que vale tanto para o caso de notificação da autoridade, como em relação à comunicação do titular dos dados.

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

Embora não faça parte dos direitos do titular dos dados em sentido estrito, o direito a ser informado sobre a ocorrência de incidentes de segurança e suas possíveis consequências também constitui um direito do titular dos dados em um sentido mais amplo, decorrendo do princípio da transparência e *accountability*, além das obrigações específicas de notificação previstas no artigo 48. A comunicação de incidentes aos titulares tem como objetivo orientar e proteger o titular dos eventuais riscos e danos decorrentes do incidente de segurança, devendo acontecer com celeridade e buscando trazer transparência e orientações objetivas para que o titular possa se defender de possíveis ameaças e usos inadequados dos seus dados.

Com esse raciocínio podemos extrair algumas diretrizes sobre a forma mais adequada de comunicação aos titulares, como (i) a comunicação ao titular deve ser transparente, em linguagem acessível, objetiva e conter todas as informações exigidas por lei e sugeridas na presente contribuição; (ii) a comunicação direta é a regra (e-mail, telefonema, mensagem ou outro meio de contato direto efetivo); (iii) a comunicação pública por nota à imprensa, sites, banners, comunicados, boletins, não exclui a necessidade de realização de comunicação direta

> na ampla maioria dos casos; (iv) além da comunicação direta é recomendável a criação de outros meios de contato aos titulares, como sites, boletins informativos, comunicados à imprensa, páginas de perguntas e respostas etc. (v) em casos em que a comunicação individual demandar "esforços desproporcionais", mencionados abaixo, ela poderá ser substituída pela comunicação pública.

/ JUSTIFICATIVA

Ao comunicar o titular busca-se possibilitar que ele tome as medidas que julgar necessárias e cabíveis para se proteger dos riscos e danos de um incidente. Assim, a comunicação ao titular deve conter informações claras e suficientes para que o titular dos dados tome medidas para resguardar seus direitos. Como tratado na pergunta 1 a proteção não se restringe a medidas preventivas, como a troca de credenciais e senhas, mas também medidas afirmativas de exercício de direitos, seja em sede judicial, administrativa ou extrajudicial.

A comunicação tem como objetivo fornecer informações específicas aos titulares dos dados sobre as etapas que eles devem realizar para se proteger, desde ações mais simples como, por exemplo, alteração de senhas, ou ações mais complexas que requeiram, por exemplo, o fornecimento de um serviço de monitoramento de fraudes. A comunicação, assim, deve ser feita em uma mensagem específica, com linguagem clara e simples.

A comunicação direta deve ser a regra, a partir da deflagração do dever de comunicar, na medida em que ela aumenta a possibilidade de que o titular efetivamente acesse e compreenda as informações sobre o incidente. Por outro lado, se essa comunicação ocorrer apenas por veículo público, ainda que de ampla circulação, torna-se difusa e reduz a chance de que os titulares impactados recebam e compreendam as informações sobre o incidente.

Além do mais, em um contexto de aumento exponencial de incidentes de segurança, não é justo atribuir ao titular, parte vulnerável na relação, a responsabilidade de se atentar a todos os incidentes de segurança que acontecem e buscar saber se seus dados foram ou não comprometidos. Se a organização era responsável pelo tratamento seguro dos dados pessoais e não evitou a ocorrência de um incidente, nada mais justo comunicar ao titular, diretamente, acerca do ocorrido e suas potenciais consequências. Nesse contexto, a comunicação pública pode, em certos casos, complementar a comunicação individual, mas, em regra, não deve substituí-la.

Para a organização, a comunicação direta também pode ser importante por diversos motivos, como (i) a comunicação direta possibilita que a organização dialogue e seja transparente com os principais interessados em ter informações sobre o incidente - os titulares dos dados (ii) a confirmação pode servir como forma da organização demonstrar, em uma eventual investigação, que o titular

recebeu as informações de forma adequada (iii) quando o incidente for parcial, a comunicação direta possibilita que a organização dialogue apenas com os titulares afetados, não criando alarde desnecessário.

Assim, a obrigação de comunicação aos titulares tem um efeito positivo para as organizações que tratam dados pessoais, moldando-se a políticas internas que incentivam a implementação de modelos de gestão e governança eficazes, transparentes e diligentes. Ser transparente em um contexto de incidente é fundamental para a reputação da organização, e assim, essa obrigação permite manter a relação de confiança que as partes interessadas nela depositaram.

É importante mencionar, como já destacado nessa contribuição, que quando houver um esforço considerado desproporcional para comunicação individual aos titulares, pode haver uma exceção, desde que a comunicação pública seja realizada de forma ampla em meios de comunicação e que seja demonstrada a sua eficácia. Um exemplo de "esforço desproporcional" seria quando o próprio meio de contato direto com o titular tenha sido objeto do incidente e torne o processo de comunicação individual excessivamente dificultoso, podendo impactar, inclusive, a celeridade do processo.

Por fim, cabe ressaltar mais uma vez a importância de que a notificação seja entregue de maneira objetiva e não seja enviada junto a outras informações, tais como atualizações, boletins informativos ou mensagens-padrão[21]. Destaca-se, também, que o dever de notificação persiste mesmo em situações em que o titular não seja mais cliente ativo do responsável, mas seus dados estejam envolvidos em um vazamento.[22]

[21] SOMBRA, Thiago Luís e CASTELLANO, Ana Carolina. **Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva.** Revista do Advogado. AASP, 2019 v. 39 n. 144 nov, p. 168-173.

[22] GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados.** *In:* BIONI, Bruno *et al* (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666.

EIXO III

Uma vez reportado qual deve ser o papel dos órgãos reguladores em termos de fiscalização e colaboração em um plano de contenção?

Para análise do papel dos órgãos reguladores em termos de fiscalização e colaboração para produção de um plano de contenção, foram analisadas as competências normativas da ANPD estabelecidas pela LGPD em seu artigo 55-J, de forma a abordar: i) o dever de informação e publicidade; ii) a cooperação para a construção de um Sistema Nacional de Proteção de Dados e iii) os limites e parâmetros para cooperação internacional com outras Autoridades de Proteção de Dados.

O artigo 55-J da LGPD estabelece, logo em seu primeiro inciso, o zelo pela proteção dos dados pessoais como o norte da atuação da ANPD[23]. Pode parecer redundante positivar esse dever de proteção como meta dentro de uma legislação de proteção de dados pessoais. No entanto, essa regra serve como norte: todas as atuações da agência devem girar em torno desta máxima, inclusive nos casos de incidentes notificados. Assim, o papel da agência reguladora é, além de mitigar os danos já concretizados (art. 48, § 2º), proteger os dados de danos adicionais, buscando formas de conter o incidente. Somado a esse norte fundamental de atuação, a LGPD foi elaborada com base em uma lógica regulatória responsiva, que se afasta do racional de comando e controle, dando lugar a um método mais cooperativo[24]. Assim, é importante manter em mente que as providências a serem tomadas também em casos de incidentes de segurança devem seguir uma toada predominantemente cooperativa com os controladores remetentes da notificação.

O artigo 48 da lei, responsável pelo dever de notificação do controlador nos casos de incidentes de segurança, prevê que "a autoridade nacional verificará

[23] Art. 55-J: Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019).

[24] WIMMER, Miriam. **Os desafios de enforcement na LGPD: fiscalização e aplicação de sanções administrativas e coordenação intergovernamental.** *In:* MENDES, Laura Schertel *et al* (org.), "Tratado de Proteção de Dados Pessoais" (Forense, 2020).

a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências [...]"[25]. Há duas providências que podem ser tomadas, quais sejam: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente, mas o artigo limita-se a esses dois exemplos. Nesse sentido, há uma preocupação sobre como a ANPD deve prosseguir nos casos de notificações de incidentes para além dessas breves providências. Para uma resposta coerente, é necessário compreender quais as competências gerais da ANPD, elencadas no artigo 55-J da LGPD elenca as competências da ANPD.

A análise desse artigo com o enfoque no papel da Agência em termos de ações a serem tomadas frente à uma notificação de incidentes de segurança possibilita a classificação de quatro frentes de atuação da agência designadas pela lei: **(1) Dever guia/orientação aos regulados; (2) Dever de fiscalização e imposição de medidas sancionatórias; (3) Dever de cooperação.** Todas essas categorias devem seguir, também por força normativa, o princípio da publicidade, que consiste na transparência ao público das ações e entendimentos da agência, culminando em uma quarta categoria de (4) Dever de publicidade. De modo sistematizado:

Competências normativas da ANPD a serem seguidas no caso de recebimento de notificação de incidente de segurança (Art. 55-J LGPD)	
Dever de orientação aos regulados	**III** - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Incluído pela Lei nº 13.853, de 2019); **VI** - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; **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; **XIII** - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei (Incluído pela Lei nº 13.853, de 2019); **XX** - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos (Incluído pela Lei nº 13.853, de 2019).

[25] **Art. 48.** 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. [...] § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.

Dever de fiscalização e imposição de medidas sancionatórias	**IV** - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso (Incluído pela Lei nº 13.853, de 2019); **XVI** - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público (Incluído pela Lei nº 13.853, de 2019); **XVII** - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Incluído pela Lei nº 13.853, de 2019).	**XI** - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei (Incluído pela Lei nº 13.853, de 2019); **XXI** - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (Incluído pela Lei nº 13.853, de 2019); **XXII** - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal (Incluído pela Lei nº 13.853, de 2019).
Dever de cooperação	**IX** - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional (Incluído pela Lei nº 13.853, de 2019); **XIII** - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação (Incluído pela Lei nº 13.853, de 2019).	

Dever de publicidade	**II** - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei (Incluído pela Lei nº 13.853, de 2019); **X** - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial (Incluído pela Lei nº 13.853, de 2019); **XII** - elaborar relatórios de gestão anuais acerca de suas atividades (Incluído pela Lei nº 13.853, de 2019); **XIV** - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento (Incluído pela Lei nº 13.853, de 2019).

Assim, tendo em mente esses três nortes: (1) objetivo último de proteger os dados, (2) regulação responsiva e (3) quatro frentes de atuação da ANPD positivadas pela LGPD, é possível adentrar um campo mais concreto de qual o papel da agência regulatória frente a notificações de incidentes de segurança.

