BAPTISTALUZ

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO – TOMADA DE SUBSÍDIOS Nº 2021

Março de 2021

Autores:

/ Fernando Bousso

/ Odélio Porto Júnior

/ Odélio Porto Júnior

/ Matheus Botsman Kasputis

/ Rafaela Marcondes Sobrinho

/ Adriane Loureiro Novaes

Sumário

Introdução

Este documento torna acessível ao público as contribuições realizadas pelo Baptista Luz Advogados para a toma de subsídios sobre incidentes de segurança da informação, realizada pela Autoridade Nacional de Proteção de Dados (ANPD), entre 22/02/2021 e 24/03/2021.[1] Assim, a disponibilização das contribuições feitas tem o objetivo de enriquecer o debate entre os atores interessados, a fim de fomentar um ambiente regulatório adequado de proteção de dados pessoais, harmonizando a proteção dos titulares com o desenvolvimento tecnológico e a inovação.

Neste documento estão transcritas as análises e recomendações referentes a cada uma das perguntas elaboradas pela ANPD (conforme o sumário abaixo). Os temas principais da tomada de subsídios referem-se: **(i)** as definições de risco e dano gerados por incidentes de segurança das informações, e os respectivos critérios de análise desses conceitos; **(ii)** as definições procedimentais sobre o prazo e nível de detalhamento das notificações de incidentes à ANPD e aos titulares; e **(iii)** possíveis exceções à obrigatoriedade de informar a ANPD e os titulares. O sumário abaixo indica cada umas das perguntas respondidas nesta consulta.

Boa leitura!

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?

1. Considerações Iniciais

1.1. Definição de Incidente de Segurança de Informação

Antes de se analisar os riscos e danos acarretados por um incidente, é importante que a ANPD estabeleça a definição de "*incidente de segurança da informação*" que a agência utilizará.

A área da ciência da computação apresenta definições variadas sobre o que seria um incidente de segurança da informação. Uma das definições tradicionais da área é a tríade de princípios "CIA"

[1] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS**. ANPD inicia processo de regulamentação sobre incidentes de segurança com tomada de subsídios**. 2021. Acesso em: 29/03/2021. Disponível em: <https://bit.ly/39rGYx1>.

que define segurança da informação como sendo a preservação da (**i**) confidencialidade, (**ii**) disponibilidade e (**iii**) integridade da informação. Esta é, inclusive, a definição utilizada pela ISO 27000 sobre sistemas de gestão de incidentes de segurança da informação.[2]

A redação do artigo 46 da LGPD, apesar de não citar diretamente os princípios da CIA, define indiretamente o conceito de incidente de segurança da informação com um conceito derivado desses princípios[3], na medida em que as ações listadas no artigo 46 remetem à violação de um ou mais dos princípios da tríade. Por exemplo, a destruição ilícita de um dado afeta a sua disponibilidade e integridade; já um acesso indevido com publicação não autorizada afeta a confidencialidade da informação.

Também nesse sentido, a definição de "segurança da informação" do NIST estadunidense - agência governamental não regulatória para promoção da inovação tecnológica – utiliza ambos os elementos destacados acima na sua definição, qual seja:

"a proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de garantir a confidencialidade, integridade e disponibilidade"[4].

/ Recomendação

Portanto, é recomendável que a ANPD esclareça quais pressupostos serão utilizados para definir e analisar um incidente de segurança da informação, o que pode ser feito, por exemplo, por meio de materiais orientativos e normas administrativas.

---

[2] "3.28 information security: preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information". THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)**. ISO/IEC 27000:2018(E)**. 2018. p.4.

[3] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os 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". Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018.

[4] "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." ESTADOS UNIDOS. National Institute of Standards and Technology (NIST). **Computer Security Resource Center – Glossary**. Acessado em: 15/03/2021. Disponível em: <https://bit.ly/3el8eek>

1.2. Fundamentos para a Compreensão de um Incidente

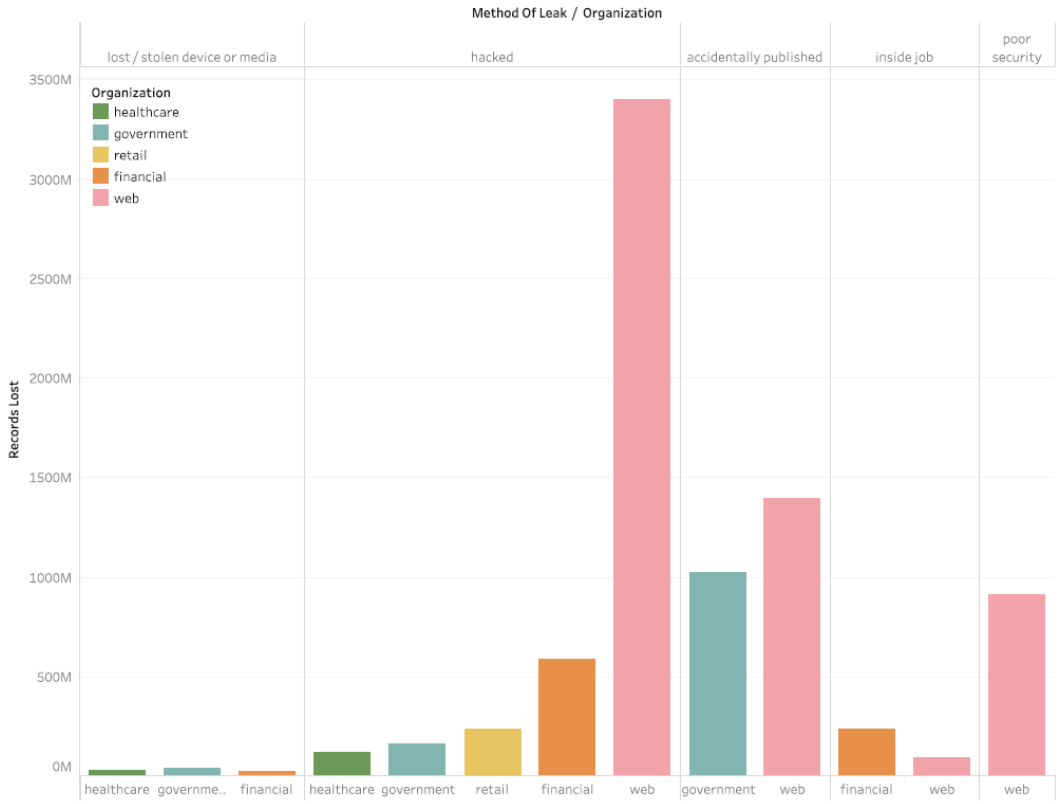

***Fig. 1** - O número de dados afetados por tipo de incidente e organização, entre 2004 e 2017, da base de dados World's Biggest Data Breaches.*[5]

Devemos considerar como premissa fundamental para o debate deste tema que não existem sistemas que sejam absolutamente seguros – o que não implica dizer que medidas proporcionais de segurança devam deixar ser adotadas. Este fundamento decorre da própria natureza das tecnologias e de sua implementação, sendo de fácil verificação que diversas organizações ao redor do globo - sejam multinacionais, Estados ou organizações da sociedade civil, de tamanhos e capacidade financeira distintas - já foram atingidas por diferentes tipos de incidentes de segurança da informação.

As técnicas de invasão a sistemas de informação são caracterizadas pelo seu desenvolvimento constante; sendo utilizadas por uma gama de agentes distintos, sejam Estados-Nação, organizações criminosas ou mesmo indivíduos, e por motivos diversos (p. ex. ganho econômico, exposição do alvo, motivações pessoais etc.).[6] Assim, a

[5] LIU, Liyuan; HAN, Meng; WANG, Yan; ZHOU, Yiyun. **Understanding Data Breach: A Visualization Aspect**. Conference: The 13rd International Conference on Wireless Algorithms, Systems, and Applications. 2018. p. 887. Acessado em: 16/03/2021. Disponível em: <https://bit.ly/2No2Qlf>.

