AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação-Geral de Fiscalização

Brasília, na data de assinatura

DESPACHO DECISÓRIO

Processo Administrativo Sancionador nº 00261.001969/2022-41

Autuado: Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo - Iamspe

Representantes Legais: Maria das Graças Bigal Barboza da Silva -Superintendente e Thaisa Lavra - Encarregada de Dados

O **COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD**, no uso de suas atribuições legais e regulamentares, com fundamento no art. 17, inciso I, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do processo em epígrafe, instaurado em face do **INSTITUTO DE ASSISTÊNCIA AO SERVIDOR PÚBLICO ESTADUAL DE SÃO PAULO - IAMSPE** , inscrito no CNPJ/MF sob o nº 60.747.318/0001-62, em razão dos indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD); e

CONSIDERANDO o teor do Relatório de Instrução nº 2/2023/CGF/ANPD (SUPER nº 4286376), cujas razões acolho e integro à presente decisão, inclusive como motivação, com fulcro no §1º do art. 50 da Lei nº 9.784/1999 c/c o art. 55 e seguintes do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021;

DECIDE:

1. Aplicar ao IAMSPE as sanções de:

2. **ADVERTÊNCIA**, por infração ao art. 48 da LGPD, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor ao IAMSPE a obrigação de:

2.1. Ajustar, no prazo de 10 (dez) dias úteis da data de intimação, o COMUNICADO já existente no sítio do IAMSPE, conforme a redação abaixo:

> Lei Geral de Proteção de Dados Pessoais - Comunicação de Incidente de Segurança:
>
> O Iamspe comunica que tomou conhecimento da ocorrência de incidente de segurança que pode ter comprometido a privacidade dos dados da organização por conta de um acesso não autorizado em dados cadastrais indicados por um usuário externo no início do ano de 2022.
>
> Dentre os dados que poderiam ter sido afetados, estariam dados pessoais cadastrais, salário e de residência de nossa base de cientes, o que poderia acarretar o risco de exposição por um determinado período de tempo até nossas correções, ressaltando-se aqui que não identificamos nem fomos comunicados de extração ocorrida.
>
> Informamos que o Instituto, imediatamente, realizou ações preventivas e corretivas

nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema de cadastro dos seus contribuintes e dependentes. Por conta destas ações, o Instituto comunicou à Autoridade respectiva somente após a realização dos ajustes necessários.

Após comunicação de incidente de segurança à Autoridade Nacional de Proteção de Dados e aos usuários em geral, informamos que estabelecemos um cronograma de ações para melhoria de nossos controles apresentados à ANPD..

Dúvidas, solicitações e reclamações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no telefone: (11) 4573-9352, e-mail: lgpd@iamspe.sp.gov.br

Estamos disponíveis para atendimento de segunda-feira a sexta-feira, das 9h às 17h. Política de Privacidade do Iamspe: http://www.iamspe.sp.gov.br/politica-de-privacidade/.

2.1.1. O IAMSPE deverá juntar aos autos, no prazo de 10 (dez) dias úteis da data de intimação, comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 1 (uma) captura de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura.

2.2. O comunicado acima deve permanecer disponível por 90 (noventa) dias corridos, contados a partir da data de cumprimento do ajuste no Comunicado, nos termos do item 2.1 acima..

2.2.1. O IAMSPE deverá juntar aos autos comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura, sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma.

2.2.2. 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.

3. **ADVERTÊNCIA**, por infração ao art. 49 da LGPD, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor ao IAMSPE a obrigação de:

3.1. Informar à ANPD, neste mesmo processo, o resultado dos programas e objetivos desenvolvidos e implementados, conforme disposto no Anexo V (Plano de três meses e seis meses) das Alegações Finais (SUPER nº 4280896), especificamente quanto aos itens 3, 4, 5, 12, 15 e 17.

3.1.1. Em relação aos itens 3, 4 e 5, o IAMSPE deverá, em até 10 (dez) dias úteis da data da intimação:

a) informar o andamento e apresentar à ANPD o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD; ou

b) em caso de já estarem cumpridos, trazer aos autos comprovação do cumprimento.

3.1.2. Em relação aos itens 12, 15, 17, o IAMSPE deverá apresentar à ANPD, em até 10 (dez) dias úteis da data da intimação, o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD.

4. **Pela intimação do autuado** para cumprimento das sanções e medidas corretivas e/ou apresentação de recurso, em até 10 (dez) dias úteis, em consonância com o art. 56 da Lei nº 9.784/99 c/c o art. 58 do Regulamento de Fiscalização.

5. Aguarde-se o trânsito em julgado. Após, em caso de não cumprimento desta decisão,

encaminhe-se este Processo Administrativo Sancionador para a Procuradoria Federal Especializada - PFE da ANPD para a execução das medidas corretivas.

6. Publique-se no DOU, segundo o art. 55 da Resolução CD/ANPD nº 1/2021.

FABRÍCIO GUIMARÃES MADRUGA LOPES
Coordenador-Geral de Fiscalização

Documento assinado eletronicamente por **Fabricio Guimarães Madruga Lopes**, **Coordenador(a)-Geral**, em 05/10/2023, às 16:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade do documento pode ser conferida informando o código verificador **4374927** e o código CRC **7A3698C3** no site:
https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.001969/2022-41 SUPER nº 4374927

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação-Geral de Fiscalização

RELATÓRIO DE INSTRUÇÃO Nº 2/2023/CGF/ANPD[1]

1. IDENTIFICAÇÃO

1.1. Nome/Razão Social do Autuado: **Instituto de Assistência ao Servidor Público Estadual de São Paulo - IAMSPE.**

1.2. CPF/CNPJ do Autuado: 60.747.318/0001-62

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

1.4. Nome do Encarregado ou Responsável Jurídico: **Maria das Graças Bigal Barboza da Silva - Superintendente e Thaisa Lavra - Encarregada de Dados**

1.5. Contado do Encarregado: **ouvidoria@iamspe.sp.gov.br**

2. REFERÊNCIAS

2.1. Processo SUPER/ANPD nº 00261.001969/2022-41;

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

2.3. Regimento Interno da Autoridade Nacional de Proteção de Dados (RI-ANPD), aprovado pela Portaria nº 01, de 08.03.2021;

2.4. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD (RPF), aprovado pela Resolução CD/ANPD nº 1, de 28.10.2021;

2.5. Regulamento de Dosimetria e Aplicação de Sanções Administrativas (RDASA), aprovado pela Resolução CD/ANPD nº 4, de 24.02.2023;

2.6. Processo SUPER/ANPD nº 00261.000518/2022-96;

2.7. Auto de Infração 12 (SUPER nº 3639487);

2.8. Nota Técnica 79 (SUPER nº 3639508);

2.9. OFICIO Solicitação (SUPER nº 3716064);

2.10. OFICIO Defesa (SUPER nº 3718361);

2.11. Relatório serviço perfis (SUPER nº 3718362);

2.12. Relatório implantação de trilhas (SUPER nº 3718363);

2.13. Relatório sumário sms (SUPER nº 3718364);

2.14. Anexo Comunicado (SUPER nº 3718365);

2.15. OFICIO Comunicação sobre nova Direção do Iamspe (SUPER nº 4085138).

3. SUMÁRIO EXECUTIVO DO PROCESSO

3.1. Número do Auto de Infração: **Auto de Infração nº 12/2022/CGF/ANPD.**

3.2. Data da lavratura do Auto de Infração: 30/09/2022.

3.3. Forma da Intimação: (X) Meio eletrônico ( ) Via postal ( ) Pessoal ( ) Comparecimento pessoal ( ) Por edital ( ) Cooperação internacional ( ) Outro meio

3.4. Dados de quem recebeu a Intimação: Carla Freitas do Nascimento (ex-Chefe de Gabinete do IAMSPE)

3.5. Descrição da Infração: **"Além de não informar adequadamente sobre a natureza dos dados que poderiam ter sido afetados ou a natureza do incidente, não utilizou uma forma adequada para alcançar os titulares. Por esta razão, entende-se que o controlador violou o comando do art. 48 da LGPD, em razão de não ter realizado, no prazo concedido, a comunicação individual à totalidade dos titulares afetados, conforme determinado pela CGF/ANPD, sem que o mesmo tenha apresentado justificativa razoável para proceder de forma diversa."**

3.6. Dispositivo(s) Legal(is) e Regulamentar(es) Infringido(s):

a) **Lei Geral de Proteção de Dados:**

Artigo 48 - ausência de comunicação eficiente de incidente de segurança à autoridade e aos titulares;

Artigo 49 - insuficiência de sistema de segurança para tratamento de dados pessoais.

3.7. Data da Apresentação da Defesa: 28/10/2023 (solicitada dilação de prazo)

3.8. Produção de Prova(s) pelo Autuado: (X) Não ( ) Sim. Se sim, informar quais:

3.9. Produção de Prova(s) pela ANPD: (X) Não ( ) Sim. Se sim, informar quais:

3.10. Terceiro(s) Interessado(s): (X) Não ( ) Sim. Se sim, informar se houve manifestação:

3.11. Termo de Ajustamento de Conduta: (X) Não ( ) Sim

3.12. Alegações Finais: ( ) Não (X) Sim

3.13. Medida(s) Preventiva(s) Aplicada(s) - Art. 32 do Regulamento de Fiscalização: Aviso nº 20/2022/CGF/ANPD (SUPER nº 3404477).

