Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Fiscalização
Coordenação de Fiscalização

RELATÓRIO DE INSTRUÇÃO Nº 4/2024/FIS/CGF

Brasília, data da assinatura.

RELATÓRIO DE INSTRUÇÃO[1]

SUMÁRIO

1. IDENTIFICAÇÃO

1.1. **Nome/razão social do autuado:** Ministério da Saúde (MS)

1.2. **CPF/CNPJ do autuado:** 00.394.544/0036-05 (0136278)

1.3. **Agente de tratamento:** (X) Controlador ( ) Operador

1.4. **Nome da Encarregada setorial:** Adriana Macedo Marques (Portaria de Pessoal GM/MS nº 953, de 11 de maio de 2023)[2]

1.5. **Nome da Encarregada setorial suplente**: Daniela Barros do Nascimento (Portaria de Pessoal GM/MS nº 953, de 11 de maio de 2023)[3]

1.6. **Contato da Encarregada titular e da Encarregada suplente:** adriana.mmarques@saude.gov.br e daniela.nascimento@saude.gov.br[4]

2. EMENTA

INCIDENTE DE SEGURANÇA EM ÓRGÃO PÚBLICO. DADOS PESSOAIS. TRATAMENTO DE LARGA ESCALA. POTENCIAL ENVOLVIMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES. POSSIBILIDADE DE ACESSO PÚBLICO A SISTEMA COM DADOS RELACIONADOS A CPFs EXISTENTES

EM BASE DE DADOS GOVERNAMENTAL QUE NÃO ESTIVESSEM CADASTRADOS NO SISTEMA PRÓPRIO DO DATASUS. NÃO COMUNICAÇÃO AOS TITULARES EM PRAZO RAZOÁVEL DETERMINADO E CONTEÚDO INADEQUADO NA COMUNICAÇÃO AOS TITULARES. AUSÊNCIA DE COMPROVAÇÃO DE ATENDIMENTO AOS REQUISITOS DE SEGURANÇA, AOS PADRÕES DE BOAS PRÁTICAS E DE GOVERNANÇA E AOS PRINCÍPIOS GERAIS DA LGPD NO SISTEMA UTILIZADO À ÉPOCA DO INCIDENTE DE SEGURANÇA. CONFIGURAÇÃO DE INFRAÇÕES. ADVERTÊNCIAS. MEDIDAS CORRETIVAS.

1. A obrigação de comunicação de incidente de segurança à ANPD e aos titulares não se limita à ocorrência de vazamento de dados pessoais, abrangendo a existência de um evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade da segurança de dados pessoais que possa acarretar risco ou dano relevante aos titulares.
2. A comunicação de incidente de segurança aos titulares independe da concretização de danos em razão do incidente, bastando que este possa acarretar-lhes risco ou dano relevante. A comunicação oferece aos titulares possibilidade de atuar para se proteger, evitar ou mitigar os potenciais riscos ou danos decorrentes do incidente.
3. Apesar de, à época da ocorrência do incidente de segurança, não haver norma geral e abstrata sobre o tempo razoável para a comunicação de incidente de segurança à ANPD e ao titular afetado, a Coordenação-Geral de Fiscalização (CGF), no caso concreto, definiu o prazo razoável para realizá-la aos titulares. Ante a ausência de comunicação no prazo indicado, que contivesse conteúdo em consonância com o art. 48, §1º, da LGPD, foi caracterizada a violação ao art. 48 do referido diploma legal.
4. Admite-se, no caso presente, a realização da comunicação de incidente de segurança de forma geral por meio de sítio eletrônico do autuado, tendo em vista a relatada inviabilidade de identificação individual dos titulares potencialmente afetados pela vulnerabilidade do sistema. Entretanto, ante a ausência dos parâmetros mencionados no art. 48, §1º, da LGPD na comunicação de incidente de segurança, necessária a aplicação de medida corretiva.
5. A não adoção de sistemas estruturados em conformidade com os requisitos de segurança, os padrões de boas práticas e de governança e os princípios gerais da LGPD configura uma violação ao art. 49, da LGPD. O Ministério da Saúde não demonstrou adotar medidas de segurança em seus sistemas aptas a proteger os dados pessoais de acessos não autorizados. A adoção de medidas de segurança técnicas e administrativas adotadas posteriormente ao incidente de segurança não afastam a violação ocorrida, naquele momento, ao art. 49, da

LGPD.

6. O afastamento da aplicação de sanções não encontra guarida no princípio da proporcionalidade, quando não verificados fundamentos suficientes na situação concreta, nos fundamentos da adequação, necessidade e proporcionalidade em sentido estrito, bem como no risco identificado e na postura do agente regulado, em consonância à atuação responsiva da Autoridade.

7. A razão fundamental do princípio da intranscendência subjetiva da sanção não é aplicável em casos de violações das normas de proteção de dados pessoais cometidas por gestão anterior à atual quando relacionada à mesma pessoa jurídica controladora de dados pessoais.

8. Há adequação da advertência para infrações graves diante da impossibilidade de outra sanção, em atenção ao princípio da proporcionalidade.

9. O autuado infringiu os arts. 48 e 49 da LGPD, ensejando a aplicação de 2 (duas) sanções de advertência, cumuladas com 2 (duas) medidas corretivas.

3. REFERÊNCIAS

3.1. Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

3.2. Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 01, de 08 de março de 2021.

3.3. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021 – doravante Regulamento de Fiscalização.

3.4. Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023 – doravante Regulamento de Dosimetria.

3.5. Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024 – doravante RCIS.

3.6. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado - Publicado em abril de 2022.

3.7. Processo de Comunicação de Incidente de Segurança (CIS) nº 00261.001021/2022-95.

3.8. Processo Administrativo Sancionador nº 00261.001882/2022-73.

3.9. Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589).

3.10. Aviso nº 30/2022/CGF/ANPD (0045608).

3.11. Nota Técnica nº 78/2022/CGF/ANPD (0050495).

3.12. Portaria COTEC nº 54/2017 (0045617).

3.13. Defesa Administrativa - Ofício nº 17/2022/AEPD/MS (0050502).

3.14. Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503).

3.15. Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504).

3.16. Alegações Finais - Nota Técnica nº 4/2024-SEIDIGI/CGOEX/SEIDIGI/MS (0098399).

4. SUMÁRIO EXECUTIVO DO PROCESSO

4.1. **Auto de Infração:** 12/09/2022 - Auto de Infração nº 8/2022/CGF/ANPD (0050494).

4.2. **Data da lavratura do Auto de Infração:** 12/09/2022 - Protocolo Digital - Recibo da Solicitação (0050500).

4.3. **Forma da intimação:** (X) Meio eletrônico ( ) Via postal ( ) Pessoal ( ) Comparecimento pessoal ( ) Por edital ( ) Cooperação internacional ( ) Outro meio: contato telefônico.

4.4. **Data da intimação:** 07/10/2022 - Certidão SDSCJPVD – Certidão de Intimação Cumprida 3710142 (0050471) e E-mail (0050472).

4.5. **Dispositivos legais e regulamentares infringidos, nos termos do auto de infração:**

a) Lei Geral de Proteção de Dados (LGPD):

> **Art. 48** – ausência de comunicação ao titular da ocorrência de incidente de segurança que possa acarretar-lhe risco ou dano relevante.
>
> **Art. 49** – não utilização de sistema adequado ao tratamento de dados pessoais.

4.6. **Data da apresentação da defesa:** 22/09/2022. Documentos:

i) Ofício nº 17/2022/AEPD/MS (0050502);

ii) Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503);

iii) Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504).

4.7. **Produção de prova(s) pelo autuado:** ( ) Não (X) Sim.

4.8. **Produção de prova(s) pela ANPD:** (X) Não ( ) Sim.

4.9. **Terceiro(s) interessado(s):** (X) Não ( ) Sim.

4.10. **Termo de Ajustamento de Conduta:** (X) Não ( ) Sim.

4.11. **Alegações Finais:** ( ) Não (X) Sim - Alegações Finais - Nota Técnica nº 4/2024-SEIDIGI/CGOEX/SEIDIGI/MS (0098399).

4.12. **Medidas preventivas aplicadas - art. 32 do Regulamento de Fiscalização:** ( ) Não (X) Sim - Aviso nº 30/2022/CGF/ANPD (0045608).

4.13. **Medidas preventivas aplicadas - art. 26, IV, do Decreto nº 10.474/2020:** (X) Não ( ) Sim.

5. RELATÓRIO

5.1. Conforme disposto no art. 37 do Regulamento de Fiscalização, o processo administrativo sancionador destina-se à apuração de infrações à legislação de proteção de dados que sejam de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD. De acordo com o art. 54 do mencionado Regulamento, o Relatório de Instrução subsidiará a decisão de primeira instância, a ser proferida pela Coordenação-Geral de Fiscalização (CGF). Assim, em consonância com os ditames normativos aplicáveis ao caso e demais documentos que constam dos autos, passa-se ao detalhamento dos atos processuais até a presente data, com o objetivo de avaliar os motivos da autuação e os argumentos apresentados pelo autuado face à legislação e às normas de proteção de dados.

5.2. Em 05/05/2022, a Receita Federal do Brasil (RFB) encaminhou à ANPD a Comunicação de Incidente de Segurança nº 00261.000938/2022-72 sobre a existência de vulnerabilidade no sistema do Ministério da Saúde (MS), que podia ser explorada ao ser executado o comando, em endereço eletrônico de sistema gerido pelo referido Ministério, correspondente XXXXXXX XXXXXX XXXXXXX XXXXXX XXXXXXX XXXXXX XXXXXXX XXXXXX XXXXXXX XXXXXX XXXXXXX XXXXXX, com o subsequente retorno de diversos dados relacionados ao CPF informado. A relação da RFB com o fato decorria do convênio celebrado entre a Secretaria Especial da Receita Federal do Brasil e o Departamento de Informática do Sistema Único de Saúde (DATASUS), órgão do Ministério da Saúde, para o fornecimento de dados cadastrais, "operacionalizado por meio da solução tecnológica b-CPF" (0033743). A RFB também contatou o DATASUS, que tomou ciência da notificação da RFB no mesmo dia, 05/05/2022 (0033744) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.3. Em 16/05/2022, o Ministério da Saúde apresentou, de forma parcial e preliminar, a Comunicação de Incidente de Segurança (CIS) (0045588) referente ao mesmo incidente comunicado pela RFB (item [5.2]), acompanhada de: i) Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589); ii) denúncia recebida pela Ouvidoria-Geral do Sistema Único de

Saúde (SUS) proveniente da Controladoria-Geral da União (0045590) e iii) evidências sobre a vulnerabilidade no Sistema de Cadastro e Permissão de Acesso (SCPA) - doravante “sistema SCPA” -, do Ministério da Saúde (0045591 e 0045592), que originaram o Processo de Comunicação de Incidente de Segurança (Processo de CIS) nº 00261.001021/2022-95. A referida CIS informou uma vulnerabilidade no sistema SCPA, XXXXX XXXXX XXXXXX XXXXX XXXXX XXXXXX XXXXXX, que possibilitaria o acesso público a informações sobre qualquer CPF existente nos cadastros da Receita Federal [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.4. De acordo com o relatado na CIS preliminar mencionada acima (0045588), o incidente teria ocorrido no dia 03/05/2022, aproximadamente às 10:25, e o MS teria tomado ciência a seu respeito no mesmo dia e horário. Tal ciência teria ocorrido por meio de manifestação recebida pela Ouvidoria-Geral do SUS, proveniente da Controladoria-Geral da União (CGU) e encaminhada ao Departamento de Informática do SUS (DATASUS/SE/MS). No entanto, o documento SEI nº 0045590, encaminhado como anexo à CIS preliminar, indica que a Ouvidoria-Geral do SUS enviou tal manifestação a seus Ouvidores em 19/11/2021.

5.5. Após a comunicação da Ouvidoria-Geral do SUS, a Equipe de Prevenção, Tratamento e Resposta a Incidentes na Rede Computacional do Ministério da Saúde (ETIR/MS) teria adotado os esforços necessários para a remediação do incidente, a fim de mitigar e/ou diminuir os impactos à Instituição, além de ter avaliado como “muito alta” a possibilidade e a severidade de violação a dados pessoais resultante do incidente. Maiores informações sobre as providências tomadas pela ETIR/MS foram descritas na Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589).

5.6. O autuado afirmou, também na CIS preliminar (0045588), que **não tinha conhecimento sobre os titulares terem sido notificados**, em razão da ausência de competência para tanto da ETIR/MS – área que realizou a CIS à ANPD. Ademais, **o MS não indicou a quantidade de titulares afetados pelo incidente de segurança em questão**, uma vez que, no campo do formulário que solicita essa informação, reportou apenas que “[a] nível de SCPA nenhum dados (*sic*) foi afetado, nenhum dado foi alterado”.

5.7. No que se refere às **medidas de segurança adotadas**, o Ministério da Saúde indicou que, a fim de prevenir a ocorrência do incidente de segurança, o autuado teria XXXXX

XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX. Quanto às medidas posteriores ao incidente, o autuado afirmou que XXXXX. Por fim, expôs que a medida adotada para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados teria sido a XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX para evitar que novos acessos indevidos a dados pudessem ocorrer (CIS preliminar [0045588]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.8. Foi informado, ademais, que o Ministério da Saúde estaria dedicando esforços para elaborar Relatórios de Impacto à Proteção de Dados Pessoais (RIPDs) e implementar outras iniciativas relacionadas à proteção de dados. Destacou, entre essas iniciativas, o Plano de Transformação Digital (PTD), firmado com a Secretaria de Governo Digital do Ministério da Economia (SGD/ME) e a repactuação do referido plano entre a Secretaria Especial de Modernização do Estado da Presidência da República (SEME/PR) e a SGD/ME. Além disso, também mencionou que o Diagnóstico de Privacidade do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), com previsão de conclusão até agosto de 2022, auxiliaria a elaboração do RIPD do Ministério da Saúde (CIS preliminar [0045588]).

5.9. Ainda conforme a CIS preliminar (0045588), os dados envolvidos no caso incluiriam dados referentes à saúde. De forma específica, indicou os seguintes dados: nome da mãe, data de nascimento, endereço, ocupação, título de eleitor, data de entrega da última declaração de Imposto de Renda, "entre outras". Os titulares afetados seriam funcionários, prestadores de serviço e usuários.

5.10. O anexo da CIS preliminar, a Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589), relata uma série de informações essenciais sobre o incidente ocorrido. No que diz respeito à descrição da falha de segurança, em suma, foi relatada a possibilidade de validar dados relacionados a um CPF na API pública XXXXX XXXXX XXXXX XXXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX e XXXXX XXXXX XXXXX XXXXXX XXXXX XXXXX XXXXX XXXXX, que retornaria dados de titulares, **caso o CPF indicado fosse válido na RFB e o titular não estivesse cadastrado no sistema SCPA**. Tal consulta podia ser realizada em área pública, antes de autenticação XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX após a inserção do CPF do titular, conforme consta das evidências anexadas aos autos (0045591 e 0045592). A Nota Técnica em

questão conclui que a falha teria afetado somente o sistema SCPA e decorreria de regra de negócio de aplicação que deixou falhas de segurança na API, não de ação causada por atores humanos. Além disso, não teria sido evidenciada a exposição ou exfiltração de dados em ambientes não autorizados [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.11. A mencionada Nota Técnica indicou, ademais, que existiam diversas medidas técnicas e administrativas em ação, medidas essas preventivas, de remediação, correção e mitigação do incidente, reiterando aquelas indicadas na CIS preliminar (0045588), além de mencionar que existiam XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX. Apontou, também, oportunidades de melhoria, como as relacionadas a:XXXXX (Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS [0045589]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.12. A Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589), de modo diverso à CIS preliminar (0045588) (item [5.9]), indicou que os dados envolvidos no caso incluiriam: CPF, nome completo, nome da mãe, data de nascimento, endereço, telefone e cartão nacional de saúde (CNS).