[6] UNIÃO EUROPEIA. European Union Agency for CyberSecurity (ENISA).

capacidade de previsão de risco de incidentes é dificultada de forma expressiva por essas características, o que deve ser levado em consideração pela ANPD.

É necessário que os incidentes sejam analisados tendo como base a sua natureza complexa. Nesse sentido, após analisar técnica e juridicamente uma série de casos de incidentes de segurança da informação, incluindo os respectivos litígios e processos administrativos que se seguiram, a pesquisadora sobre o tema Josephine Wolff esclarece que:

> *"Diferentes tipos de organizações - de desenvolvedores de software a administradores de sistemas e formuladores de políticas públicas - são capazes de influenciar e intervir apenas em diferentes estágios de um incidente de segurança da informação.* ***O fato de que cada defensor individual possui um escopo limitado de atuação é crucial para entender quais responsabilidades de segurança da informação eles podem razoavelmente e realisticamente assumir.***
>
> *Quando analisamos (e relatamos ou litigamos) incidentes de segurança que obtiveram êxito, muitas vezes nossa inclinação é agarrar-se ao primeiro ponto de acesso [de um hacker] ou ao ponto de acesso mais fácil de ser compreendido (p. ex. o e-mail de phishing [...] a rede sem fio desprotegida), e insistir que a simples defesa desse único ponto teria feito toda a diferença (p. ex. autenticação de dois fatores ou limitação de tentativas de logins [...]).*
>
> *Mas essa perspectiva simplifica demasiadamente a realidade muito mais complexa de que um incidente de segurança se desenvolve de forma gradual e crescente; bem como ofusca as ações de defesa limitadas e o ambiente desafiador em que os defensores individuais de um ataque operam na prática." (JOSEPHINE WOLFF, 2018, tradução nossa)*[7]

[7] *"Different types of organizations and defenders – from software developers to system administrators to policymakers – are able to influence and intervene at very different stages of security breaches. Each individual defender limited scope of control that is crucial for understanding which defensive responsibilities they can reasonably and realistically be expected to assume. When we talk about (and report on and litigate) successful security incidents, too often our inclination is to latch onto the first or the most easily understood point of access – the phishing email [...] the unprotected wireless network – and harp on the simple line defense that seems like it would have made all the difference – two factor authentication, or rate limiting logins [...] But that perspective oversimplifies the much more complicated narrative of the gradual, escalating capabilities acquired by*

/ Recomendação

Desse modo, é recomendável que a ANPD busque preparar seu corpo técnico a fim de ter a real dimensão da complexidade que envolve a investigação e entendimento de um incidente de segurança da informação. Principalmente para que a atribuição de responsabilidades seja feita de forma proporcional, e seja fomentado um ambiente de cooperação entre os agentes de tratamento e a ANPD. A complexidade técnica dos incidentes exige tal ação conjunta para se evitar e mitigar os danos aos titulares.

2. Definição de Risco e Dano

Neste tópico será feito uma síntese sobre o conceito de risco conforme ele tem sido utilizado e debatido na União Europeia, em relação à GDPR; e nos EUA (abordado no **item** 4). A partir desses subsídios são feitas algumas ponderações sobre como a ANPD pode tomar como base os cenários estrangeiros para a regulação no Brasil.

2.1. União Europeia

2.1.1. Risco

A GDPR define risco ao titular por meio de conceitos amplos e pela utilização de alguns exemplos no texto legal. O Considerando (75) da lei estabelece que há risco quando as operações de tratamento forem "*suscetíveis de causar danos físicos, materiais ou imateriais*", citando como como exemplos àqueles que puderem ocasionar:

I. Discriminação;

II. Roubo da identidade;

III. Perdas financeiras;

IV. Dano à reputação,

V. Perda de confidencialidade de dados protegidos por sigilo profissional;

VI. Reversão da pseudonimização;

---

perpetrators, as well the much more limited and challenging environment in which individual defenders operate". WOLFF, Josephine. **You'll See This Message When It Is Too Late - The Legal and Economic Aftermath of Cybersecurity Breaches**. 1ª edição (versão Kindle): The MIT Press. 2018. Capítulo 1, Loc 470 de 6938.

VII. Prejuízos econômicos ou sociais; e

VIII. Privação de direitos, liberdades, e do controle sobre os dados.

Também poderá haver risco quando o tratamento envolver dados sensíveis[8]; dados relacionados a aspectos de natureza pessoal (p. ex. desempenho no trabalho, situação econômica, saúde, interesses pessoais, confiabilidade, comportamentos, localização e deslocamentos, a fim de se fazer uso de perfis); dados pessoais de vulneráveis, em particular crianças; e quando houver o tratamento de grande quantidade de dados pessoais que afetem muitos titulares.

Já o Considerando (76) da GDPR esclarece que os riscos aos titulares devem ser avaliados em relação à (**i**) **probabilidade** de ocorrem e (**ii**) **gravidade** do risco gerado; considerando a natureza, escopo, contexto e finalidade da atividade tratamento.[9]

Em 2017 a Working Party 29 (WP29)[10] elaborou um guia geral de orientações sobre notificações de incidentes de segurança da informação.[11] [12] O documento busca orientar de forma mais concreta como deve ser feita a análise de risco para verificar a necessidade de notificação; explicando em mais detalhes certos critérios legais, e utilizando casos exemplificativos. Nesse sentido a WP29 lista os seguintes critérios em adição ao estabelecido na Diretiva 95/46 (substituída pela GDPR):[13]

IX. Tipo de incidente

Este item não é muito desenvolvido no guia, sendo utilizado apenas alguns exemplos com base na tríade de princípios CIA. Assim, uma

[8] Artigo 9º, GDPR: "origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa."

[9] Considerando (76), GDPR: "A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado."

[10] A Working Party 29 era uma entidade pública consultiva da União Europeia, formada por representantes das autoridades de proteção de dados de cada um dos membros da EU. Com a entrada em vigor da GDPR ela foi substituída pela European Data Protection Board (EDPB).

[11] O guia da WP29 sobre notificação de incidentes de segurança da informação foi ratificado pela European Data Protection Board (EDPB). Ver: ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679**. 18/EN - WP250 rev.01. 2018. p.23. Acessado em 17/03/2021. Disponível em: <https://bit.ly/30SnhtO>

[12] Este guia foi posteriormente revalidado pela European Data Protection Board.

[13] *Ibid*. pp 24-26.

violação da confidencialidade de dados de saúde, a princípio, ofereceria maiores riscos em relação a mera perda dos mesmos.

X. Natureza, sensibilidade e volume dos dados

Além de avaliar o tipo de dado (p. ex. dados financeiros, de saúde etc.) o agente deve também considerar como os dados afetados pelo incidente podem ser combinados com outros e o possível dano resultante da combinação. Por fim, a WP29 alerta para o fato de que o fator volume de dados não pode ser analisado isoladamente, pois poucos dados sensíveis podem acarretar um nível alto de dano a titular.

XI. Facilidade de identificação dos titulares

Além de verificar o grau de facilidade de se identificarem os titulares pelos dados afetados, o agente de tratamento também deve considerar como esses dados podem ser combinados com outros (p. ex. dados publicamente disponíveis) para permitir a identificação; e verificar se os dados afetados estavam criptografados de forma adequada.