I. DEVER DE ORIENTAÇÃO AOS REGULADOS

Primeiramente, conforme o dever de orientar os regulados, entende-se que um papel central da ANPD consiste na **elaboração e publicação de materiais como guias e diretrizes de orientações em seu site oficial.** Especificamente, esse material deve versar sobre: (a) Como evitar um incidente de segurança (medidas preventivas)[26]; (b) O que fazer se um incidente acontecer (incluindo instruções de notificação); e (c) Os passos que a Agência irá tomar após o recebimento da notificação.

É fundamental que a ANPD possua um guia de "Próximos Passos - O que fazer depois de um incidente de segurança" (b), contendo orientações como, por exemplo: **quando é necessário notificar a autoridade** (uma tabela com exemplos de casos concretos seria interessante). **Orientações sobre quando é necessário notificar os titulares** dos dados também parece ser uma medida importante. Essa é uma prática sugerida pelo WP29, por meio da qual "[...] ao notificar a autoridade supervisora, os controladores podem obter aconselhamento sobre se os indivíduos afetados precisam ser informados"[27]. A Agência francesa segue na mesma toada, ao determinar que, em caso de dúvidas

[26] Este item não será abordado aqui, visto que a pergunta refere-se à atuação da agência após o recebimento de notificação de incidente de segurança.

[27] ARTICLE 29 DATA PROTECTION WORKING PARTY - WP29. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

sobre a necessidade de se notificar os titulares, é possível contatar a CNIL, que determinará se tal comunicação deve ou não ser feita.[28]

A agência australiana, por sua vez, possui sobre a matéria o guia "Data breach preparation and response", publicado pelo Office of the Australian Information Commissioner (OAIC) em julho de 2019[29], no qual apresenta o design do Esquema para Incidentes de Segurança Notificáveis como uma espécie de estandarte metodológico para orientar o Controlar de suas ações diante de um incidente de segurança, que deve ser entregue à Comissão. Tratam-se de orientações para formatação de um completo Plano de Resposta a Incidentes de Segurança[30]. Em um dos itens, a OAIC algumas medidas que podem ser tomadas pela Autoridade diante de uma notificação pelo controlador de dados, dentre as quais informar o controlador sobre quando uma notificação não é necessária ou modifique, a depender da circunstância do caso, o prazo para que seja realizada a notificação. O guia também estabelece que a OAIC orientará o notificante a realizar a comunicação do incidente para a própria agência e para indivíduos - no caso destes estiverem em situação que possa ensejar sérios danos.[31]

Além disso, um **material sobre o que os regulados devem esperar da atuação da ANPD após o recebimento da notificação** também consiste em prática transparente e responsiva. Especificamente, a elaboração de um documento padrão sobre os passos gerais que serão tomados pela ANPD em resposta às notificações de incidentes. Por exemplo, é importante que a ANPD **tenha canais de comunicação com o controlador bem definidos**. Uma medida técnica estabelecida pelo Guia Espanhol consiste na atribuição de um identificador único a cada caso, o qual estará presente durante todas as comunicações relacionadas ao incidente. Se as comunicações são feitas por e-mail, este identificador aparece no campo "assunto" e não deve ser modificado ou eliminado, visto

[28] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Security of Personal Data.** 2018. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf>.

[29] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Data breach preparation and response.** 2019. Disponível em: <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/>.

[30] A estrutura do Guia é a seguinte: **Parte 1:** Explicações sobre o conceito e a caracterização de incidente de segurança e exposição de obrigações dos agentes de tratamento na ocorrência de incidente e esquema visual; **Parte 2:** Passo a passo para a preparação de um Plano de Resposta a Incidentes de Segurança, com checklist visual para fins de orientação. Especificamente nesse tópico, o guia se debruça em aspectos como a composição de uma equipe de resposta e ações a serem tomadas pelos agentes. **Parte 3:** O Guia apresenta 4 passos práticos para colocar em ação o Plano de Resposta a Incidentes de Segurança, quais sejam: **(i)** conter; **(ii)** avaliar; **(iii)** notificar e **(iv)** rever. As informações também são apresentadas no formato de infográfico visual; e **Parte 4:** Denominada "Esquemas para Incidentes de Segurança Notificáveis - *NDB Scheme*" (trad. nossa), o Guia aprofunda conceitos e procedimentos metodológicos de pontos de interesse trabalhados em suas outras seções, com orientações para: **(i)** incidentes que envolvem múltiplas entidades; **(ii)** exceções ao dever de notificação; **(iii)** notificação ao titular de dados; **(iv)** metodologia para avaliação de gravidade de incidente e **(iv)** o papel da *OAIC* diante de uma notificação de incidente de segurança.

[31] A autoridade, por sua vez, pode até mesmo solicitar uma notificação - apesar de sempre solicitar ao controlador que concorde em realizar a notificação. Esse é o tipo de caso no qual a Comissão realiza orientações ao agente mesmo antes da Notificação, quando se tornou ciente da ocorrência de um incidente de segurança.

que isso retardaria o gerenciamento e a resolução final do incidente cibernético[32]. Assim, para além de delimitar o canal de comunicação, é fundamental **estabelecer previamente as regras procedimentais dessa comunicação**.

Importante que seja publicizado, por exemplo, **quando e se os casos notificados acompanhados pela agência serão transformados em materiais de estudos e em quais termos** - o nome da empresa será publicado? Será necessário o consentimento da empresa? Por exemplo, a ICO, possui em seu website uma aba sobre políticas internas, dentre as quais se encontra um documento intitulado "Comunicando nosso regulatório e Política de Atividades de Execução" ("Communicating our Regulatory and Enforcement Activity Policy")[33]. Além de outras informações, constam diretrizes de interação com os regulamentados e princípios de atuação regulatória - por exemplo: "Ação após incidentes serem relatados e preocupações levantadas: Podemos publicar ou divulgar informações que destacam a melhoria de práticas nos direitos de informação após reclamações e incidentes são relatados para nós. Isso incluirá nomes de organizações se o interesse público justificar isto").

Sugere-se, por fim, que este guia contenha **esclarecimentos jurídicos**, como: O operador tem o dever de notificar um incidente de segurança à autoridade? Se sim, em quais casos? O pagamento de resgate nos casos de *Ransomwares* é legal? Se sim, como deve ser feito? Dentre outros.

Por fim, se a autoridade tem de realizar uma avaliação sobre a gravidade do incidente (art. 48, § 2º), cabe explicar nesse documento público o que, exatamente, significa essa análise: quais as metodologias e critérios adotados pela agência.

1. ANÁLISE DE GRAVIDADE

Sugere-se, especificamente para essa adoção de metodologias e critérios que seja adotada a lógica de risco, na qual quanto maior for a probabilidade e/ou a severidade do dano, maior a gravidade do incidente de segurança e, assim, maior atenção deve ser direcionada ao caso. A GDPR, por exemplo, estabelece que somente incidentes que representem um risco provável aos direitos e liberdade dos titulares titulares, bem como a comunicação ao próprio titular só é necessária em caso de probabilidade de resultar em um alto risco aos seus direitos e liberdades - seguindo o mesmo racional de que

[32] ESPANHA, **Guía Nacional de Notificación y Gestión de Ciberincidentes da Espanha.** 2020. Disponível em: <https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf>.

[33] INFORMATION COMMISSIONER'S OFFICE. **Communicating our Regulatory and Enforcement Activity Policy.** 2019. Disponível em: <https://ico.org.uk/media/about-the-ico/policies-and-procedures/1890/ico_enforcement_communications_policy.pdf>.

a magnitude do risco[34] está ligada aos fatores de severidade e probabilidade (conforme disposto nos considerandos 75 e 76 da GDPR). Conforme o Guia sobre Notificações de Vazamento de Dados conforme a Regulação 2016/679 ("Guidelines on Personal data breach notification under Regulation 2016/679"), publicado em 2017 pelo Working Party 29[35], a concretização do risco se dá "[...] quando a violação pode levar a danos físicos, materiais ou imateriais para os indivíduos cujos dados foram violados. Exemplos de tais danos são discriminação, roubo de identidade ou fraude, perda financeira e danos à reputação." Ainda quando a violação envolve dados pessoais que revelam origem racial ou étnica, opinião política, religião ou crenças filosóficas, ou filiação em sindicatos, ou inclui dados genéticos, dados relativos à saúde ou dados relativos à vida sexual, ou condenações criminais e ofensas ou medidas de segurança relacionadas, tal dano deve ser considerado provável de ocorrer.

A Seção IV do Guia - parte dedicada à explicação de fatores a serem considerados ao se avaliar os riscos - elenca critérios para avaliação de risco de maneira bastante objetiva: **(i)** O tipo de incidente; **(ii)** A natureza, sensibilidade e volume dos dados pessoais; **(iii)** Facilidade com que se consegue identificar os indivíduos; **(iv)** A severidade das consequências para os indivíduos; **(v)** Características especiais do indivíduo; **(vi)** Características especiais do controlador e **(vii)** O número de indivíduos afetados.

Consolidou-se a definição e exemplos de cada um desses critérios na Tabela Anexa, que, além de conceituar os sete critérios elaborados pela WP29, mapeia as diretrizes de outras sete Autoridades de Proteção de Dados, em busca de similaridades e diferenças desses critérios elaborados pelo WP29. Algo em comum, no entanto, é a existência de guias com critérios mais ou menos claros sobre qual o entendimento da autoridade sobre quais critérios devem ser usados para mensurar o risco dos incidentes de segurança.

As autoridades possuem, também, orientações em grau mais ou menos detalhado, qual a metodologia que será usada para essa avaliação de risco. Sugere-se que a escolha de uma metodologia padrão seja feita pela ANPD, para geral coerência e segurança jurídica aos regulados, e que essa escolha seja pública e de fácil acesso.

A análise da gravidade do risco é fundamental nesse processo todo, visto que a rapidez e precisão dessa avaliação permite uma resposta da agência com uma rapidez proporcional à severidade do caso - i.e., maior probabilidade e gravidade dos danos decorrentes do incidente de segurança.