5.13. Em 19/05/2022 e em 20/05/2022, a CGF requereu (0045594 e 0045595): i) a complementação da CIS preliminar, no prazo de 30 (trinta) dias corridos da comunicação inicial; ii) a juntada ao processo do Relatório de Tratamento de Dados Pessoais e do Relatório das Operações do Tratamento de Dados Pessoais, restinguindo-se aos fluxos identificados no incidente; bem como iii) a conclusão a respeito do comprometimento de dados pessoais no incidente e das demais informações requeridas no formulário de CIS, em cumprimento ao disposto no art. 48, §1º, da LGPD.

5.14. Em 24/05/2022, a CGF complementou seus pedidos ao autuado (0045596) para solicitar também os seguintes esclarecimentos: i) se havia registros de acesso (logs) do sistema, por qual período eram mantidos, e se permitiam avaliar a possível extração em massa dos dados do sistema em

razão da vulnerabilidade identificada; ii) qual o volume mensal de consultas realizadas por meio da API afetada, nos últimos 6 meses; iii) qual a natureza dos dados acessíveis sem autenticação em razão da vulnerabilidade identificada; iv) se a disponibilidade do sistema SCPA foi afetada, por qual período, e quais outros sistemas se tornaram indisponíveis em razão do ocorrido; e v) caso o sistema SCPA ainda estivesse indisponível, se haveria previsão de retorno. Ademais, a CGF esclareceu que o número de titulares afetados indicado "não estaria relacionado apenas ao comprometimento da integralidade dos dados pessoais, como sugerido pela resposta dada, mas também aos titulares cujos dados possam ter tido sua confidencialidade ou mesmo a disponibilidade impactada".

5.15. No dia 25/05/2022, o autuado acusou recebimento (0045597) dos requerimentos da CGF. Ato contínuo, o MS realizou o encaminhamento de novo formulário de CIS (0045598), cuja única distinção para a CIS preliminar relacionava-se à aba de comunicação aos titulares. Nesta CIS complementar (0045598), o autuado alegou que não teria sido realizada a comunicação do incidente à "sociedade, a eventuais titulares ou outras pessoas envolvidas", pois não teria sido possível identificar vazamentos de informação, mas sim uma constatação de uma falha de sistema.

5.16. Em 28/06/2022, o MS apresentou nova CIS complementar (0045601) e Anexo (0045602). Foram adicionados os seguintes esclarecimentos aos questionamentos realizados pela CGF (0045594e 0045596):

5.16.1. No formulário da CIS (0045601), o campo indicando que o incidente envolveria dados de saúde foi desmarcado, restando apenas o campo "Dado de comprovação de identidade oficial" selecionado. Além disso, os titulares não teriam sido comunicados, pois não teria sido possível identificar vazamentos de informação.

5.16.2. Quanto ao pedido de registro de acesso (*logs*) do sistema (ponto "i" do item [5.14]), o autuado respondeu que: "XXXXX XXXXX" [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.16.3. Em relação ao volume de consultas realizadas por meio da API afetada (ponto "ii" do item [5.14]), o MS informou que "XXXXX XXXXX

XXXXX ”. XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX (0045602) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.16.4. No que tange à natureza de dados (ponto “iii” do item [5.14]), o autuado esclareceu que “XXXXX XXXXX, e hoje os dados não são mais retornados pela API de usuários após as melhorias propostas e entregues em produção no dia 10/05/2022”. Os dados pessoais mapeados na API de usuários seriam: XXXXX [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.16.5. Em relação à disponibilidade do sistema SCPA afetado e seu retorno (pontos “iv” e “v” do item [5.14]), o autuado informou que o SCPA não teria ficado indisponível, porém duas funcionalidades do sistema teriam sido temporariamente desativadas e voltaram a funcionar após a correção das fragilidades, o que levou, neste caso específico, cerca de 10 dias. Segundo o autuado, o incidente não impactou ou indisponibilizou outros sistemas.

5.17. Em 21/07/2022, a CGF proferiu o Despacho (0045604), para sinalizar i) inconsistências entre os documentos acerca dos dados que poderiam ser expostos e a consequente necessidade de retificação e esclarecimento sobre quais dados pessoais, de fato, eram retornados e ii) a ausência de indicação das medidas técnicas e administrativas adotadas para prevenir a ocorrência do incidente.

5.18. No Despacho (0045604), também foi destacado não ser possível avaliar a real extensão da violação de dados pessoais no incidente, ante a XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX, relatada pelo controlador. Nessa conjectura, a CGF apontou que as evidências técnicas apresentadas não permitiam excluir a possibilidade de a vulnerabilidade ter sido utilizada para acessar, de forma indevida, dados de cidadãos vulneráveis e menores de

idade e qualquer titular presente na base de dados. Para mais, não foi informada a data em que a vulnerabilidade foi introduzida no sistema, de modo que não seria possível avaliar há quanto tempo ela poderia estar sendo explorada. [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.19. Em razão do número extremamente alto de titulares potencialmente afetados e dos riscos potenciais relacionados ao conjunto de dados retornados pelo sistema, **entendeu-se que o incidente poderia causar risco ou dano relevante a esses titulares**. Assim, por meio do Despacho (0045604), encaminhado pelo Ofício nº 188/2022/CGF/ANPD/PR (0045605) e E-mail (0045606), a CGF determinou ao autuado que:

> a) comunicasse aos titulares a respeito do incidente de segurança com dados pessoais;
>
> b) apresentasse no processo a comprovação da referida comunicação, informando a data, o meio e a forma como foi realizada, no prazo de 10 (dez) dias úteis após o recebimento do Ofício (0045605); e
>
> c) retificasse o formulário de comunicação de incidente de forma a esclarecer exatamente os dados pessoais afetados no incidente, o número total de titulares potencialmente afetados e as medidas de segurança adotadas antes da ocorrência do incidente.

5.20. Segundo o mesmo Despacho (0045604), a comunicação aos titulares deveria ser feita preferencialmente de forma individual, em linguagem acessível e conter aspectos mínimos, previstos no art. 48, §1º, da LGPD, abordando: a) descrição da natureza e da categoria dos dados pessoais afetados; b) riscos ou consequências do incidente aos titulares; c) indicação das medidas que foram ou que seriam adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis; d) data do conhecimento do incidente de segurança; e e) informações de contato para obtenção de informações sobre o incidente.

5.21. Em 08/08/2022, ante a ausência de resposta por parte do Ministério da Saúde, após o prazo estabelecido, foi emitido o Aviso nº 30/2022/CGF/ANPD (0045608), oportunidade na qual foram concedidos mais 5 (cinco) dias úteis para comprovar as determinações requeridas no Despacho (0045604). O Aviso em questão foi encaminhado por e-mail (0045609) e recebido pelo autuado no mesmo dia, 08/08/2022 (0045612).

5.22. Tendo em vista o **silêncio do autuado após o encerramento do**

prazo para cumprimento da medida preventiva correspondente ao Aviso nº 30/2022/CGF/ANPD (0045608), foi emitida, em 01/09/2022, a Nota Técnica nº 78/2022/CGF/ANPD (0050495), que destacou as inconsistências ou ausências relacionadas:

> i) à apuração da quantidade e de quais seriam os titulares afetados (itens [5.6], [5.14], [5.15], [5.16], [5.19] e [5.21] deste RI e itens 6 e 8 da Nota Técnica);
>
> ii) à data em que a vulnerabilidade teria sido introduzida no sistema (item [5.18] deste RI e itens 6 e 5.6 da Nota Técnica);
>
> iii) à natureza dos dados pessoais afetados, que variou entre os documentos apresentados (itens [5.9], [5.12], [5.16.1], [5.11] e [5.16.4] deste RI e itens 9 a 11 da Nota Técnica);
>
> iv) à comprovação do comunicado do incidente aos titulares de dados (itens [5.19] e [5.21] deste RI e itens 6, 8 e 4.2 da Nota Técnica);
>
> v) às medidas de segurança do sistema, registrando que o sistema SCPA XXXXX (itens [5.16.2], [5.16.3], [5.19] e [5.21] deste RI e itens 12 a 14, 5.5, 5.6 e 5.8 a 5.13 da Nota Técnica); e [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].
>
> vi) às medidas técnicas e administrativas adotadas para prevenir a ocorrência do incidente (itens [5.16.2], [5.16.3], [5.19] e [5.21] deste RI e itens 12 a 14, 5.5, 5.6 e 5.8 a 5.13 da Nota Técnica).

5.23. Quanto às medidas de segurança, segundo constatado pela CGF, não seria possível avaliar o período em que a vulnerabilidade teria sido explorada, uma vez inexistentes mecanismos de controle e monitoramento de acessos, com a consequente falha da garantia da confidencialidade dos dados de toda a base de CPF, que contém centenas de milhões de registros (itens 5.6 e 5.10 da Nota Técnica nº 78).

5.24. Nesse sentido, foram mencionadas as obrigações constantes da Portaria COTEC nº 54, de 08 de junho de 2017 (0045617), que impõe aos órgãos que consumirem as informações disponibilizadas pela RFB a adoção de XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXXXXXXX XXXXX

XXXXX XXXXX XXXXX XXXXX XXXXX :

> Art. 8º Os sistemas de informação de âmbito interno dos órgãos convenentes ou dos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, que consumirem as informações disponibilizadas, deverão implementar, no mínimo, os seguintes requisitos:
>
> XX
> XXXXX
> XX
> XXXXX
>
> [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.25. A Nota Técnica nº 78/2022/CGF/ANPD (0050495) também apontou que as medidas de melhoria indicadas pela ETIR/MS na Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589) tampouco foram implementadas pelo MS.

5.26. Diante do exposto, a referida Nota Técnica nº 78/2022/CGF/ANPD (0050495) constatou a possível violação ao art. 49, da LGPD, cujo teor dispõe sobre o uso de sistemas que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança, e aos princípios gerais previstos na LGPD, bem como a possível violação ao art. 48, da LGPD, em razão da ausência de comprovação da comunicação do incidente aos titulares. Recomendou-se, assim, a instauração de Processo Administrativo Sancionador (PAS), com base no art. 37 do Regulamento de Fiscalização c/c artigos 52 e 55-J, IV da LGPD, o que foi acatado pelo Despacho Decisório nº 8/2022/CGF/ANPD (0045618), a fim de instaurar o presente PAS nº 00261.001882/2022-73. Foi, então, **lavrado o Auto de Infração nº 8/2022/CGF/ANPD (0050494), em 12/09/2022, com a indicação de infração aos arts. 48 e 49, da LGPD**.

5.27. Em 12/09/2022, foi encaminhada a intimação ao autuado, para que apresentasse defesa no prazo de 10 (dez) dias úteis, a partir da ciência do

Auto de Infração (0050494), conforme Ofício nº 211/2022/CGF/ANPD/PR (0050498), Despachos (0050499 e 0050501) e Recibo do protocolo digital encaminhado ao Ministério da Saúde (0050500).

5.28. Em 23/09/2022, tempestivamente, sobreveio Defesa Administrativa – Ofício nº 17/2022/AEPD/MS (0050502), acompanhada dos seguintes documentos: Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503) e Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504).

5.29. Em sede de Defesa Administrativa (0050502), o autuado esclareceu que teria realizado a comunicação oficial aos titulares dos dados sobre o incidente no dia 16/09/2022, às 15h07, no sítio eletrônico do Ministério da Saúde[5], com "detalhamento do incidente de segurança, bem como as ações tomadas por parte deste Ministério para conter a falha identificada" (item 6 da Defesa). A comunicação não teria sido realizada individualmente, tendo em vista a impossibilidade de comunicação direta aos titulares afetados.

5.30. Em relação aos mecanismos de segurança tomados quanto à estrutura dos sistemas, o autuado alegou que providências estariam sendo realizadas, conforme também relatado no item [5.8] deste RI.

5.31. Ainda na sua Defesa Administrativa (0050502), o MS relatou que a intempestividade teria decorrido por "imposição tanto das condições contratuais firmadas com a fábrica de software que executa as manutenções nos sistemas daquele Departamento quanto pelas metodologias de trabalho do Datasus" (item 13 da Defesa). Sustenta que os prazos estabelecidos nas notificações da ANPD não teriam sido cumpridos em razão de reestruturação interna, com a realização de transições de processos administrativos, alinhamento entre unidades do MS e intercorrências com a composição da Assessoria Especial de Proteção de Dados (AEPD) do MS. Esclarece, por fim, que o descumprimento inicial ao art. 48, da LGPD, teria sido sanado com a realização de comunicação no portal do MS e que, em relação ao art. 49, do mesmo diploma legal, o DATASUS estaria buscando "reestruturar o SCPA de forma a atender aos requisitos de segurança, por meio de ações que possam garantir a integridade dos dados e a proteção das informações" (item 19 da Defesa).

5.32. A Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503), por sua vez, ademais das informações trazidas na Defesa Administrativa (0050502), informa que, no caso do sistema SCPA, teriam sido realizadas ações para garantir o sigilo e a confidencialidade dos dados, tais como XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX, enquanto outras estariam em curso, como a implantação de XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX. Também foi citada a existência das seguintes infraestruturas de controles de

segurança: XXXXXXXXXX [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

5.33. Além disso, a Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503) também destacou que as manutenções nos sistemas do MS ocorrem de forma condicionada às condições contratuais com a fábrica de software, “o que nem sempre permite sua conclusão em tempo menor que o estritamente necessário” (item 2.3.4 da Nota Técnica nº 106).

5.34. O Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504), igualmente anexado à Defesa Administrativa (0050502), esclareceu 3 (três) pontos que foram requeridos pela CGF ao longo do Processo de CIS nº 00261.001021/2022-95 (itens [5.13], [5.14]; [5.17]; [5.18]; [5.19], c); [5.21]), conforme quadro abaixo:

Questionamento	**Resposta CDESS**
I- Esclarecimento dos dados pessoais afetados de fato no incidente e prestação dos devidos esclarecimentos aos questionamentos apresentados pela ANPD.	Os dados expostos foram: CPF, nome completo, endereço, telefone, data de nascimento, nome da mãe e cartão nacional de saúde (CNS).
II- Informação sobre o número total de titulares potencialmente afetados.	A nível de SCPA, nenhum dado foi afetado, nenhum dado foi alterado.
III- Informação sobre o período que a API ficou disponível, permitindo a consulta indevida aos dados pessoais a partir da informação do número do CPF.	A publicação/atualização que gerou a fragilidade apontada na API foi disponibilizada de 27/11/2021 a 04/05/2022.