3.14. Medida(s) Preventiva(s) Aplicada(s) com base no Art. 7º, IV, da Portaria nº 1/2021 (RI-ANPD): (x) Não ( ) Sim.

4. RELATÓRIO

4.1. Nos termos do art. 54 da Resolução CD/ANPD nº 1, de 28/10/2021 (RPF), este processo foi instaurado pela Coordenação-Geral de Fiscalização (CGF/ANPD) com base no processo preparatório nº 00261.000518/2022-96. Assim, em consonância com os ditames normativos aplicáveis ao caso e demais documentos que constam dos autos, passa-se ao detalhamento dos atos processuais do processo originário e deste processo administrativo sancionador até a presente data.

4.2. Em 15/03/2022, o processo 00261.000518/2022-96 foi iniciado pela Coordenação-Geral de Fiscalização (CGF) após o recebimento de denúncia, encaminhada por e-mail no dia 19/01/2022, que informava a respeito de uma falha de segurança em um site, não especificado, sob controle do Governo do Estado de São Paulo. Por meio da exploração da referida falha, seria possível acessar dados pessoais como CPF, Nome, RG, endereço, telefone, salário, bem como imagens de documentos como CNH, RG e comprovante de residência, conforme constante no Relatório nº 01/2022/CFG/ANPD (SUPER nº 3237413).

4.3. Ainda no processo originário 00261.000518/2022-96, foram enviados o Ofício nº 79/2022/CGF/ANPD/PR (SUPER nº 3239095), datado de 15/03/2022, e o Ofício nº 111/2022/CGF/ANPD/PR (SUPER nº 3286533), em 04/04/2022, para colher informações sobre os problemas reportados.

4.4. Em 27/05/2022, em cumprimento ao Ofício nº 131/2022/CGF/ANPD/PR (SUPER nº 3349883), o IAMSPE encaminhou o Formulário de Comunicação de Incidente de Segurança (SUPER nº 3399646), confirmando os fatos denunciados.

4.5. Todavia, diante do reiterado descumprimento da determinação de comunicação do incidente aos titulares dos dados afetados, emitiu-se o Aviso nº 20/2022/CGF/ANPD (SUPER nº 3404477), em 02/06/2022, com fulcro no art. 55-J, inciso IV, da LGPD; no art. 17 do Regimento Interno da ANPD e no art. 34 do RPF. Determinou-se ao controlador a comprovação da comunicação individual do incidente a todos os titulares de dados afetados.

4.6. Ainda no processo originário, após a análise da documentação apresentada e das alegações do agente de tratamento por meio dos Ofícios e seus anexos enviados [nº 467/2022 (SUPER nº 3311140), 427/2022 (SUPER nº 3341091), 708/2022 (SUPER nº 3440640)], foi elaborada a Nota Técnica nº 79 (SUPER nº 3600888) com indicativo de violação ao artigo 48 da LGPD por não ter sido realizada, no prazo concedido, a comunicação individual à totalidade dos titulares afetados, conforme determinado pela CGF/ANPD.

4.7. Também foi verificada possível violação do artigo 49 do mesmo diploma legal, que impõe ao controlador o dever de utilizar sistemas que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança, e aos princípios gerais previstos na legislação.

4.8. Diante de tais fatos, foi recomendada, por meio da Nota Técnica nº 79 (SUPER nº 3639508), a instauração de processo sancionador, com base no art. 37 do RPF c/c artigos 52 e 55-J, IV da LGPD.

4.9. Ato contínuo, em 13/09/2022, o Despacho Decisório nº 11/2022/CGF/ANPD (SUPER nº 3620085) acolheu a referida Nota Técnica e determinou a instauração do Processo Sancionador nº 00261.001969/2022-41 e, assim, foi lavrado o ANPD - Auto de Infração 12 (SUPER nº 3639487) em desfavor do autuado IAMSPE que apontou a infringência aos seguintes dispositivos:

4.10. Art. 48 da Lei nº 13.709, de 14/08/2018 (LGPD)[2] e;

4.11. Art. 49 da Lei nº 13.709, de 14/08/2018 (LGPD)[3].

4.12. Em 30/09/2022, o autuado foi intimado conforme Certidão de Intimação Cumprida (SUPER nº 3696347).

4.13. Em 27/10/2022, após pedido de dilação de prazo por meio do OFICIO Solicitação (SUPER nº 3716064), sobreveio o OFICIO Defesa (SUPER nº 3718361), no qual se apresentam argumentos e se requer a anulação do Auto de Infração lavrado. Acompanham a defesa: Relatorio serviço perfis (SUPER nº 3718362), Relatorio implantação de trilhas (SUPER nº 3718363), Relatorio sumário sms (SUPER nº 3718364) e Anexo Comunicado (SUPER nº 3718365).

4.14. Não houve solicitação para produção de novas provas conforme disposto no artigo 48 do RPF.

4.15. Em 10/11/2022, o Despacho (SUPER nº 3727648) sobrestou o processo até que o Regulamento de Dosimetria e Aplicação de Sanções Administrativas fosse aprovado, fato este ocorrido em 27/02/2023, o que levou à suspensão do sobrestamento em 17/04/2023, com o Despacho (SUPER nº 4168480).

4.16. Em 20/04/2023, foi emitido o ANPD - Ofício 79 Alegações Finais (SUPER nº 4177231) intimando o IAMSPE para, no prazo de 10 (dez) dias úteis, apresentar Alegações Finais. O recebimento foi confirmado por meio da Certidão de Intimação Cumprida (SUPER nº 4221534).

4.17. Em 19/05/2023, o IAMSPE apresentou, de forma tempestiva, suas Alegações Finais (SUPER nº 4280896).

4.18. Em 25/05/2023, foi realizada a análise de confidencialidade dos documentos que instruem o presente processo administrativo sancionador por meio da Nota Técnica 69 (SUPER nº 4281068), acolhida pelo Despacho (SUPER nº 4283750).

4.19. É o relatório.

5. PRELIMINARES

Competência da ANPD

5.1. A Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados (LGPD), art. 5º, I, considera dado pessoal toda *"informação relacionada a pessoa natural identificada ou identificável"*. Por

essa razão, o nome completo, estado civil, data de nascimento, CPF, RH, endereço e telefones e também cópias de documentos tais como RG, CNH e comprovante de residência são dados pessoais de funcionários públicos do estado de São Paulo e seus dependentes. Trata-se, portanto, de informações relacionadas a pessoa natural identificada ou identificável.

5.2. A leitura do processo revelou que a atividade desenvolvida pelo IAMSPE configura tratamento de dados pessoais, já que a utilização de dados pessoais em sua base para administrar um sistema de saúde que atende aproximadamente 1,2 milhão de funcionários públicos do Estado de São Paulo e seus dependentes pode ser enquadrada na previsão do art. 5º, X, 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"*. Com efeito, está-se diante de utilização de dados pessoais.

5.3. 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 IAMSPE efetua o tratamento de dados pessoais para operacionalizar o sistema de saúde dos servidores públicos beneficiados, não há dúvidas de que ao Instituto competem as decisões referentes ao tratamento de dados pessoais, motivo pelo qual é controlador.

5.4. A circunstância de a atividade do IAMSPE estar inserida nas disposições da LGPD implica a competência de atuação ANPD, definida pelo art. 5º, XIX da LGPD, 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"*.

5.5. No âmbito da ANPD, a Coordenação-Geral de Fiscalização (CGF) é responsável por identificar as infrações à LGPD, o que consiste em desdobramento do objetivo estratégico de promoção do fortalecimento da cultura de proteção de dados pessoais. 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:
>
> (...)
>
> III - promover ações de fiscalização sobre as ações de tratamento de dados pessoais efetuadas pelos agentes de tratamento, incluído o Poder Público;
>
> (...)
>
> IX - requisitar aos agentes de tratamento de dados a apresentação de Relatório de Impacto à Proteção de Dados Pessoais;

5.6. O art. 48 do Regimento Interno da ANPD, ainda, determina que as *"atividades da ANPD obedecerão, além dos princípios estabelecidos na Lei nº 13.709, de 2018, aos princípios da legalidade, motivação, moralidade, eficiência, celeridade, interesse público, impessoalidade, igualdade, devido processo legal, ampla defesa, contraditório, razoabilidade, proporcionalidade, imparcialidade, publicidade, economicidade, segurança jurídica, entre outros"*. Esta é, portanto, a justificativa para análise da atividade desenvolvida pelo IAMSPE em processo administrativo próprio, pois é necessário observar as diretrizes e os princípios incidentes sobre a atuação administrativa no cumprimento da atribuição de fiscalização.

5.7. A Resolução CD/ANPD nº 1, de 28/10/2021, que aprovou o regulamento do processo de fiscalização e do processo administrativo sancionador no âmbito da ANPD, dispõe de forma fundamental sobre a estruturação das atividades previstas no art. 17 do Regimento Interno da ANPD. De acordo com o art. 2º do Regulamento, a fiscalização volta-se à orientação, à prevenção e à repressão das infrações à LGPD, de sorte a, conforme o art. 3º, proteger os direitos dos titulares de dados, promover a implementação da legislação de proteção de dados pessoais e zelar pelo cumprimento das disposições da LGPD.