XII. Gravidade das consequências

Apesar deste critério já estar elencando na GDPR, o Guia da WP29 cita alguns exemplos práticos. Ela esclarece que o agente de tratamento deve considerar se os danos aos titulares podem ter um caráter permanente ou de longo prazo. É importante destacar que a entidade considera que apresentam baixo risco os casos em que os dados são indevidamente compartilhados com fornecedores/parceiros.

XIII. Características dos titulares

O guia apenas destaca que determinados indivíduos possuem características pessoais que podem potencializar os riscos de um incidente, como no caso de crianças.

XIV. Características do controlador

O guia apenas destaca que a depender da natureza das atividades do agente de tratamento pode haver automaticamente um risco maior no incidente, como no caso de instituições de saúde.

XV. Quantidade de indivíduos afetados

A WP 29 apenas alerta para o fato de que, geralmente, quanto maior o número de titulares maior o risco, mas que também poucos ou apenas um indivíduo pode ser afetado de forma grave.

Apesar das orientações elaboradas pela antiga WP29, a European Data Proctection Board (EDPB) considerou que, mesmo sendo ainda válidas, elas seriam insuficientes para orientar os agentes de tratamento de forma mais concreta. Assim, em 2021 foi lançando uma versão prévia para consulta pública de um guia de notificação de incidentes baseado em casos práticos específicos (p. ex. ransomware, exfiltração de dados, roubo de equipamentos, etc).[14] A par disso, pode-se inferir que a EDPB reconhece que a GDPR apenas fornece critérios abstratos para avaliação dos riscos gerados por um incidente, sendo necessário que os reguladores intervenham com orientações de cunho mais prático aos agentes de tratamento.

Adicionalmente, a WP29 esclarece que a definição da análise de risco de um incidente pode ser mais bem compreendida quando comparada a análise de risco feita em um Relatório de Impacto à Proteção de Dados[15] (*Data Protection Impact Assessment* - DPIA). Em relação a diferença entre uma análise de risco de incidente (para notificação) e um DPIA, a WP29 esclarece que a avaliação de um incidente se aplica apenas depois que ele ocorreu, enquanto em um DPIA são analisados cenários hipotéticos sobre os diferentes riscos acarretados pelo tratamento, incluindo, mas não se limitando a incidentes de segurança.

2.1.2. Dano

O texto legal da GDPR não define parâmetros específicos para análise do dano ao titular. Os trechos que tratam de dano, apenas mencionam alguns fatos decorridos de um incidente de segurança que podem gerar dano aos titulares, sejam eles físicos, materiais ou imateriais (p. ex. roubo de identidade, fraude, dano à reputação etc.) - conforme já listados neste documento (ver **item** 2.1.**1**).[16]

A falta de parâmetros específicos na GDPR parece se justificar pelo fato de o conceito de dano já ser tema de outras áreas do direito, principalmente em relação à responsabilidade civil. Este entendimento é reforçado ao se verificar o Considerando 146, o qual estabelece que o conceito de dano deve ser interpretado com base na jurisprudência do Tribunal de Justiça da União Europeia e os objetivos das GDPR, sem prejuízo aos tipos de danos previstos no direito dos países membros da UE.[17]

---

[14] "However, due to its nature and timing, this guideline did not address all practical issues in sufficient detail. Therefore, the need has arisen for a practice-oriented, case-based guidance that utilizes the experiences gained by Supervisory Authorities since the GDPR is applicable". UNIÃO EUROPEIA. Draft: **Guidelines 01/2021 on Examples regarding Data Breach Notification**. Acessado em: 17/03/2021. p. 4. Disponível em: <https://bit.ly/3cIKQun>.

[15] Art.5º, XVII, LGPD.

[16] Considerandos 75, 85, GDPR.

[17] "The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for

Assim, pode se inferir que o conceito de risco se refere aos cenários hipotéticos/possíveis em que um ou mais tipos de danos podem se concretizar em relação às normas de proteção de dados pessoais.

2.2. Estados Unidos – Risco e Dano

2.2.1. Contexto

Na jurisprudência estadunidense os tribunais também têm discutido como definir os conceitos de risco e dano relacionados a incidentes de segurança da informação (data breaches). A definição de dano é importante nos EUA especificamente porque ela é também um dos requisitos processuais para que uma pessoa possa iniciar um processo nas cortes federais (standing18), de acordo com a Constituição19 e a jurisprudência estadunidenses. Ou seja, a conceituação de "dano" no direito dos EUA refere-se tanto ao direito material (qual o dano sofrido pelo titular, e em qual medida) como também ao direito processual (se a pessoa pode ou não iniciar um processo).[20]

2.2.2. Entendimento dos Tribunais

Apesar de não haver um consenso sobre os conceitos, parte dos tribunais federais (*federal courts*) têm diferenciado as noções de riso (*risk*) e dano (*harm*). Por exemplo, no caso *Reilly v. Ceridian Corp*, a empresa Ceridian prestava serviços de pagamento de folha e, em 2009, sofreu um incidente de segurança da informação no qual, potencialmente, houve acesso aos dados pessoais de 27.000 empregados.[21] Não foi possível confirmar tecnicamente se os dados foram acessados ou copiados.[22]

---

damage deriving from the violation of other rules in Union or Member State law.". Considerando 146, GDPR.

[18] 'Legitimidade para propor a ação". CASTRO, Marcílio Moreira de. **Dicionário de Direito, Economia e Contabilidade – Português-Inglês - Inglês Português**. Rio de Janeiro: Editora Forense. 2013. p. 238.

[19] ESTADOS UNIDOS. **Constituição dos Estados Unidos**. Artigo III. Acessado em:18/03/2021. Disponível em: <https://bit.ly/3qXpoH7>.

[20] The "case or controversy" clause of Article III of the Constitution imposes a minimal constitutional standing requirement on all litigants attempting to bring suit in federal court. In order to invoke the court's jurisdiction, the plaintiff must demonstrate, at an "irreducible minimum," that: (1) he/she has suffered a distinct and palpable injury as a result of the putatively illegal conduct of the defendant; (2) the injury is fairly traceable to the challenged conduct; and (3) it is likely to be redressed if the requested relief is granted. The United States Department of Justice. Civil Resource Manual. Acesso em:12/03/2021. Disponível em: <https://bit.ly/3rCQ4hz>

[21] ESTADOS UNIDOS. United States Court of Appeals for the Third Circuit. Reilly v. Ceridian Corp – No. 11-1738. 27/10/2011. p.3. Acessado em: 12/03/2021. Disponível em: <https://bit.ly/2PXzCKW>.

[22] *Ibid.*

Os titulares possivelmente afetados foram notificados pela Ceridian sobre o possível tratamento indevido e, em 2010, parte do atingidos iniciaram uma ação coletiva contra a empresa alegando: (**a**) risco maior de sofrerem roubo de identidade; (**b**) prejuízo financeiro pela necessidade de contratarem serviços de monitoramento de crédito; e (**c**) estresse emocional com a situação.[23]

Na segunda instância a Corte Recursal do 3º Circuito[24] confirmou o entendimento de que o caso configurava apenas uma alegação hipotética de dano futuro, por se basear numa mera especulação de que o hacker teve acesso e copiou as informações.[25] **Até que se comprovasse que os dados foram usados de forma ilícita não seria possível afirmar que houve dano**.[26] Desse modo, a corte entendeu que os apelantes não tinham legitimidade por falta de comprovação de dano.