5.35. Ademais, o Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504) informou que a vulnerabilidade encontrada permitia apenas que um CPF por vez fosse consultado, de modo que não era possível a busca de dados em massa, **tampouco sendo possível acessar dados de titulares já cadastrados no Sistema de Cadastro e Permissão de Acesso (SCPA)**.

5.36. Em 14/10/2022, no já encerrado Processo de CIS nº 00261.001021/2022-95, foi anexado novo Formulário de CIS (0045624), no qual o autuado descartou a possibilidade de exposição de um grande volume de

dados em razão da vulnerabilidade encontrada no sistema SCPA, tendo em vista a ausência de um consumo extremamente elevado de recursos computacionais, o que seria necessário em uma ação de extração em massa. Essa informação foi ratificada posteriormente em sede de Alegações Finais, ocasião em que o autuado mencionou, ademais, que a "recuperação de um volume expressivo de dados estava condicionada à posse de uma lista de números de CPF corretos, sem a qual não seria possível" (item 2.5 das Alegações Finais).

5.37. Em 27/10/2022, o processo foi sobrestado pelo Despacho (0050509), até que o Regulamento de Dosimetria e Aplicação de Sanções Administrativas fosse aprovado, o que ocorreu em 27/02/2023. Em 19/04/2023, a tramitação do presente PAS foi retomada, conforme Despacho (0050510).

5.38. Em 30/01/2024, foi emitido o Ofício nº 12/2024/FIS/CGF/ANPD (0067107), por meio do qual o autuado foi instado a apresentar alegações finais no prazo de 10 (dez) dias úteis. Em 15/02/2024, tempestivamente, o MS juntou aos autos o Ofício nº 27/2024/SEIDIGI/CGOEX/SEIDIGI/MS (0098398), com suas Alegações Finais (Nota Técnica nº 4/2024-SEIDIGI/CGOEX/SEIDIGI/MS [0098399]).

5.39. Em suas Alegações Finais (0098399), o MS relata uma nova lista de dados que teria ficado disponível para consulta durante a ocorrência da vulnerabilidade, caso fossem pesquisados CPFs válidos: "unidade administrativa, data nascimento, nome Mãe, CPF, número título eleitor, sexo, situação estrangeiro, situação residente exterior, tipo sexo, tipo situação CPF; Município IBGE, data atualização RFB, data processamento, nome bairro, nome logradouro, nome Município, Nome, número CEP, número logradouro, sigla UF, situação registro ativo" (item 2.5 das Alegações Finais).

5.40. Além disso, o autuado indicou **não ser possível definir um número exato de titulares afetados**, tendo sido potencialmente exposto o Cadastro de Pessoa Física, o que representaria parte significativa da população brasileira. Para mais, reiterou o teor do Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504) em relação ao período e à forma de consulta aos dados pela API vulnerável, além de reafirmar as informações adicionais constantes do Formulário de CIS (0045624), como relatado no item 5.36 supra.

5.41. Ainda em suas Alegações Finais (0098399), o MS reiterou o alegado em sua Defesa Administrativa (0050502) quanto à CIS aos titulares ter sido realizada em 16/09/2022, às 15h07 (item [5.29]) e à intempestividade de suas manifestações no processo (item [5.31]); e repisou as medidas indicadas na Defesa Administrativa (0050502) em relação à comunicação do incidente aos titulares (item [5.29]), bem como quanto às medidas de segurança

adotadas em seus sistemas (item [5.30]).

5.42. Em complementação ao aduzido em Defesa Administrativa (0050502), o autuado requereu a ponderação ao caso do princípio da proporcionalidade previsto no Regulamento de Fiscalização e no Regulamento de Dosimetria, sustentando, ainda, ser necessária a observância de uma atuação responsiva por parte da ANPD, conforme o Regulamento de Fiscalização. Nesse sentido, afirmou ser possível o afastamento da metodologia da dosimetria e a substituição de aplicação de sanção por outra prevista no Regulamento de Dosimetria. Pontuou-se, ainda, 3 (três) critérios para a análise da aplicação do princípio da proporcionalidade: adequação; necessidade; e proporcionalidade em sentido estrito (Alegações Finais [0098399]).

5.43. Por fim, igualmente em Alegações Finais (0098399), o autuado arguiu pelo cabimento do princípio da intranscendência subjetiva aplicável às sanções relacionadas às operações de crédito, de modo que as irregularidades verificadas em gestão anterior inibiriam a aplicação de sanções à nova gestão.

5.44. É o relatório.

6. PRELIMINARES

Competência

6.1. A Lei nº 13.709/18, Lei Geral de Proteção de Dados (LGPD), art. 5º, I, considera dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável". Apesar de terem variado, a base de dados envolvida no incidente de segurança em questão contém, ao menos, dados de: data de nascimento, nome da mãe, CPF, número título eleitor, sexo, nome bairro, nome logradouro, nome município, nome, número CEP, número logradouro, sigla UF (conforme informado em Alegações Finais 0098399). Portanto, **os dados envolvidos no incidente de segurança tratado nesta hipótese são dados pessoais**, pois consistem em informação relacionada a pessoa natural identificada ou identificável.

6.2. A leitura do processo revelou que a atividade desenvolvida pelo Ministério da Saúde configura tratamento de dados pessoais, já que realizava, ao menos, **a recepção, o armazenamento e a utilização desses dados para proporcionar o cadastro dos titulares no sistema SCPA**. Essas atividades se enquadram na previsão do art. 5º, X, da LGPD, que classifica como tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

6.3. A LGPD, ainda, define a figura do controlador no art. 5º, VI,

como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Tendo em vista que o Ministério da Saúde efetuou – e continua efetuando – o tratamento de dados pessoais para cadastrar e identificar os titulares em suas plataformas e para operacionalizar os sistemas de informação e suporte de informática para o serviço de saúde do SUS, resta estabelecido que **a ele competem as decisões referentes ao tratamento de dados pessoais, motivo pelo qual é controlador**.

6.4. Ademais, por força do art. 4º, I, do mencionado Regulamento, o MS é considerado agente regulado pela ANPD, haja vista ser um agente de tratamento – no caso, controlador (item [6.3]). Cumpre especificar os deveres a que os agentes regulados estão submetidos:

> Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros:
>
> I - fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;
>
> II - permitir o acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros;
>
> III - possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos;
>
> IV - submeter-se a auditorias realizadas ou determinadas pela ANPD;
>
> V - manter os documentos físicos ou digitais, os dados e as informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários; e
>
> VI - disponibilizar, sempre que requisitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.

6.5. A competência de atuação da ANPD decorre da circunstância de a atividade realizada pelo MS na gestão do sistema SCPA estar inserida nas disposições da LGPD, definida pelo art. 5º, XIX da mencionada Lei, como "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional". Cabe à ANPD, de acordo com o art. 55-J, "I - zelar pela proteção dos dados pessoais,

nos termos da legislação", bem como "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" e "XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos".

6.6. No âmbito da ANPD, a Coordenação-Geral de Fiscalização (CGF) é a responsável por identificar as infrações à LGPD. De acordo com o Regimento Interno da ANPD:

> Art. 17. São competências da Coordenação-Geral de Fiscalização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável:
>
> I - fiscalizar e aplicar as sanções previstas no artigo 52 da Lei nº 13.709, de 2018, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
>
> [...]
>
> III - promover ações de fiscalização sobre as ações de tratamento de dados pessoais efetuadas pelos agentes de tratamento, incluído o Poder Público;
>
> [...]
>
> VII - receber as notificações de ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares e dar o tratamento necessário;
>
> [...]
>
> IX - requisitar aos agentes de tratamento de dados a apresentação de Relatório de Impacto à Proteção de Dados Pessoais;

6.7. Pelo exposto, à luz da LGPD, fica estabelecida a competência da ANPD no caso concreto para avaliar a conduta do Ministério da Saúde, controlador de dados e agente regulado.

Outras questões preliminares

6.8. O autuado não arguiu questões preliminares de mérito em sua defesa, tampouco esta CGF verificou a existência de tais questões a serem trazidas a este Relatório de Instrução.

7. ANÁLISE

<u>Circunstâncias da infração</u>

7.1. Os documentos apresentados aos autos são suficientes para afirmar que **houve um incidente de segurança no Sistema de Cadastro e Permissão de Acesso (SCPA) do autuado, utilizado para o gerenciamento de cadastro de usuários no Departamento de Informática do Sistema Único de Saúde (DATASUS) do Ministério da Saúde** O incidente resultou na **permissão**

de que qualquer pessoa pudesse ter acesso a dados pessoais, relacionados a qualquer titular com CPF existente nos cadastros da Receita Federal, desde que o titular não tivesse cadastro no SCPA do DATASUS, consoante informado na comunicação de incidente de segurança preliminar encaminhada à Autoridade, na Defesa Administrativa do autuado e em seus respectivos documentos técnicos (itens [5.3] , [5.10] e [5.35]).

7.2. Conforme constatado por esta CGF no âmbito do Processo de CIS nº 00261.001021/2022-95, a exposição indevida de dados pessoais referente a pessoas portadoras de CPF na RFB **configura a ocorrência de um incidente de segurança capaz de acarretar risco ou dano relevante aos titulares dos referidos dados**, em razão do **número extremamente alto de titulares potencialmente afetados**, bem como dos **riscos potenciais relacionados ao conjunto de dados** retornados pelo sistema (0045604; ver item [5.19]).

7.3. Ao longo das manifestações apresentadas pelo autuado, houve considerável variação sobre os dados que seriam retornados quando do preenchimento do CPF do titular na API (itens [5.9] , [5.11] , [5.16] , [5.34] , [5.39] e [6.1] e documentos 0045588, 0045598, 0045589, 0045592, 0045601, 0050504, 0098399). Visando ao reconhecimento, no âmbito deste PAS, da boa-fé do autuado e de sua diligência nas manifestações aportadas, considerar-se-á que os dados afetados no incidente são aqueles informados em Alegações Finais (0098399) : **unidade administrativa, data nascimento, nome mãe, CPF, número título eleitor, sexo, situação estrangeiro, situação residente exterior, tipo sexo, tipo situação CPF, município IBGE, data atualização RFB, data processamento, nome bairro, nome logradouro, nome município, nome, número CEP, número logradouro, sigla UF, situação registro ativo** (item [5.39]).

7.4. No que diz respeito à quantidade de titulares de dados afetados, tampouco foi confirmado o número exato ou aproximado de usuários que poderiam ser impactados. Diante da ausência de delimitação de tal número por parte do autuado, apesar de instado a apresentar essa informação (itens [5.14] e [5.19]), será **considerado que um elevado número de pessoas pode ter sido atingido**, já que: i) os dados eram disponibilizados a partir da informação de um CPF cadastrado na RFB (mais de 220 milhões de inscrições regulares[6]), desde que o titular não possuísse cadastro no sistema SCPA (quantidade não especificada); e ii) diante da ausência de informações por parte do autuado, será adotada a abordagem mais protetiva aos titulares para considerar que milhões de brasileiros foram potencialmente atingidos pelo incidente de segurança.

7.5. Durante todo o Processo de CIS nº 00261.001021/2022-95, anterior a este Processo Administrativo Sancionador, a CGF constatou a **falta de adoção e de comprovação de medidas** relacionadas à comunicação do

incidente de segurança aos titulares de dados e às medidas de segurança implementadas no sistema antes da ocorrência do incidente.

7.6. Para melhor clarificar a **linha cronológica dos fatos e circunstâncias que ensejaram a instauração deste PAS,** relacionados ao conhecimento do incidente pelo autuado, ao período em que a vulnerabilidade esteve disponível no sistema do autuado e à efetiva comunicação do incidente de segurança aos titulares, veja-se ilustração abaixo:

Conduta: não comunicar aos titulares a ocorrência de incidente de segurança que possa lhes acarretar risco ou dano relevante – art. 48 da LGPD

Defesa apresentada pelo autuado

7.7. **A comunicação do incidente aos titulares de dados ocorreu em 16/09/2022, às 15h07** (itens [5.29] e [5.41]), já no âmbito deste PAS.

7.8. A princípio, no Formulário de CIS preliminar (0045588) e no item 4.1.4 da Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589), o autuado alegou que não seria competência da ETIR/MS – área que realizou a CIS preliminar (0045588) à ANPD –, tampouco da COSEGI – área que elaborou a Nota Técnica nº 17/2022 (0045589) – realizar a comunicação aos titulares. Em seguida, nos formulários de CIS complementares (0045598e 0045601), foi informado que a CIS aos titulares não teria sido efetuada, pois não teria sido possível identificar vazamentos de informação, apenas a constatação de uma falha de sistema.

7.9. Em sede de Defesa Administrativa (0050502) e Alegações Finais (0098399), o autuado informou que teria realizado a CIS aos titulares e argumentou que a comunicação foi realizada no sítio eletrônico do Ministério da Saúde[7], uma vez verificada a impossibilidade de comunicação direta aos titulares afetados, bem como em virtude do alcance pretendido. Para mais, a demora em realizar o comunicado teria decorrido de dificuldades em razão de i) atendimento a condições contratuais firmadas com a fábrica de software que executa as manutenções nos sistemas do DATASUS; ii) procedimentos de metodologia de trabalho do DATASUS; e iii) reestruturação interna, com a realização de transições de processos administrativos (alinhamento entre unidades do MS, e intercorrências com a composição da Assessoria Especial de Proteção de Dados (AEPD) do MS [itens [5.31] e [5.41]).

7.10. Em Alegações Finais (0050490), o autuado também suscita a observância, pela ANPD, de uma atuação responsiva, conforme previsto no Regulamento de Fiscalização e no Regulamento de Dosimetria, além da ponderação do princípio da proporcionalidade, de forma afastar a aplicação da sanção no caso.

Subsunção do fato ao tipo infracional correspondente

7.11. O art. 48 da LGPD determina que cabe ao controlador comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Nos termos do §1º do mencionado artigo, a comunicação deverá ser feita em prazo razoável. Ainda que a regulamentação do prazo para a comunicação do incidente estivesse pendente até a apresentação das Alegações Finais (0050490)[8] , o §2º do art. 48 da LGPD confere à ANPD o poder de determinar ao controlador providências para a salvaguarda dos direitos dos titulares, tais como medidas para reverter ou mitigar os efeitos do incidente e a ampla divulgação do fato em meios de comunicação.

7.12. Ocorre que, no caso em comento**, o infrator realizou a comunicação geral aos titulares em seu sítio eletrônico somente em 16/09/2022, às 15h07** (item [5.29])**, mesmo que a primeira determinação da CGF para efetuá-la tenha ocorrido quase 2 (dois) meses antes, em 21/07/2022** (item [5.19] , a). Adicionalmente, o **conteúdo da comunicação geral aos titulares não cumpriu os requisitos do art. 48, §1º, da LGPD** (item [5.20]).