5.8. Por força do art. 4º, I, do mencionado Regulamento, o IAMSPE é considerado agente regulado pela ANPD, já que se enquadra na categoria de *"agentes de tratamento e demais integrantes ou*

interessados no tratamento de dados pessoais". Cumpre especificar as atividades 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.

5.9. Pelo exposto, não há dúvidas quanto à competência da ANPD no caso concreto para avaliar a conduta do IAMSPE, controlador de dados e agente regulado, à luz da LGPD.

5.10. No mais, o autuado não arguiu questões preliminares de mérito em sua defesa e, em análise preliminar, não se verificaram questões relevantes a serem trazidas de ofício a este Relatório de Instrução.

6. ANÁLISE

Circunstâncias da infração e autoria

6.1. Conforme disposto no Regulamento do Processo de Fiscalização da ANPD em seu art. 37, o processo administrativo sancionador destina-se à apuração de infrações à legislação de proteção de dados de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD e, de acordo com o art. 54, o Relatório de Instrução subsidiará a decisão de primeira instância. Assim, a análise tem por objetivo avaliar os motivos da autuação e os argumentos apresentados pelo controlador face à legislação e às normas de proteção de dados, no âmbito do presente processo. Para tanto, segue um breve histórico mais detalhado do Relatório para compor esta análise.

6.2. O presente processo administrativo sancionador foi instaurado com base na Nota Técnica nº 79 (SUPER nº 3639508) que, em sua análise, traz um compilado do ocorrido ao longo do processo originário nº 00261.000518/2022-96. Em sua conclusão, recomendou-se a instauração de processo administrativo sancionador, com base no art. 37 da Regulamento de Fiscalização c/c artigos 52 e 55-J, IV da LGPD, feito este instaurado por meio de despacho decisório que deu origem ao ANPD - Auto de Infração 12 (SUPER nº 3639487). Entendeu-se, na oportunidade, que houve possível descumprimento dos artigos 48 e 49 da LGPD pelo IAMSPE.

6.3. Numa análise prévia de autoria, não há o que se questionar com relação à figura do IAMSPE como controlador dos dados, uma vez que, conforme disposto em seu sítio eletrônico[4]: "(...)*é um sistema de saúde que atende aproximadamente 1,2 milhão de funcionários públicos do Estado de São Paulo e seus dependentes (...)*". Nesta linha, no mesmo endereço eletrônico na parte da introdução de sua Política de Privacidade, informa que "*reconhece a relevância e o seu dever de zelar pela privacidade das informações e dados pessoais dos usuários que acessem o Portal Iamspe, protegendo-as de acessos indevidos.*" Portanto, fica clara a sua condição de controlador de acordo com o inciso VI do artigo 5º da LGPD.

6.4. Analisando-se um dos dispositivos supostamente infringidos conforme o auto lavrado, a LGPD determina, no art. 48, 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 art. 48, a comunicação deverá ser feita em prazo razoável, a ser regulamentado pela ANPD. Ainda que pendente a regulamentação do prazo para a comunicação do incidente, 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.

6.5. Conforme se depreende dos documentos mencionados, o possível descumprimento do art. 48 se deu em razão de o IAMSPE não ter realizado, no prazo concedido, a comunicação individual à totalidade dos titulares afetados, conforme determinado pela CGF/ANPD. Adicionalmente, o instituto não apresentou justificativa razoável para proceder de forma diversa.

6.6. Já em relação ao art. 49 do mesmo diploma legal, a Nota Técnica nº 79 sinaliza que houve falha na implementação de controles para garantir a confidencialidade dos dados, de modo a assegurar que a informação fosse acessível apenas àqueles autorizados a ter acesso, pois é de se esperar que o controlador adote medidas adequadas para a proteção de base de dados pessoais sob sua custódia, sobretudo quando envolvem grande quantidade, inclusive de grupos vulneráveis - crianças, adolescentes e idosos, tendo em vista que o acesso indevido a tais dados pode ocasionar riscos ou danos relevantes a seus titulares. Ressalte-se que o art. 49 da LGPD determina que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma 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.

6.7. Em breve síntese, o processo originário foi aberto por conta de denúncia que reportava vulnerabilidades em sistemas de informação mantidos pelo IASMPE que permitiriam, sem o uso de credenciais válidas, o acesso a informações constantes em sua base de dados. Em um primeiro momento, esse acesso poderia ser feito inclusive por terceiros não autorizados, que poderiam consultar não só o conjunto de dados pessoais descrito em anexo à denúncia - tais como nome completo, estado civil, data de nascimento, CPF, RH, endereço e telefones -, como também cópias de documentos como RG, CNH e comprovante de residência.

Da defesa apresentada pelo Autuado

6.9. Por meio de Ofício (SUPER nº 3311140) no processo originário, reiterado posteriormente nas alegações constantes do OFICIO Defesa (SUPER nº 3718361), o IAMSPE informou que teria tomado conhecimento do incidente com certo atraso, uma vez que a denúncia foi realizada à PRODESP, em 19/01/2022, e que "*não havia dados suficientes que pudessem comprovar as alegações ou sequer identificar a entidade pública a que se referia*". Por esta razão, a Ouvidoria Geral do Estado de São Paulo (OGE-SP) alegou que arquivou esta primeira denúncia por falta de informações. Ainda em sua defesa, o IAMSPE alegou que tomou conhecimento do incidente por meio de contato telefônico com o setor de imprensa da instituição em 14/02/2022, mas que, em razão dos poucos detalhes apresentados, não pode identificar estas falhas.

6.10. Após um mês da primeira comunicação do denunciante com o OGE-SP para reportar a falha identificada, o mesmo realizou novo contato com a ANPD, por e-mail, alegando que a irregularidade detectada não teria sido adequadamente corrigida. Isso porque, de acordo com o autor da denúncia, embora o acesso de terceiros não autorizados tenha sido bloqueado, usuários logados de forma válida no sistema ainda poderiam acessar indevidamente dados de terceiros não relacionados a seu grupo familiar.

6.11. Ocorre que, no mês seguinte, em 15/03/2022, nos autos do processo originário, foi solicitado ao IAMSPE, por meio do Ofício nº 79 (SUPER nº 3239095), que informasse a respeito das medidas tomadas para sanar a vulnerabilidade, auditasse o sistema para verificar a ocorrência de acessos não autorizados e, confirmado o incidente, comunicasse sua ocorrência, nos termos do art. 48 da LGPD. Foi solicitado, também, que fizesse a divulgação, nos termos o art. 41 da LGPD, dos dados de contato de seu encarregado, no prazo de 10 (dez) dias úteis.

6.12. Após algumas trocas de ofícios solicitando dilações de prazo, somente em 02/05/2022 o IAMSPE informou que, por meio de testes, teria confirmado a existência de vulnerabilidades no sistema. Em razão disso, o instituto teria implementado, a partir de 17/02/2022, controles para restringir o acesso aos dados somente a usuários autenticados e, em 14/03/2022, teria implementado mecanismos para que os usuários tivessem acesso somente a dados de seu grupo familiar. Além disso, estaria em desenvolvimento a substituição de identificadores sequenciais por *hashes*. Em paralelo, foram introduzidas modificações para que o sistema passasse a registrar os acessos, tornando-o auditável. Todavia, o instituto ainda estaria

investigando a ocorrência de exposição indevida de dados e que, somente se constatada, providenciaria a comunicação aos titulares e à ANPD. Ou seja, mesmo após quase três meses após a ciência do ocorrido, não se verificou a comunicação formal do incidente aos usuários e à ANPD.

6.13. Passados mais dois meses, em 06/05/2022, após novo Ofício nº 131 (SUPER nº 3349883) emitido pela Coordenação-Geral de Fiscalização determinando a comunicação imediata do incidente aos titulares e à ANPD, o IAMSPE então protocolou o Formulário de Comunicação de Incidente de Segurança (SUPER nº 3399647). Segundo o formulário, foram identificados 4 (quatro) pontos de acesso na API do site app.iamspe.sp.gov.br que não contariam com controles de segurança adequados. Apesar de reconhecer a falha, na época, o controlador não foi capaz de apurar se ela teria sido efetivamente explorada por terceiros.

6.14. No que tange à determinação para se comunicar as partes interessadas, ainda no Formulário, o autuado justificou não ter comunicado o incidente no prazo sugerido pela ANPD por não ter constatado destruição, perda, alteração ou vazamento de dados. Segundo o controlador, as falhas teriam sido identificadas após acesso autenticado no sistema por meio de credenciais válidas, o que reduziria o risco de a falha ter sido explorada. Entendeu, portanto, não haver incidente que necessitasse ser comunicado à ANPD.

6.15. A título de conhecimento, o IAMSPE também informou no Formulário que poderiam ter sido afetados 1.489.304 (um milhão, quatrocentos e oitenta e nove mil, trezentos e quatro) titulares de dados, beneficiários e seus dependentes, incluindo crianças e adolescentes. Especificou que poderiam ter sido acessados: identificação completa de beneficiários e titulares (nome, nome social, sexo, CPF, RG, número Pis-Pasep, data de nascimento, nome de pai e mãe, estado civil); contato completo (endereço, e-mail e telefone); relação de parentescos (pai, mãe, titular e beneficiários); escolaridade; órgão de trabalho; vínculo com Estado; tipo de plano; e forma de pagamento do plano.

