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

Relatório de Instrução nº 01/2024/CGF/ANPD

Brasília/DF, na data da assinatura.

1. IDENTIFICAÇÃO

1.1. Nome/Razão Social do Autuado: Instituto Nacional do Seguro Social (INSS)

1.2. CNPJ do Autuado: 29.979.036/0001-40

1.3. Porte do Autuado: - *Grande porte*

1.4. Agente de Tratamento: (X) Controlador ( ) Operador

1.5. Nome do Encarregado ou Responsável Jurídico: Edson Pinheiro Alvarista

1.6. Contado do Encarregado: edson.alvarista@inss.gov.br; encarregado@inss.gov.br

2. REFERÊNCIAS

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

2.2. Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 01, de 08/03/2021 (RI-ANPD);

2.3. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28/10/2021 (Regulamento de Fiscalização);

2.4. Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24/02/2023 (Regulamento de Dosimetria);

2.5. Processo 1.1. de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93.

2.6. Processo Administrativo Sancionador nº 00261.001888/2023-21.

3. SUMÁRIO EXECUTIVO DO PROCESSO

3.1. Auto de Infração: 03/08/2023– Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146)

Dispositivo(s) Infringido(s)	Descrição da Infração
Art. 48 da Lei nº 13.709/2018.	Não comunicar aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
Art. 32, §2º da Resolução CD/ANPD nº 1/2021	Não atendimento às determinações da ANPD.

3.2. Intimação: 03/08/2023 – *Certidão de Intimação Cumprida (SEI nº 0048150)*;

3.3. Dados de quem recebeu a Intimação: Edson Pinheiro Alvarista.

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

3.5. Data da Apresentação da Defesa: 17/08/2023 – Recibo Eletrônico de Protocolo *(SEI nº 0048155)*;

3.5.1. Defesa *(SEI nº 0048151*);

3.5.2. Processo SEI 35014.293086/2023-34 *(SEI nº 0048152)*;

3.5.3. Processo SEI 35014.437670/2022-27 *(SEI nº 0048153)*; e

3.5.4. Processo SEI 35014.528489/2022-29 *(SEI nº 0048154)*.

3.6. Produção de Prova(s) pelo Autuado: (X) Não ( ) Sim;

3.7. Produção de Prova(s) pelo Denunciante/ Titular: (X) Não ( ) Sim;

3.8. Produção de Prova(s) pela ANPD: (X) Não ( ) Sim;

3.9. Terceiro(s) Interessado(s): (X) Não ( ) Sim;

3.10. Termo de Ajustamento de Conduta: (X) Não ( ) Sim;

3.11. Alegações Finais: (X) Não ( ) Sim;

3.12. Medida(s) Preventiva(s) Aplicada(s) com base no Art. 32 do Regulamento de Fiscalização: ( ) Não (X) Sim. - Aviso nº 33/2022/CGF/ANPD (*SEI nº 0045825) e* Despacho decisório nº 3/2023/CGF/ANPD (*SEI nº 0045840*)

3.13. Medida(s) Preventiva(s) Aplicada(s) com base no Art. 7º, IV, do RI-ANPD: (X) Não ( ) Sim.

4. RELATÓRIO

4.1. Conforme disposto no art. 37 do Regulamento de Fiscalização da ANPD, 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 pela autuada face à legislação e às normas de proteção de dados.

4.2. O Instituto Nacional do Seguro Social (INSS) apresentou, em 19/10/2022, à Coordenação-Geral de Fiscalização (CGF), com fundamento no art. 48 da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), Comunicação de Incidente de Segurança (CIS) preliminar (0045818). A entidade pública autuada identificou aumento no número de consultas a dados sem justificativa operacional ou de negócio aparente. Os acessos teriam origem em uma rede autorizada, por órgão da administração pública, e com utilização de credenciais de acesso válidas, concedidas por meio de convênio pelo controlador Instituto Nacional do Seguro Social (INSS) à Advocacia Geral da União (AGU). Além disso, o autuado informou que, nos meses de agosto e setembro de 2022, foram realizadas mais de 90 milhões de consultas ao Sistema Corporativo de Benefícios do INSS (SISBEN) e 9 milhões de consultas ao Sistema Único de Benefícios DATAPREV (BLH00), quantidade quase três vezes maior que a registrada no mês de junho do mesmo ano.