7.13. Cabe destacar que o autuado informou a ocorrência do incidente à ANPD em 16/05/2022, tendo a CGF indicado a necessidade de o MS realizar a comunicação do incidente aos titulares em prazos específicos. Veja-se que, em que pese ausente norma específica sobre o prazo temporal para a CIS aos titulares à época da comunicação do incidente à ANPD, é incontestável que a CGF informou os prazos que considerou serem razoáveis: em **21/07/2022**, determinou a comunicação em até 10 (dez) dias úteis (item [5.19]); e, em **08/08/2022,** ante a ausência de CIS aos titulares, definiu, em sede de medida preventiva, o prazo de 5 (cinco) dias úteis (item [5.21]). **A comunicação aos titulares, no entanto, ocorreu somente em 16/09/2022**, já no âmbito deste PAS, e decorridos quase dois meses da primeira determinação para que o comunicado fosse emitido dentro dos prazos indicados.

7.14. Em princípio, o autuado afirmou que a CIS aos titulares não teria sido realizada ante a ausência de identificação de vazamentos de informação (0045598 e 0045601) (item [7.8]). Nesse ponto, cumpre esclarecer, com intuito educativo, e em consonância ao apontado pela CGF no Processo de CIS (item [5.14]), que a constatação de todo incidente de segurança parte do pressuposto da existência de um evento adverso confirmado, relacionado à violação de determinadas propriedades da segurança de dados pessoais[9] .

7.15. Desconsiderou-se, portanto, que a obrigação de realização de CIS tem como fato gerador necessário (embora não suficiente) um incidente com dados pessoais que viole quaisquer das propriedades de segurança dos

dados (autenticidade, confidencialidade, integridade ou disponibilidade). **A denúncia anônima que indica a vulnerabilidade e a constatação de tal falha pelo autuado (ver item [5.3] , ii), portanto, são suficientes para demonstrar a ocorrência do incidente de segurança**, pois tal denúncia demonstra que terceiros conseguiram acessar dados pessoais que não poderiam, em tese, ser por eles acessados. Para fins de constatação da existência, ou não, de um incidente de segurança, é indiferente que o acesso a tais dados decorra de vazamentos (motivo pelo qual, segundo o autuado, seria justificada a não comunicação aos titulares – ver item [7.8]): o acesso indevido a esses dados representa comprometimento da confidencialidade desses dados e, por isso, fica caracterizada a existência do incidente de segurança.

7.16. Para a realização da CIS, além da ocorrência do incidente de segurança, é necessário verificar a presença de risco ou dano relevante aos titulares, o que, embora não constatado pelo autuado, foi indicado pela CGF em oportunidade posterior, junto à indicação do prazo em que a CIS ao titular deveria ser realizada (0045604, itens [5.19] e [7.12]).

7.17. Para mais, de acordo com o verificado no sítio eletrônico do autuado[10] , **a CIS em análise também não contém os requisitos que foram elencados pela CGF (e baseados no art. 48, §1º da LGPD), quando da determinação da CIS aos titulares (item[5.20])**. Em particular, consta da comunicação apenas alguns dos dados pessoais elencados ao longo deste processo, que diferem, inclusive, dos dados listados em sede de Alegações Finais (0098399), não tendo sido esclarecido quais seriam efetivamente os dados pessoais afetados.

7.18. Entretanto, cumpre salientar a boa prática do autuado em alocar todos os seus incidentes de segurança em uma página específica de seu sítio eletrônico[11] , o que permite que os titulares de dados consultem um local centralizado para se cientificarem sobre eventuais incidentes de segurança que possam envolvê-los.

7.19. Ademais, em que pese seja compreensível a alegação de que a demora em realizar a comunicação aos titulares por meio do sítio eletrônico teria decorrido de dificuldades de condições contratuais firmadas com a fábrica de *software* e de reestruturação interna do órgão (0050502; 0098399; item [7.9]), tais explicações não se sustentam como justificativa para o cumprimento intempestivo da obrigação legal de realizar a comunicação do incidente aos titulares em prazo razoável, nos termos do art. 48, da LGPD, por dois motivos principais.

7.20. A um, não foi suscitado o nexo causal entre a condição contratual com a fábrica de *software* (item [7.9], i) e o impedimento da publicação de comunicação do sítio eletrônico do MS. Importa esclarecer, ainda, que, embora a modalidade de CIS geral no sítio eletrônico possa ser

considerada como suficiente, dada as circunstâncias do caso em concreto, a CIS individual poderia se concretizar e alcançar titulares específicos caso houvesse o devido controle de acesso no sistema que permitisse a identificação individual dos titulares afetados, como será melhor explorado no item [7.57] , conforme orientação da CGF para que tal comunicação fosse efetuada preferencialmente de forma individual (item [5.20]). No entanto, em virtude da impossibilidade de comunicação individual dos titulares potencialmente afetados, conforme indicado pelo próprio autuado (item [7.9]), a CGF entendeu que a CIS geral e indireta, por meio do sítio eletrônico, seria a medida adequada ao caso presente.

7.21. A dois, é descabido considerar que a CIS aos titulares não poderia ter sido realizada previamente à implementação da Assessoria Especial de Proteção de Dados (AEPD) do MS (itens [5.31] e [7.9]). Afinal, o MS é o controlador dos dados pessoais desde antes – e independentemente – da reestruturação supracitada, de modo que a CIS poderia ter sido publicada, no mínimo, desde o momento em que a **CGF determinou a realização da comunicação aos titulares pela primeira vez**, em 21/07/2022 [0045604, item [5.19] , a)]. Consequência disso é que não há que se falar em descontinuidade de obrigações previstas explicitamente em lei sob a alegação de mera troca de gestões ou governos, de modo que tal argumento apresentado pelo autuado (itens [5.31] e [7.9]) não se sustenta frente à violação ao art. 48 da LGPD, tampouco afasta sanção em decorrência da infração, como será abordado nos tópicos seguintes.

7.22. Ademais, essencial ressaltar que conflitos internos de competência, conforme apontou o autuado em sua defesa (ver item [7.8]), não justificam o descumprimento de obrigação legal imposta pela LGPD. Caberia ao MS avaliar a atribuição das unidades dentro da sua estrutura e definir aquela à qual competiria a realização da comunicação em análise, na condição de controlador de dados pessoais.

7.23. Por todo o exposto, i) tendo em vista o período transcorrido entre a primeira determinação da CGF com a indicação de prazo para a comunicação de incidente de segurança até a realização, de fato, da CIS geral aos titulares (ver itens [7.12] e [7.13]); e ii) considerando que o conteúdo disposto na CIS geral aos titulares no sítio eletrônico do MS não contém os requisitos que foram elencados pela CGF (e baseados no art. 48, §1º da LGPD), quando da determinação da CIS aos titulares (Alegações Finais - 0098399) (item [7.17]), **configura-se a violação ao art. 48 da LGPD.**

Classificação da infração

7.24. O art. 48 da LGPD determina que o controlador deve apresentar CIS adequada tanto à ANPD quanto ao titular em prazo razoável. Conforme visto nos itens [7.11] a [7.23] , o autuado fez comunicado geral

intempestivamente e com conteúdo inadequado aos titulares potencialmente afetados pelo incidente de segurança.

7.25. Segundo prevê o art. 8º, §2º, do Regulamento de Dosimetria[12], a infração pode ser considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares. Nesse sentido, a falta de CIS ao titular em prazo razoável, neste caso específico, pode ser classificada como média sob quatro aspectos.

7.26. Em primeiro lugar, o incidente ocorrido permitiu que terceiros pudessem acessar um volume considerável de dados relativos a uma quantidade de titulares numerosa (ver item [7.4]), sem que fossem autorizados a fazê-lo.

7.27. Em segundo lugar, a eventual atividade de tratamento decorrente do incidente pode impedir ou limitar que os titulares tenham seu devido acesso aos recursos provenientes da conta criada no sistema, uma vez que a vulnerabilidade facilitava o processo de cadastro de um usuário por um terceiro, desde que o último possuísse o CPF do titular. Tal fato poderia impedir o uso dos recursos decorrentes do sistema SCPA pelo verdadeiro titular, limitando o exercício do direito do usuário a acessar os serviços do SUS que se valem do apoio prestado pelo DATASUS, o que também poderia causar danos materiais ou morais ao titular afetado.

7.28. Em terceiro lugar, intimamente atrelado aos parâmetros anteriores, os dados expostos no caso concreto – unidade administrativa, data nascimento, nome mãe, CPF, número título eleitor, sexo, situação estrangeiro, situação residente exterior, tipo sexo, tipo situação CPF, município IBGE, data atualização RFB, data processamento, nome bairro, nome logradouro, nome município, nome, número CEP, número logradouro, sigla UF, situação registro ativo – possibilitam o risco de o titular sofrer danos em situações[13], por exemplo, de discriminação, perturbações por fraudes em processos de autenticação ou validação de identidade em serviços específicos. Isso é especialmente relevante ao ponderar-se que a conjugação de múltiplos dados relativos a uma mesma pessoa pode facilitar que mais ações de fraudes possam ser efetuadas em seu nome, além de conferir maior plausibilidade de que o terceiro seja reconhecido como o verdadeiro titular dos dados expostos[14].

7.29. Por fim, em quarto lugar, a conclusão a que se chega dos elementos supracitados é a de que a falta de conhecimento sobre o incidente impede que o titular possa i) exercer o seu direito fundamental à proteção de dados e ii) diminuir possíveis consequências, já que diversas são as hipóteses de danos, como acima relatado, caso não sejam tomadas as precauções necessárias por parte do titular.

7.30. Congruente a isso, o Cert.br/Nic.br/Cgi.br, com contribuição da ANPD, elaborou o Fascículo de "Vazamento de Dados"[15], cujo objetivo é informar algumas medidas que podem ser tomadas pelos titulares para a redução do impacto de eventuais vazamentos de dados. A relevância de a CIS ser realizada para o titular, portanto, decorre do fato de que o titular, após ter conhecimento sobre um incidente de segurança que o tenha afetado, pode adotar algumas providências, como as já divulgadas no documento.

7.31. Logo, **a infração ao art. 48 ora analisada se enquadra nos requisitos do art. 8º, §2º, do Regulamento de Dosimetria, atendendo ao critério para ser classificada como média**.

7.32. Além disso, no presente caso, a infração versa sobre tratamento de dados pessoais em **larga escala**, considerando i) tratar-se de dados relativos a quaisquer titulares com CPF na RFB – ou seja, número significativo de titulares –, que, cumulativamente, não tivessem cadastro no sistema SCPA do DATASUS (item [5.35]) – quantidade que, por não ter sido especificada pelo autuado (item [5.40]), foi considerada como de milhões de portadores de CPF potencialmente atingidos (ver item [7.4]); ii) o considerável número de dados que eram retornados a cada CPF pesquisado (conforme conjunto de dados informados no item [6.1]); e iii) a possibilidade de envolver titulares naturais de quaisquer regiões do Brasil e até mesmo de estrangeiros ou residentes no exterior, desde que portadores de CPF cadastrados na base da RFB (item [6.1]).

7.33. Adicionalmente, **crianças, adolescentes e idosos** podem estar entre esses portadores de CPF, e o autuado não afastou a potencialidade de os dados desses titulares terem sido atingidos pelo incidente de segurança, (consoante relatado no item [5.18]). Essas características elevam o grau de classificação da infração que, por esse motivo, **passa a ser considerada como grave, segundo art. 8º, §3º, I, "a" e "d", do Regulamento de Dosimetria**[16].

Definição do tipo de sanção administrativa

7.34. Para a definição do tipo de sanção adequada, o art. 10º do Regulamento de Dosimetria indica ser aplicável multa simples quando a infração for classificada como grave[17]. No entanto, o art. 52, §3º, da LGPD, ao estabelecer as sanções que podem ser impostas a entidade ou a órgãos públicos, afasta, por omissão, a possibilidade de aplicação de multa ou de multa diária a esses agentes de tratamento.

7.35. Por outro lado, o Regulamento de Dosimetria define, em seu art. 9º, que a advertência pode ser aplicada quando a infração for leve ou média, ou quando houver necessidade de imposição de medida corretiva[18]. Esta hipótese se aplica à presente infração, tendo em vista a necessidade de impor ao autuado a retificação de comunicação aos titulares de dados, em

atenção ao disposto no art. 48, §1º, da LGPD.

7.36. **Aplica-se, portanto, a sanção de advertência, cumulada com medida corretiva.**

7.37. Tendo em vista o exposto acima, cabe a imposição da seguinte medida corretiva:

> 1) Ajuste, no **prazo de 10 (dez) dias úteis** da data de intimação do Despacho Decisório, do comunicado já existente no sítio eletrônico do Ministério da Saúde, para que sejam retificados:
>
> a) a descrição das categorias de dados pessoais que ficaram disponíveis para consulta durante a ocorrência da vulnerabilidade, caso fossem pesquisados CPFs válidos na RFB, a fim de que a informação esteja em consonância ao informado nas Alegações Finais (0098399) do autuado neste Processo Administrativo Sancionador;
>
> i. o autuado deve retificar a coluna "Natureza dos dados potencialmente expostos" disponível em seu sítio eletrônico[19], com indicação da data de atualização, para que conste os seguintes dados pessoais: "unidade administrativa, data nascimento, nome mãe, CPF, número título eleitor, sexo, situação estrangeiro, situação residente exterior, tipo sexo, tipo situação CPF, município IBGE, data atualização RFB, data processamento, nome bairro, nome logradouro, nome município, nome, número CEP, número logradouro, sigla UF, situação registro ativo", conforme mencionado no item [6.1] deste Relatório de Instrução.
>
> b) as medidas técnicas e de segurança utilizadas para a proteção dos dados, com a indicação de que foram adotadas melhorias ou que estão em curso as relacionadas a: controles de acesso, medidas de verificação de vulnerabilidades e demais ações que o Ministério da Saúde entenda ser pertinente sua publicação, observada eventual restrição de acesso legalmente aplicável;
>
> c) os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares, indicando-se os

riscos mencionados nos itens [7.29] e [7.30], quais sejam: i) riscos de impedir ou limitar que os titulares tenham seu devido acesso à conta do sistema e ii) riscos de dano em situações, por exemplo, de discriminação e perturbações por fraudes em processos de autenticação ou validação de identidade em serviços específicos; e

d) os motivos da demora da realização da realização da comunicação do incidente aos titulares.

7.38. A fim de se comprovar que a medida corretiva imposta em razão da violação ao art. 48 da LGPD foi cumprida:

a) o comunicado citado no item [7.37] "1)", deverá ser mantida no sítio eletrônico do Ministério da Saúde por pelo menos mais 90 (noventa) dias corridos a contar da data da intimação do Despacho Decisório;

b) deverá ser juntada aos autos comprovação de que a medida corretiva do item [7.37] “1)” foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela do sítio eletrônico do Ministério da Saúde, com intervalo mínimo de 9 (nove) dias entre cada uma, contendo o comunicado e com visualização clara da data da captura;

c) a comprovação de cumprimento da medida corretiva deverá ser juntada aos autos em até **5 (cinco) dias úteis** do final de cada período de 30 (trinta) dias, independentemente de nova intimação para tanto.

Conduta: não utilizar sistemas que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios da LGPD – art. 49 da LGPD (incidente de segurança).