6.16. Ademais, o investigado informou não haver registro de danos aos titulares em razão do incidente, além da eventual exposição de dados e que não teria havido acesso a dados pessoais sensíveis, como relatórios médicos. Por fim, informou que os titulares não foram comunicados sobre o incidente de segurança com dados pessoais porque a investigação do incidente ainda estaria em curso. O IAMSPE entendeu, portanto, que não seria oportuna a comunicação aos titulares de dados.

6.17. Entretanto, após quase seis meses da primeira denúncia, em razão do regulado não ter atendido ao determinado pela CGF por meio do Ofício nº 131 (SUPER nº 3349883), tornou-se imperativa a emissão do Aviso nº 20/2022 (SUPER nº 3404477). O Aviso, datado de 02/06/2022, determinou a comprovação da comunicação individual do incidente a todos os titulares de dados afetados.

6.18. Em 15/06/2022, o IAMSPE apresentou Ofício (SUPER nº 3440640) em resposta ao Aviso nº 20/2022. Por meio desse documento, o instituto esclareceu que apenas um único titular de dados teria sido afetado, e que foi providenciada a devida comunicação do ocorrido ao interessado, por e-mail e pelos correios, conforme documentos anexados no processo originário. Além disso, o instituto informou ter enviado comunicado aos demais usuários informando a ocorrência de um acesso não autorizado em dados cadastrais de terceiros, conforme anexo (SUPER nº 3440644).

6.19. A despeito da argumentação do IAMSPE de que realizou os devidos testes no sistema e de que não teria verificado destruição, perda, alteração ou vazamento de dados de forma prejudicial aos demais usuários, a CGF entendeu que o tempo decorrido até a comunicação e a forma como ela foi realizada não atendiam adequadamente ao princípio da prevenção, previsto no inciso VIII do art. 6º da LGPD[5]. Sendo assim, por entender que o controlador não procedeu à adequada comunicação dos titulares afetados, tendo em vista que apenas um usuário fora individualmente contatado, e que conteúdo do comunicado amplo feito no sítio eletrônico (3440644) não atendeu ao previsto no art. 48 da LGPD, ou às orientações encaminhadas por meio de ofício, decidiu-se lavrar auto de infração e instaurar o presente processo administrativo sancionador em face do IAMSPE.

6.21. Em sua defesa, por meio do OFICIO Defesa (SUPER nº 3718361), o IAMSPE alegou ter adotado diversas medidas técnicas de segurança adicionais, e reforçou que implantou *Tokens* que restringiram o acesso a dados pessoais, tornando-os acessíveis exclusivamente ao respectivo titular e a seu grupo familiar, mediante identificação individualmente autenticada pelo sistema. O instituto também relatou que houve a transformação do Id Sequencial em um *hash* não sequencial, trazendo à guisa o anexo 1 (Relatorio serviço perfis, SUPER nº 3718362) com as evidências coletadas que comprovam essas ações.

6.22. O IAMSPE argumentou, ainda, que o denunciante explorou possíveis falhas em seu sistema a partir de acesso autorizado utilizando credenciais válidas de *login* e senha de usuário do instituto. Portanto, tal fato, isoladamente, não permitiria concluir que o sistema seria vulnerável a acessos externos indevidos. Ademais, o IAMSPE ponderou que a imagem apresentada pelo denunciante como evidência seria uma amostra dos dados que poderiam ser obtidos no sistema, mas que contém dados cadastrais de um único usuário.

6.23. O instituto então reiterou que, em atenção ao art. 48 da LGPD, o usuário afetado foi devidamente comunicado sobre o ocorrido por e-mail e por carta enviada pelos correios, conforme documentos comprobatórios apresentados nos autos. Adicionalmente, o IAMSPE declarou que encaminhou mensagem (SMS) aos 260.874 usuários com número de celular cadastrado (anexo Relatorio sumário sms (SUPER nº 3718364), informando acerca da falha identificada e que, em 21/06/2022, inseriu o comunicado de incidente de segurança no site da instituição. De acordo com o autuado, o processo para efetivação de comunicados adicionais individualizados para cada usuário da Instituição estaria em andamento e somente não foi concluído por motivos operacionais relacionados a inconsistências de cadastro, cujos dados são inseridos por órgãos externos, fora da governança do instituto.

6.24. Nesse ponto, é preciso ressalvar que, a despeito das comunicações efetuadas, comparando-se o conteúdo do documento que comunica a fragilidade e o disposto no artigo 48 da LGPD, verifica-se a ausência das informações sobre os dados pessoais que poderiam ter sido afetados, quais titulares poderiam ter sido afetados, os eventuais riscos relacionados ao incidente, além do motivo da demora na comunicação.

6.25. Ao fim, em sua argumentação sob os aspectos técnicos da defesa (SUPER nº 3718361), o IAMSPE informou que foram realizados procedimentos de verificação que chegaram à conclusão de que não havia evidência de perdas ou alterações de dados nas bases de beneficiários. Isso porque nenhuma das URL´s relacionadas ao Portal do Beneficiário (sejam as citadas na denúncia ou as demais que dele fazem parte) permite, por parte dos usuários, ações de alteração ou exclusão de dados. O instituto alegou se tratar de ferramenta usada primordialmente para meras consultas de informações do beneficiário e de seus dependentes, à exceção do cadastramento de acompanhantes. Ao cabo, afirmou que não foram recebidas reclamações de usuários acerca de perdas ou alterações indevidas de dados e apresentou o Relatorio implantação de trilhas (SUPER nº 3718363) como prova das evidências coletadas que comprovam as ações de implantação das trilhas de auditoria nas URL's denunciadas.

Das alegações finais apresentadas pelo Autuado

6.26. Em Alegações Finais (SUPER nº 4280896), apresentadas tempestivamente, o autuado informou que melhorou alguns aspectos operacionais de controle por meio da definição de encarregado, da recente nomeação de Comitê de Privacidade com diversas responsabilidades e também do início do Programa de Privacidade do IAMSPE "*com o objetivo de garantir a proteção e o tratamento adequado dos dados pessoais dos titulares*". Ademais, informou diversas ações adotadas envolvendo equipes multidisciplinares do instituto, o mapeamento de toda a cadeia de custódia relacionada à proteção de dados e planos operacionais para o curto e médio prazos. Dentre eles, há um plano de formação e capacitação interna cujo objetivo é aumentar a cultura organizacional na prática da proteção de dados.

6.27. Além disso, informou que seus sistemas de infraestrutura e segurança estão em processo de adequação e melhorias, tais como migração do portal para nuvem Oracle visando diversos benefícios listados, implementação de *firewalls*, de *endpoints* (*SSL - secure sockets layer*) e anexou um relatório com vulnerabilidades identificadas após simulação de intrusão em todas as interfaces de processamento de aplicações (APIs) que está tratando, sendo que as mais críticas foram corrigidas. Por fim, o IAMSPE se propôs a prestar contas do desenvolvimento do programa e dos objetivos a serem concretizados ao longo dos próximos meses para mitigar riscos de privacidade e segurança. Nesta linha, propôs-se a demonstrar e evidenciar o cumprimento do seu Programa de Privacidade e dos respectivos planos anexados junto à ANPD.

Subsunção do fato ao tipo infracional correspondente

6.28. O ANPD - Auto de Infração 12 (SUPER nº 3639487) baseou-se nos seguintes diplomas para imputar a prática de infrações ao Instituto de Assistência ao Servidor Público Estadual de são paulo -

IAMSPE:

Art. 48 da Lei Geral de Proteção de Dados - ausência de comunicação eficiente de incidente de segurança à autoridade e aos titulares;

6.29. Com relação art. 48, demonstrou-se acima a ocorrência de violação. Isto porque o texto do artigo da LGPD diz o seguinte:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

6.30. Pelo que se depreende de toda a análise acima realizada, não houve cumprimento adequado integral da obrigação legal do art. 48 da LGPD, mesmo com as reiteradas determinações para a comunicação individual do incidente aos titulares dos dados afetados, i.e., aos 1.489.304 (um milhão, quatrocentos e oitenta e nove mil, trezentos e quatro) beneficiários da base de dados do IAMSPE (informado no Formulário de Comunicação de Incidente de Segurança).

6.31. O IAMSPE argumentou que, por motivos operacionais relacionados ao cadastro, lidou com a necessidade de validação dos contatos dos usuários registrados no cadastro para efetivação da comunicação adicional. Assim, dada a comunicação de 260.874 pessoas via mensagem de texto SMS, a comunicação às demais 1.228.430 pessoas restantes (considerando os dependentes), cerca de 82% do total da base cadastrada, teria ocorrido por e-mail.

6.32. Cabe ressaltar que, para a Autoridade Nacional de Proteção de Dados, mesmo com a ciência do ocorrido desde janeiro/fevereiro, a comunicação de incidente de segurança somente foi enviada ao final de maio, ou seja, com cerca de 3 (três) meses de atraso.

6.33. Ademais, ao vermos o comunicado para os titulares presente no sítio eletrônico do IAMSPE, nota-se a ausência das informações determinadas pelo inciso I (descrição da natureza dos dados afetados), inciso II (informações dos titulares envolvidos), inciso IV (os riscos relacionados ao incidente) e V (os motivos da demora, no caso da comunicação não ter sido imediata) do aludido artigo. Observa-se, portanto, a necessidade de correção do referido comunicado apresentado no sítio eletrônico do IAMSPE.