4.3. Por se tratar de comunicação preliminar, no dia 3/11/2022, a Coordenação-Geral de Fiscalização encaminhou comunicação eletrônica ao autuado E-mail - 3725180 (SEI nº 0045820) solicitando a apresentação da complementação da comunicação em até 30 (trinta) dias corridos da comunicação inicial. Decorrido o prazo estabelecido sem que houvesse manifestação do agente de tratamento, a solicitação de complementação foi reiterada no dia 22/11/2022, por intermédio do E-mail - 3760075 (SEI nº 0045821), e concedido prazo adicional de 5 (cinco) dias úteis para resposta.

4.4. Embora o autuado tenha respondido à solicitação da CGF, em 22/11/2022 (SEI nº 0045823), afirmando que iria encaminhar o relatório e informar as ações efetivadas, o prazo se findou sem que as solicitações fossem atendidas. Diante do descumprimento das determinações desta Coordenação-Geral de Fiscalização, a CGF emitiu, em 29/12/2022, o **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825), em que determinou que o autuado apresentasse (a) esclarecimentos a respeito da atuação do agente de tratamento

notificante, ou seja, se atua como controlador ou operador dos dados pessoais; (b) formulário de incidente de segurança com informações complementares; (c) relatório técnico de tratamento do incidente; e ***(d) comunicação aos titulares a respeito da possível violação do sigilo dos dados no incidente, se cabível***.

4.5. Em cumprimento parcial ao **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825), o autuado apresentou os documentos solicitados em 30/12/2022, por meio do Formulário de Comunicação de Incidente de Segurança Complementar - ANPD - Aviso (SEI nº 0045828). O INSS, porém, justificou a não realização da CIS aos titulares sob alegação de ainda estar analisando a legitimidade dos acessos suspeitos. Ressaltou, ademais, que as medidas de contenção do incidente foram adotadas imediatamente após o registro do incidente pela Comissão de Tratamento e Resposta a Incidentes Cibernéticos (CTIR) da Empresa de Tecnologia e Informações da Previdência (DATAPREV).

4.6. A CGF, em 09/04/2023, por meio do **Despacho Decisório nº 3/2023/CGF/ANPD** (SEI nº 0045840), que acatou a Nota Técnica nº 13/2023/CGF/ANPD (SEI nº 0045838), determinou ao INSS que realizasse, no **prazo de 10 (dez) dias úteis,** nos termos dispostos no art. 48 da Lei nº 13.709 de 14 de agosto de 2018 (LGPD), a comunicação a todos os titulares afetados pelo incidente de segurança comunicado à ANPD e juntasse aos autos do Processo de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93 comprovação do cumprimento da presente determinação.

4.7. O autuado, no entanto, não realizou a comunicação do incidente de segurança aos titulares afetados. Em resposta, tanto no Despacho DTIR - INSS (SEI nº 0045857) quanto no Ofício 1/2023/COPDP/CGCONF/DIGOV-INSS (SEI nº 0045856), o INSS pleiteou pela inviabilidade da comunicação a todos os titulares afetados em razão da impossibilidade técnica de levantamento dos nomes dos segurados, bem como pela desproporcionalidade da comunicação universal. Solicitou, ainda, prorrogação do prazo de cumprimento das medidas preventivas até a conclusão do relatório pela AGU para reavaliação da ação a ser executada. No Ofício 2/2023/COPDP/CGCONF/DIGOV-INSS (SEI nº 0045859), o INSS solicitou prazo indeterminado para a adequação e estruturação do plano de comunicação da entidade pública e atendimento da determinação.

4.8. A CGF, por meio do Despacho (SEI nº 0045861), deferiu a solicitação de prazo adicional para que o referido plano fosse apresentado até 12/05/2023. Do mesmo modo, indicou-se que fosse apontada a data prevista para a comunicação da ocorrência do incidente aos titulares de dados, nos termos do art. 48 da LGPD. Em resposta, foram protocolados pela autuada, no dia 24/05/2023, os documentos Anexo Plano Estratégico de Comunicação Externa (SEI nº 0045866) e Anexo Plano Estratégico de Comunicação Interno (SEI nº 0045867). Entretanto, os documentos enviados à CGF não versam sobre a comunicação ao titular do incidente de segurança em questão, de maneira que a

medida preventiva determinada pela ANPD não foi cumprida.