[34] No Guia sobre Notificação de Vazamento de Dados conforme a Regulação 2016/679, o Working Party 29 (WP29) ressalta que há uma diferença nessa avaliação de riscos quando comparada à avaliação necessária para elaborar um DPIA. Nesta, a avaliação dos riscos existe tanto em dois cenários hipotéticos: **(i)** no caso do tratamento se dar conforme o planejado e **(ii)** no caso de acontecer um incidente. No caso de um incidente de segurança que já aconteceu, há avaliação somente do risco resultante desse acontecimento.

[35] ARTICLE 29 DATA PROTECTION WORKING PARTY - WP29. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

Um interessante caso de estudo para análise é o Caso Equifax, birô de crédito, no qual ocorreu o vazamento de dados pessoais e financeiros de 145 milhões de estadunidenses, 8 mil canadenses e 693 mil cidadãos do Reino Unido[36] no ano de 2017[37]. Dentre as informações divulgadas, estavam, além de documentos e informações pessoais, os números de cartão de crédito de 209 mil titulares. Uma das primeiras ações de mitigação de risco tomadas pela empresa foi a criação de um website com o objetivo de conscientização da população, de modo a evitar fraudes financeiras[38]. Apesar disso, diversos websites falsos foram criados na internet, na tentativa de propagar informações falsas e aplicar novos golpes na população afetada[39]. No próprio Twitter oficial da Equifax, foram divulgados, erroneamente, links que direcionam os consumidores a sites de *phishing*[40]. A falta de uma estratégia concreta de avaliação e mitigação dos riscos do vazamento, no primeiro momento, contribuiu para a confusão pública e perda de confiança no sistema quanto ao caso.

Devido à natureza e à dimensão do vazamento, a resposta ao caso foi feita de maneira multissetorial, com: **(i)** o envolvimento de todos os 50 Procuradores de Estado dos EUA para elaboração de acordo indenizatório no valor de 600 milhões de dólares[41]; **(ii)** a condução de investigações dos sistemas de segurança da Equifax pelas agências Internal Revenue Service (IRS), Social Security Administration (SSA) e U.S. Postal Service (USPS), que também adaptaram seus contratos para exigir notificações mais tempestivas em futuros casos de incidente e/ou encerraram contratos com a empresa; **(iii)** a condução de investigação administrativa pelo Bureau of Consumer Financial Protection e pela

[36] Para compreender a utilização dos critérios de análise de gravidade de incidente de segurança em um caso concreto, é possível observar a decisão da ICO para aplicação de multa diante do Caso Equifax, no qual a Autoridade realizou uma apreciação gradual da gravidade do incidente. Nesse sentido, a ICO levou em conta: **(i)** volumetria de dados vazados; **(ii)** total de indivíduos atingidos; **(iii)** falta de medidas de segurança, como utilização de criptografia, segregação de network ou proteção de senhas dos usuários; **(iv)** tempo de disponibilidade indevida dos dados; **(v)** a falta de consciência dos sujeitos de dados de que seus dados eram objeto de tratamento pela Equifax; **(vi)** a natureza da atividade de tratamento; **(vii)** a natureza dos dados e a possibilidade de sua utilização para atividades fraudulentas; **(viii)** as consequências potenciais da utilização maliciosa dos dados; **(ix)** percepção pública do incidente, ou seja, capacidade do vazamento em ocasionar uma quebra de confiança no sistema financeiro como um todo. (ICO, 2018)

[37] THOMAS, Jason. **A Case Study Analysis of the Equifax Data Breach.** 2019. Disponível em: <https://www.researchgate.net/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach_1_A_Case_Study_Analysis_of_the_Equifax_Data_Breach>.

[38] EQUIFAX. **2017 Cybersecurity Incident & Important Consumer Information.** 2017. Disponível em: <https://www.equifaxsecurity2017.com>.

[39] ATLESON, Michael. **Equifax Data Breach: Beware of Fake Settlement Websites.** Federal Trade Commission Consumer Information. 2019. Disponível em: <https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-beware-fake-settlement-websites>.

[40] Técnica de engenharia social com o objetivo de enganar usuários e obter informações pessoais para fins fraudulentos. Saiba mais em: DEAHL, Dani; CARMAN, Ashley. **For weeks, Equifax customer service has been directing victims to a fake phishing site.** The Verge. 2017. Disponível em: <https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishing-identity-monitoring>.

[41] OREGON DEPARTMENT OF JUSTICE. **50 State Attorney Secure 600 Million from Equifax in the Largest Data Breach Settlement in History.** 2019. Disponível em: <https://www.doj.state.or.us/media-home/news-media-releases/50-state-attorneys-general-secure-600-million-from-equifax-in-largest-data-breach-settlement-in-history/>.

Federal Trade Commission (FTC)[42]; **(iv)** a participação ativa do Congresso Nacional que, além de realizar audiências para apuração e investigação do vazamento, propôs diversos Projetos de Lei de regulamentação do setor.[43]

Apesar do agravamento da gravidade do vazamento pela demora excessiva de notificação por parte da empresa, foi realizada uma cooperação efetiva entre diversas agências federais, junto ao legislativo, para tentar solucionar e mitigar os efeitos do vazamento com foco na proteção dos titulares de dados afetados.

No Brasil, a natureza e a complexidade de um incidente de segurança pode exigir uma rápida avaliação de riscos e danos a fim de criar medidas rápidas e efetivas de contingência, a depender da complexidade e natureza das informações comprometidas e a adoção de uma estratégia de cooperação entre demais órgãos regulatórios que tenham interesse na matéria, como Banco Central do Brasil, a Comissão de Valores Mobiliários, a Secretaria Nacional do Consumidor, o Ministério Público e, eventualmente, demais entes.

Isso nos leva a:

II. DEVER DE COOPERAÇÃO E DEVER DE FISCALIZAÇÃO E IMPOSIÇÃO DE MEDIDAS SANCIONATÓRIAS

O caso do Equifax dá a dimensão da importância da cooperação com demais reguladores e da necessidade de articulação em diversos níveis da administração pública no caso de incidentes de segurança de alta complexidade.

Mesmo antes da LGPD entrar em vigor, o ordenamento jurídico brasileiro já estava permeado de normas (gerais e específicas) que estabeleciam mecanismos protetivos para os cidadãos quanto

[42] Agência governamental dos EUA que possui o objetivo de promover a defesa dos consumidores e promover a lei antitruste.

[43] GAO - UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. **Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.** 2018. Disponível em: <https://www.gao.gov/assets/gao-18-559.pdf>.

ao tratamento de seus dados[44] por meio dos quais é possível "[...] vislumbrar a grande quantidade de órgãos e entidades públicos que potencialmente poderiam ser considerados competentes para atuar em casos concretos envolvendo o mau uso de dados pessoais"[45]. Wimmer destaca os órgãos de proteção e defesa do consumidor (em particular, os Procons e o Ministério Público), agências reguladoras e órgãos com competências normativas e sancionadoras em áreas como telecomunicações, saúde, mercado financeiro e educação.

Os casos de competência concorrente[46] acentuam-se ao se considerar a "[...] tendência de que também Estados e municípios adotem legislações referentes à proteção de dados pessoais, podem ainda existir órgãos competentes quanto ao tema em níveis estadual e municipal"[47]. Essa tensão, por fim, não se restringe aos sistemas normativos que cuidam de proteção de dados pessoais, mas pode ocorrer entre normas que objetivam proteger diferentes bens jurídicos, "[...] ensejando, eventualmente, decisões conflitantes entre órgãos públicos competentes para analisar um mesmo objeto a partir de distintos vetores interpretativos"[48]. Isso demonstra como é fundamental o "[...] estabelecimento de relações permanentes entre tais órgãos, que se encontram submetidos a cadeias hierárquicas distintas, de modo a evitar que a ação de um deles obstaculize o desempenho das competências do outro"[49].

[44] "Os exemplos são inúmeros. O Código de Defesa do Consumidor (Lei 8.078, de 11 de setembro de 1990 – CDC) assegura o direito de acesso, pelos consumidores, a informações existentes em bases de dados e cadastros, estabelecendo, dentre outros direitos, o de retificação de informações inexatas. A Lei do Cadastro Positivo (Lei 12.414, de 9 de junho de 2011) dispõe de maneira detalhada sobre os direitos do cadastrado, incluindo os direitos de acesso a informações, de cancelamento do cadastro, de retificar informações errôneas, de ter seus dados pessoais utilizados somente para finalidade para a qual foram coletados, de revisão de decisão realizada exclusivamente por meios automatizadas e, ainda, de conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial. No campo da legislação setorial, a Lei Geral de Telecomunicações (Lei 9.472, de 16 de julho de 1997 – LGT) estabelece o direito do usuário de serviços de telecomunicações à inviolabilidade e ao segredo de sua comunicação, à não divulgação de seu código de acesso e ao respeito à sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço. Na área da saúde, o Código de Ética Médica (Resolução 2.217/2018 do Conselho Federal de Medicina) regula o sigilo médico e assegura ao paciente o acesso ao seu prontuário e veda o seu fornecimento a terceiros, exceto mediante ordem judicial ou requisição pelos Conselhos Regionais de Medicina, autorização do paciente ou para a defesa do próprio médico. No que tange a dados custodiados pelo Poder Público, a Lei de Acesso à Informação (Lei 12.527, de 18 de novembro de 2011 – LAI) traz regras de proteção às informações pessoais, estabelecendo hipóteses de tratamento com e sem consentimento expresso do titular.". Disponível em: WIMMER, Miriam. Os desafios de enforcement na LGPD: fiscalização e aplicação de sanções administrativas e coordenação intergovernamental. p. 34. *In:* MENDES, Laura Schertel *et al* (org.), **"Tratado de Proteção de Dados Pessoais"** (Forense, 2020).

[45] WIMMER, *op. cit*

[46] "[...] casos concretos em que uma mesma conduta envolvendo o uso de dados pessoais seja considerada ilícita à luz de duas ou três normas simultaneamente" (WIMMER, *op. cit.*, p. 9).

[47] WIMMER, *op. cit*

[48] "Trata-se de situação de competências complementares, em que órgãos sem qualquer relação de hierarquia possuem competências coincidentes quanto ao objeto, mas distintas quanto às tarefas ou fins públicos perseguidos." (WIMMER, *op. cit.*, p. 10).