6.34. Pelo exposto acima, entende-se que o IAMSPE não realizou a comunicação em tempo razoável e, mesmo quando o fez, seu teor foi insuficiente, em infringência ao art. 48 da LGPD.

Art. 49 da Lei Geral de Proteção de Dados - insuficiência de sistema de segurança para tratamento de dados pessoais.

6.35. No que tange ao dispositivo constante no art. 49 do mesmo diploma legal, também observamos sua violação, senão vejamos:

> *Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.*

6.36. Conforme reportado anteriormente na presente Nota Técnica, o processo originário (incidente de segurança) foi aberto por conta de denúncia que reportava vulnerabilidades em sistemas de informação mantidos pelo IASMPE que permitiriam, sem o uso de credenciais válidas, o acesso a informações constantes em sua base de dados. Num primeiro momento, esse acesso poderia ser feito até por terceiros não autorizados que poderiam acessar não só o conjunto de dados pessoais descrito em anexo à denúncia, tais como nome completo, estado civil, data de nascimento, CPF, RH, endereço e telefones, como também cópias de documentos tais como RG, CNH e comprovante de residência.

6.37. De acordo com o próprio autuado em manifestação a esta CGF, foram identificados 4 pontos de acesso na API do site app.iamspe.sp.gov.br que não contariam com controles de segurança adequados. Apesar de reconhecer a falha, o controlador não foi capaz de apurar se ela foi efetivamente explorada por terceiros.

6.38. Tais fatos demonstram, de forma inequívoca, que os sistemas do IAMSPE, à época do incidente, não atendiam às exigências do art. 49 da LGPD.

6.39. Em sua defesa e em suas alegações finais, o IAMSPE adeclara que, a partir do conhecimento das falhas de segurança, passou a adotar medidas corretivas.

6.40. Assim, com relação à infração ao art. 49 da LGPD, o IAMSPE alerta que já seria possível identificar eventuais tentativas de acessos suspeitos, pois em todas as requisições feitas pelos usuários no "Portal do Beneficiário" ficaria registrada uma trilha de auditoria. Ao lado disso, o IAMSPE informa que várias medidas foram adotadas, conforme descrito na Nota Técnica 79 (SUPER nº 3639508).

6.41. Conforme citado em sua defesa e anexado por meio do Relatorio implantação de trilhas (SUPER nº 3718363), o IAMSPE enfatiza que foram realizados procedimentos de verificação que chegaram à conclusão de que não há evidência de perdas ou alterações de dados nas bases de beneficiários e nem foram recebidas reclamações de usuários de perdas ou alterações indevidas de dados.

6.42. Todavia, importa lembrar que parte da razão de não haver evidências de exploração da falha decorre de não haver guarda de registros (*logs*) de acesso pelo IAMSPE à época da denúncia. Essas e outras medidas foram adotadas tardiamente, após a constatação das falhas de segurança no sistema. Nesse sentido, a argumentação do IAMSPE acerca da adoção de medidas de segurança por si só não é capaz de afastar a incidência da infração ao art. 49 da LGPD, uma vez que foi constatada a fragilidade dos sistemas do instituto.

6.43. Importa esclarecer que, nos termos da LGPD, o tratamento de dados pessoais, inclusive a guarda deles, necessariamente atrai para o controlador o dever de protegê-los.

6.44. Na linha desse raciocínio, convém citar dois princípios que a LGPD expressamente traz em seu artigo 6º: o princípio da *segurança* e o princípio da *responsabilização e prestação de contas*. Enquanto o primeiro, ao prever "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão", é reforçado pelo disposto nos art. 46 e 49; o segundo dispõe sobre "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

6.45. Especificamente sobre os princípios da segurança e da responsabilização e prestação de contas, é oportuno citar que deles decorrem, não exclusivamente, não só a obrigação de proteger tais dados com também a obrigação de demonstrar que estão protegidos. Nesse sentido, leciona a Profa. Miriam Wimmer[6] acerca do princípio da segurança:

> No que tange especificamente aos princípios da segurança e da prevenção, interessa observar que, nos termos do art. 44 da LGPD, **o tratamento de dados pessoais é considerado irregular quando não fornecer a segurança que o titular dele pode esperar**, considerando, dentre outros aspectos, o resultado e os riscos que razoavelmente dele se esperam. **A legislação deixa claro, também, que dos agentes de tratamento de dados pessoais é esperada a adoção tanto de medidas técnicas como de medidas administrativas para proteger os dados pessoais**. Nessa linha, ganha importância a ideia de *privacy by design*, também prevista na LGPD, que estabelece que as medidas técnicas e administrativas de segurança devem ser observadas desde a fase de

concepção do produto ou do serviço até a sua execução. (Grifamos)

6.46. Vale reiterar, por conseguinte, que, nos termos da LGPD, o tratamento de dados pessoais necessariamente atrai para o controlador o dever de protegê-los. Em consequência disso e do exposto acima, surge para este agente de tratamento o compromisso quando falha em cumprir esse dever.

6.47. É importante complementar a análise do compromisso do controlador com o que dispõe o princípio da responsabilização e prestação de contas. Novamente, recorre-se à lição da Profa. Miriam Wimmer[7]:

> 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**. (Grifamos)

6.48. É consequência lógica do princípio acima, em leitura conjunta com os art. 46 e 49 da LGPD, que a ausência de registros (*logs*) constitui falha no dever de proteger os dados pessoais sob sua custódia. Não há como o controlador cumprir, ou demonstrar que cumpre, seu dever de protegê-los "de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" sem que saiba quando e por quem são acessados.

6.49. Não é razoável que a falha no dever de proteger os dados, e consequente incapacidade de demonstrar que tais dados não foram acessados e de determinar quantas vezes a vulnerabilidade foi explorada, que essa incerteza, provocada por falha em cumprir dever legal, seja aproveitada em favor daquele que deixou de cumprir seu dever.

6.50. Nessa circunstância, é inafastável a incidência do **princípio de que a ninguém é dado se beneficiar de sua própria torpeza**. Do contrário, estar-se-ia criando um estímulo completamente incompatível com os princípios da *segurança* e da *responsabilização e prestação de contas* acima expostos em que o agente de tratamento em conduta irregular seria premiado, neste caso, com a desoneração de comunicar aos titulares.

6.51. Muito embora a comunicação não decorra especificamente da violação do dever de proteger os dados, e sim da possibilidade de que o incidente possa acarretar risco ou dano relevante aos titulares, uma vez caracterizada essa possibilidade, é incabível o argumento da impossibilidade de demonstrar quais titulares foram afetados ou a proporção em que a vulnerabilidade foi explorada, em razão de falha no dever de proteger dados pessoais, para afastar o dever de comunicar sobre o incidente aos titulares.

6.52. Adicionalmente, mesmo que a incapacidade de demonstrar que os dados não foram acessados e de determinar quantas vezes a vulnerabilidade foi explorada não decorresse de uma situação de falha no cumprimento de dever legal, ainda caberia sopesar a realização da comunicação do incidente aos titulares ante o risco ou dano relevante que esse incidente acarreta para os titulares, sob o amparo do princípio da prevenção (art. 6º, VIII), que determina adoção de medidas para prevenir a ocorrência de danos, em conjunto com o §1º, VI do art. 48, que trata das medidas para reverter ou mitigar os efeitos do prejuízo.

6.53. Adicionalmente, importa para o caso concreto, considerar que o controlador igualmente não sabe informar desde quando a falha existe porque tampouco registra as alterações que faz em seus sistemas.

6.54. Nesta linha de entendimento, resta clara a falha na implementação de controles para garantir um dos pilares da segurança da informação, qual seja, a confidencialidade dos dados, de modo a garantir que a informação fosse acessível apenas àqueles autorizados a ter acesso. Em especial, por envolver quantidade considerável de dados pessoais, inclusive de grupos vulneráveis - crianças, adolescentes e idosos - é esperado que o controlador adote medidas adequadas para a proteção da base de dados pessoais sob sua custódia. Portanto, entendeu-se pela elevada plausibilidade de ter sido violado o disposto no art. 49 da LGPD que impõe ao controlador o dever de utilizar sistemas que atendam aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na legislação.

6.55. É importante considerar que, por conta do sobrestamento do processo e retorno de sua análise somente 6 (seis) meses após a apresentação da defesa, em complemento, conforme visto em suas alegações finais, o IAMSPE adotou outras importantes medidas como a criação de um Comitê de Privacidade, um programa de Privacidade e Segurança com diversos planos e etapas, ações de capacitação interna em LGPD, incrementos na infraestrutura de proteção de dados e segurança da privacidade, descrito no [item 6.24] e no [item 6.25].

6.56. Não obstante, não se pode olvidar que, apesar de constar na sua Política de Privacidade e Proteção de Dados, em seu site[8], o compromisso com a adoção de medidas para *"salvaguarda de informações de natureza sigilosa previstas em Lei e nos atos normativos da Administração Pública Estadual, a fim de garantir a necessária restrição de acesso ao seu conteúdo, suporte ou registro (metadados), preservando o seu sigilo",* não foi exatamente tal comportamento que ocorreu durante um tempo indeterminado, até a denúncia ocorrida e tratada.