Conforme observa Solove e Citron, a maioria das cortes federais dos EUA tem se posicionado de forma semelhante ao caso *Reilly v. Ceridian Corp*, no qual a alegação de um possível dano futuro (p. ex. maiores chances de fraude ou roubo de identidade) ocasionado por incidente de segurança da informação é considerada demasiadamente especulativa.[27]

Desse modo, percebe-se que a jurisprudência majoritária dos EUA diferencia as noções de risco e dano, considerando o primeiro como uma possiblidade de ocorrência de um dano. Assim, por exemplo, no caso de um acesso indevido a dados pessoais, a configuração de dano dependeria da comprovação de que aqueles dados foram utilizados de forma ilícita em um caso concreto (p. ex. fraude econômica). Noutro sentido, algumas cortes federais têm entendido que o risco gerado por um incidente de segurança seria "substancial" o suficiente para configurar o requisito de dano (*harm*) para que um autor tenha legitimidade processual (*standing*) em uma corte federal.[28] Nessa linha de raciocínio, contudo, os conceitos de risco e dano

---

[23] *Ibid*. p.4.

[24] United States Court of Appeals for the Third Circuit.

[25] *Ibid*. p.7.

[26] "Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.". *Ibid*. p.7.

[27] "Much like Reilly, the majority of courts have ruled that injuries from data breaches are too speculative and hypothetical, too reliant on subjective fears and anxieties, and not concrete or significant enough to warrant recognition". SOLOVE, Daniel J.; e CITRON, Danielle Keats. **Risk and Anxiety: A Theory of Data Breach Harms**). GWU Legal Studies Research Paper No. 2017-2. 2017. p. 741. Acessado em:11/03/2021. Disponível em: <https://bit.ly/2ONEzFs>.

[28] "In those cases, plaintiffs were found to have suffered actual, not hypothetical, injuries where hackers stole personal data from inadequately secured systems [...]". *Ibid*, p. 742.

tendem a se confundir pois um "risco substancial" seria considerado um tipo de dano.

Por fim, importante notar que esse caso exemplifica que nem sempre é possível averiguar detalhadamente as consequências de um incidente de segurança da informação, o que demonstra que a complexidade técnica do tema precisa ser levada em consideração - conforme já mencionado no **item 1.2** deste documento - a fim de se evitar reducionismos que são comuns, principalmente quando a mídia reporta sobre incidentes de segurança.

/ Recomendação

Risco

Conclui-se, portanto, que a análise de risco de um incidente na União Europeia é determinada pelos critérios abstratos de (**i**) probabilidade e (**ii**) gravidade do risco(s) originado pelo incidente. Apesar de tanto a redação da GDPR como as orientações institucionais da WP29/EDPB buscarem dar maior concretude a como esses critérios devem ser utilizados, ainda faltam orientações mais claras sobre o tema.

Após realizarmos um paralelo com a definição de risco na União Europeia e com os EUA, é importante que ANDP estabeleça critérios de avaliação mais concretos para que os agentes possam determinar quais são as situações que exigem notificação; ainda mais ao se considerar que o disposto na LGPD sobre risco ("*risco ou dano relevante aos titulares*"[29]) é mais genérico que o estabelecido na GDPR. Ademais, recomenda-se que também sejam elaboradas orientações mais práticas, sendo uma solução possível a elaboração de análise de casos específicos de incidentes de segurança, em modelo semelhante ao que vem sendo elaborado pela EDPB.

Desse modo, recomenda-se que a ANPD considere a proporcionalidade entre os riscos do incidente e as medidas técnicas e administrativas previamente adotadas pelos agentes de tratamento, para evitá-los e/ou mitigá-los. Assim, a análise deve partir de um **enfoque contextual** e não de uma simples constatação sobre a ocorrência ou não de um incidente.

Dano

[29] Art. 48, LGPD.

Em relação ao dano**,** verificou-se que os seus parâmetros de avaliação não são especificados na GDPR, sendo o termo utilizado para definir o conceito de risco. Raciocínio semelhante é encontrado na jurisprudência dos EUA que diferencia o risco do dano pela comprovação de que este último ocorreu, sendo o risco um mero cenário possível/hipotético de dano acarretado por um incidente. Considera-se tal diferenciação adequada e elevado parâmetro a ser seguido pela ANPD.

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?

3. Categorias de Dano e Risco

3.1. Risco

A LGPD é uma norma baseada na noção de risco (risk-based approach), a qual impõe aos agentes de tratamento o dever de avaliar os riscos relacionados ao uso de dados pessoais, a fim de que possam evitá-los e ou mitigá-los de forma proporcional. Desse modo, é intrínseco a ideia de análise de risco a necessidade de subdividi-lo em categorias/graus distintos.

Por exemplo, a Agência Espanhola de Proteção de Dados Pessoais defende que o risco pode ser classificado e definido como baixo, médio, alto e super alto, considerando os seguintes parâmetros: volume de dados pessoais, tipo de dados pessoais, impacto ou exposição dos dados pessoais[30]

3.2. Dano

O conceito de dano comporta raciocínio semelhante pois, seria violar a própria LGPD considerar, por exemplo, que o dano acarretado por um incidente de violação de confidencialidade com dados sensíveis afete da mesma forma um titular que teve um comprovante de escolaridade da sua pré-escola exposto.

[30] Guia para la gestión y notificación de brechas de seguridad. Agencia Española de Protección de Datos. pp. 53. Disponível em: < https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf> Acesso em 12/03/2021.

Ainda, quando se considera que ANPD tem a competência de aplicar sanções administrativas, a mesmas deverão ser aplicadas se utilizando o critério da proporcionalidade/razoabilidade, o qual é pacificamente reconhecido pela doutrina e jurisprudência do direito administrativo.[31] Assim, a não avaliação do risco e do dano por meio de graus/categorias distintas impede inclusive a adequa aplicação dos poderes sancionatórios da ANPD.

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

4. Distinção entre Risco e Dano

De forma simples, considerando interpretações internacionais sobre o tema (ver **item 2**), o risco se refere à possibilidade de um dano ocorrer. Já o dano é a materialização de tal risco, ou seja, no caso em questão, é o efetivo prejuízo para o titular decorrente do incidente, como, por exemplo: fraude, clonagem do cartão de crédito, danos reputacionais, dentre outros.

Esses conceitos se relacionam à medida que o risco é abstrato e o é dano concreto. O risco é anterior ao dano. Existir um risco não significa que o dano vai ocorrer, porém, quanto mais alto o risco, maior é a chance da ocorrência do dano e vice-versa.

Ainda, o risco também está atrelado ao tipo de dano, de modo que o risco pode ser mais alto se os possíveis danos têm prejuízos maiores aos titulares dos dados pessoais afetados; ao passo que o risco pode ser baixo se o possível dano significa grande prejuízo ao titular.

Ver **item 5.**

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

5. Critérios de Risco

[31] Ver art. 2º, Parágrafo Único, VI, da Lei nº 9.784.

5.1. União Europeia

Conforme já apontado no item 2 deste documento, baseado na regulação europeia, para a devida avaliação dos riscos do incidente pode-se considerar como critérios:

- **XVI.** Probabilidade de o dano(s) ocorrer;
- **XVII.** Gravidade do possível dano;
- **XVIII.** Tipo de incidente;
- **XIX.** Natureza, sensibilidade e volume dos dados;
- **XX.** Facilidade de identificação dos titulares;
- **XXI.** Características dos titulares;
- **XXII.** Características do agente de tratamento; e
- **XXIII.** Quantidade de indivíduos afetados.

Ver itens 1 e 2.