[49] WIMMER, *op. cit.*

Concorda-se com a sugestão de Wimmer sobre como a ANPD deve proceder para evitar esses conflitos com outros órgãos reguladores:

> *"Esse cenário complexo e fragmentado de enforcement requer a busca ativa por ferramentas hermenêuticas e por mecanismos de coordenação e articulação de competências, que podem ser construídos a partir da* ***definição de procedimentos e parâmetros para a fixação de competências primárias e secundárias no endereçamento de casos concretos."***[50] (grifos nossos)

A ICO, por exemplo, adotou essa prática de procedimentalizar a cooperação com outros órgãos: possui, em seu website, memorandos de entendimento com quarenta e cinco instituições, desde a Advocacia Geral da União até o Centro de Informações de Saúde e Assistência Social. Recomenda-se que **a ANPD constitua esses acordos com demais agências e órgãos reguladores que poderão, eventualmente, possuir competência concorrente ou complementar para lidar com um caso de incidente de segurança.**

Nesse mesmo sentido, **a ANPD deve, ao receber a notificação, realizar uma análise inicial sobre quem deve gerir o incidente**, avaliando e indicando se é o caso de competência própria ou competência concorrente ou complementar com quais outros reguladores. Como é feita essa avaliação inicial deve constar no guia de orientações aos regulados, mencionado no item anterior. Essa é uma das providências indicadas pelo Guia Nacional de Notificação e Gestão de Incidentes Cibernéticos da Espanha ("Guía Nacional de Notificación y Gestión de Ciberincidentes"), publicado em 2020. Sempre que a agência responsável recebe uma notificação sobre um possível incidente cibernético, a equipe técnica realiza uma análise inicial que determinará se o caso é passível de ser gerido por ela mesma ou por um terceiro[51]. Esse ponto é fundamental para delimitar quem tem o dever de fiscalizar e, eventualmente, sancionar as práticas em questão. Em outras palavras, a cooperação entre reguladores produz uma fiscalização mais eficiente.

A cooperação vai além de uma solução ao problema de eventuais conflitos de competências: surge como uma medida para aprender com outros agentes reguladores que têm maior experiência acumulada ao lidar com notificações de incidentes de segurança. Ou seja, **a determinação das ações necessárias a serem tomadas pela ANPD pode contar com a experiência de outras instituições que lidam há mais tempo com notificações de incidentes de segurança**. Por exemplo, o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração

[50] WIMMER, *op. cit.*

[51] ESPANHA. **Guía Nacional de Notificación y Gestión de Ciberincidentes da Espanha**. 2020. Disponível em: <https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf>.

Pública Federal (CTIR), que já possui diretrizes para lidar com incidentes. Parte do processo de tratamento de incidentes perpassa pela análise de incidentes, suporte à recuperação de incidentes, coordenação na resposta a incidentes, distribuição de alertas e cooperação com outras equipes de tratamento de incidentes. (Delimitado em documento "Padrões Para Notificação De Incidentes De Segurança ao Ctir Gov.")

Há, ainda, que se considerar e planejar como será a **cooperação com autoridades de proteção de dados internacionais** no caso do incidente de segurança envolver atores de fora do Brasil[52]. Como sintetiza Wimmer:

> *"[...] uma vez que a LGPD pode produzir efeitos extraterritoriais semelhantes aos do Marco Civil da Internet, aplicando-se a pessoas naturais e jurídicas independentemente do país de sua sede ou do país onde estejam localizados os dados, uma condição crucial para que a legislação seja dotada de efetividade é que a ANPD se engaje ativamente em arranjos internacionais de cooperação para, ao mesmo tempo, simplificar os fluxos globais de dados e viabilizar o enforcement no caso de condutas ilícitas."*[53]

Ou seja, em um caso de breach global, como a ANPD pode cooperar em nível internacional/entre agências?[54] É importante observar estruturas de cooperação internacional e diálogo entre Autoridades Nacionais de Proteção de Dados já existentes. Nesse sentido cita-se como exemplo a Red Iberoamericana de Protección de Datos (RIPD) e a Global Privacy Enforcement Network (GPEN).

Importa destacar que há estratégias de cooperação internacional entre Autoridades de Proteção de Dados organizadas por diferentes critérios, como a French-speaking Association of Personal Data

[52] "Dada a natureza global da chamada economia digital, um desafio importante a ser enfrentado pela ANPD diz respeito à cooperação internacional para enforcement quanto à proteção de dados pessoais e ao desenvolvimento de conceitos e standards comuns que permitam a interoperabilidade de marcos normativos em diferentes países. O estabelecimento de mecanismos de cooperação internacional quanto à proteção de dados pessoais é justificado não apenas em razão da necessidade de assegurar a proteção de direitos para além das fronteiras nacionais, mas também em vista da crescente importância econômica dos fluxos transnacionais de dados pessoais e da sua estreita relação com os fluxos globais de bens e serviços." (WIMMER, 2020, p. 7)

[53] WIMMER, *op. cit.*

[54] "De fato, as dificuldades para a aplicação da lei em atividades envolvendo o fluxo transnacional de dados têm sido vivenciadas de maneira intensa no Brasil, especialmente em conexão com investigações criminais em que há necessidade de coleta de provas detidas por provedores de aplicações de Internet sediados em outros países. Os bloqueios de aplicativos de comunicação interpessoal por ordem judicial, ocorridos no Brasil em 2015 e 2016, tiveram como pano de fundo não apenas o debate acerca do uso de criptografia forte, mas também a discussão sobre o cumprimento de ordens judiciais brasileiras por empresas sediadas no exterior e, consequentemente, sobre a necessidade, ou não, de utilização de mecanismos de cooperação jurídica internacional para obtenção de elementos probatórios." (WIMMER, *op. cit.*, p. 7).

Protection Authorities (AFAPDP), conferência internacional que reúne membros de Autoridades de países que falam a língua francesa, ou como a Asia Pacific Privacy Forum (APPA), que reúne Autoridades territorialmente localizadas na região do pacífico asiático.

Observando especificamente a cooperação entre países localizados na América do Sul, é possível perceber que trocas têm sido realizadas pela Agencia de Acceso a la Información Pública (AAIP, Argentina) e pela Unidad Reguladora y de Control de Datos Personales (URCDP, Uruguai), com a elaboração de orientações conjuntas, como é o caso da publicação conjunta Guía de Evaluación de Impacto en la Protección de Datos.[55]

Nesse sentido, é recomendável que a ANPD, em nível internacional, colabore com outras Autoridades não apenas para desenvolver respostas para incidentes de segurança em nível transnacional, mas também para estabelecer diretrizes, orientações e estratégias de cooperação que visem a garantia de um Sistema Internacional de Proteção de Dados. Sugere-se, ainda, que parcerias e colaborações nesse sentido busquem demais Autoridades de Proteção de Dados de países da América do Sul, fato que se justifica pela proximidade territorial, histórica e contextual a fim de estabelecer compreensões em comum da região quanto à formação de conhecimentos, políticas e estratégias de proteção de dados.

Realizados os apontamentos iniciais gerais sobre a atuação da ANPD uma vez reportado um incidente de segurança, os próximos tópicos respondem às perguntas específicas propostas pelo órgão.

[55] AAIP; URCDP. **Guía de Evaluación de Impacto en la Protección de Datos.** 2019. Disponível em: <https://www.argentina.gob.ar/sites/default/files/guia_final.pdf>.

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

Entende-se que critérios mínimos de análise da gravidade do incidente de segurança perpassam pela lógica da probabilidade e severidade do risco e de dano relevante para os titulares. **Ou seja, quanto maior for a probabilidade e/ou a severidade do dano, maior a gravidade do incidente de segurança** e, assim, maior atenção deve ser direcionada ao caso.

Sugere-se que os critérios elaborados busquem se amoldar a acúmulos internacionais, cujos critérios são similares em diversas jurisdições, inclusive para que se facilite a cooperação em casos de incidentes de seguranças que ultrapassam as fronteiras brasileiras. Especificamente, sugere-se a discussão em tornos de critérios que levem em consideração: o tipo de incidente; a natureza, sensibilidade e volume dos dados pessoais; facilidade com que se consegue identificar os indivíduos; a severidade das consequências para os indivíduos e as características especiais do indivíduo. A análise da gravidade do risco é fundamental nesse processo todo, visto que a rapidez e precisão dessa avaliação permite uma resposta da agência com uma rapidez proporcional à severidade do caso - i.e., maior probabilidade e gravidade dos danos decorrentes do incidente de segurança.

De maneira geral, pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

Assim como na LGPD, a GDPR estabelece que somente somente incidentes que representem um risco provável aos direitos e liberdade dos titulares titulares, bem como a comunicação ao próprio titular só é necessária em caso de probabilidade de resultar em um alto risco aos seus direitos e liberdades - seguindo o mesmo racional de que a magnitude do risco está ligada aos fatores de severidade e probabilidade (conforme disposto nos considerandos 75 e 76 da GDPR).

No Guia sobre Notificação de Vazamento de Dados conforme a Regulação 2016/679 (“Guidelines on Personal data breach notification under Regulation 2016/679”), publicado em 2017, o Working Party 29 (WP29) ressalta que há uma diferença nessa avaliação de riscos quando comparada à avaliação necessária para elaborar um DPIA. Nesta, a avaliação dos riscos existe tanto em dois cenários hipotéticos: (i) no caso do tratamento se dar conforme o planejado e (ii) no caso de acontecer um incidente. No caso de um incidente de segurança que já aconteceu, há avaliação somente do risco resultante desse acontecimento.

Conforme o Guia, a concretização do risco se dá "[...] quando a violação pode levar a danos físicos, materiais ou imateriais para os indivíduos cujos dados foram violados. Exemplos de tais danos são discriminação, roubo de identidade ou fraude, perda financeira e danos à reputação."[56] Ainda quando a violação envolve dados pessoais que revelam origem racial ou étnica, opinião política, religião ou crenças filosóficas, ou filiação em sindicatos, ou inclui dados genéticos, dados relativos à saúde ou dados relativos à vida sexual, ou condenações criminais e ofensas ou medidas de segurança relacionadas, tal dano deve ser considerado provável de ocorrer.