6.57. Pelo exposto, do exame dos autos, ainda que o autuado tenha empreendido seus melhores esforços no intuito de aprimorar seus sistema de segurança de dados, tais providências somente foram tomadas após a ocorrência de um incidente que demonstrou que havia falhas no sistema e, assim, entende-se caracterizada conduta em violação ao art. 49 da LGPD.

7. DOSIMETRIA DAS SANÇÕES

7.1. Em 27/02/2023, foi publicada a Resolução CD/ANPD nº 4, de 24/02/2023, que aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas e, assim, regulamentou o art. 53 da LGPD. Nesse regulamento, são adotadas as seguintes definições, importantes para a conclusão do presente processo:

> Art. 2º Para fins deste Regulamento adotam-se as seguintes definições:
>
> (...)
>
> II - infração: descumprimento de obrigação estabelecida na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), e nos regulamentos expedidos pela ANPD;
>
> (...)
>
> IV - infrator: agente de tratamento que comete infração;
>
> (...)

7.3. Além disso, o regulamento previu balizas para a aplicação das sanções administrativas, conforme preconizado no art. 3º:

> Art. 3º As infrações sujeitarão o infrator às seguintes sanções administrativas:
>
> I - advertência, nos termos do art. 9º deste Regulamento;
>
> II - multa simples, nos termos dos arts. 10 a 15 deste Regulamento;
>
> III - multa diária, nos termos do art. 16 deste Regulamento;
>
> IV - publicização da infração, após devidamente apurada e confirmada a sua ocorrência, nos termos dos arts. 20 e 21 deste Regulamento;
>
> V - bloqueio dos dados pessoais a que se refere a infração, até a sua regularização, nos termos do art. 22 deste Regulamento;
>
> VI - eliminação dos dados pessoais a que se refere a infração, nos termos do art. 23 deste Regulamento;
>
> VII - suspensão parcial do funcionamento do banco de dados a que se refere a infração, nos termos do art. 24 deste Regulamento;
>
> VIII - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração, nos termos do art. 25 deste Regulamento; e
>
> IX - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, nos termos do art. 26 deste Regulamento.
>
> § 1º As sanções previstas nos incisos VII, VIII e IX do caput deste artigo somente serão aplicadas após já ter sido imposta ao menos uma das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto.
>
> (...)
>
> § 5º O disposto nos incisos I e IV a IX, do caput deste artigo, poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

7.5. Destaca-se que o §5º afasta a aplicação das sanções de multa simples e multa diária para entidades e órgãos públicos, sem prejuízo da aplicação da Lei de Improbidade Administrativa, além da Lei de Acesso à Informação e da Lei nº 8.122. Ao mesmo tempo, o art. 55-J, XXII, da LGPD, determina que a ANPD deve comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública.

7.6. Como consequência, o § 1º indica que entidades e órgãos públicos que não sofreram sanções anteriores no mesmo caso concreto, apenas podem se sujeitar às infrações de advertência, publicização da infração, bloqueio e eliminação dos dados pessoais.

7.7. De acordo com o art. 8º do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, a classificação das infrações divide-se desta maneira:

> 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.
>
> § 1º A infração será considerada leve quando não verificada nenhuma das hipóteses relacionadas nos §§ 2º ou 3º deste artigo.
>
> § 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.
>
> § 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;
>
> b) o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida;
>
> c) a infração implicar risco à vida dos titulares;
>
> d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos;
>
> e) o infrator realizar tratamento de dados pessoais sem amparo em uma das hipóteses legais previstas na LGPD;
>
> f) o infrator realizar tratamento com efeitos discriminatórios ilícitos ou abusivos; ou
>
> g) verificada a adoção sistemática de práticas irregulares pelo infrator;
>
> II - constituir obstrução à atividade de fiscalização.

7.9. No caso sob análise, ficaram caracterizadas infrações aos arts. 48 e 49 da LGPD, cuja dosimetria será empreendida a seguir, em acordo com o Regulamento de Dosimetria.

Da Ofensa ao art. 48.

Classificação da infração ao art. 48, LGPD

7.11. O art. 48, caput e incisos, determina que o controlador deve apresentar o Comunicado de Incidente de Segurança (CIS) ao titular e à ANPD em prazo razoável. Como visto anteriormente nesta Nota Técnica, o autuado realizou a CIS de forma individualizada por 2 meios: (i) mensagens SMS para um grupo de titulares e (ii) e-mails para um grupo maior de titulares. Todavia, essas comunicações foram realizadas pelo IAMSPE em prazo superior ao determinado por esta ANPD e com conteúdo não conforme à LGPD.

7.12. Acrescente-se, ainda, que, para a Autoridade Nacional de Proteção de Dados, mesmo com a ciência do ocorrido desde janeiro/fevereiro, a comunicação de incidente de segurança somente foi enviada

ao final de maio, ou seja, com cerca de 3 (três) meses de atraso.

7.13. A falta de CIS aos titulares em prazo razoável, especialmente quando resulta na exposição de dados pessoais em espaço de acesso não controlado, pode afetar significativamente seus interesses e direitos fundamentais. Isso porque o titular não sabe que seus dados foram expostos e, com isso, não é capaz de adotar os cuidados necessários para evitar uso indevido de identidade, proteger-se fraudes financeiras e de outros danos que a exposição de dados possa causar. No caso concreto, os dados expostos permitem que o titular sofra esse tipo de dano, além de perturbações por ligações indevidas e fraudes em processos de autenticação ou validação de identidade em serviços específicos.

7.14. Para que a infração seja classificada como média, ela deve, além de infringir os interesses dos titulares, poder afetar significativamente os seus direitos fundamentais, como descrito no art. 8º, §2º, do Regulamento de Dosimetria. A falta de CIS põe em risco o direito fundamental de proteção de dados, já que essa ausência de comunicação ao titular o impede de exercer os direitos previstos na LGPD, que são basilares para a construção da proteção de dados como direito fundamental.

7.15. Ou seja, quando o titular não conhece o incidente de segurança que o afetou, ele fica impedido de exercer as prerrogativas inerentes às variadas dimensões do direito fundamental de proteção de dados, o qual possui como um de seus pilares os direitos da LGPD e as obrigações por ela impostas.

7.16. Logo, ainfração ao art. 48 ora analisada se enquadra nos requisitos doart. 8º, §2º, do Regulamento de Dosimetria, para ser classificada como média, no mínimo.

7.17. Entretanto, considerando que a classificação das infrações à LGPD, nos termos do Regulamento de Dosimetria, orienta-se segundo uma escala de gravidade em que os requisitos para uma infração ser classificada como média também integram o rol de requisitos para que uma infração seja classificada como grave, importa avaliar se também estão presentes os demais requisitos para que a classificação se torne mais severa, passando para grave.

7.18. Nos termos do art. 8º, §3º do Regulamento de Dosimetria, a infração será classificada como grave quando, além de preencher as condições do §2º, for verificada uma das seguintes hipóteses:

> § 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;
>
> b) o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida;
>
> c) a infração implicar risco à vida dos titulares;
>
> d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos;
>
> e) o infrator realizar tratamento de dados pessoais sem amparo em uma das hipóteses legais previstas na LGPD;
>
> f) o infrator realizar tratamento com efeitos discriminatórios ilícitos ou abusivos; ou
>
> g) verificada a adoção sistemática de práticas irregulares pelo infrator;
>
> II - constituir obstrução à atividade de fiscalização.

7.19. Conforme registrado no [item 6.6], no [item 6.15] e no [item 6.54], é possível constatar que a infração envolveu dados de crianças e de adolescentes. Tal circunstância, combinada com a constatação de que a infração preenche os quesitos para ser classificada como média, é suficiente para elevar o grau de classificação da infração, que por esse motivo, passa a ser considerada como grave, segundo art. 8º, §3º, 'd', da LGPD.

Definição do tipo de sanção administrativa

7.20. Neste momento, importa considerar o disposto no art. 3º, § 5º, do Regulamento de Dosimetria, que replica previsão constante do §3º do art. 52 da LGPD. Em tais dispositivos, limitam-se as sanções que podem ser impostas a entidade ou a órgãos públicos, afastando-se, por omissão, a possibilidade aplicação de multa ou de multa diária. Consequentemente, as circunstâncias atenuantes e agravantes identificadas têm sua utilidade mitigada na presente dosimetria.

7.21. Quanto às circunstâncias agravantes previstas no art. 12, no caso em tela, houve descumprimento de medida preventiva determinada com fundamento no dever do art. 48 da LGPD, consubstanciada no **Aviso nº 20/2022/CGF/ANPD** (SUPER nº 3404477), que determinou ao autuado a comunicação do incidente de segurança. A determinação contida nesse Aviso não foi atendida e, portanto, houve descumprimento dessa medida preventiva. Tal conduta é um fator agravante na apreciação da infração, conforme leitura do art. 12, III, do Regulamento de Dosimetria, e consoante o art. 32, §2º, II, do Regulamento da Fiscalização.

7.22. Quanto às circunstâncias atenuantes previstas no art. 13, registre-se que houve a cessação da infração com a implementação das medidas de segurança antes da instauração deste PAS, a partir do informado no Relatorio RIPD (SUPER nº 3666470), que invocam a incidência de circunstâncias atenuantes nos termos do art. 13, I, b) e III, b), do Regulamento de Dosimetria.