5.2. Espanha

O guia de gestão e notificação de incidentes da Agência Espanhola de Proteção de Dados Pessoais, propõe, em seu Anexo III[32], a utilização de fórmula matemática para o cálculo do risco e da necessidade de informar a autoridade e titulares. A fórmula atribui um peso para os fatores para (**i**) a quantidade de dados afetados (p. ex. menos de 100; entre 1k e 100k); (**ii**) categoria dos dados (sensíveis ou não); e (**iii**) nível de exposição dos dados acarretado pelo incidente (p. ex. dados foram tornados públicos):

"Riesgo = P (Volumen) x Impacto (Tipología x Impacto)"

Entendemos que esta fórmula poderá ser utilizada como referência pela ANPD na elaboração de seus critérios de avaliação de risco.

5.3. Medidas de Segurança da Informação

[32] ESPANHA. Agencia Española de Protección de Datos (AEPD). Guia para la gestión y notificación de brechas de seguridad. Anexo III. Acesso em 12/03/2021. Disponível em: <https://bit.ly/3lxveOA>

Uma vez que a resposta de um incidente de segurança envolve conjuntamente ações de investigação, contenção e mitigação desde a detecção, a autoridade deve considerar os esforços empreendidos pelo agente para evitar e/ou reduzir a extensão e os efeitos do incidente – e não apenas a capacidade de evitar a vulnerabilidade. Em outras palavras, o agente que reage proativamente e em tempo hábil a um incidente reforça sua presunção de boa-fé e deve ser recompensado por isso; ao passo que situações opostas (e.g. negligência, conduta omissiva) também devem ser tratadas como tais. A ocorrência de um incidente não se traduz automaticamente no entendimento de que não foram adotadas medidas de segurança adequadas pelo agente de tratamento.

Dois outros pontos de destaque referem-se ao fato de ser (**i**) comum em muitos incidentes haver mais de um agente de tratamento envolvido, devido à complexidade das cadeias de tratamento de dados, principalmente quando da utilização de sistemas de informação de terceiros (p. ex. serviços de cloud; licenciamento de software etc.); e (**ii**) a realidade técnica de que incidentes de segurança são complexos e multicausais.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?

6. Espanha

A Agência Espanhola de Proteção de Dados Pessoais disponibiliza, ao final de seu guia sobre incidentes de segurança, um modelo de formulário com as informações que devem constar em uma notificação de incidente à autoridade[33].

Tal formulário é bastante completo e pode ser utilizado como modelo por outras jurisdições. Se compararmos às informações exigidas pela lei brasileira, verifica-se que as informações constantes do modelo espanhol de notificação à autoridade são mais detalhadas e permitem uma avaliação melhor do incidente ocorrido, tendo em vista, por exemplo, que detalha não só os riscos, mas também as possíveis consequências

[33] AEPD. **Guia para la gestión y notificación de brechas de seguridad**. pp. 48-52.

concretas daquele incidente (como danos à reputação do titular dos dados).

O modelo espanhol abarca todas as informações exigidas pela lei brasileira (descrição da natureza dos dados pessoais afetados, informações sobre os titulares envolvidas etc.), porém exige maiores detalhamentos para uma melhor avaliação da autoridade.

Seguem abaixo as informações que, para a autoridade espanhola, devem constar em uma notificação de incidente à autoridade:[34]

XXIV. Dados do encarregado de proteção de dados pessoais

XXV. Identificação do responsável pelo tratamento – controlador

XXVI. Identificação do operador dos dados pessoais

XXVII. Informações temporais do incidente (data de notificação, meios de detecção, eventual justificação de notificação tardia etc.)

XXVIII. Sobre o incidente:

a. Resumo do incidente;

b. Tipo do incidente: de confidencialidade (acesso não autorizado), de integridade (alteração não autorizada), de disponibilidade (perda dos dados pessoais);

c. Por qual meio se materializou o incidente (exemplos: malware; dispositivo perdido ou furtado/roubado; dados pessoais enviados a alguém equivocadamente; phishing; hacking etc.);

d. Contexto da ocorrência do incidente (interno por ação intencional; interno por ação não intencional; externo por ação intencional; externo por ação não intencional; outros); e

e. Medidas tomadas antes do incidente para a proteção dos dados pessoais.

XXIX. Sobre os dados pessoais afetados

a. Categorias de dados pessoais (dados básicos; dados sobre infrações ou condenações penais; credenciais de acesso ou identificação; dados bancários; dados de contato; dados de localização; outros);

b. Categorias especiais de dados (religião, saúde; origem racial; afiliação sindical; dados genéticos; dados biométricos; opinião política; vida sexual; outros); e

[34] *Ibid*. pp. 22 e 23.

c. Número aproximado de dados pessoais afetados.

XXX. Sobre os titulares afetados

a. Perfil dos titulares afetados (clientes, estudantes, usuários, pacientes, empregados, outros);

b. Número aproximado de titulares afetados.

XXXI. Possíveis consequências

a. Nos casos de incidente de confidencialidade: divulgação a terceiros/divulgação na internet; enriquecimento de outras bases de dados; dados podem ser tratados para outro fim; outras;

b. Nos casos de incidentes de integridade: dados foram modificados de modo que não podem ser recuperados; dados foram modificados e usados para outro fim; outras;

c. Nos casos de incidentes de disponibilidade (impossibilidade de prestação de um serviço aos interessados; deterioração das condições de prestação de um serviço aos interessados; outras);

d. Natureza do impacto potencial aos titulares (perda do controle sobre seus dados pessoais; falsificação de identidade; danos à reputação; limitação dos direitos; fraude; discriminação; danos materiais; perda da confidencialidade de dados protegidos por segredo de negócio; outros);

e. Severidade das consequências aos titulares (baixa, média, alta, muito alta); e

f. Medidas tomadas para solucionar os incidentes e minimizar o impacto aos titulares dos dados pessoais.

XXXII. Comunicação aos titulares

a. Os titulares foram comunicados a respeito do incidente?

b. Se sim: em que data, quantos titulares foram informados; meios ou ferramentas de comunicação.

c. Se ainda não: data em que serão informados. Se a comunicação não será feita: justificativa para não os informar.

d. Se titulares foram informados, anexar documento que comprove.

XXXIII. Implicações internacionais

a. Existem sujeitos de outros países afetados pelo incidente? Se sim, quais países?

XXXIV. Documentos anexos

7. França

A autoridade francesa de proteção de dados pessoais, a *Commission Nationale de L'informatique et des Libertés* (CNIL), destaca que lhe devem ser notificadas as seguintes informações[35]:

- a natureza da violação;
- as categorias e o número aproximado de pessoas envolvidas;
- as categorias e o número aproximado de arquivos afetados;
- as prováveis consequências da violação;
- as medidas tomadas para mitigar e/ou limitar as consequências negativas do incidente;
- se aplicável, a justificativa de ausência de notificação à autoridade e/ou aos titulares dos dados pessoais envolvidos; e
- os motivos de atraso na notificação à autoridade, quando aplicável.

Ao compararmos os elementos exigidos na notificação da CNIL, verificamos que há uma certa convergência com a notificação espanhola. O que pode indicar que a par de um núcleo específico de determinadas perguntas, eventuais requisições das autoridades irão variar em relação a documentos técnicos ou de risk assessment dos agentes de tratamento relacionados ao incidente.