A Seção IV do Guia - parte dedicada à explicação de fatores a serem considerados ao se avaliar os riscos - elenca critérios para avaliação de risco de maneira bastante objetiva: **(i)** O tipo de incidente; **(ii)** A natureza, sensibilidade e volume dos dados pessoais; **(iii)** Facilidade com que se consegue identificar os indivíduos; **(iv)** A severidade das consequências para os indivíduos; **(v)** Características especiais do indivíduo; **(vi)** Características especiais do controlador e **(vii)** O número de indivíduos afetados. Consolidou-se a definição e exemplos de cada um desses critérios na Tabela anexada a esse documento, que, além de conceituar os sete critérios elaborados pela WP29, mapeia as diretrizes de outras sete Autoridades de Proteção de Dados, em busca de similaridades e diferenças desses critérios elaborados pelo WP29.

Os países das autoridades escolhidas foram: Reino Unido (ICO), França (CNIL), Espanha (AEPD), Argentina (ADPA), Uruguai (URCDP) e Austrália (OAIC). A ICO, por exemplo, possui um breve guia sobre avaliação de risco e, para maiores esclarecimentos, indica especificamente a seção IV do WP29 no guia sobre notificação de incidentes. Assim como recomenda a WP 29, o critério geral é severidade do risco e probabilidade. A autoridade australiana, por sua vez, reuniu seis dos sete critérios elaborados pelo WP29, deixando de fora somente a "facilidade com que se consegue identificar os indivíduos". O Relatório da Argentina e do Uruguai também estabelece como critérios cinco dos sete acima mencionados.

Sugere-se que a maioria dos critérios adotados pela ANPD estejam em consonância com aqueles aplicados pelas demais Agências de Proteção de Dados, para que eventual necessidade de cooperação internacional seja facilitada pelo uso de critérios similares.

Por fim, sugere-se que não é desejável elaborar um critério específico para incidentes de segurança envolvendo políticos. No entanto, pode ser interessante considerar a motivação política do incidente por alguns proxies, como tem ocorrido em organizações da sociedade civil.

[56] ARTICLE 29 DATA PROTECTION WORKING PARTY - WP29. **Guidelines on Personal data breach notification under Regulation 2016/679.** 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

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

Sugere-se, especificamente para a elaboração de metodologias e critérios, que seja adotada a lógica de risco, na qual quanto maior for a probabilidade e/ou a severidade do dano, maior a gravidade do incidente de segurança e, assim, maior atenção deve ser direcionada ao caso. Através do estudo comparado da atuação e dos Guias disponibilizados por diversas Autoridades de Proteção de Dados ao redor do mundo, foi possível sistematizar algumas das melhores práticas metodológicas em termos de: **i)** organização da informação; **ii)** avaliação sistemática do risco e impacto e **iii)** exposição de critérios objetivos para análise de gravidade. São eles:

- Proposta de análise quantitativa para avaliação de gravidade de incidente de segurança, disponível no documento "Data Breach Severity Methodology", da European Union Agency for Network (Enisa)[57];

- Metodologia quantitativa e qualitativa para elaboração de análise de probabilidade e impacto, sistematizada pelo Guía de Evaluación de Impacto en La Protección de Datos, feito, de forma conjunta, pela Agencia de Acceso a la Información Pública (AAIP, Argentina) e pela Unidad Reguladora y de Control de Datos Personales (URCDP, Uruguai)[58];

- Aplicação faseada de critérios de avaliação de riscos, expostos no Guia "Data breach preparation and response", preparado pelo Office of the Australian Information Commissioner (OAIC, Austrália)[59];

- Tabelas e planejamento de avaliação de risco disponíveis nos Guias "Security of Personal Data"[60] e "Methodology for Privacy Risk Management"[61], ambos da Commission Nationale de l'Informatique et des Libertés (CNIL, França).

[57] ENISA, **Recommendations for a methodology of the assessment of severity of personal data breaches.** 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>.

[58] AAIP; URCDP. **Guía de Evaluación de Impacto en la Protección de Datos.** 2019. Disponível em: <https://www.argentina.gob.ar/sites/default/files/guia_final.pdf>.

[59] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Data breach preparation and response.** 2019. Disponível em: <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/>.

[60] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Security of Personal Data.** 2018. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf>.

[61] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Methodology for Privacy Risk Management: How to Implement the Data Protection Act.** 2012. Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>.

Uma proposta metodológica para análise da gravidade de violações de dados pessoais foi proposta pela European Union Agency for Network and Information Security (Enisa), de 2011. O documento foi elaborado a partir de uma revisão das medidas e procedimentos existentes em Estados da União Europeia, no que diz respeito a violações relacionadas a incidentes de segurança de proteção de dados, como parte de um estudo sobre a implementação técnica da Diretiva ePrivacy do Parlamento Europeu sobre proteção da privacidade. O objetivo da metodologia proposta pela Enisa é servir de ferramenta quantitativa para avaliação da gravidade do incidente, auxiliar os controladores de dados a tomarem rápidas medidas de mitigação e dar ferramentas às Autoridades Nacionais de Proteção de Dados para realizar uma avaliação de gravidade do incidente.

Alguns aspectos principais da metodologia quantitativa elaborada pela Enisa serão apresentados abaixo.

1. METODOLOGIA GERAL

De acordo com a metodologia proposta, a **gravidade** do incidente deve ser definida pela **estimação da magnitude do potencial de impacto aos titulares afetados pela violação de dados pessoais.** São três os critérios que devem ser considerados na avaliação, quais sejam:

- **O contexto do tratamento de dados (CTD):**
  O que envolve a avaliação da categoria dos dados pessoais envolvidos no incidente de forma aplicada ao contexto no qual são utilizados; nesse sentido, diz respeito à avaliação do critério de "criticidade" de uma base de dados em um determinado contexto de tratamento.

- **A facilidade de identificação dos indivíduos afetados (FI):**
  Fator corretivo do critério CTD. A criticidade de uma atividade de tratamento pode ser reduzida dependendo do valor de FI, ou seja, quão mais difícil for identificar o titular de dados afetado, menor é o resultado final de análise da gravidade do incidente. Por esse motivo, a multiplicação dos fatores CTD e FI gera o *score* inicial da de gravidade (SG) do incidente de segurança.

- **As circunstâncias do incidente, o que pode ter influência adicional na avaliação da gravidade do incidente (CI):**
  Esse critério quantifica as circunstâncias específicas do incidente que podem se apresentar ou não em determinadas situações. Quando presente, o CI soma a potencial gravidade do incidente, servindo como critério de ajuste.

De tal forma, o score final de avaliação de gravidade é feito a partir da seguinte fórmula:

SG	=	CTD	×	FI	+	CI
(score de gravidade)		(contexto do tratamento)		(facilidade de identificação)		(circunstâncias do incidente)

O resultado é classificado em quatro níveis de gravidade: baixa, média, alta ou muito alta. Ao final da avaliação, outros critérios relevantes como o número de indivíduos afetados (para a Enisa, deve ser fator de aumento de gravidade caso exceda 100 indivíduos afetados) e o nível de inteligibilidade dos dados (utilização de criptografia forte pode ser fator de diminuição da gravidade) não considerados na valoração inicial, devem ser incluídos na análise.

2. ANÁLISE DOS CRITÉRIOS

2.1 CONTEXTO DO TRATAMENTO DE DADOS (CTD)

A fim de estabelecer o CTD, deve-se seguir 2 passos de avaliação:

Definir e classificar as categorias de dados pessoais envolvidos no incidente

1. Definir os tipos de dados pessoais envolvidos no incidente

2. Classificar os dados em quatro categorias de análise, quais sejam: simples, comportamental, financeiro ou dado sensível. Trata-se de lista não exaustiva que pode ser adaptada dependendo do caso concreto.

Dentro das quatro categorias propostas (simples, comportamental, financeiro ou sensível), caso um dado pessoal tenha correspondência com mais de uma, o cálculo deve ser repetido para tantas categorias forem. O critério CTD deverá ser aquele com maior *score* final. Na análise individual, as categorias possuem os seguintes *scores* básicos:

Categoria de dados	Score Inicial
Dados simples	3
Dados comportamentais	2
Dados financeiros	3
Dado sensível	4

Em uma segunda etapa, deve-se ajustar a avaliação pela análise de outros fatores relacionados ao tratamento de dados, estabelecendo uma quantificação de 1-4, capaz de avaliar a ocorrência de fatores capazes de aumentar ou diminuir o *score* básico (volume de dados, características especiais do controlador ou dos indivíduos afetados, inexatidão ou falta de acurácia dos dados, disponibilidade pública dos dados antes do incidente e natureza dos dados).

2.2 FACILIDADE DE IDENTIFICAÇÃO (FI)

Há quatro níveis de Facilidade de Identificação estabelecidos pela metodologia, quais sejam: i) negligenciável; ii) limitado; iii) significante; iv) máximo, com uma progressão linear entre eles para avaliação do *score*.

Para definição desse *score*, é importante considerar que a forma de identificação pode ser direta (ex: baseada no nome completo do indivíduo afetado) ou indireta (baseada em um número de CPF). Além disso, pode depender do contexto do incidente.

Além disso, deve-se avaliar todos os meios razoáveis para identificação do titular de dados. Isso inclui outras informações públicas ou disponíveis na internet, bem como o cruzamento dos dados do incidente com outras bases de dados. Ao final, escolhe-se um nível de 1 a 4 a fim de atribuir o *score* **FI**.

2.2 CIRCUNSTÂNCIAS DO INCIDENTE (CI)

Nessa etapa, considera-se a perda de segurança (confidencialidade, integridade e disponibilidade) e a intenção maliciosa do incidente, de acordo com os seguintes parâmetros:

A. **Perda de confidencialidade:** Ocorre quando a informação é acessada por partes não autorizadas ou que não possuem finalidade legítima no acesso. A extensão da perda deve levar em conta o escopo da revelação, como o número potencial de indivíduos e tipos de indivíduos que podem ter tido acesso à informação.

B. **Perda de integridade:** Ocorre quando a informação original é alterada e o dado substituído pode ser prejudicial ao indivíduo. A situação mais severa ocorre quando o dado alterado pode ser utilizado para causar dano ao indivíduo.