7.23. Considerando que a infração foi classificada como grave, afasta-se de pronto a possibilidade da aplicação da sanção de advertência com fundamento no art. 9º, I do Regulamento de Dosimetria. Todavia, o art. 9º, II, do Regulamento de Dosimetria, indica que a sanção de advertência é igualmente adequada quando houver necessidade de imposição de medidas corretivas. Esta hipótese se aplica a esta infração tendo em vista a necessidade de impor ao autuado a realização nova comunicação, desta vez abrangendo o conteúdo adequado em atenção ao disposto no §1º do art. 48, em conformidade com as razões expostas no [item 6.21] e no [item 6.32].

7.24. Assim, por infração ao art. 48, em razão de haver realizado comunicação de conteúdo insuficiente, **sugere-se cominar a pena de advertência com imposição de medida corretiva**, uma vez necessária e cabível a determinação de realização de nova comunicação aos titulares, nos seguintes termos:

> a) Ajustar, no prazo de 10 (dez) dias úteis da data de intimação, o COMUNICADO já existente no sítio do IAMSPE, conforme a redação abaixo sugerida:
>
> > Lei Geral de Proteção de Dados Pessoais - Comunicação de Incidente de Segurança:
> >
> > O Iamspe comunica que tomou conhecimento da ocorrência de incidente de segurança que pode ter comprometido a privacidade dos dados controlados pela organização, em razão de um acesso não autorizado ao sistema que armazena dados de beneficiários, no início do ano de 2022.
> >
> > Dentre os dados que podem ter sido acessados, incluem-se dados pessoais cadastrais, além de informações de salário e de residência de nossos beneficiários. Por um determinado período, até que fossem implementadas as devidas correções, tais dados estiveram sujeitos a risco de exposição. De todo modo, ressalte-se que não identificamos a ocorrência de qualquer extração.
> >
> > Informamos que o Instituto, imediatamente, realizou ações preventivas e corretivas nos processos e sistemas informatizados da entidade, visando mitigar a vulnerabilidade detectada no sistema de cadastro dos seus contribuintes e dependentes. Por conta destas ações, o Instituto comunicou o ocorrido à Autoridade Nacional de Proteção de Dados (ANPD) somente após a realização dos ajustes necessários.
> >
> > Após a comunicação de incidente de segurança à ANPD e aos usuários em geral, informamos que foi desenvolvido e submetido à Autoridade um cronograma de ações para melhoria de nossos controles.
> >
> > Dúvidas, solicitações e reclamações podem ser encaminhadas à Encarregada pelo Tratamento dos Dados no telefone: (11) 4573-9352, e-mail: lgpd@iamspe.sp.gov.br
> >
> > Estamos disponíveis para atendimento de segunda-feira a sexta-feira, das 9h às 17h. Política de Privacidade do Iamspe: http://www.iamspe.sp.gov.br/politica-de-privacidade/.
>
> a.1) O IAMSPE deverá juntar aos autos, no prazo de 10 (dez) dias úteis da data de intimação, comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 1 (uma) captura de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura.
>
> b) O comunicado acima deve permanecer disponível por 90 (noventa) dias corridos, contados a partir da data de cumprimento do ajuste no Comunicado, nos termos do item 'a' acima.
>
> b.1) O IAMSPE deverá juntar aos autos comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura,

sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma.

b.2) 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.

Da Ofensa ao art. 49.

Classificação da infração

7.25. A partir do quanto apurado, consoante o abordado no tópico 6, considerando que as características técnicas do sistema de informação do IAMSPE permitiam o acesso indiscriminado a dados como o nome completo, estado civil, data de nascimento, CPF, RH, endereço e telefones, e também a cópias de documentos tais como RG, CNH, e que o acesso a desses dados pode expor os titulares a situações de furto de identidade e, consequentemente, a situações de fraude financeira, entende-se como caracterizado o disposto no §2º do art. 8º, havendo risco de que os titulares tenham seus interesses e direitos significativamente afetados, inclusive por danos materiais.

7.26. Os agentes de tratamento devem utilizar 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. No entanto, o IAMSPE, neste caso concreto, não observou esta obrigação ao não utilizar controle de acesso seguro em seus sistemas.

7.27. O direito fundamental à proteção de dados não guarda vínculo apenas com o debate sobre privacidade e sigilo, de forma a se constituir enquanto direito autônomo e ser compromissado com o devido tratamento de dados pessoais, sejam eles de conhecimento público, de terceiros ou apenas de seus titulares. O sistema do IAMSPE permitiu a violação desse direito fundamental por retirar a possibilidade de o grupo de titulares afetados controlar informações que terceiros conhecem sobre eles, que podem gerar, especialmente, danos ao patrimônio, à honra do titular ou tratamentos discriminatórios. As peculiaridades do caso concreto são determinantes para definir se houve ou não violação de direitos fundamentais. Em observância à LGPD, norma que funciona como uma moldura para conformar esse direito fundamental, nos termos do art. 5º, LXXIX, o uso de sistema não seguro expôs dados pessoais, um conjunto de informações que permitem fraudes e roubos de identidade.

7.28. Ainda sobre o escopo de aplicação desse direito fundamental, Ingo Sarlet destaca que:

> [C]alha mencionar decisão proferida pelo Ministro Gilmar Mendes no âmbito da ADPF 695, sustentando que a dimensão subjetiva do referido direito importa na proteção do indivíduo contra riscos que ameacem sua personalidade em face da coleta, processamento, utilização e circulação de dados pessoas, ao passo que a dimensão objetiva implica a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados.[261] Quanto aos limites e restrições, toda e qualquer captação (levantamento), armazenamento, utilização e transmissão de dados pessoais, em princípio, constitui uma intervenção no âmbito de proteção do direito, que, portanto, não prescinde de adequada justificação.[262] Embora não se trate de direito absoluto, o direito à proteção dos dados, especialmente na medida de sua conexão com a dignidade humana, revela-se como um direito bastante sensível, tanto mais sensível quanto mais a sua restrição afeta a intimidade e pode implicar violação da dignidade da pessoa humana.[9]

7.29. Além disso, o sistema que não atende a requisito de segurança pode afetar significativamente o direito fundamental à proteção de dados pessoais. O Professor Danilo Doneda destaca caber à proteção de dados pessoais "definir, mais que tudo, a quem cabe o controle sobre os dados pessoais – e assim, consequentemente, realizar uma forma de distribuição de poder na sociedade que favoreça a autonomia do indivíduo".[10] Nesse sentido, um direito fundamental à proteção de dados visa garantir que as pessoas possam se autodeterminar a partir de suas informações, seja controlando ou participando do tratamento de dados.

> A inserção de um direito à proteção de dados de forma explícita no rol de direitos fundamentais da Constituição da República proporcionaria, portanto, uma isonomia entre esses direitos que, formalmente, afigura-se fundamental para a proteção de liberdades fundamentais, servindo, inclusive, para proporcionar uma nova chave de leitura [...] que não se afigure anacrônica em relação à tutela constitucional dos dados pessoais e seus reflexos para o cidadão.[11]
>
> O reconhecimento do caráter constitucional da proteção aos dados pessoais opera a superação de

> uma concepção, hoje anacrônica, segundo a qual seria possível realizar a governança de dados pessoais a partir de considerações sobre o direito à privacidade e o segredo ou sigilo. A consolidação deste direito garante que os dados pessoais possam ser utilizados com maior facilidade e com base jurídica sólida quando necessários e para fins legítimos, garantida a transparência, segurança e os direitos individuais, diminuindo os riscos sobre as operações de tratamento.[12]

7.30. O uso do sistema em questão põe em risco a dimensão objetiva desse direito fundamental. A infração ao art. 49 é barreira para garantia do indivíduo se autodeterminar e ter seus dados protegidos de um tratamento indevido.

7.31. O enquadramento do descumprimento do art. 49 como violação ao direito fundamental à proteção de dados, no caso concreto da atuação administrativa da ANPD, não prejudica eventual proteção de outros direitos fundamentais em uma esfera judicial, seja individual ou coletiva.

7.32. Adicionalmente, constatou-se que o IAMSPE trata dados pessoais de aproximadamente 1,5 milhão de pessoas, incluídos dependentes dos servidores públicos do estado de São Paulo entre os quais estão crianças, adolescentes e idosos, fato que invoca a alínea 'd' do inciso I do §3º do art. 8º, fato suficiente para elevar a classificação de infração de média (§2º) para grave (§3º).

Definição do tipo de sanção administrativa

7.33. Ordinariamente, essa circunstância requer a aplicação de multa simples, por expressa imposição do art. 10, II, do Regulamento de Dosimetria e Aplicação de Sanções Administrativas:

> *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; ou*
>
> *III - pela natureza da infração, da atividade de tratamento ou dos dados pessoais, e pelas circunstâncias do caso concreto, não for adequado aplicar outra sanção.*

7.35. Não obstante, considerando a inexistência de previsão legal de imposição da sanção de multa conforme mandamento do art. 52, §3º da LGPD, passa-se a analisar a adequação das outras sanções possíveis.

7.36. Para fins de definição das sanções aplicáveis, considere-se o disposto no art. 52 da LGPD, regulamentado pelo art. 3º do Regulamento de Dosimetria em seu § 5º ao disciplinar que o disposto nos incisos I e IV a IX, do caput do artigo, poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112/1990, na Lei nº 8.429/1992 e na Lei nº 12.527/2011.