Defesa apresentada pelo autuado

7.39. Conforme relatado acima, o Ministério da Saúde (MS) comunicou a ocorrência de um incidente de segurança com dados pessoais (CIS preliminar 0045588 – item [5.3]), em razão de uma vulnerabilidade no sistema SCPA, que permitia que qualquer pessoa pudesse preencher o CPF de um titular, em uma API do MS, e acessar vários dados relacionados ao mesmo CPF, desde que este estivesse cadastrado na RFB e não estivesse cadastrado no sistema próprio do DATASUS (0045588, 0045589, 0050504 e 0045624; itens [5.3], [5.10] e [5.35]).

7.40. De acordo com as comunicações de incidente de segurança do autuado (0045588, 0045598, 0045601 e 0045624), o MS somente teria tomado

conhecimento do incidente em 03/05/2022. Por outro lado, a Ouvidoria-Geral do SUS teria informado aos Ouvidores, em 19/11/2021, sobre o cadastro de uma denúncia anônima proveniente da CGU no Sistema OuvidorSUS e a encaminhado ao Departamento de Informática do SUS (0045590) referente a uma vulnerabilidade no sistema gerenciado pelo DATASUS. Em outra manifestação do autuado (0050504), a publicação/atualização que teria gerado a fragilidade na API teria sido disponibilizada de 27/11/2021 a 04/05/2022 (ver linha do tempo do item 7.6).

7.41. Ademais, de acordo com a Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589), o órgão relatou que, em relação às medidas de segurança adotadas previamente ao incidente, existiam: XXXXX (item [5.11]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.42. Em CIS complementar (0045601) e no Anexo (0045602), o autuado afirmou que XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX, à época do incidente, apenas que XXXXX. Ademais, também foi relatado que o sistema SCPA XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX (item [5.16.3]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.43. Como contraponto, foi informado na CIS complementar (0045601) que não teria sido identificado qualquer comportamento fora do normal quanto à utilização de recursos computacionais, o que foi evidenciado por meio de anexos relacionados aos meses de janeiro a maio de 2022 (item [5.16.3]). Nesse sentido, no Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504), que acompanhava a Defesa Administrativa (0050502) – bem como reiterado na terceira CIS complementar (0045624) e em Alegações Finais (0098399) –, o MS esclareceu que, em razão de o consumo de recursos computacionais não ter sido extremamente elevado, o autuado teria descartado a possibilidade de exposição de um grande volume de dados e de uma extração de dados em massa (item [5.36]).

7.44. Logo após o recebimento da denúncia da vulnerabilidade da ETIR/MS, o MS relata que teria realizado esforços para a remediação do

incidente (item [5.5]). Nessa conjectura, no que se refere às medidas de segurança que o autuado compreendia como medida "preventiva", bem como aquelas tomadas para fins de remediação, correção e mitigação do incidente, o autuado citou que teria: XXXXX, conforme CIS preliminar (0045588, item [5.7]), Nota Técnica nº 17/2022-COSEGI (0045589, item [5.11]) e reiterado nas CIS complementares (0045598, 0045601 e 0045624) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.45. Além disso, na Nota Técnica nº 17/2022-COSEGI (0045589, item [5.11]), foram mencionadas as seguintes ações que poderiam ser tomadas para melhorar o sistema: XXXXX (Nota Técnica 17/2022-COSEGI/CGGOV/DATASUS/SE/MS [0045589]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.46. No que tange às medidas administrativas de segurança que estariam em andamento à época da comunicação do incidente, o autuado informou, na CIS preliminar (0045588) – reiterado na Defesa Administrativa (0050502) –, que adotaria as seguintes providências: i) elaboração de RIPDs; ii) construção do Diagnóstico de Privacidade, que auxiliaria na elaboração de RIPD, com previsão de conclusão até dezembro de 2022; iii) implementação do Plano de Transformação Digital (PTD) repactuado entre o MS com a SEME/PR e SGD/ME; iv) observância às orientações dispostas no Guia de Boas Práticas da LGPD, editado pela Secretaria de Governo Digital do Ministério da Economia; além de ressaltar seu esforço para a v) implementação completa de controles no SCPA.

7.47. Na Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503), que acompanhava a Defesa Administrativa (0050502), o MS apresentou outras

ações que também teria realizado para garantir o sigilo e a confidencialidade dos dados, tais como XXXXX. Também foi citada a existência das seguintes infraestruturas de controles de segurança: XXXXX (item [5.32]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.48. Em sede de Defesa Administrativa (0050502) e em Alegações Finais (0098399), o autuado relatou que não teria se manifestado dentro dos prazos determinados pela CGF, pois i) teria passado por mudanças na estrutura interna do órgão e ii) sujeitava-se à imposição de condições contratuais firmadas com a fábrica de *software* que executava as manutenções nos sistemas (item [5.31]). Quanto ao último ponto, a Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503), destacou que, em razão das manutenções nos sistemas do MS estarem condicionadas à empresa de *software*, isto nem sempre permitia a conclusão de providências em tempo menor que o estritamente necessário (item 2.3.4 da Nota Técnica nº 106 e item [5.33] deste RI).

7.49. Em Alegações Finais (0098399), foi suscitada a necessidade de aplicação do princípio da proporcionalidade em razão da adequação do MS à LGPD, endossada pela implementação de 6 (seis) medidas administrativas relacionadas à proteção de dados no Ministério da Saúde: criação da Secretaria de Informação e Saúde Digital no Ministério da Saúde; designação de nova Encarregada de Dados e publicação no sítio eletrônico; criação de Grupo de Trabalho para tratar especificamente sobre a LGPD; obtenção de assento para futura composição no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); realização da 1º Jornada de Proteção de Dados Pessoais no SUS; adoção de Programa de Privacidade e Segurança da Informação (PPSI) e mais 1 (uma) medida em andamento, relacionada à capacitação para servidores das unidades descentralizadas do MS e do SUS, conforme descrito nos tópicos de A) a G) do item 3.24 das Alegações Finais (0098399).

7.50. Quanto à proporcionalidade, o autuado afirmar ser necessária a

observância às premissas responsivas dos Regulamentos da ANPD, bem como ao exame dos elementos do princípio da proporcionalidade para o afastamento da sanção, quais sejam: de adequação, necessidade e proporcionalidade em sentido estrito.

Subsunção do fato ao tipo infracional correspondente

7.51. Viola o art. 49 da LGPD o sistema utilizado para tratar dados pessoais que não seja estruturado de modo a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na lei e às demais normas regulamentares.

7.52. Como relatado, o autuado informou que havia uma vulnerabilidade no sistema SCPA, que ocorreu em razão de uma falha de segurança que permitia a exposição, sem a obrigatoriedade de autenticação prévia, de vários dados relacionados a um CPF da base da RFB, desde que o referido CPF não estivesse cadastrado no mencionado sistema (0045588, 0045589, 0050504 e 0045624) (itens [5.3], [5.10] e [5.35]).

7.53. Apesar de ter relatado a existência de algumas medidas de segurança adotadas previamente ao incidente, estas **não se demonstraram suficientes para prevenir a ocorrência de acessos não autorizados, tampouco para avaliar a real extensão do incidente.** Essas medidas não evidenciaram i) o monitoramento de acessos à base de dados do sistema SCPA; ii) a volumetria dos titulares que teriam sido afetados, bem como a natureza e as categorias de dados que puderam ser consultados; e iii) o momento em que a vulnerabilidade teria sido introduzida, de fato, no sistema (itens [5.18] e [5.22]).

7.54. A ausência de medidas preventivas de segurança, portanto, permitia que dados pessoais de usuários não cadastrados fossem expostos a partir do preenchimento de um CPF, sem que houvesse sequer uma etapa prévia de autenticação, o que evidenciou a **falta de implementação de controles adequados para garantir a confidencialidade dos dados pessoais**.

7.55. Diante disso, à época do recebimento da CIS pela ANPD, a CGF entendeu pela necessidade de aprofundar-se nas medidas adotadas pelo autuado, para compreender a real extensão do incidente de segurança. Desta forma, foram requeridos, especificamente, os seguintes esclarecimentos: i) se havia registros de acesso (*logs*) do sistema, por qual período eram mantidos, e se permitiam avaliar a possível extração em massa dos dados do sistema em razão da vulnerabilidade identificada; ii) qual o volume mensal de consultas realizadas por meio da API afetada, nos últimos 6 meses; iii) qual a natureza dos dados acessíveis sem autenticação em razão da vulnerabilidade identificada; iv) se a disponibilidade do sistema SCPA foi afetada, por qual período, e quais outros sistemas se tornaram indisponíveis em razão do ocorrido; e v) caso o sistema SCPA ainda estivesse indisponível, se haveria

previsão de retorno (item [5.14]).

7.56. Conforme informado pelo autuado, por um lado, houve a constatação das medidas de segurança descritas no item [7.41]; por outro, foi confirmada a inexistência de XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX (item [7.42]), fato este que demonstrou **a inadequação da estrutura do sistema utilizada pelo autuado à época do incidente**. Não bastasse isso, tendo em vista que os dados pessoais que compunham a base de dados provinham da RFB, o Ministério da Saúde, como receptor de tais dados, tinha a obrigação de XXXXX ”, nos termos do art. 8º, XXXXXX, da Portaria COTEC nº 54/2017 (0045617 e item [5.24]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.57. O referido **monitoramento** XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX **era essencial para a compreensão do comprometimento da base de dados pessoais do autuado**. A ausência de XXXXX XXXXX impossibilita, por exemplo, XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX – como exemplificativamente apontado na página 9 da Nota Técnica nº 17/2022-COSEGI/CGGOV/DATASUS/SE/MS (0045589) –, o que revelaria quantos e quais CPFs relacionados a titulares teriam sido afetados durante o período em que o sistema SCPA esteve vulnerável. Consequência disso é a conclusão de que dados pessoais de quaisquer titulares - inclusive de idosos, crianças e adolescentes -, podiam ser acessados de modo indevido (item [5.18]), mediante a consulta na API do autuado, caso tais titulares possuíssem um CPF cadastrado na RFB e, cumulativamente, não estivessem cadastrados no sistema SCPA. [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.58. Para mais, embora a CGF tenha considerado que os dados afetados foram os mencionados no âmbito das Alegações Finais (0098399), verificou-se, ao longo das manifestações do autuado, uma variação acerca dos dados pessoais que poderiam ser retornados quando do preenchimento do CPF de algum titular no sistema (itens [5.9], [5.11], [5.16.4], [5.34], [5.39] e [6.1] e documentos 0045588, 0045598, 0045589, 0045592, 0045601, 0050504, 0098399). Deste modo, **ressalta-se que houve frequentes inconsistências acerca de quais dados poderiam ter sido expostos, fato que reitera a ausência**

de controles efetivos da API.

7.59. Ademais, embora o MS tenha colacionado aos autos relatórios de registros de utilização de recursos computacionais de janeiro a maio de 2022 (item [7.43]), tais relatórios não abarcam o XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX , como apontado pela CGF, em oportunidade anterior (item [5.22], "v)") [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.60. Por fim, no que tange ao período em que a vulnerabilidade da API teria perdurado, foi relatado, em todos os formulários de CIS (0045588, 0045598, 0045601 e 0045624), que o autuado teria tido ciência do incidente em 03/05/2022, aproximadamente às 10h25 (item [5.4]). Contudo, conforme pôde ser verificado no Anexo (0045590) da CIS preliminar (0045588), a CGU recebeu uma denúncia anônima quanto ao incidente no sistema SCPA do MS, a qual foi encaminhada à Ouvidoria-Geral do SUS (item [5.4]). No dia 19/11/2021, às 22:17, a Ouvidoria-Geral do SUS informou aos Ouvidores que teria cadastrado a denúncia no Sistema OuvidorSUS e a encaminhado ao Departamento de Informática do SUS (0045590) (item [5.4]). Ademais, no âmbito do PAS, foi ressaltado que a vulnerabilidade no sistema SCPA teria sido disponibilizada de 27/11/2021 a 04/05/2022 (0050504), ou seja, momento também anterior à data informada nas CIS à ANPD (item [5.34]) (ver linha do tempo do item [7.6]).

7.61. Dito isto, percebe-se que o Ministério da Saúde, por meio da Ouvidoria do SUS, tomou ciência do incidente ao menos no dia 19/11/2021, quando do encaminhamento da denúncia anônima proveniente da CGU aos Ouvidores. Contudo, alega ter tomado conhecimento apenas no dia 03/05/2022. **É de se destacar, portanto, com base nas provas colacionadas aos autos, o lapso temporal de mais de 5 (cinco) meses – de 19/11/2021 a 03/05/2022 – para o MS tomar providências de segurança a partir da denúncia recebida pela Ouvidoria do SUS, período no qual a vulnerabilidade pôde ser explorada**. Registra-se, assim, a importância da implementação de medidas de segurança administrativas para o tratamento de dados pessoais, que se complementam às medidas de segurança técnicas[20]. No caso presente, a inexistência ou a não aplicação de medidas como um plano de comunicação de incidente de segurança interno ou de medidas similares, que permitissem maior agilidade para o encaminhamento em prazo razoável para a área competente do Ministério da Saúde, **resultou na ausência de providências de segurança do MS, desde o momento da recepção da denúncia**.

7.62. Além disso, o Ministério da Saúde anexou, em sua Defesa Administrativa (0050502), o Despacho CDESS/CGSIO/DATASUS/SE/MS (0050504), mediante o qual foi constatada que a fragilidade da API, que

permitia a exposição dos dados pessoais, **teria se mantido entre o período de 27/11/2021 a 04/05/2022**.

7.63. Em que pese a data inicial (27/11/2021) indicada pelo autuado no Despacho CDESS (0050504) difira da data (19/11/2021) em que a Ouvidoria-Geral do SUS informa aos Ouvidores que teria cadastrado a denúncia no Sistema OuvidorSUS e a encaminhado ao Departamento de Informática do SUS (DATASUS) (0045590) – ver linha do tempo do item [7.6] –, fato é que **não existiram verificações de vulnerabilidades na API por pelo menos 5 (cinco) meses (no mínimo durante o mês inteiro de dezembro de 2021 a abril de 2022)** – ou ao menos provas de que providências foram tomadas, caso tal brecha tenha sido constatada previamente. Esta lacuna corrobora a constatação da **ausência de mecanismos de segurança que protegessem o sistema SCPA de ser acessado de forma indevida e que demonstrassem quando, de fato, a vulnerabilidade teria sido introduzida no sistema** (itens [5.18] e [5.23]).

7.64. A fim de afastar a violação ao art. 49, da LGPD, o autuado alegou que as manutenções nos sistemas do MS ocorriam de forma subordinada às condições contratuais com a fábrica de *software*, o que nem sempre permitiria sua conclusão em tempo menor que o estritamente necessário (itens [5.31], [5.33] e [7.48]). Ocorre que não foi possível vincular como a vulnerabilidade da API estaria sujeita às condições contratuais com a empresa terceira, já que, na presente hipótese, **caberia ao controlador autuado, ao menos, supervisionar as ações do prestador de serviços de *software***, que garantissem que os dados não pudessem ser expostos para quaisquer terceiros que pesquisassem um CPF válido de um titular. O autuado tampouco explicitou quaisquer interações prévias com a empresa que demonstrassem que aquele teria tomado providências frente à prestadora de serviços em relação à vulnerabilidade.