C. **Perda de disponibilidade:** Ocorre quando o dado não pode ser mais acessado, mesmo sendo necessário. Pode ser temporal (limite de tempo no qual a falta de acesso é prejudicial ao indivíduo) ou permanente.

D. **Dolo:** Avaliação de se o incidente ocorreu por erro, negligência, por causa humana ou técnica, ou se foi causado de forma dolosa. Exemplos de incidentes não intencionais incluem perda acidental, erro humano. Exemplos de incidentes dolosos envolvem a venda de dados pessoais ou ações que visam expor dados pessoais do titular a terceiros com a finalidade de causar dano.

Para avaliação do critério CI, devem ser dados pontos para cada elemento. Os pontos devem ser somados para obter o *score* final.

GRAVIDADE DO INCIDENTE DE SEGURANÇA		
SG < 2	**Baixo**	Indivíduos não serão afetados ou sofrerão pequenos inconvenientes sem maiores problemas, como irritações.
2 ≤ SG < 3	**Médio**	Indivíduos podem encontrar inconveniências significativas, que poderão superar com alguma dificuldade (custos extras, perda de acesso, estresse, perda de interesse).
3 ≤ SG < 4	**Alto**	Indivíduos podem encontrar consequências significativas, as quais podem superar com sérias dificuldades como perda financeira, negativação, danos à propriedade e perda de emprego.
4 ≤ SG	**Muito Alto**	Indivíduos podem encontrar consequências de perdas significativas ou irreversíveis às quais podem não superar, como dívidas substanciais, incapacidade para trabalho, danos psicológicos de longo prazo, morte etc.

Além disso, para a elaboração de resposta a esse quesito, foi realizada análise comparada dos Guias de Notificação de Incidentes de Segurança, bem como dos guias de elaboração de Relatório de Impacto à Proteção de Dados Pessoais das Autoridades de Proteção de Dados da Argentina, Austrália, Espanha, França, Reino Unido e Uruguai.

No que diz respeito ao rigor metodológico, bem como à estruturação organizada de uma análise de impacto de um incidente de segurança, elegeu-se a apresentação do Guia "Security of Personal Data"[62] do **Esquema de Notificação de Incidentes de Segurança - NBD-Scheme**, vigente na Austrália.

[62] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Data breach preparation and response.** 2019. Disponível em: <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/>.

Em 2017, o Parlamento Australiano promulgou o "Privacy Amendment (Notifiable Data Breaches) Act"[63]. O Ato, além de oferecer provisões concretas para uma notificação de incidente de segurança, também oferece perspectivas positivas para uma boa realização de compreensão do impacto e da gravidade de um incidente de segurança.

Na Seção 26WG do documento, é estabelecida uma metodologia de análise de gravidade de incidentes. Os critérios, também presentes no Guia Data Breach preparation and response, foram transcritos abaixo para referência.

Os motivos de eleição de exposição dos critérios adotados pela OAIC são: **i)** o nível de detalhamento do Esquema para Incidentes de Segurança Notificáveis; **ii)** a utilização de critérios estabelecidos pela revisão de literatura realizada para apreciação da gravidade de um incidente de segurança e **iii)** a compreensão dialógica e propositiva adotada pelo conteúdo.

1. **Avalia se, da perspectiva de uma "pessoa razoável", o incidente de segurança será possivelmente capaz de gerar sério dano para o indivíduo que teve suas informações pessoais comprometidas.**

Por 'pessoa razoável', a OAIC compreende como uma pessoa que esteja na posição da entidade Notificante, e não do indivíduo que teve suas informações comprometidas no incidente de segurança e que esteja propriamente informada baseada em informações imediatamente disponíveis ou após a realização de inquéritos para compreensão do incidente.

A frase "possivelmente capaz de gerar" se refere aos riscos à danos severos à avaliação de se o risco de dano severo aos titulares é mais provável de ocorrer do que não (usa-se o termo provável, ao invés de possível, de forma proposital).

Dano severo, para a OAIC, é caracterizado como: dano psicológico, físico, emocional, financeiro ou reputacional.

As orientações da OAIC indicam que os agentes devem endereçar a avaliação do "risco severo" de forma holística, apreciando a probabilidade de dano e as consequências de dano. A apreciação inclui:

- O tipo ou tipos de informações;
- A sensibilidade da informação;

[63] AUSTRALIA. **Privacy Amendment (Notifiable Data Breaches) Act 2017. An Act to amend the Privacy Act 1988, and for related purposes.** 2017. Disponível em: <https://www.legislation.gov.au/Details/C2017A00012>.

- Se a informação está protegida por uma ou mais medidas de segurança e a possibilidade de que essas medidas de segurança possam ser superadas;
- As pessoas ou os tipos de pessoas que obtiveram ou que podem vir a obter as informações;
- Se foi utilizada uma metodologia de segurança ou de tecnologia:
  - » Em relação à informação;
  - » Feita de forma a tornar a informação inteligível ou sem significado para pessoas não autorizadas a obter a informação.
- A possibilidade que as pessoas ou tipos de pessoas que:
  - » Obtiveram ou que podem obter informações possuem intenção de causar dano aos indivíduos titulares de dados ou capaz de superar as medidas de tecnologia da segurança aplicadas.
- A natureza do dano;
- Quaisquer outros aspectos relevantes.

2. Avaliação da categoria de titular de dados envolvida no incidente

Há algumas categorias de informação que são mais capazes de causar dano sério ao indivíduo se comprometidas. Alguns exemplos dos tipos de informação que podem causar dano severo no caso de incidente de segurança incluem:

- Dados sensíveis, como informação sobre a saúde do indivíduo;
- Documentos utilizados de forma comum para roubo de identidade, como detalhes de plano de saúde, carteira de motorista ou dados do passaporte;
- Informação financeira;
- Uma combinação dos tipos de informação pessoal (ao invés de apenas um único tipo de informação) que permite maior conhecimento sobre o titular de dados afetado.

3. Avaliação das circunstâncias do incidente de segurança

As circunstâncias específicas do vazamento são importantes para a consideração da existência de dano severo a um indivíduo. Isso pode incluir as seguintes considerações:

- Quem são as pessoas que tiveram as informações pessoais afetadas pelo incidente?
- Quantos indivíduos foram afetados?
- As circunstâncias do incidente afetam a sensibilidade da informação?

- Por quanto tempo a informação ficou acessível?
- A informação estava adequadamente encriptada, anonimizada ou, de outra forma, inacessível?
- Que pessoas ganharam acesso ou controle aos dados pessoais objeto do incidente de segurança?

4. Avaliação da natureza do dano

Ao avaliar a natureza do dano, as entidades devem pensar a diversa quantidade de danos que podem seguir um incidente de segurança. Para isso, seria importante considerar um número de cenários que podem resultar em dano severo e a possibilidade de que cada um ocorra. São eles:

- Roubo de identidade;
- Perda financeira significativa pelo indivíduo;
- Ameaças para a integridade física do indivíduo;
- Perda de emprego ou de oportunidades de emprego;
- Humilhação, dano à reputação ou à relacionamentos;
- Bullying social ou no ambiente de trabalho e marginalização.

Além disso, é importante que seja avaliada a probabilidade de dano, bem como que sejam antecipadas as possíveis consequências aos titulares de dados.

Por fim, uma última abordagem metodológica de relevante interesse foi apresentada pela Agencia de Acceso a la Información Pública (AAIP) - Argentina e pela Unidad Reguladora y de Control de Datos Personales (URCDP) - Uruguai no Guia conjunto "Evalución de Impacto en la Protección de Datos"[64].

Embora o Guia tenha sido proposto para realização de avaliação de risco de forma a prevenir riscos de incidente de segurança, a metodologia abordada pode ser considerada para nortear uma análise baseada em um risco material - que se concretizou com um incidente ou que pode estar em vias de se concretizar. Nesse sentido, é importante possuir critérios de avaliação do impacto efetivamente ocorrido ou provável de ocorrer diante da aplicação dos estándares aqui disponíveis, com base em um caso concreto.

A metodologia apresentada segue a seguinte matriz:

RISCO = PROBABILIDADE X IMPACTO

[64] AAIP; URCDP. **Guía de Evaluación de Impacto en la Protección de Datos.** 2019. Disponível em: <https://www.argentina.gob.ar/sites/default/files/guia_final.pdf>.

Probabilidade diz respeito às possibilidades existentes de que a ameaça se materialize. Impacto, por sua vez, é um critério determinado com base nos danos que se podem produzir caso a ameaça se materialize.

A realização de uma **avaliação de impacto** baseada em um caso concreto no qual foi constatada a existência de um incidente de segurança é uma metodologia possível para compreensão da análise de gravidade de um incidente e será explorada abaixo.

De acordo com o Guia, a **avaliação de impacto** deve ser considerada a partir de uma perspectiva valorativa material e moral. Ressalte-se que a fórmula para valoração dos critérios deve ser desenhada para cada organização, tendo em vista as atividades do Titular de Dados, a natureza dos dados pessoais tratados, o volume de dados vazados e demais informações sobre o incidente e critérios de avaliação, já explanados em resposta à pergunta 11.

Da avaliação de impacto:

<table>
<tr><th colspan="2">IMPACTO BAIXO</th></tr>
<tr><td colspan="2">Os titulares de dados não serão afetados ou somente sofrerão alguns inconvenientes, que poderão ser solucionados sem muitas dificuldades</td></tr>
<tr><td>Exemplos de Impactos Materiais:

• Perda de tempo com a repetição e formalidades ou com a espera de sua realização;
• Recebimento de correio eletrônico não solicitado (spam);
• (Re)utilização de suas informações, publicadas em sites ou plataformas web, para propaganda direcionada.</td><td>Exemplos de Impactos Morais:

• Mera perturbação causada pela solicitação ou recebimento de suas informações;
• Medo de perder o controle de seus próprios dados;
• Sensação de invasão de sua privacidade, mesmo que não tenha se materializado um dano objetivo ou real;
• Acesso negado à site ou plataforma web que deixa de prestar serviço importante ao titular por erro de acesso.</td></tr>
</table>

IMPACTO MÉDIO	
Os titulares de dados são afetados de maneira significativa, mas são capazes de superar a situação com alguma dificuldade	
Exemplos de Impactos Materiais: • Cobranças impostas de maneira errônea ou indevida; • Recusa de acesso a serviços administrativos ou comerciais; • Perda de oportunidade de conforto (cancelamento de compra ou transação vinculada ao período de férias); • Bloqueio de conta ou de serviços eletrônicos; • Recebimento de emails direcionados com intenção de causar dano ou ameaçar a reputação do titular de dados; • Desatualização de informações relevantes ao titular de dados.	**Exemplos de Impactos Morais:** • Medo ou negativa de utilizar um serviço relevante da sociedade da informação ou rede social; • Danos psicológicos objetivos, porém menores; • Danos à reputação ou à honra; • Problemas com relacionamentos pessoais ou no âmbito laboral; • Sensação de invasão de privacidade sem um dano significativo; • Intimidação em redes sociais.