4.9. A CGF, finalmente, em 23/06/2023, acatou as razões da Nota Técnica nº 54/2023/CGF/ANPD (SEI nº 0045864) e, diante da inércia do autuado em adotar as medidas preventivas determinadas pelo **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825) e pelo Despacho Decisório nº 3/2023/CGF/ANPD (SEI nº 0045840), decidiu pela instauração de processo administrativo sancionador em desfavor do Instituto Nacional do Seguro Social (INSS), nos termos do art. 17, incisos I e III do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 08/03/2021.

4.10. Em 03/08/2023, foi exarado o Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146), devidamente recebido pelo autuado no mesmo dia, conforme a certidão de intimação cumprida (SEI nº 0048150). Conforme o Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146), os dispositivos infringidos pela autuada têm como fundamento (i) a ausência de comunicação de incidente de segurança aos titulares – art. 48 da LGPD; e (ii) a falta de atendimento de medida preventiva – art. 32, §2º, do Regulamento de Fiscalização (Resolução CD/ANPD nº 1/2021).

4.11. Ato contínuo, foi conferido ao autuado o prazo de 10 (dez) dias úteis, a partir da ciência do Auto de Infração em tela, para apresentar **Defesa** perante a Coordenação-Geral de Fiscalização da Autoridade Nacional de Proteção de Dados, via SEI, conforme instruções do Anexo 01, de acordo com o art. 47, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

4.12. Em 17/08/2023, portanto, dentro do prazo indicado, foram encaminhados à CGF os seguintes documentos: Defesa SEI_12906070 (SEI nº 0048151); Processo SEI_35014.293086_2023_34 (SEI nº 0048152); Processo SEI_35014.437670_2022_27 (SEI nº 0048153); e Processo SEI_35014.528489_2022_29 (SEI nº 0048154). No entanto, não foram apresentadas novas provas pela entidade regulada após a intimação. Com isso, em virtude da faculdade disposta no art. 53 do Regulamento de Fiscalização, foi encaminhado ao Coordenador de Proteção de Dados Pessoais (COPDP) do INSS, por meio do Ofício nº 72/2023/FIS/CGF/ANPD (SEI nº 0048156), intimação para que o autuado apresentasse **alegações finais,** no prazo de 10 (dez) dias úteis, a partir da ciência deste Ofício, perante a Coordenação-Geral de Fiscalização da ANPD.

4.13. Do mesmo modo, informou-se à entidade pública autuada que ela poderia indicar eventuais informações constantes no presente processo sancionatório que, a seu ver, encontrar-se-iam protegidas por hipótese legal de sigilo, devendo-se indicar as razões de fato e de direito que sustentariam

eventual restrição de acesso a informações.

4.14. O autuado foi considerado intimado, em 02/01/2024, por decurso do prazo tácito, conforme Certidão de Intimação Cumprida (SEI nº 0048157).

4.15. É o relatório.

5. PRELIMINARES

5.1. Competência.

5.1.1. 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". Os dados envolvidos no incidente de segurança aqui tratado – CPF, nome completo, data de nascimento, diagnóstico, data de encaminhamento médico, responsável pela criança, números de telefone e endereço – são dados pessoais (alguns até mesmo sensíveis), pois consistem em informação relacionada a pessoa natural identificada ou identificável.

5.1.2. Diante disso, resta claro que o incidente de segurança informado à ANPD envolve o tratamento de dados pessoais de terceiras pessoas, uma vez que o evento adverso teria afetado a base de beneficiários e segurados do INSS, que inclui dados pessoais como Nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes. Além disso, observa-se que, por se tratar de banco de dados com informações sobre benefícios previdenciários, o incidente de segurança potencialmente envolve dados pessoais sensíveis. Nos termos do inciso II do art. 5º da LGPD, considera-se dados pessoais sensíveis os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5.1.3. No que se refere ao papel dos agentes de tratamento responsáveis pela base de dados envolvida no incidente de segurança, verifica-se que a DATAPREV atua como a operadora do Sistema Corporativo de Benefícios do INSS (SISBEN), por se tratar de pessoa jurídica de direito privado, vinculada ao Ministério da Gestão e Inovação em Serviços Públicos (MGI), responsável pelo tratamento de dados pessoais em nome do controlador. O INSS, por sua vez, atua como a entidade controladora da referida base de dados, por se tratar de, nos termos do art. 5º, VI, pessoa jurídica de direito público a quem compete as decisões referentes ao tratamento de dados pessoais dos beneficiários.