7.65. De qualquer modo, não poderia ser negligenciada a implementação de controles sobre o sistema, como monitoramento XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX; e testes periódicos de vulnerabilidade do sistema, de modo que a intempestividade de sua efetivação não foi robustamente justificada. Não bastasse isso, reprisa-se que, conforme supracitado, as condições contratuais com a empresa de *software* tampouco seriam suficientes para afastar a obrigação de o autuado, como controlador de dados pessoais, observar o art. 49 da LGPD, bem como o art. 8º, XXXXX, da Portaria COTEC nº 54/2017, da qual decorria a compulsoriedade dos XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX, com diversas especificidades para ambas as obrigações (0045617 e item [5.24]) [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema

– art. 13, II, do Decreto nº 7.724/2012].

7.66. Ainda assim, percebe-se que existem esforços do autuado para que seu sistema se alinhe às disposições da LGPD. Estritamente quanto às falhas mais relevantes observadas no caso presente, ressaltam-se as iniciativas apontadas no item [7.47], uma vez que se referem às medidas de segurança adotadas na estrutura do sistema SCPA do MS, mesmo que posteriores ao incidente de segurança.

7.67. Ante a confirmação de que **não foram adotadas medidas de segurança suficientes para garantir a adequada estrutura dos sistemas utilizados no tratamento dos dados pessoais dos titulares à época do incidente, fica caracterizada a violação ao art. 49, da LGPD.**

Classificação da infração

7.68. É dever dos agentes de tratamento a utilização de sistemas para tratamento de dados pessoais que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios da LGPD e às normas regulamentares. Considerando o supracitado, percebe-se que o sistema do MS não continha salvaguardas adequadas que estivessem alinhadas à efetiva segurança dos dados pessoais, conforme demonstrado nos itens [7.51] a [7.67].

7.69. Segundo prevê o Regulamento de Dosimetria, a infração pode ser considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares. No presente caso, a ausência de medidas suficientes a proteger os dados do titular pode ser classificada como média sob três aspectos, nos termos do art. 8º, §2º, do Regulamento de Dosimetria.

7.70. Em primeiro lugar, o incidente ocorrido permitiu a exposição de dados pessoais em espaço e por de tempo significativo, sem o devido controle de acesso, de forma que terceiros podiam acessar um volume considerável de dados relativos a uma numerosa quantidade de titulares, já que podiam ser expostos dados pessoais relacionados a qualquer pessoa que possuísse um CPF cadastrado na RFB, e que, cumulativamente, não estivesse inscrito no sistema SCPA (ver item [7.4]).

7.71. Em segundo lugar, a eventual atividade de tratamento decorrente do incidente pode impedir ou limitar que os titulares tenham seu devido acesso aos recursos provenientes da conta criada no sistema, uma vez que a vulnerabilidade facilitava o processo de cadastro de um usuário por um terceiro, desde que o último possuísse o CPF do titular. Tal fato poderia impedir o uso do sistema SCPA pelo verdadeiro titular, limitando o exercício do direito do usuário a acessar os serviços do SUS que se valem do apoio prestado pelo DATASUS, o que também poderia causar danos materiais ou morais ao titular afetado.

7.72. Em terceiro lugar, intimamente atrelado aos parâmetros anteriores, os dados expostos no caso concreto – unidade administrativa, data nascimento, nome mãe, CPF, número título eleitor, sexo, situação estrangeiro, situação residente exterior, tipo sexo, tipo situação CPF, município IBGE, data atualização RFB, data processamento, nome bairro, nome logradouro, nome município, nome, número CEP, número logradouro, sigla UF, situação registro ativo – possibilitam o risco de o titular sofrer danos em situações, por exemplo, de discriminação, perturbações por ligações indevidas e fraudes em processos de autenticação ou validação de identidade em serviços específicos. Isso é especialmente relevante ao ponderar-se que a conjugação de múltiplos dados relativos a uma mesma pessoa pode facilitar que mais ações de fraudes possam ser efetuadas em seu nome, além de conferir maior plausibilidade de que o terceiro seja reconhecido como o verdadeiro titular dos dados expostos.

7.73. Portanto, a falta de cuidado no desenvolvimento de um sistema adequado aos requisitos exigidos pela LGPD permitiu que o incidente de segurança ocorresse, o que oportuniza a potencial afetação dos interesses e direitos fundamentais dos titulares de forma significativa.

7.74. **Conclui-se que os requisitos previstos no art. 8º, §2º, do Regulamento de Dosimetria são verificados na infração ao art. 49 da LGPD ora analisada, para ser classificada como média.**

7.75. Além disso, no presente caso, a infração versa sobre tratamento de dados pessoais em larga escala, conforme explicado no item [7.32]. Adicionalmente, não foi afastada a potencialidade de os dados envolverem dados de crianças, adolescentes e idosos, conforme explicitado no item [7.33]. Essas características elevam o grau de classificação da infração que, por esse motivo, **passa a ser considerada como grave, segundo art. 8º, §3º, I, "a" e "d", do Regulamento de Dosimetria**.

Definição do tipo de sanção administrativa

7.76. Para a definição do tipo de sanção adequada, o art. 9º do Regulamento de Dosimetria indica que a sanção de advertência pode ser aplicada quando a infração for leve ou média, ou quando houver necessidade de imposição de medidas corretivas. Esta hipótese se aplica à presente infração, tendo em vista a necessidade de impor ao infrator medida corretiva frente à ausência de adequação da estrutura de seus sistemas aos ditames do art. 49 da LGPD.

7.77. **Aplica-se, portanto, a sanção de advertência, cumulada com medida corretiva.**

7.78. Tendo em vista o relatado acima, impõe-se a seguinte medida corretiva, acompanhada de suas comprovações:

1) Envio de informações sobre o andamento de medidas técnicas que estão em curso no sistema SCPA, em especial quanto i) aos registros (logs) de acesso à API afetada e volume de consultas realizadas ao sistema SCPA; ii) à implementação da ferramenta relacionada à verificação de vulnerabilidades relatada no item 2.3.3 da Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503) e iii) às ações de melhoria que foram suscitadas na Nota Técnica nº 17/2022 (0045589), conforme item [5.11] deste Relatório de Instrução, mediante apresentação de um cronograma de implementação, com a especificação das etapas a serem adotadas, caso aplicável.

a) A fim de se comprovar o cumprimento desta medida corretiva, o MS deve juntar aos autos, **no prazo de 20 (vinte) dias úteis** da data de intimação do Despacho Decisório, documento (e.g. planilha, documento escrito de forma digital, apresentação de slides etc.) em que conste: i) a previsão das etapas do cronograma e ii) a forma por meio da qual se comprovará o cumprimento de cada uma das etapas.

b) O prazo de cumprimento de todas as etapas previstas no cronograma não deverá ultrapassar 100 (cem) dias úteis, contados da data de intimação do Despacho Decisório.

2) Subsidiariamente, caso alguma medida técnica citada no item [7.78], 1), caput, já tenha sido cumprida, determina-se a juntada de comprovação dos elementos supracitados no item [7.78], 1), caput, que poderá ser realizada através de declaração assinada pela autoridade máxima do ministério e juntada aos autos, **no prazo de 20 (vinte) dias úteis** da data de intimação do Despacho Decisório.

Da impossibilidade de afastamento das sanções

Atendimento ao princípio da proporcionalidade e da atuação responsiva da ANPD

7.79. Em suas Alegações Finais (0098399), o autuado requereu o afastamento das sanções relativas aos arts. 48 e 49 da LGPD, em observância ao princípio da proporcionalidade como corolário de uma atuação responsiva da ANPD, conforme disposto no art. 17 do Regulamento de Fiscalização[21] e no art. 27 do Regulamento de Dosimetria[22].

7.80. Nesse sentido, ressalta-se que a CGF, no âmbito de sua

atividade de fiscalização, instaurou o presente Processo Administrativo Sancionador **na medida em que não obteve resposta satisfatória do autuado, entre outras, quanto i) à realização de CIS aos titulares nos prazos determinados**, nos termos do art. 48 da LGPD (itens [7.12] e [7.13]) e **ii) às medidas de segurança adotadas no sistema utilizado no tratamento dos dados pessoais** em questão, nos termos do art. 49, da LGPD (item [7.53]).

7.81. Ressalta-se que a atuação responsiva da ANPD ocorreu ao longo de toda sua atuação frente ao regulado; no entanto, a postura não colaborativa do autuado culminou na atividade repressiva da ANPD. A fim de analisar a observância ao princípio da proporcionalidade da imposição das sanções, serão destacados seus três principais fundamentos: adequação, necessidade e proporcionalidade em sentido estrito.

Adequação

7.82. A adequação das sanções a serem aplicadas encontra fundamento no seu caráter preventivo, educativo, repressivo[23] e dissuasório[24].

7.83. No que diz respeito à violação ao art. 48 da LGPD, a sanção visa a i) prevenir que esse comportamento ocorra novamente, reafirmando que os prazos declarados pela CGF no âmbito do processo fiscalizatório são cogentes; ii) corrigir a CIS realizada aos titulares, a fim de que esta seja apresentada em plena conformidade ao disposto no art. 48, §1º, da LGPD, conforme visto no tópico de "Definição do tipo de sanção administrativa"; bem como iii) censurar a violação efetuada e concretizada frente ao artigo 48 do referido diploma legal.

7.84. Já no que diz respeito à violação ao art. 49 da LGPD, a sanção visa a i) prevenir que isto aconteça novamente, enfatizando a importância de se ter controle sobre o que ocorre nos sistemas do autuado; ii) requisitar a comprovação ou implementação das medidas corretivas que estavam em curso pelo autuado e que foram sugeridas como pontos de melhoria na Nota Técnica nº 17/2022 (0045589), bem como iii) censurar a violação efetuada frente ao artigo 49 do referido diploma legal.

Necessidade

7.85. A aplicação das sanções revela-se necessária em razão de não haver outro meio menos gravoso compatível às infrações cometidas, que viabilize, a uma só vez, a prevenção de riscos futuros relacionados à ausência de i) comunicação a titulares de incidentes de segurança e ii) medidas de segurança em sistemas que envolvam dados pessoais; a proteção da vigência e compulsoriedade das normas; a correção das infrações, bem como a censura das condutas[25].

7.86. Em relação à sanção ao art. 48, da LGPD, a necessidade de sua aplicação figura como o ápice do escalonamento de determinações e medidas que foram requisitadas pela ANPD frente à inércia do autuado em comprovar nos autos a comunicação do incidente aos titulares ou ao menos justificar, à época dos fatos, de forma plausível, o descumprimento da obrigação de realizar a CIS aos titulares mesmo após as determinações da CGF. Portanto, a sanção, como meio mais gravoso, somente sobreveio à discussão após o envio, pela CGF, de i) E-mails que buscavam o melhor entendimento do incidente de segurança (0045594, 0045595 e 0045596), ii) Despacho com a determinação de CIS aos titulares (0045604) e iii) Aviso de reiteração da determinação de CIS (0045608), como medida preventiva, (itens [5.13], [5.14], [5.19], [5.20] e [5.21]).

7.87. Nesse mesmo sentido, a sanção referente ao art. 49 da LGPD somente sobreveio à discussão após o escalonamento de medidas de contato da CGF com o autuado, por meio de i) E-mails que buscavam o melhor entendimento do incidente de segurança (0045594; 0045595 e 0045596), ii) Despacho com pedidos de esclarecimento sobre quais dados e quantos titulares foram potencialmente afetados, bem como quais medidas de segurança teriam sido adotadas antes da ocorrência do incidente (0045604) e iii) Aviso de reiteração das determinações requeridas no Despacho 0045604, como medida preventiva (0045608).

Proporcionalidade em sentido estrito

7.88. Conforme prevê o Regulamento de Fiscalização, a atuação responsiva da Autoridade considera a postura dos agentes regulados e os riscos identificados para a adoção de medidas proporcionais – dentre elas, a aplicação de sanções.

7.89. Quanto à **postura do autuado**, percebe-se que este falhou em colaborar com a Autoridade, na medida em que as tentativas de diálogo do regulador não foram correspondidas e, portanto, escalaram gradualmente para instrumentos mais interventivos, conforme visto nos itens [7.81], [7.86] e [7.87].

7.90. No que tange aos **riscos identificados**, a ausência de comunicação de incidente de segurança ao titular atraiu para o autuado o risco de ter impedido o titular de adotar medidas para evitar riscos ou danos provenientes do incidente, conforme supracitado nos itens [7.29] e [7.30]. Ademais, como será melhor explorado no tópico *"Primazia dos efeitos da sanção sobre os efeitos reputacionais ao órgão. Inaplicabilidade do princípio da intranscendência subjetiva das sanções"*, a ausência da CIS aos titulares, nos termos do art. 48, §1º, LGPD, também move ao autuado o risco de impedir o exercício da autodeterminação informativa dos titulares (art. 2º, II, da LGPD), uma vez que o titular não tem conhecimento do fluxo de seus dados e dos

possíveis riscos aos quais foi exposto.

7.91. Além disso, embora não tenha sido avaliada a necessidade de recebimento de todos os dados compartilhados pela RFB, é possível afirmar que o autuado, no mínimo, assumiu o risco de não adotar medidas de segurança suficientes para receber e armazenar dados pessoais de titulares com os quais sequer possuía uma relação prévia, já que os dados que poderiam ser acessados referiam-se àqueles que não possuíam cadastro no sistema do DATASUS, mas sim na RFB. Somado a isso, a ausência de adoção de um sistema estruturado em consonância ao previsto no art. 49 da LGPD atrai para o autuado o risco de ocorrer acessos indevidos a dados de modo indiscriminado quando opta por não adotar medidas de segurança suficientes para proteger seu sistema por meio de controles e monitoramento de acesso e consumo, bem como de testes de vulnerabilidade. Demonstrada, portanto, a proporcionalidade da aplicação das sanções de advertência frente à postura do autuado e aos riscos (mais eminentes) relacionados às infrações em questão.

7.92. Quanto à ponderação da proporcionalidade em sentido estrito especificamente diante da sanção imposta frente à violação ao art. 48 da LGPD, reconhece-se que a CIS foi realizada, ainda que intempestivamente. Entretanto, tal fato não impede que a sanção seja aplicada, uma vez que os titulares não tiveram conhecimento do incidente em prazo razoável – consoante preceitua o art. 48 da LGPD –, tendo sido efetuada após dois meses da primeira determinação da CGF[26] (ver item [7.13]). O prolongado período entre o recebimento da denúncia sobre o incidente, a determinação da CGF para o autuado realizar a CIS e a efetuação, de fato, da CIS aos titulares pode ter privado titulares de adotarem medidas para evitar ou mitigar os potenciais riscos ou danos decorrentes do incidente.

7.93. Além disso, a CIS no sítio eletrônico (documento SEI 0136279)[27] não incluiu em seu conteúdo as informações mínimas elencadas pelo art. 48, §1º, da LGPD. Deste modo, a aplicação da sanção, somada a uma medida corretiva, ainda tem por objetivo a correção da CIS aos titulares, de maneira que sejam prestadas a estes as informações devidas sobre a ocorrência do evento adverso.