IMPACTO ALTO	
Os titulares de dados são afetados de maneira significativa e apenas poderão superar a situação com grandes dificuldades	
Exemplos de Impactos Materiais: • Transferência errônea de ativos financeiros do titular à outras pessoas sem compensação; • Dificuldades financeiras a médio e longo prazo; • Perda de oportunidades únicas, não recorrentes; • Perda de trabalho; • Separação ou divórcio; • Dano à propriedade; • Perda financeira como resultado de uma fraude.	**Exemplos de Impactos Morais:** • Danos psicológicos sérios (depressão, paranoia, desenvolvimento de fobia); • Sensação de invasão da privacidade com dano irreversível; • Sensação de vulnerabilidade por ter que intervir em um procedimento judicial; • Sensação de violação de direitos fundamentais (discriminação, liberdade de expressão); • Sofrimento de extorsões ou de manifestações públicas contrárias; • Ciberbullying e assédio moral.

IMPACTO CRÍTICO	
Os titulares de dados enfrentam consequências gravíssimas ou irreversíveis que talvez não sejam capazes de superar	
Exemplos de Impactos Materiais: • Risco financeiro; • Dívidas substanciais; • Incapacidade laboral; • Incapacidade de seguir vivendo em um mesmo lugar ou de mudar-se para outro; • Perda de prova no contexto de um litígio; • Perda de acesso à infraestrutura essencial (água, eletricidade).	**Exemplos de Impactos Morais:** • Dano psicológico permanente; • Condenação penal; • Sequestro; • Perda de vínculos familiares e de amizade; • Incapacidade de demandar em justiça; • Mudança de status administrativo; • Status de perda de capacidade.

Outro material relevante foi proposto pela Commission Nationale de L'informatique et des Libertés (CNIL), autoridade francesa de proteção de dados pessoais, no Guia "Security of Personal Data"[65].

A Autoridade apresenta tabela de avaliação da gravidade do incidente, abaixo transcrita para referência:

Riscos	Efeitos nos indivíduos	Principais fontes de risco	Principais ameaças	Medidas existentes ou planejadas para mitigação	Gravidade	Probabilidade
Acesso não legítimo a dados						
Modificação indesejada de dados						
Perda de dados						

Dentro da avaliação, deve-se levar em consideração os critérios já levantados anteriormente, o que permitirá o estabelecimento de um score de gravidade que pode variar entre: negligenciável, moderado, significante ou máximo.

[65] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Security of Personal Data.** 2018. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf>.

Buscou-se, com a apresentação de materiais, metodologias e critérios utilizados por diferentes Autoridades de Proteção de Dados ao redor do mundo, disponibilizar ferramentas para que a ANPD possa elaborar uma metodologia própria, capaz de melhor atender a realidade brasileira.

Sugere-se que as providências a serem tomadas pela ANPD devam girar em torno de três nortes fundamentais: 1. Procurar alinhar as providências à lógica de regulação responsiva adotada pela LGPD; 2. Os deveres da própria agência, quais sejam: (i) guia/orientação aos regulados (ii) fiscalização e imposição de medidas sancionatórias (iii) Cooperação e (iv) Publicidade; e 3. Manter em mente que o papel da ANPD nesse contexto é, além de mitigar os danos já concretizados (art. 48, § 2º), proteger os dados de danos adicionais, buscando formas de conter o incidente. Nesse sentido, sugere-se os seguintes encaminhamentos:

1. A elaboração de um documento padrão sobre os passos gerais que serão tomados pela ANPD em resposta às notificações de incidentes;

2. Esclarecimento sobre quando e se os casos notificados acompanhados pela agência serão transformados em materiais de estudos e em quais termos;

3. Orientação aos controladores acerca da necessidade (ou não) da comunicação aos titulares;

4. Realização de uma análise inicial sobre quem deve gerir o incidente ao receber a notificação;

5. Elaboração de memorandos de entendimentos de cooperação procedimental com demais órgãos;

6. Avaliação inicial de nível de periculosidade e impacto, a qual deve comunicada ao remetente, indicando as ações necessárias para a resolução do incidente (o que pode e deve ser feito consultando experiências de outras instituições que lidam com notificações de incidentes de segurança);

7. Delimitação sobre qual será o meio de comunicação oficial entre ANPD e controlador e quais as regras procedimentais desta comunicação;

8. Esclarecimentos de natureza jurídica (exemplos: O operador tem o dever de notificar um incidente de segurança à autoridade? Se sim, em quais casos? O pagamento de resgate nos casos de *Ransomwares* é legal? Se sim, como deve ser feito?).

Conforme o art. 48, § 2º da LGPD, a ANDP, além do dever de verificar a gravidade do incidente, "[...] poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente." Importante manter em mente que, em uma lógica de regulação responsiva, as providências a serem tomadas pela ANPD também em casos de incidente devem seguir uma toada cooperativa com os controladores remetentes da notificação, visto que a meta principal de todo esse processo é, além da contenção do incidente, a proteção dos dados de danos adicionais.[66]

As competências da ANPD estão elencadas no artigo 55-J da LGPD. A análise desse artigo com o enfoque no papel da Agência em termos de ações a serem tomadas frente à uma notificação de incidentes de segurança possibilita a classificação de quatro frentes de atuação da agência designadas pela lei: (1) **Dever guia/orientação aos regulados** (incisos III, VI, VIII, XIII e XX) ; (2) **Dever de fiscalização e imposição de medidas sancionatórias** (IV, XVI, XVII); (3) **Dever de cooperação** (IX e XXIII) (Incisos que se aplicam tanto à fiscalização e cooperação: XI, XXI e XXII). Todas essas categorias devem seguir, também por força normativa, o princípio da publicidade, que consiste na transparência ao público das ações e entendimentos da agência, culminando em uma quarta categoria de (4) **Dever de publicidade** (II, X, XII e XIV).

As sugestões seguem nesse sentido de: regulação responsiva, proteção de dados como norte fundamental e categorias de competências da ANPD.

→ Entende-se que os planos de ação podem divergir conforme o incidente de segurança. No entanto, sugere-se a **elaboração de um documento padrão sobre os passos gerais que serão tomados pela ANPD em resposta às notificações de incidentes.** Importante que este seja publicizado, em respeito ao princípio da publicidade, assegurando aos controladores uma previsibilidade importante acerca do que esperar da agência após a notificação. Importante que seja publicizado, por exemplo, **quando e se os casos notificados acompanhados pela agência serão transformados em materiais de estudos e em quais termos** - o nome da empresa será publicado? Será necessário o consentimento da empresa? Por exemplo, além do já mencionado Padrões para Notificação de Incidentes de Segurança do Ctir Gov., a ICO, possui em seu website uma aba sobre políticas internas, dentre as quais se encontra um documento intitulado "Comunicando nosso regulatório e Política de Atividades de Execução" ("Communicating our Regulatory and Enforcement Activity Policy")[67]. Além de outras informações, constam diretrizes de interação com os regulamentados e princípios de atuação regulatória - por exemplo: "Ação após incidentes serem relatados e preocupações

[66] INFORMATION COMMISSIONER'S OFFICE. **Data Breach Management Workshop.** 2019. Disponível em: <https://ico.org.uk/for-organisations/gdpr-resources/pdb/>.

[67] INFORMATION COMMISSIONER'S OFFICE. **Communicating our Regulatory and Enforcement Activity Policy.** 2019. Disponível em: <https://ico.org.uk/media/1890/ico_enforcement_communications_policy.pdf>.

levantadas: Podemos publicar ou divulgar informações que destacam a melhoria de práticas nos direitos de informação após reclamações e incidentes são relatados para nós. Isso incluirá nomes de organizações se o interesse público justificar isto").

→ **Orientar os controladores acerca da necessidade (ou não) da comunicação aos titulares.** Essa é uma prática sugerida pelo WP29, por meio da qual "[...] ao notificar a autoridade supervisora, os controladores podem obter aconselhamento sobre se os indivíduos afetados precisam ser informados". A Agência francesa segue na mesma toada, ao determinar que, em caso de dúvidas sobre a necessidade de se notificar os titulares, é possível contatar a CNIL, que determinará se tal comunicação deve ou não ser feita.

→ **Ao receber a notificação, realizar uma análise inicial sobre quem deve gerir o incidente.** Essa é uma das providências indicadas pelo Guia Nacional de Notificação e Gestão de Incidentes Cibernéticos da Espanha ("Guía Nacional de Notificación y Gestión de Ciberincidentes da Espanha"), publicado em 2020. Sempre que a agência responsável recebe uma notificação sobre um possível incidente cibernético, a equipe técnica realiza uma análise inicial que determinará se o caso é passível de ser gerido por ela mesma ou por um terceiro.

- Neste cenário complexo e fragmentado de enforcement, casos de competências concorrentes podem facilmente acontecer. Assim, é fundamental uma "[...] busca ativa por ferramentas hermenêuticas e por mecanismos de coordenação e articulação de competências, que podem ser construídos a partir da definição de procedimentos e parâmetros para a fixação de competências primárias e secundárias no endereçamento de casos concretos". Nesse sentido, sugere-se que a ANPD elabore memorandos de entendimentos de cooperação procedimental com demais órgãos que possam enquadrar-se como competentes para lidar com os incidentes de segurança. A ICO, por exemplo, adotou essa prática de procedimentalizar a cooperação com outros órgãos: possui memorandos de entendimento com quarenta e cinco instituições, desde a Advocacia Geral da União até o Centro de Informações de Saúde e Assistência Social.