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

8. Critérios para o Prazo

8.1. Contagem

A contagem do prazo deve se iniciar com a confirmação do incidente pela empresa. Ou seja, a suspeita de que houve um incidente necessita de uma verificação adequada antes de que seja necessário notificação à ANDP. Posicionamento semelhante

[35] CNIL. **Les violations de données personnelles**. Disponível em <https://bit.ly/3lsgrEu>. Acesso em 18/03/2021.

foi adotado pela WP29 ao esclarecer em suas *guidelines* que um incidente deve ser informado apenas após haver um grau razoável de certeza de que ele ocorreu.[36] Este critério também evita com que a ANPD seja notificada de forma excessiva pelos agentes de tratamento.

onforme a Agência Espanhola de Proteção de Dados, o prazo de 72 horas estabelecido pela GDPR refere-se à primeira notificação à autoridade após a ciência do incidente. Ainda, se, no momento da notificação, não for possível fornecer todas as informações necessárias, exigidas pela lei, isso poderá ser feito posteriormente, de forma gradual e em diferentes fases. Quando a comunicação não for possível no prazo estabelecido em lei, ela deverá ser feita da mesma forma, mas justificando o motivo da demora[37].

8.2. Prazo de Notificação

Entendemos que uma notificação pode ser dividida entre parcial e complementar. Assim, após a confirmação da ocorrência do incidente, o agente de tratamento pode realizar uma notificação parcial à ANPD, enquanto realiza as medidas adequadas de investigação e mitigação. Considerando a natureza complexa dos incidentes de segurança da informação (ver **item** 1.2), pode ser inviável tecnicamente exigir em todos os casos uma avaliação completa do incidente na primeira notificação – em alguns casos não é possível nem mesmo compreender totalmente um incidente – por isso a importância de notificações parciais.

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?

[36] "WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679.** pp 10-11.

[37] Guia para la gestión y notificación de brechas de seguridad. Agencia Española de Protección de Datos. p. 53. Disponível em: < https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf> Acesso em 12/03/2021.

9. Espanha

De acordo com o guia de incidentes de segurança da Agência Espanhola de Proteção de Dados Pessoais, a comunicação aos titulares dos dados pessoais deve ser feita em linguagem clara e simples, e deve conter, no mínimo, os seguintes elementos[38]:

- Dados de contato do encarregado de proteção de dados pessoais ou um canal de contato onde o titular possa obter mais informações;
- Descrição geral do incidente e do momento em que ocorreu;
- Resumo das medidas adotadas desde o momento do incidente para controlar possíveis danos; e
- Outras informações úteis aos titulares para proteger os seus dados pessoais ou prevenir possíveis danos.

Ainda, de acordo com o referido guia, para verificar a necessidade de comunicação dos titulares dos dados pessoais, diversos fatores devem ser levados em consideração, como os seguintes[39]:

- Quais são as obrigações legais e contratuais;
- Quais são os riscos decorrentes da perda dos dados pessoais: p. ex. danos materiais, danos reputacionais etc.;
- Se existe risco razoável de falsificação de identidade ou fraude (em razão do tipo de informação afetada e levando em consideração se a informação foi pseudonimizada ou criptografada); e
- Até que ponto a pessoa afetada pode evitar ou mitigar possíveis danos posteriores.

As sugestões acima podem ser utilizadas como parâmetros pela ANPD na análise de um documento de comunicação aos titulares feito por uma empresa. Sobre o prazo para a referida comunicação, diferente do indicado no **item 8** acima, importante que os titulares sejam notificados após a confirmação da ocorrência, e não também para os casos de mera suspeita, e apenas nos casos em que tal comunicação se faz necessária (ver **item 12**).

AEPD. **Guia para la gestión y notificación de brechas de seguridad**. p. 43.

[39] *Ibid.*

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.)?

10. Forma da Comunicação

A comunicação deve, preferencialmente, ocorrer de forma direta, seja por telefone, e-mail, SMS, correio etc., prevalecendo meio de comunicação usualmente praticado pela empresa com o titular. A notificação indireta (p. ex. por meio de avisos públicos em sites, blogs corporativos ou comunicados na imprensa) deve ser utilizada quando (**i**) os custos de uma notificação direta forem excessivos para a empresa em questão ou (**ii**) quando não seja possível entrar em contato com os titulares afetados (por exemplo, porque são desconhecidos ou os dados de contato estão desatualizados).

Caso não se verifique nenhuma dessas situações, deve-se privilegiar a comunicação direta. Nesse mesmo sentido é o guia de incidentes de segurança da Agência Espanhola de Proteção de Dados Pessoais[40].

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

11. União Europeia

A legislação europeia determina que não será necessária comunicação à autoridade quando o controlador puder demonstrar que o incidente de proteção de dados pessoais não trará risco aos direitos e às liberdades fundamentais dos titulares (e.g. os dados pessoais já se encontravam

[40] Idem.

publicamente disponíveis e sua divulgação não representou nenhum risco adicional ao titular dos dados).

/ Recomendações

A ANPD pode seguir no mesmo sentido elencado acima, uma vez que há situações claras de incidentes que não acarretam risco ou dano relevante aos titulares (p. ex. dados criptografados que tornem os dados afetados pelo incidente ininteligíveis).

A notificação excessiva é uma questão com a qual a ANPD deve estar atenta no processo de elaboração das normas sobre o tema. As autoridades de proteção de dados pessoais da União Europeia têm enfrentado essa questão, conforme mostram os dados da pesquisa quantitativa abaixo:

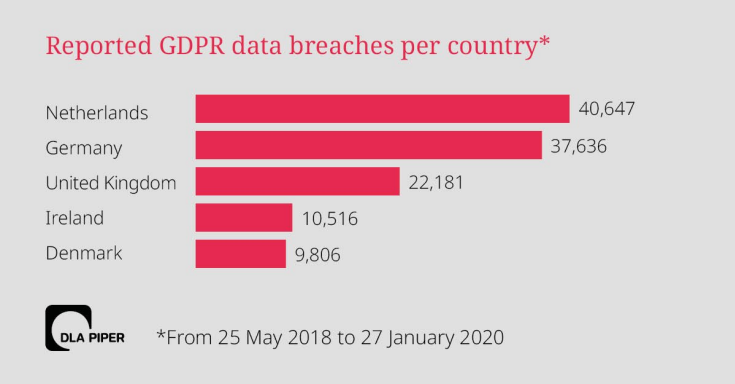

***Fig. 2** – As 5 autoridades de proteção de dados da EU que mais receberam notificações de incidentes.*[41]

Assim, os critérios de notificação devem buscar filtrar os casos realmente necessários de serem notificados a fim de proteger os direitos dos titulares.

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

12. União Europeia

No direito europeu, somente há necessidade de informar os titulares dos dados afetados pelo incidente em situação de alto risco às pessoas afetadas. Quando a comunicação aos titulares puder comprometer o

[41]DLA PIPER. **DLA Piper GDPR data breach survey: January 2020**. p. 6. Acessado em:18/03/2021. Disponível em: <https://bit.ly/3tr8OkG>.

resultado de uma investigação em curso, a comunicação poderá ser adiada, mas com a supervisão da autoridade. Além disso, mesmo nas hipóteses de alto risco ao titular dos dados, as autoridades de proteção de dados destacam algumas situações excepcionais em que pode ser dispensada a comunicação, quais sejam:

Os dados pessoais afetados pelo incidente foram submetidos a medidas de segurança técnica e administrativa adequadas para garantir que os dados pessoais não sejam compreensíveis por pessoas ou sistemas não autorizados, seja, por exemplo, por meio do uso criptografia prévia, minimização no uso dos dados, acesso a ambientes de teste sem dados reais etc.;

Detectado o incidente, o agente de tratamento tomou as medidas necessárias para garantir que o risco alto aos direitos e às liberdades dos titulares dos dados não deva mais se concretizar;

A comunicação aos titulares dos dados exigiria um esforço desproporcional do agente de tratamento, a nível técnico e administrativo, por exemplo, quando os dados de contato foram perdidos em razão do incidente; quando um novo processo deva ser desenvolvido para realizar a comunicação; ou se requer dedicação excessiva de recursos internos para a identificação dos titulares afetados

/ Recomendações

LGPD somente dispõe como exceção à obrigatoriedade de notificação aos titulares os casos que não acarretam risco ou dano relevante aos titulares.[42] A ANPD, contudo, deverá regulamentar tal norma, trazendo critérios e casos específicos de dispensa de comunicação, as quais podem se basear no diploma europeu, conforme narrado acima.