7.94. Quanto à ponderação da proporcionalidade em sentido estrito especificamente diante da sanção imposta frente à violação ao art. 49 da LGPD, reconhece-se o desenvolvimento significativo de providências tomadas pelo autuado após a ocorrência do incidente de segurança, conforme apontado nos itens [7.47] e [7.49]. Entretanto, isto não impede que a sanção seja aplicada, uma vez que houve uma falha na garantia do direito à proteção dos dados tratados dos titulares no sistema SCPA antes da adoção de tais medidas, em especial porque a estrutura do sistema, à época do incidente,

era insuficiente para garantir a devida segurança das operações de tratamento de dados pessoais realizadas pela entidade, o que vai de encontro ao art. 49, da LGPD, conforme já demonstrado.

7.95. Cabe destacar, ademais, que, mesmo que i) a CIS aos titulares tivesse sido efetuada em total alinhamento com o determinado no art. 48, §1º, da LGPD e ii) já houvesse a confirmação e comprovação de que todos as providências cabíveis de adequação da estrutura do sistema já tivessem sido efetuadas, em total alinhamento com o determinado no art. 49 da LGPD, e, portanto, não fosse necessária a imposição de medidas corretivas, a CGF ainda entenderia ser a gravidade das infrações proporcional à aplicação das infrações de advertência, **a mais branda** prevista no art. 52, da LGPD. Este posicionamento já foi explicitado[28], inclusive, na Análise de Impacto Regulatório que precedeu o Regulamento de Dosimetria - Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

7.96. Tal ponto corrobora com o fato de que a ANPD impôs medida proporcional à postura do autuado e aos riscos identificados, em consonância à atuação responsiva da Autoridade, como disposto no art. 17, do Regulamento de Fiscalização, precisamente por existirem sanções mais graves frente a violações à LGPD.

7.97. Diante do exposto, verifica-se o **tríplice fundamento do princípio da proporcionalidade[29], em consonância a uma atuação responsiva da ANPD para a aplicação das sanções administrativas de advertência cumuladas com medidas corretivas em face das violações aos arts. 48 e 49 da LGPD.**

Primazia dos efeitos da sanção sobre os efeitos reputacionais ao órgão. Inaplicabilidade do princípio da intranscendência subjetiva das sanções

7.98. A aplicação das sanções indicadas nos tópicos anteriores decorre da própria leitura do art. 52, da LGPD, ao sujeitar os agentes aos tipos de sanções discriminadas no referido artigo, quando da verificação de infrações cometidas às normas da LGPD. No caso presente, foram esclarecidos todos os fatos e provas que levaram à conclusão das violações aos arts. 48 e 49, da LGPD.

7.99. Neste sentido, não se vislumbra, como requerido pelo MS, o afastamento de sanções que recaem sobre condutas violadoras às previsões da LGPD sob o argumento de que o infrator poderá suportar efeitos reputacionais negativos. De forma diversa ao que o autuado faz crer, o objetivo das sanções supracitadas não se resume à provocação de “intensos efeitos negativos reputacionais” (item 3.31 das Alegações Finais [0098399]).

7.100. Além de as sanções apresentarem seus vieses preventivo, educativo, repressivo e dissuasório, consoante supracitado no item [7.82], no presente caso, os efeitos das sanções cumuladas com as medidas corretivas

sobrepujam o efeito reputacional negativo para o autuado. Isso, porque as sanções visam a estimular a observância ao princípio da responsabilização e prestação de contas (art. 6º, X, da LGPD), bem como a propiciar o exercício da autodeterminação informativa dos titulares (art. 2º, II, da LGPD), elementos pilares da proteção de dados pessoais.

7.101. Tendo em vista que a potencial aplicação de sanção já era de conhecimento da sociedade, como foi reconhecido pelo autuado (item 3.31 das Alegações Finais [0098399]), a sua concretização e o consequente reconhecimento da ocorrência das infrações pelo Ministério da Saúde são uma oportunidade para o autuado demonstrar as medidas de adequação técnicas e administrativas adotadas (ou em curso) posteriormente ao incidente, o que poderá causar o efeito oposto ao suscitado, alinhando-se aos fundamento e princípio supracitados no item [7.100], por dois motivos principais.

7.102. Em primeiro lugar, porque esta postura do regulado estaria em consonância com o princípio da responsabilização e prestação de contas, nos termos do art. 6º, X, da LGPD. Nesse sentido, leciona Miriam Wimmer:

> Merece também exame mais aprofundado o princípio da "responsabilização e da prestação de contas" (...).
>
> Apesar de sua relativa imprecisão conceitual e da dificuldade de traduzir o termo para outros idiomas, trata-se de ideia frequentemente associada à ideia de regulação responsiva ou de corregulação, e, ainda, à noção de uma abordagem baseada em riscos (*risk-based approach*), **uma vez que atribui ao próprio agente regulado a responsabilidade por adotar e demonstrar a efetividade de medidas técnicas e organizacionais para prevenir eventuais tratamentos irregulares**[30]. (Grifamos)

7.103. Veja-se que, ao passo em que se assume a responsabilidade pelo cometimento das infrações passadas, oportuniza-se a chance de informar a adoção de medidas técnicas e administrativas a partir do incidente, a fim de prevenir que outras situações semelhantes voltem a ocorrer – esforço este que será, inclusive, reconhecido pela CGF, nos itens de [7.115] a [7.117] abaixo. Tendo isto em vista, trata-se de cenário propício ao fortalecimento da credibilidade do referido órgão autuado frente aos titulares potencialmente afetados, em claro atendimento ao fim público a que se destinam as sanções impostas face aos dispositivos infringidos.

7.104. Em segundo lugar, porque tal medida possibilita o exercício da autodeterminação informativa dos titulares (art. 2º, II, da LGPD), uma vez que é concedida aos titulares a ciência dos termos requeridos no art. 48, §1º, da LGPD, em decorrência da ausência de medidas de segurança no sistema do autuado que geraram o incidente de segurança (art. 49 da LGPD).

7.105. Isso decorre do fato de que o reconhecimento do incidente de

segurança e da causa geral de sua ocorrência - a ausência de mecanismos de segurança no sistema SCPA - facilita a participação do próprio titular no controle de seus dados, ao permitir que ele tome medidas que julgue necessárias para se precaver quanto a eventuais consequências negativas advindas do incidente, bem como esteja ciente do tratamento e fluxo informacional atribuído a seus dados pessoais. Este desdobramento da autodeterminação informativa foi recentemente ressaltado no voto do Juiz Rodrigo Mudrovitsch, no caso *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia,* julgado na Corte Interamericana de Direitos Humanos, em outubro de 2023, ocasião em que se reconheceu, no âmbito do sistema interamericano de proteção de direitos humanos, a autodeterminação informativa como direito autônomo:

> No entanto, embora sejam interdependentes, há três diferenças cruciais[31] que nos permitem depreender da Convenção dois direitos humanos autônomos. Primeiramente, o âmbito de proteção da autodeterminação informativa recai sobre o agente: ele abrange o poder de controle do indivíduo sobre os seus dados pessoais. Há, nesse sentido, uma maior ênfase na autonomia da pessoa humana, e não na esfera, privada ou não, a que pertencem os dados relativos ao indivíduo em questão[32]. O poder de controle do indivíduo sobre seus dados pessoais desdobra-se tanto (i) no seu poder de tomar decisões quanto ao tratamento das informações, por exemplo, fornecendo ou não o consentimento, quanto (ii) **o controle das informações em si, que se concretiza a partir da transparência sobre diversos aspectos do tratamento, os quais ajudam a calibrar a legítima expectativa do indivíduo sobre o fluxo informacional dos seus dados**. Nesse sentido, a autodeterminação informativa também é garantida quando, apesar de o indivíduo não concordar diretamente com o tratamento, por não se tratar de hipótese de coleta de consentimento, **ele tem acesso às informações sobre como seus dados são tratados**. Assim, transcendendo a ideia de privacidade como mera liberdade negativa, adota-se a ideia de autodeterminação informativa como direito positivo, que confere ao titular protagonismo nas decisões relacionados ao fluxo de dados, exigindo sua participação ativa e conferindo-lhe o direito de desenvolver livremente a sua personalidade[33]. (Grifamos)

7.106. Compreender a função da proteção de dados pessoais também perpassa o reconhecimento de que um dos seus objetivos é "oferecer instrumentos para que os cidadãos possam exercer a autodeterminação informativa quanto a seus dados pessoais"[34]. Assim, a aplicação das sanções com as medidas corretivas reforça o papel do autuado em contribuir com o exercício da autodeterminação informativa do titular.

7.107. Em consonância a todos os argumentos expostos, tampouco aplica-se, no caso em concreto, a razão fundamental do princípio da intranscendência subjetiva, como arguido pelo autuado. Inicialmente, cabe

destacar que o referido princípio foi aplicado pelo Supremo Tribunal Federal (STF) e pelo Superior Tribunal de Justiça (STJ) em contextos diversos da presente hipótese, importando em medidas restritivas a recursos financeiros/participações em convênios, entre outras consequências decorrentes da inscrição de ente federativo em cadastros de inadimplentes[35].

7.108. Ainda que assim não fosse, o recente entendimento do STF[36] é de que tampouco tal previsão deve ser acolhida em casos de mudança de gestão governamental. Confira-se voto proferido pelo Ministro Gilmar Mendes no julgamento da ACO 2745/DF, oportunidade em que foi ressaltado que a aplicação do princípio da intranscendência subjetiva tratar-se-ia de hipótese antirrepublicana e incoerente ao Estado de Direito:

> A Lei de Responsabilidade Fiscal (LRF) não deve ser aplicada de forma limitada ao mandato dos gestores do Poder Executivo, haja vista ser **antirrepublicano e incoerente ao Estado de Direito a hipótese de se apagar o passado por simples mudança de governante, no mínimo, a cada quatro anos.**
>
> [...]
>
> Importante salientar que, ao mesmo tempo em que o gestor não pode ser pessoalmente responsabilizado por irregularidades cometidas outrora pelo Ente Federativo, **este deve suportar as sanções decorrentes de sua atuação ilegal**, seja no passado remoto ou próximo ou mesmo no presente, como corolário do princípio republicano.
>
> É claro que não pode haver punição do gestor, individualmente considerado, que não tenha participado ativa ou passivamente para a consecução da ilicitude.
>
> Nesse caso, a **responsabilidade deve recair sobre o Estado-Membro, enquanto responsável pela atuação de seus governantes passados,** uma vez que não pode existir a incidência das sanções previstas nas disposições da Lei de Responsabilidade Fiscal apenas a cada gestão, tal como se **findassem as práticas anteriores e se reiniciassem as relações jurídicas**.[37] (Grifamos)

7.109. Importa mencionar que o posicionamento recente do STF se coaduna ao entendimento desta Autoridade na medida em que a responsabilidade das infrações, no caso concreto, recai **sobre a pessoa jurídica na qualidade de controladora dos dados pessoais**, **não sobre as "pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta",** como explicitado no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, publicado em abril de 2022[38]. Desta forma, neste caso, cabe à Autoridade aplicar sanções à pessoa jurídica considerada como controladora, cujas obrigações típicas de controlador, recaem sobre o Ministério da Saúde, conforme mencionado no

item 6.2, não à gestão ou gestores do Ministério quando da ocorrência da infração.

7.110. Ademais, a relação jurídica do controlador com o titular não termina, necessariamente, com a mera alteração de gestão governamental. Entendimento diverso pressuporia que os direitos dos titulares de dados fossem restringidos a cada troca de governo. Não foram demonstradas, no caso em concreto e em razão das sanções a serem aplicadas, restrições que incorressem em empecilhos à execução de políticas públicas ou a benefícios da coletividade, como outrora suscitados em julgados dos referidos Tribunais Superiores; pelo contrário, conforme supracitado, há diversos efeitos benéficos aos titulares de dados (itens [7.100] a [7.106]), que decorrem da implementação das determinações suscitadas durante o processo de fiscalização prévio e do presente processo sancionador.

7.111. Alinhado a isso, a garantia do interesse público e fim público também foram preservados no caso, ao contrário do que faz crer o autuado ao afirmar que a aplicação da sanção, em 2024, por infração ocorrida em 2021, em "outro Governo", não seria razoável, violando-se o art. 39, VI, do Regulamento de Fiscalização. Isso, pois a interpretação dos dispositivos deve considerar a observância do interesse público primário sobre o interesse público secundário. Conforme suscitado no Relatório de Instrução nº 01/2024/CGF/ANPD (itens 6.4.25. a 6.4.36.), no âmbito do PAS nº 00261.001888/2023-21, esta CGF já esclareceu que o interesse público primário, como interesse de toda a sociedade, é o próprio parâmetro para a ponderação, em oposição ao interesse público secundário, interesse este último que o autuado pretende proteger ao defender o afastamento da sanção tendo em vista o transcurso do tempo, a potencial desconfiança da população e a mudança de gestão governamental.

7.112. Nesse sentido, leciona Barroso (2024)[39] sobre o interesse público primário:

> O interesse público primário, consubstanciado em valores fundamentais como justiça e segurança, há de desfrutar de supremacia em um sistema constitucional e democrático. **Deverá ele pautar todas as relações jurídicas e sociais** – dos particulares entre si, deles com as pessoas de direito público e destas entre si. O **interesse público primário desfruta de supremacia porque não é passível de ponderação; ele é o parâmetro da ponderação**. Em suma: o interesse público primário consiste na melhor realização possível, à vista da situação concreta a ser apreciada, da vontade constitucional, dos valores fundamentais que ao intérprete cabe preservar ou promover.

7.113. Portanto, em dissonância ao pretendido pelo autuado na hipótese presente, trata-se de proteger o interesse público da sociedade em

ver garantidos, em especial, i) a proteção de seus dados pessoais em sistemas adequados aos requisitos de segurança que diminuam os riscos de incidentes de segurança (item [7.91]), bem como ii) o recebimento da comunicação do incidente de segurança aos titulares, que possibilita, entre outros, a diminuição de riscos e danos decorrentes do incidente e propicia o exercício da autodeterminação informativa (item [7.90]).

7.114. Diante do exposto, não há que se falar em inaplicabilidade das sanções à pessoa jurídica do MS, em razão de i) potenciais efeitos reputacionais ao autuado e ii) atos praticados por gestão diversa da presente, tendo em vista que não foram suscitados argumentos e provas capazes de afastar a autoria e materialidade do autuado das violações aos arts. 48 e 49, da LGPD.

Adoção de medidas para adequação à LGPD

7.115. Conforme indicado na Nota Técnica nº 106/2022-CGIE/DATASUS/SE/MS (0050503), que acompanhava a Defesa Administrativa (0050502), o MS informou que teria implementado algumas medidas, tais como XXXXX . Também foi citada a existência das seguintes infraestruturas de controles de segurança: XXXXX [ACESSO RESTRITO - trechos sombreados são de acesso restrito ao autuado – detalhamento do incidente de segurança, de medidas de segurança implementadas em sistema ou de características de funcionamento de sistema – art. 13, II, do Decreto nº 7.724/2012].