Quando há indícios de que o caso pode ser gerido pela própria agência, faz-se uma **avaliação inicial de nível de periculosidade e impacto, a qual é comunicada ao remetente, indicando as ações necessárias para a resolução do incidente.**

- Para além do uso dos critérios e metodologias sugeridos acima, a determinação das ações necessárias podem contar com a experiência de outras instituições que lidam com notificações de incidentes de segurança. Por exemplo, o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR), que já possui diretrizes para lidar

> com incidentes. Parte do processo de tratamento de incidentes perpassa pela análise de incidentes, suporte à recuperação de incidentes, coordenação na resposta a incidentes, distribuição de alertas e cooperação com outras equipes de tratamento de incidentes (Delimitado em documento "Padrões Para Notificação De Incidentes De Segurança ao Ctir Gov").[68]

Fundamental delimitar qual será o meio de comunicação oficial entre ANPD e controlador e quais as regras procedimentais desta comunicação. Uma medida técnica estabelecida pelo Guia Espanhol consiste na **atribuição de um identificador único a cada caso**, o qual estará presente durante todas as comunicações relacionadas ao incidente. Se as comunicações são feitas por e-mail, este identificador aparece no campo "assunto" e não deve ser modificado ou eliminado, visto que isso retardaria o gerenciamento e a resolução final do incidente cibernético.

→ Sugere-se, por fim, que este guia contenha **esclarecimentos jurídicos**, como: O operador tem o dever de notificar um incidente de segurança à autoridade? Se sim, em quais casos? O pagamento de resgate nos casos de Ransomwares é legal? Se sim, como deve ser feito? Dentre outros.

Novamente, um bom exemplo regulatório é o guia "Data breach preparation and response"[69], publicado pela OAIC. Em seu Guia, a OAIC apresenta o design do Esquema para Incidentes de Segurança Notificáveis como uma espécie de estandarte metodológico para orientar o Controlador de suas ações diante de um incidente de segurança, que deve ser entregue à Comissão. Tratam-se de orientações para formatação de um completo Plano de Resposta a Incidentes de Segurança. A estrutura do Guia é a seguinte:

> **Parte 1:** Explicações sobre o conceito e a caracterização de incidente de segurança e exposição de obrigações dos agentes de tratamento na ocorrência de incidente e esquema visual.
>
> **Parte 2:** Passo a passo para a preparação de um Plano de Resposta a Incidentes de Segurança, com *checklist* visual para fins de orientação. Especificamente nesse tópico, o guia se debruça em aspectos como a composição de uma equipe de resposta e ações a serem tomadas pelos agentes.

[68] <https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf>.

[69] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Data breach preparation and response.** 2019. Disponível em: <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/>.

Information to be included	Yes/No	Comments
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsabilities		
Details of any external expertise that should be engaged in particular circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial actions		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC) or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record keeping policy to ensure that breaches are documented		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response plan		

Parte 3: O Guia apresenta 4 passos práticos para colocar em ação o Plano de Resposta a Incidentes de Segurança, quais sejam: **(i)** conter; **(ii)** avaliar; **(iii)** notificar e **(iv)** rever. As informações também são apresentadas no formato de infográfico visual.

Parte 4: Denominada "Esquemas para Incidentes de Segurança Notificáveis - NDB Scheme" (trad. nossa), o Guia aprofunda conceitos e procedimentos metodológicos de pontos de interesse trabalhados em suas outras seções, com orientações para: **(i)** incidentes que envolvem múltiplas entidades; **(ii)** exceções ao dever de notificação; **(iii)** notificação ao titular de dados; **(iv)** metodologia para avaliação de gravidade de incidente e **(iv)** o papel da OAIC diante de uma notificação de incidente de segurança.

Sobre este último ponto, a OAIC estabelece as seguintes medidas que podem ser tomadas pela Autoridade diante de uma notificação pelo controlador de dados:

(i) Da entrega voluntária de informações técnicas e organizacionais necessárias para apuração e diligências do incidente de segurança:
Apesar de não obrigadas pelo Privacy Act australiano, a Autoridade apresenta como uma prática de boa fé que os controladores repassem informações adicionais sobre o incidente ocorrido, bem como sobre as respostas tomadas pelo agente. Como exemplo, cita o fornecimento de informações técnicas que não necessitariam, necessariamente, de comunicação direta ao titular de dados pessoais. Esse tipo de informação auxilia a OAIC a estabelecer se deve realizar maiores diligências investigatórias ou tomar quaisquer outras ações. Esse tipo de informação também é utilizado pela OAIC para redigir relatórios estatísticos sobre as notificações recebidas. Além disso, a entidade que ofereceu a informação pode realizar uma requisição de sigilo à Comissão, que deverá respeitar a confiança das informações comerciais ou operacionais sensíveis fornecidas de forma voluntária em suporte à notificação realizada. A orientação da OAIC é de que a divulgação das informações só será realizada após consulta com a entidade notificadora, com seu consentimento ou quando assim for exigido por lei.

(ii) Da resposta da Autoridade às notificações:
A OAIC reconhece todas as notificações de incidentes de segurança recebidas. Ela poderá realizar inquéritos ou oferecer conselhos em resposta à notificação. Para isso, a Comissão se orienta pelo tipo e pela sensibilidade dos dados pessoais, pelo número de indivíduos potencialmente afetados ou em risco de sofrerem dano severo e pela extensão pelas quais a Notificação e quaisquer informações adicionais providas demonstrarem que:

- O incidente de segurança foi contido ou está em processo de contenção, quando possível;

- A entidade notificante tomou ou está tomando medidas razoáveis para mitigar os impactos do incidente nos indivíduos que possuem alto risco de dano potencial;
- A entidade tomou ou está tomando medidas razoáveis para minimizar a possibilidade de que um incidente similar ocorra novamente.

(iii) Da ação regulatória e das prioridades da Comissão:
A prioridade de orientação da OAIC no processo é garantir e assistir indivíduos em risco de sofrer dano severo. Apesar disso, a Comissão estabelece a possibilidade de tomar medidas regulatórias, por sua própria iniciativa, em resposta à Notificação, nos termos do Privacy Act Australiano.

(iv) Dos poderes de enforcement e da aplicação de um Esquema para Incidentes de Segurança Notificáveis - NBD scheme:
A Comissão avalia se a instituição notificante tomou medidas razoáveis para lidar com o incidente de segurança ocorrido. Uma falha da entidade de cumprir qualquer um dos seguintes requisitos representa, na interpretação da OAIC, uma interferência negativa à privacidade dos titulares de dados capaz de justificar uma ação de *enforcement*:

- Realizar uma avaliação razoável e rápida do incidente de segurança, tomando todas as medidas razoáveis para garantir que a avaliação seja concluída dentro de 30 dias da ciência do Notificante do incidente;
- Preparar uma declaração sobre o incidente segurança e prover uma cópia à Comissão, no tempo mais rápido possível;
- Notificar os titulares de dados em risco de sério dano sobre os conteúdos da declaração ou, dependendo da natureza do caso, realizar a publicação da declaração;
- Cumprir com as diretrizes da OAIC no procedimento de elaboração de declaração e de notificação de forma tempestiva e ágil.

Os poderes de enforcement da OAIC incluem:

- Aceitar um Acordo e iniciar procedimentos para garantir o cumprimento do Acordo;
- Realizar uma determinação e os procedimentos para obrigar o cumprimento da determinação;
- Buscar uma liminar para evitar o incidente em curso ou sua recorrência;
- Direcionar a demanda para uma Corte para que seja aplicada multa.

Em muitos casos, a Comissão é provocada por indivíduos em situações nas quais o agente falhou em realizar seu dever de notificação. A ação preferencial da OAIC é estabelecer diálogo com o agente para que eles cumpram os passos delimitados pelo NBD Scheme, antes de aplicar medidas impositivas.

(v) Da obrigação de notificar - comunicação com o Controlador prévia à Notificação:
A Comissão pode orientar o Notificante a realizar a comunicação do incidente para indivíduos em risco de sofrerem sério dano, bem como para a própria OAIC. Antes de solicitar a notificação, usualmente, a Comissão solicita que o agente concorde em realizar a notificação. Esse é o tipo de caso no qual a Comissão realiza orientações ao agente mesmo antes da Notificação, quando se tornou ciente da ocorrência de um incidente de segurança.
Além disso, também é plausível que a OAIC informe o controlador sobre quando uma notificação não é necessária ou modifique, a depender da circunstância do caso, o prazo para que seja realizada a notificação.

(vi) Da busca de apoio técnico e legal pelo Controlador:
A OAIC é responsável por informar e guiar a sociedade sobre as matérias relativas à proteção de dados pessoais na Austrália. Apesar disso, a OAIC não considera ser capaz de oferecer apoio legal e técnico próprio para cada incidente de segurança sobre o qual é notificada. Nesse sentido, embora haja orientações claras sobre a formulação do NBD Scheme, bem como acompanhamento do caso pela Comissão, os Controladores devem constituir suas próprias equipes para gerir o incidente de segurança.

(vii) Da publicação de informações sobre o incidente pela Comissão:
A OAIC opta por publicar informações sobre as formas com que as entidades têm tratado incidentes de segurança de dados pessoais na forma de dados estatísticos não identificados.

No caso específico do Sistema Nacional de Proteção de Dados no Brasil, percebe-se, entretanto, uma preocupação do legislador brasileiro de que a divulgação do fato em meios de comunicação esteja garantida nos casos em que isso for necessário para a salvaguarda dos direitos dos titulares (art. 48, § 2º, I). Nesse sentido, apesar de reconhecer a importância da publicação de dados estatísticos e relatórios que deem publicidade às informações sobre incidentes nacionais, também é relevante a ponderação sobre os casos em que se é apropriado determinar que os próprios controladores deem a devida publicidade ao ocorrido.

Por fim, uma última referência de extrema relevância consiste no documento da União Europeia com exemplos de atuações das autoridades de proteção de dados nos casos de incidentes de segurança. A delimitação de como será a atuação da ANPD frente às notificações pode se basear nessas experiências internacionais documentadas.