Outro critério interessante de ser considerado é que os titulares sejam notificados após a confirmação da ocorrência, e não também para os casos de mera suspeita. Precauções nesse sentido evitam com que o titular possa ser excessivamente notificando, e que desse modo, não consiga discernir as situações mais críticas que possam exigir a tomada de precauções de sua parte (p. ex. troca de senha, realização de back-ups, etc).

[42] Art. 48, LGPD.

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

13. Espanha

A Agência Espanhola de Proteção de Dados (AEPD) estabelece critérios detalhados para se determinar o risco de um incidente e as tomadas de decisões subsequentes. Conforme guia publicado AEPD, para a gestão de um incidente de segurança, deve-se determinar o perigo potencial do incidente e estimar a magnitude do impacto potencial sobre os indivíduos, o que simplesmente reflete os comandos da GDPR[43]. Para esta avaliação, também deve se recorrer à análise de risco/avaliação de impacto realizada antes do início das atividades de tratamento.

A periculosidade/gravidade do incidente, conforme a Agência Espanhola, dependerá dos seguintes fatores[44]:

XXXV. Categoria ou o nível de criticidade da segurança dos sistemas afetados:

a. Crítico (afeta dados valiosos, grande volume e em pouco tempo).

b. Muito alto (capacidade de afetar dados valiosos, em quantidade considerável).

c. Alto (capacidade de afetar dados valiosos).

d. Médio (capacidade de afetar um volume considerável de dados).

e. Baixo (pouca ou nenhuma capacidade de afetar um volume considerável de dados).

XXXVI. Natureza, sensibilidade e categoria dos dados pessoais afetados:

a. Dados de baixo risco: dados de contato, de educação, familiares, profissionais, dados biográficos.

b. Dados de comportamento: localização, trânsito, hábitos e preferências.

c. Dados financeiros: transações, posições, receitas, contas, faturas.

d. Dados sensíveis: dados de saúde, dados biométricos, dados relacionados à vida sexual etc.

---

[43] Considerando 76, GDPR.

[44] AEPD. **Guia para la gestión y notificación de brechas de seguridad**. p. 22.

XXXVII. Dados legíveis/ilegíveis:

a. Dados protegidos por meio de algum sistema de pseudonimização, por exemplo, criptografia ou hash.

XXXVIII. Volume de dados pessoais:

a. Expresso em quantidade (registros, arquivos, documentos) e/ou em períodos de tempo (uma semana, um ano etc.).

XXXIX. Facilidade de identificação dos indivíduos:

a. Facilidade com que se pode deduzir a identidade de indivíduos envolvidos na violação

XL. Severidade das consequências aos indivíduos:

a. Baixa: as pessoas não serão afetadas ou poderão encontrar alguns inconvenientes que poderão superar sem problemas (irritações, aborrecimentos etc.).

b. Médio: as pessoas podem encontrar inconvenientes significativos, que serão capazes de superar, apesar de algumas dificuldades (custos adicionais, negação de acesso a serviços comerciais, medo, falta de compreensão, estresse, pequenos males físicos etc.).

c. Alto: as pessoas podem enfrentar consequências importantes, que podem ser capazes de superar, porém com sérias dificuldades (danos materiais, perda de emprego, intimações judiciais, deterioração da saúde etc.).

d. Muito alto: as pessoas podem enfrentar consequências graves e até irreversíveis, que não poderão superar (exclusão ou marginalização social, dificuldades financeiras como dúvidas consideráveis ou incapacidade de trabalhar; doenças psicológicas ou físicas a longo prazo, morte etc.).

XLI. Características especiais dos indivíduos:

a. Se afetam indivíduos com características ou necessidades especiais.

XLII. Número de indivíduos afetados:

a. Dentro de uma escala determinada, por exemplo, mais de 100 indivíduos.

XLIII. Características especiais do controlador dos dados pessoais:

a. Com base na atividade exercida pela empresa.

XLIV. Perfil dos indivíduos afetados:

a. Sua posição na estrutura administrativa da empresa e, em consequência, seus privilégios de acesso a informações sensíveis ou confidenciais.

XLV. O número ou o tipo dos sistemas afetados

XLVI. O impacto que o incidente pode ter para a organização

Do ponto de vista da proteção da informação, da prestação dos serviços, do cumprimento legal e/ou da imagem pública (reputacional). Ele estará relacionado à categoria ou criticidade dos serviços afetados e das pessoas afetadas. Nesse sentido, diferencia-se os seguintes impactos:

a. Baixo: prejuízo limitado

b. Médio: prejuízo grave

c. Alto: prejuízo muito grave

XLVII. Os requerimentos legais e regulatórios:

a. Notificação do incidente à autoridade de controle e qualquer outra obrigação de notificação.

Conforme elencando acima verifica-se que a AEPD utilizou como base o Guia sobre Incidentes da WP29 (ver **item 2.1**) a partir do qual foram incluídos novos elementos de análise e maiores detalhes. Desse modo, a ANPD pode utilizar como base a metodologia estabelecida pela AEPD para análise da gravidade do incidente.

14. Canadá

De acordo com a autoridade canadense de proteção de dados pessoais, as perguntas que devem ser feitas para se analisar um incidente são[45]:

/ O que aconteceu e qual a probabilidade de alguém ser prejudicado pelo incidente?

[45] DLA PIPER. **DLA Piper GDPR data breach survey: January 2020**. p. 6. Acessado em: 12/03/2021. Disponível em: <https://bit.ly/3tr8OkG>.

- Quem realmente acessou ou pode ter acessado os dados pessoais?
- Há quanto tempo os dados pessoais foram expostos?
- Existe evidência de intenção maliciosa (por exemplo, roubo, invasão de hacker)?
- Dados pessoais foram violados, aumentando, portanto, o risco de uso indevido?
- Os dados pessoais violados foram expostos a indivíduos ou empresas/entidades que representam risco a reputação do titular (por exemplo, ex-cônjuge ou chefe)?
- Os dados pessoais foram expostos a empresas/entidades conhecidas que se comprometeram a destruir e não divulgar os dados pessoais?
- Os dados pessoais foram expostos a indivíduos, empresas ou entidades com baixa probabilidade de compartilhá-los de uma forma que causaria danos (por exemplo, no caso de uma divulgação acidental para destinatários)?
- Os dados pessoais foram expostos a indivíduos, empresas ou entidades que são desconhecidos, ou a um grande número de indivíduos, onde certos indivíduos podem usar ou compartilhar as informações de uma forma que causaria danos?
- Os dados pessoais foram expostos a indivíduos, empresas ou entidades que provavelmente tentarão causar danos a partir de tais informações (por exemplo, ladrões de informações)?
- O dano se materializou (demonstração de uso indevido)?
- Os dados pessoais foram perdidos, acessada indevidamente ou furtada/roubada?
- Os dados pessoais foram recuperados?
- Os dados pessoais estão adequadamente criptografados, anônimos ou não são facilmente acessíveis.

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

15. ENISA

Nas recomendações para uma metodologia de avaliação de gravidade de incidente de segurança da informação (*data breach*),[46] a ENISA define a gravidade de um incidente como a "*estimativa da magnitude de um impacto potencial em indivíduos derivado de um incidente*". Resumidamente, a metodologia é baseada em três variáveis:

- o contexto do tratamento dos dados (DPC);
- a facilidade da identificação dos indivíduos envolvidos (EI); e
- as circunstâncias específicas do incidente (CB).