7.116. Ademais, em Alegações Finais (0098399), o autuado informou que foram implementadas 6 (seis) medidas administrativas relacionadas à: i) proteção de dados no Ministério da Saúde - criação da Secretaria de Informação e Saúde Digital no Ministério da Saúde; ii) designação de nova Encarregada de Dados e publicação no sítio eletrônico; iii) criação de Grupo de Trabalho para tratar especificamente sobre a LGPD; iv) obtenção de assento para futura composição no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD); v) realização da 1º Jornada de Proteção de Dados Pessoais no SUS, vi) adoção do Programa de Privacidade e Segurança da Informação (PPSI), e que mais 1 (uma) medida estaria em andamento, relacionada à capacitação para servidores das unidades descentralizadas do MS e do SUS, conforme descrito nos tópicos de A) a G) do item 3.24 das Alegações Finais (0098399).

7.117. Reconhecendo-se os esforços empreendidos pelo autuado para a cessação da vulnerabilidade da API, que permitia a exposição de dados contidos no sistema SCPA, bem como as providências já implementadas e em andamento quanto à adoção de mecanismos administrativos e técnicos (itens [7.47] e [7.49]), consideram-se ausentes a conveniência e a oportunidade de encaminhar notícia ao órgão de controle interno do autuado para apuração de eventual falta funcional, nos termos do art. 55-J, XXII, da LGPD.

8. CONCLUSÃO

8.1. Ante o exposto, considerando que o conjunto probatório demonstra que a autoria e a materialidade restam devidamente comprovadas nos autos, e que os fatos descritos correspondem às infrações tipificadas pelos enquadramentos indicados no Auto de Infração nº 8/2022/CGF/ANPD (0050494), conclui-se pelas seguintes recomendações, nos termos do art. 55, §2º, do Regulamento de Fiscalização:

8.1.1. Por violação ao art. 48 da LGPD, a aplicação da sanção de ADVERTÊNCIA ao Ministério da Saúde, com a imposição de 1 (uma) medida corretiva, acompanhada de suas comprovações, nos termos dos itens [7.37] e [7.38] deste Relatório de Instrução.

8.1.2. Por violação ao art. 49 da LGPD, a aplicação da sanção de ADVERTÊNCIA ao Ministério da Saúde, com a imposição de 1 (uma) medida corretiva, acompanhada de suas comprovações, nos termos do item [7.78] este Relatório de Instrução.

8.2. Por fim, é importante registrar que a classificação das infrações, a definição das sanções e a adoção de medidas corretivas restringem-se às circunstâncias deste caso em concreto e não vinculam a análise e o posicionamento da CGF em futuros processos sancionadores.

9. ENCAMINHAMENTOS

9.1. O presente Relatório de Instrução deve ser encaminhado ao Coordenador-Geral de Fiscalização para decisão, de acordo com art. 55 do Regulamento de Fiscalização.

9.2. Em razão do comunicado enviado pela Receita Federal do Brasil a esta ANPD, conforme indicado no item [5.2], sugere-se que este Relatório de Instrução e o posterior Despacho Decisório sejam remetidos à RFB no âmbito do Processo de CIS nº 00261.000938/2022-72.

9.3. Após proferida a decisão, o autuado deverá ser intimado para cumprimento da sanção e/ou apresentação de recurso, em até 10 dias úteis, em consonância com o art. 58 do Regulamento de Fiscalização.

9.4. A decisão deve ser publicada no DOU, segundo o art. 55 do Regulamento de Fiscalização.

9.5. Após trânsito em julgado, este Processo Administrativo Sancionador deverá ser encaminhado para a fase de cumprimento da decisão para acompanhamento das obrigações de fazer determinadas.

À consideração superior.

GABRIELLA VIEIRA OLIVEIRA GONÇALVES
Especialista em Politicas Públicas e Gestão Governamental

De acordo. Encaminhe-se.

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA
Coordenador de Fiscalização

_____

[1] Este Relatório de Instrução foi elaborado com a colaboração de **SAYURI PACHECO HAMAOKA**, assistente desta Coordenação-Geral de Fiscalização.

[2] Conforme publicizado no site do Ministério da Saúde e colacionado aos autos (0095694). Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/encarregado-pelo-tratamento-de-dados-pessoais. Acesso em 30 jul 2024.

[3] Conforme publicizado no site do Ministério da Saúde e colacionado aos autos (0095694). Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/encarregado-pelo-tratamento-de-dados-pessoais. Acesso em 30 jul 2024.

[4] De acordo com o OFÍCIO Nº 24/2024/SEIDIGI/CGOEX/SEIDIGI/MS (0095694).

[5] Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais. Acesso em 30 jul 2024. Disponível também em: Ver Documento SEI nº 0136279.

[6] Conforme informado pelo Serviço Federal de Processamento de Dados (SERPRO) ao Tribunal de Contas da União (TCU), em 2020. Consultar o Processo nº 016.834/2020-8, tramitado no âmbito do TCU. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/KEY:ACORDAO-COMPLETO-2416107/NUMACORDAOINT%20asc/0. Acesso em 30 abr 2024.

[7] A CIS aos titulares foi realizada em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais.

[8] O Regulamento de Comunicação de Incidente de Segurança (RCIS), Resolução CD/ANPD nº 15, de 24 de abril de 2024, entrou em vigor na data de

sua publicação, em 26 de abril de 2024. O RICIS está disponível no link https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

[9] Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 30 abr 2024. Ademais, o recente publicado Regulamento de Comunicação de Incidente de Segurança (RCIS) reforça os atributos de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais ao mencionar os atributos de sistemas a serem considerados nas medidas para reverter ou mitigar os efeitos de incidentes de segurança (art. 19, §7º).

[10] Teor da comunicação: "**Período do incidente**: 27/11/2021 a 04/05/2022. **Natureza dos dados potencialmente expostos**: Foi identificado risco de acesso indevido ao SCPA. A referida falha permitiria a consulta individual, a partir do número do CPF, aos seguintes dados pessoais: nome completo, endereço, telefone, data de nascimento, nome da mãe e cartão nacional de saúde (CNS). **Comunicação do incidente aos titulares de dados**: O Ministério da Saúde, em cumprimento ao disposto no art. 48 da Lei 13.709/2018 (LGPD), comunica aos titulares que, ao tomar conhecimento do incidente de segurança envolvendo risco de acesso indevido a dados pessoais, desabilitou emergencialmente a aplicação e realizou manutenção corretiva na falha identificada. Não houve comprovação de efetivo acesso indevido ao sistema e, consequentemente, aos dados cadastrais. Caso queira solicitar mais informações referentes ao incidente de segurança, acesse a Plataforma Fala.BR." Ver Documento SEI nº 0136279. Disponível também em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais. Acesso em 30 abr 2024.

[11] Ver nota de rodapé nº 10.

[12] Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em:
I - leve;
II - média; ou
III - grave.
[...]
§ 2º A infração será considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave.

[13] Julgados nesse sentido constam nos Relatórios de Instrução nº 2/2023, nº 4/2023, nº 1/2024 e nº 2/2024, respectivamente nos processos 00261.001969/2022-41, 00261.001886/2022-51 e 00261.001192/2022-14.

[14] Julgado nesse sentido consta no Relatório de Instrução nº 3/2024/FIS/CGF, no processo 00261.001963/2022-73.

[15] Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 30 abr 2024.

[16] Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em:
I - leve;
II - média; ou
III - grave.
§ 3º A infração será considerada grave quando:
I - verificada a hipótese estabelecida no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes:
a) envolver tratamento de dados pessoais em larga escala, caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado;
[...]
d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos;

[17] Art. 10. A ANPD aplicará a sanção de multa simples quando:
I - o infrator não tenha atendido as medidas preventivas ou corretivas a ele impostas, dentro dos prazos estabelecidos, quando aplicável;
II - a infração for classificada como grave;

[18] Art. 9º. A ANPD poderá aplicar a sanção de advertência quando:
I - a infração for leve ou média e não caracterizar reincidência específica; ou
II - houver necessidade de imposição de medidas corretivas.

[19] Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais. Acesso em 30 abr 2024.

[20] Por este ponto de vista: “Nesse sentido, a segurança que se espera não é aplicada exatamente aos dados em si, mas sim aos sistemas que os mantêm (medidas técnicas) e ao ambiente geral da instituição (medidas organizativas). Isso significa que não bastam as medidas técnicas, como o uso de firewalls, métodos criptográficos e controles de conteúdo, se elas não vierem acompanhadas de outras medidas, como treinamentos de segurança, criação de políticas de segurança da informação, inventários de ativos etc.”. MENKE, Fabiano; GOULART, Guilherme. **Segurança da informação e vazamento de**

dados. In: BIONI, Bruno; DONEDA, Danilo; JUNIOR, Otavio Luiz Rodrigues; MENDES, Laura Schertel; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2023, p. 348.

[21] Art. 17. O processo de fiscalização da ANPD observará as seguintes premissas:
[...]
IV - atuação de forma responsiva, com a adoção de medidas proporcionais ao risco identificado e à postura dos agentes regulados;

[22] Art. 27. A ANPD poderá afastar a metodologia de dosimetria de sanção de multa ou substituir a aplicação de sanção por outra constante neste Regulamento, nos casos em que for constatado prejuízo à proporcionalidade entre a gravidade da infração e a intensidade da sanção, observado o disposto no inciso XI do §1º do art. 52 da LGPD, neste Regulamento e nas demais normas aplicáveis.

[23] ANPD. **Relatório de Análise de Impacto Regulatório - Construção do modelo regulatório previsto na LGPD com relação à aplicação de sanções administrativas e às metodologias de cálculo do valor-base das sanções de multa**, Brasília, 2021, p. 77; OSÓRIO, Fábio Medina. **Direito Administrativo Sancionador**. 5ª ed. São Paulo: Thomson Reuters Brasil, 2023, p. 211.

[24] ARANHA, Márcio Iorio. **Manual de Direito Regulatório: Fundamentos de Direito Regulatório**. 8ª ed. rev. ampl. Londres: Laccademia Publishing, 2023, p. 144; e KOLIEB, Jonathan. **When to Punish, When to Persuade and When to Reward: Strengthening Responsive Regulation with the Regulatory Diamond**. Monash University Law Review. Vol. 41(1), 2015, p. 150. Disponível em: https://ssrn.com/abstract=2698498. Acesso em 22 abr 2024.

[25] OSÓRIO, Fábio Medina. **Direito Administrativo Sancionador**. 5ª ed. São Paulo: Thomson Reuters Brasil, 2023, p. 26.

[26] Julgados nesse sentido constam nos Relatórios de Instrução nº 2/2023, nº 4/2023 e nº 2/2024, respectivamente nos processos 00261.001969/2022-41, 00261.001886/2022-51 e 00261.001192/2022-14.

[27] Disponível também em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd/registro-de-incidentes-com-dados-pessoais. Acesso em 30 abr 2024.

[28] Veja-se: “Ao debruçar-se sobre o art. 52 da LGPD, pode-se interpretar que a aplicação da sanção de advertência deveria estar condicionada à determinação de adoção de medidas corretivas com indicação de prazo para seu cumprimento”. **No entanto, se tal condição fosse obrigatória, para os casos em que não houvesse a necessidade de adoção de medidas corretivas, principalmente para aqueles em que o infrator já corrigiu a conduta inadequada, a ANPD estaria impedida de aplicar a sanção de advertência, a**

mais branda dentre as estabelecidas no rol do art. 52. Tal medida soaria desproporcional quando comparada com a situação em que o infrator não corrigiu a conduta, permanecendo em descumprimento legal, em que a ANPD poderia aplicar a sanção de advertência com a determinação de adoção de medidas corretivas".

[29] FILHO, José dos Santos C. **Manual de Direito Administrativo**. 38ª ed., rev., atual. e ampl. Barueri: Atlas, 2024, p. 36; BRANCO, Paulo Gustavo G. Teoria Geral Dos Direitos Fundamentais. In: MENDES, Gilmar F.; BRANCO, Paulo Gustavo G. **Curso de direito constitucional**. (Série IDP). 18ª ed. São Paulo: Editora Saraiva, 2023, p. 83.

[30] WIMMER, Miriam. A LGPD e o balé dos princípios: tensões e convergências na aplicação dos princípios de proteção de dados pessoais no setor público. In: FRANCOSKI, Denise. de S. L; TASSO, F. A. (Coords.). **A lei geral de proteção de dados pessoais LGPD: aspectos práticos e teóricos relevantes no setor público e privado**. São Paulo: Revista dos Tribunais, 2021, p. 4.4.

[31] "*MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar: Revista de Ciências Jurídicas, v. 25, n. 4, p. 1–18, 2020. p. 12. As diferenças aqui enunciadas não são exaustivas. A relação entre privacidade e autodeterminação informativa mereceria uma análise muito mais aprofundada do que aquela que a extensão deste voto permite. Ver, nesse sentido, DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Nova Edição. São Paulo, Brasil: Revista dos Tribunais, 2019; SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel Ferreira; DONEDA, Danilo; SARLET, Ingo Wolfgang; et al (Orgs.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2020, p. 21–59. p. 32-33.*"

[32] "*ALBERS, Marion. A complexidade da proteção de dados. Revista Brasileira de Direitos Fundamentais & Justiça, v. 10, n. 35, p. 19–45, 2016. p. 25-26*."

[33] Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506. Voto concurrente del Juez Rodrigo Mudrovitsch, par. 90.

[34] Wimmer, Miriam. Interfaces entre Proteção de Dados Pessoais e Segurança da Informação: um debate sobre a relação entre Direito e Tecnologia em Lei Geral de Proteção de Dados (Lei nº 13.709/2018). In: Cueva, Ricardo Villas Bôas, Doneda, Danilo, MENDES, Laura Schertel (Coords.). **Lei geral de proteção de dados (Lei nº 13.709/2018) [livro eletrônico]: a caminho da efetividade: contribuições para a implementação da LGPD** - 1. ed. - São Paulo: Thomson Reuters Brasil, 2020, p. 8.1.

[35] Os julgados colacionados pelo autuado, inclusive, referem-se a casos

desta situação (itens 3.37 e 3.38 das Alegações Finais [0098399]).

[36] Vide: STF, DJ 16 mar. 2022, ACO 3090 AGR/DF, Voto do Rel. Min. Roberto Barroso; STF, DJ 01 out. 2020, ACO 3402/DF, Rel. Min. Alexandre de Moraes; STF, DJ 17 set. 2020, ACO 3083/DF, Rel. Min. Ricardo Lewandowski.

[37] STF, DJ 26 set. 2017, ACO 2745/DF, Voto do Rel. Min. Gilmar Mendes.

[38] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em 30 abr 2024.

[39] BARROSO, Luís R. **Curso de direito constitucional contemporâneo**. São Paulo: Editora Saraiva, 2024.

Documento assinado eletronicamente por **Gabriella Vieira Oliveira Goncalves, Servidor(a) em Exercício Descentralizado-ANPD**, em 07/08/2024, às 13:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Coordenador(a)**, em 07/08/2024, às 15:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

QRCode Assinatura

A autenticidade deste documento pode ser conferida no site https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **XXXXXXX** e o código CRC **XXXXXXXX**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900
Telefone: (61) 2025-8168 - https://www.gov.br/anpd/pt-br