> *"Art. 3º As infrações sujeitarão o infrator às seguintes sanções administrativas:*
>
> *I - advertência, nos termos do art. 9º deste Regulamento;*
>
> *(...)*
>
> *§ 5º O disposto nos incisos I e IV a IX, do caput deste artigo, poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011."*

7.37. Analisando-se por sanção aplicável, o inciso I do artigo 3º trata da sanção de advertência para a qual o artigo 9º do RDASA estabelece duas hipóteses de aplicação: (i) nos casos de infração leve ou média quando não se caracterizar reincidência específica; alternativamente, (ii) quando houver necessidade de imposição de medidas corretivas.

> *"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."*

7.38. No que se refere às outras sanções do artigo 3º aplicáveis, constantes dos incisos IV (publicização da infração), V (bloqueio de dados pessoais) e VI (eliminação de dados pessoais) se mostram inapropriadas para a situação ora em análise, igual raciocínio é aplicável às sanções dos incisos VII (suspensão parcial do funcionamento), VIII (suspensão do exercício de atividade de tratamento de dados) e IX (proibição parcial ou total do exercício de tratamento de atividades relacionadas ao tratamento de dados), que devem ser aplicadas somente após aplicação anterior das sanções previstas nos II a VI. Corroboram

para tanto, as medidas já adotadas pelo autuado e a atenção ao princípio da proporcionalidade. Assim, dada a inadequação de aplicação das sanções previstas nos incisos IV a IX, volta-se à possibilidade de aplicação de advertência.

7.39. Neste sentido, considerando o inciso II do artigo 9º, a aplicação de sanção de advertência com a definição de medidas corretivas face às medidas até então adotadas pelo IAMSPE para a comunicação dos titulares sobre o incidente e de melhoria da segurança e privacidade dos dados dos titulares tende a ser a melhor alternativa.

7.40. No que se refere às medidas corretivas aplicáveis, entende-se que, pela infringência do art. 49 da LGPD, o IAMSPE deve informar à ANPD, no mesmo processo em curso, o resultado dos programas e objetivos desenvolvidos e implementados conforme disposto no Anexo V (Plano de três meses e seis meses) das Alegações Finais (SUPER nº 4280896), especificamente quanto aos itens 3, 4, 5, 12, 15 e 17.

a) Em relação aos itens 3, 4 e 5, o IAMSPE deverá, em até 10 (dez) dias úteis da data da intimação:

a.1) informar o andamento e apresentar à ANPD o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual seu cumprimento será comprovado à ANPD; ou

a.2) em caso de já estarem cumpridos, trazer aos autos comprovação do cumprimento.

b) Em relação aos itens 12, 15, 17, o IAMSPE deverá apresentar à ANPD, em até 10 (dez) dias úteis da data da intimação, o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD.

8. CONCLUSÃO

8.1. Ante o exposto, considerando que o conjunto probatório dos autos demonstra que autoria e materialidade restam devidamente comprovadas nos autos, e que os fatos descritos correspondem às infrações tipificadas pelos enquadramentos indicados no Auto de Infração - arts. 48 e 49 da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), conclui-se pelas seguintes recomendações:

8.1.1. Por violação ao art. 48 da LGPD, pela aplicação da sanção de ADVERTÊNCIA ao IAMSPE, com imposição de medida corretiva abaixo, conforme disposto no art. 52 da LGPD c/c o artigo 9º inciso II do Regulamento de Dosimetria e Aplicação de Sanções Administrativas;

a) Ajustar, no prazo de 10 (dez) dias úteis da data de intimação, o COMUNICADO já existente no sítio do IAMSPE, conforme a redação abaixo sugerida:

> Lei Geral de Proteção de Dados Pessoais - Comunicação de Incidente de Segurança:
>
> O Iamspe comunica que tomou conhecimento da ocorrência de incidente de segurança que pode ter comprometido a privacidade dos dados da organização por conta de um acesso não autorizado em dados cadastrais indicados por um usuário externo no início do ano de 2022.
>
> Dentre os dados que poderiam ter sido afetados, estariam dados pessoais cadastrais, salário e de residência de nossa base de cientes, o que poderia acarretar o risco de exposição por um determinado período de tempo até nossas correções, ressaltando-se aqui que não identificamos nem fomos comunicados de extração ocorrida.
>
> Informamos que o Instituto, imediatamente, realizou ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema de cadastro dos seus contribuintes e dependentes. Por conta destas ações, o Instituto comunicou à Autoridade respectiva somente após a realização dos ajustes necessários.
>
> Após comunicação de incidente de segurança à Autoridade Nacional de Proteção de Dados e aos usuários em geral, informamos que estabelecemos um cronograma de ações para melhoria de nossos controles apresentados à ANPD..
>
> Dúvidas, solicitações e reclamações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no telefone: (11) 4573-9352, e-mail: lgpd@iamspe.sp.gov.br
>
> Estamos disponíveis para atendimento de segunda-feira a sexta-feira, das 9h às 17h. Política de Privacidade do Iamspe: http://www.iamspe.sp.gov.br/politica-de-privacidade/.

a.1) IAMSPE deverá juntar aos autos, no prazo de 10 (dez) dias úteis da data de intimação, comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 1 (uma) captura de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura.

b) O comunicado acima deve permanecer disponível por 90 (noventa) dias corridos, contados a partir da data de cumprimento do ajuste no Comunicado, nos termos do item 'a' acima.

b.1) O IAMSPE deverá juntar aos autos comprovação de que a medida corretiva acima descrita foi cumprida por meio da apresentação de, pelo menos, 9 (nove) capturas de tela do sítio do IAMSPE contendo o comunicado e com visualização clara da data da captura, sendo que cada captura deve ser feita no intervalo mínimo de 9 (nove) dias entre cada uma.

b.2) 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.

8.1.2. Por violação ao art. 49 da LGPD, pela aplicação da sanção de ADVERTÊNCIA ao IAMSPE, com imposição de medida corretiva, conforme disposto no art. 52 da LGPD c/c o artigo 9º inciso II do Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

8.1.3. No que se refere à medida corretiva aplicável, entende-se que pela infringência do art. 49 da LGPD, o IAMSPE deve informar à ANPD, no mesmo processo em curso, o resultado dos programas e objetivos desenvolvidos e implementados conforme disposto no Anexo V (Plano de três meses e seis meses) das Alegações Finais (SUPER nº 4280896), especificamente quanto aos itens 3, 4, 5, 12, 15 e 17.

a) Em relação aos itens 3, 4 e 5, o IAMSPE deverá, em até 10 (dez) dias úteis da data da intimação:

a.1) informar o andamento e apresentar à ANPD o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD; ou

a.2) em caso de já estarem cumpridos, trazer aos autos comprovação do cumprimento.

b) Em relação aos itens 12, 15, 17, o IAMSPE deverá apresentar à ANPD, em até 10 (dez) dias úteis da data da intimação, o cronograma para o seu cumprimento, sendo que o cronograma deve (i) ter prazo máximo de 1 (um) ano para sua conclusão e deve (ii) indicar a forma por meio da qual se comprovará seu cumprimento à ANPD.

8.2. Por fim, é importante salientar que a classificação das infrações, a definição das sanções (inclusos agravantes e atenuantes) e a adoção de medidas corretivas restringem-se às circunstâncias deste caso.

9. ENCAMINHAMENTOS

9.1. O presente Relatório de Instrução deve ser encaminhado ao Coordenador-Geral de Fiscalização para decisão, de acordo com art. 55 da Resolução CD/ANPD nº 1/2021.

9.2. 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 da Resolução CD/ANPD nº 1/2021 e art. 56 da Lei nº 9.784/99.

9.3. A decisão deve ser publicada no DOU, segundo o art. 55 da Resolução CD/ANPD nº 1/2021.

9.4. Após trânsito em julgado, este Processo Administrativo Sancionador passa para a fase de cumprimento da decisão para acompanhamento das obrigações de fazer determinadas.

RAVVI AUGUSTO DE ABREU C. MADRUGA
Coordenador de Fiscalização

---

[1] Este Relatório de Instrução foi elaborado com a colaboração de Geraldo Lopes da Conceição Cunha, quando servidor nesta Coordenação-Geral de Fiscalização.

[2] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

[3] Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

[4] https://www.iamspe.sp.gov.br/quem-somos/. Acessado em 29/09/2023.

[5] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;"

[6] 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.

[7] Idem.

[8] http://www.iamspe.sp.gov.br/politica-de-privacidade/. Acessado em 29/09/2023.

[9] MITIDIERO, Daniel F.; MARINONI, Luiz Guilherme B.; SARLET, Ingo W. **Curso de direito constitucional**. Editora Saraiva, 2023. E-book. ISBN 9786553624771. p. 218

[10] DONEDA, Danilo. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art 2º, caput e §§ 1º e 3º da MP 954/2020. Civilística.com, v. 9, n. 1, 2020.

[11] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo: Thomson Reuters Brasil, 2021.

[12] Idem.

Documento assinado eletronicamente por **Ravvi Augusto de Abreu Coutinho Madruga**, **Coordenador(a)**, em 05/10/2023, às 15:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade do documento pode ser conferida informando o código verificador **4286376** e o código CRC **D83111F7** no site:
https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00261.001969/2022-41 SEI nº 4286376