A gravidade do incidente é classificada entre baixa, média, alta e muito alta e calculada pelo produto entre o contexto do tratamento dos dados e a facilidade de identificação dos indivíduos somado com as circunstâncias específicas do incidente ($SE = DPC \times EI + CB$.). Os critérios para o cálculo da pontuação de cada variável e a determinação da gravidade do incidente podem ser encontrados em mais detalhes no relatório.

16. Breach Level Index (BLI)

O *Breach Level Index* (BLI) é a metodologia desenvolvida pela IT-Harvest que se propõe a criar um índice para mensurar a gravidade de um incidente de segurança.[47] Segundo a proposta, deve ser atribuído um índice aos incidentes de segurança da mesma forma que são atribuídos índices a fenômenos naturais como ventos, erupções vulcânicas e terremotos. O índice baseia-se em uma operação logarítmica – Log10(NxTxSxA) – exposta a quatro variáveis, cada qual com um valor próprio: número de incidentes registrados (N), origem do vazamento (S), tipos de dados afetados (T) e danos causados com os dados (A) – p. ex.: roubo de identidade, solicitações de empréstimos, transferências bancárias.

---

[46] ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches**. Disponível em <https://bit.ly/3r7JoHn>. Acesso em 18/03/2021.

[47] STIENNON, Richard. **Categorizing Data Breach Severity with a Breach Level Index**. Disponível em: <https://bit.ly/3bZESpT>. Acesso em 18/03/2021.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?

17. Compartilhamento de Informações sobre Incidentes

Quando se considera a complexidade e a constante evolução das práticas de violação da segurança da informação, verifica-se que incentivos meramente negativos/punitivos são insuficientes para atingir um dos principais objetivos da LGPD: a garantia da confidencialidade, integridade e disponibilidade dos dados pessoais.[48] Assim, a ANPD deve considerar incentivos positivos para fomentar um ambiente de cooperação entre agentes de tratamento e reguladores, a fim de se desenvolver um ecossistema de segurança da informação mais robusto no Brasil.

A preocupação com o desenvolvimento de ambientes de cooperação quanto à segurança da informação também tem ocorrido em outros países, principalmente devido à constatação de que a complexidade do tema impede que apenas uma das partes envolvidas seja capaz de, isoladamente, garantir o melhor nível de segurança possível. Com o objetivo de garantir um ecossistema mais integrado e colaborativo tem sido elemento chave à implementação de políticas de fomento ao compartilhamento de informações sobre segurança da informação.

Esse tema já tem sido debatido a certo tempo nos Estados Unidos. O fomento ao compartilhamento de informações nos EUA tem sido feito tanto do viés legislativo e regulatório, como na elaboração de guias de boas práticas.

A lei federal *Cybersecurity Information Sharing Act* (CISA)[49] estabelece mecanismos voluntários de troca de informações sobre incidentes e ameaças de segurança da informação entre o setor público e privado. Como uma das principais dificuldades de se fomentar o compartilhamento está na criação de um ambiente de confiança institucional e de segurança jurídica, a CISA buscou endereçar este ponto por meio de determinadas

[48] Art. 46, LGPD.

[49] ESTADOS UNIDOS. **S.2588 - Cybersecurity Information Sharing Act of 2014**. 113th Congress (2013-2014). Acessado em: 11/03/2021. Disponível em: <>

proteções contra processos judiciais para agentes que compartilham determinadas informações.[50] A qual pode ser complementada por meio de acordos de confidencialidade.

No mesmo sentido a Presidência dos EUA elaborou a "*Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing*"[51] que estabelece procedimentos para a criação de organizações de troca voluntária de informações sobre segurança da informação entre governo e setor privado, os *Information Sharing Analysis Organizations* (ISAOs).[52] A criação de ISAOs é flexível, podendo ser formadas a partir de diversos critérios, como, por exemplo, por área de atuação no mercado, por região ou para incidentes específicos.

Já o *National Institute of Standards and Technology* (NIST) dos EUA elaborou um guia para compartilhamento de informações sobre ameaças de cyber segurança.[53] O guia foi elaborado com base na premissa de que o compartilhamento de informações sobre incidentes contribui para um maior nivelamento no acesso à informação; maior capacidade de prevenção e resposta à incidentes; maior maturação do tema pelo incentivo ao cruzamento de informações; e mais agilidade nas respostas defensivas dos agentes.[54] De forma resumida, o incidente sofrido/detectado por uma organização transforma-se em prevenção para as demais.[55]

---

[50] "*Protection from liability. (b) Sharing or receipt of cyber threat indicators. — No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or countermeasures under subsection (c) of section 4 if:*

(1) such sharing or receipt is conducted in accordance with this Act; and (2) in a case in which a cyber threat indicator or countermeasure is shared with the Federal Government in an electronic format, the cyber threat indicator or countermeasure is shared in a manner that is consistent with section 5(c).". Ibid. Sec. 6.

[51] ESTADOS UNIDOS. Executive Order 13691. 12/02/2015

[52] Para uma avaliação governamental dos impactos na privacidade e na proteção das liberdades civis da Executive Order nº 13691 ver: DEPARTMENT OF HOMELAND SEDCURITY. Executive Order 13636 Privacy and Civil Liberties Assessment Report. Novembro de 2018. Acessado em: 11/03/2021. Disponível em: <https://bit.ly/3clda5S>

[53] ESTADOS UNIDOS. The National Institute of Standards and Technology (NIST). NIST Special Publication 800-150 - Guide to Cyber Threat Information Sharing. 2016. Acessado em: 11/03/2021. Disponível em:<https://bit.ly/2PONOpj>

[54] *Ibid*. pp 3-4.

[55] *Ibid*. p 3.

Este caminho regulatório também pode ser complementado pela suspensão da aplicação de determinados regulamentos, sendo que esta prática já vem sendo adotada nos EUA. Por exemplo, a agência regulatória estadunidense *Food and Drug Administration* (FDA) elaborou guia em 2016 orientando que não iria aplicar determinadas exigências de notificação de vulnerabilidades de segurança da informação em equipamentos médicos se o fabricante fosse membro de uma ISAO e compartilhasse a informação com a organização.[56]

[56] "If the manufacturer actively participates as amember of an ISAO and shares information about the vulnerability within the ISAO, FDA does not intend to enforce compliance with the reporting requirements in21 CFR part806.For class III devices, the manufacturer does submit a summary of theremediation as part of itsperiodic (annual) report to FDA."ESTADOS UNIDOS. Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. 28/12/2016. p.23. Acessado em 11/03/2021. Disponível em: <https://bit.ly/3tdA2eC>

/ SÃO PAULO
Rua Ramos Batista, 444 / 2° Andar
Vila Olímpia / São Paulo / SP
Tel +55 11 3040 7050

/ PORTO ALEGRE
R. Carlos Trein Filho, 599 / 11° andar
Auxiliadora / Porto Alegre / RS
Tel +55 51 3207 9057

/ FLORIANÓPOLIS
Rua Bento Gonçalves, 183 / Sala 1001,
Centro / Florianópolis / SC
Tel +55 48 3225-6468

/ LONDRINA
Rua Ayrton Senna da Silva, 300 / Sala n° 1801
Gleba Palhano / Londrina / PR
Tel +55 43 3367 7050

/ MIAMI
78 SW 7th Street / Suite 500
Miami / FL 33130 / US
Tel +1 786 622 2002

contato@baptistaluz.com.br
www.baptistaluz.com.br

BAPTISTA LUZ
ADVOGADOS