5.1.4. A Lei nº 13.709, de 14/08/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), por sua vez, determina no art. 48 que "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". O §1º, por

sua vez, estabelece que a comunicação deve ocorrer em prazo razoável e indicar a natureza dos dados pessoais afetados, os titulares envolvidos, as medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente, os motivos da demora e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

5.1.5. Ainda, cabe à ANPD, de acordo com o art. 55-J, I, da LGPD "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".

5.1.6. 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;
>
> (...)
>
> IX - requisitar aos agentes de tratamento de dados a apresentação de Relatório de Impacto à Proteção de Dados Pessoais;

5.1.7. 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 do suposto incidente de segurança ocorrido no Instituto de Pesquisas Jardim Botânico do Rio de Janeiro em processo administrativo próprio, pois é necessário observar as diretrizes e os princípios incidentes sobre a atuação administrativa no cumprimento da atribuição de fiscalização.

5.1.8. O Regulamento de Fiscalização da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28/10/2021, 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.

5.1.9. Por força do art. 4º, I, do mencionado Regulamento, o Instituto de Pesquisas Jardim Botânico do Rio de Janeiro é considerado agente regulado pela ANPD, haja vista ser um agente de tratamento (ver. art. 5º, IX da LGPD). Cumpre especificar as atividades a que os agentes regulados estão submetidos, a teor do art. 5º:

> 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.

5.1.10. Pelo exposto, não há dúvidas quanto à competência da ANPD no caso concreto para avaliar a conduta do Instituto de Pesquisa Jardim Botânico do Rio de Janeiro, controlador de dados e agente regulado, à luz da LGPD.

5.2. **Prescritibilidade.**

5.2.1. No presente processo, não há que se analisar a prescrição intercorrente, a qual pode ser verificada quando existe paralisação do processo por mais de 3 (três) anos, a teor do Art. 1º, §1º, Lei nº 9.873/99. Com

efeito, os documentos recebidos pela ANPD e que subsidiaram a abertura do processo de fiscalização foram recebidos em 26/01/2022, e considerando as ações desenvolvidas, bem como a data de apresentação do presente relatório, não há que se falar em paralisação do processo por mais de 3 (três) anos. Tampouco foi verificada a prescrição punitiva, a qual incide após cinco anos da data do ato, consoante disposto no art. 1º, *caput*, da Lei nº 9.873/99.

5.3. No mais, o autuado não arguiu questões preliminares de mérito em sua defesa e em nossas análises preliminares não verificamos questões relevantes a serem trazidas a este Relatório de Instrução.

6. ANÁLISE

6.1. *Circunstâncias da infração*

6.1.1. Os documentos apresentados aos autos são suficientes para afirmar que houve um incidente de segurança, envolvendo dados do Sistema Corporativo de Benefícios do INSS (SISBEN), conforme detalhado na Nota Técnica 13/2023/CGF/ANPD (SEI nº 0045838), Processo de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93. Conforme disposto no documento, a comunicação do evento adverso aos titulares afetados justificar-se-ia em virtude do elevadíssimo número de pessoas naturais potencialmente afetadas, uma vez que a base de dados envolvida armazena uma grande quantidade de dados pessoais, tais como nome, CPF, NIT, RG, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes, cuja publicação indevida poderia expor os titulares a riscos de fraudes e roubo de identidade. O próprio autuado, nesse sentido, informou que utilizou como critério de comunicação à ANPD que "O incidente de segurança pode acarretar risco ou dano relevante aos titulares".

6.1.2. A determinação de comunicação aos titulares, no prazo de 10 (dez) dias úteis, foi formalizada no Despacho Decisório 3 (SEI nº 0045840) e encaminhada ao INSS por meio do Ofício 58 (SEI nº 0045841). O INSS foi intimado da referida decisão por via eletrônica no dia 10/04/2023, conforme Certidão de Intimação Cumprida (SEI nº 0045844). O agente de tratamento também confirmou o recebimento do Ofício, conforme e-mail do INSS (SEI nº 0045852), de 12/04/2023 e e-mail do DATAPREV (SEI nº 0045853), de 13/04/2023.

6.1.3. Em resposta, o INSS apresentou a Portaria PRES/INSS nº 30, de 15 de fevereiro de 2023 (SEI nº 0045847), com a alteração do Encarregado, protocolou Ofício (SEI nº 0045856) e Despacho (SEI nº 0045857), em 25/04/2023. Em resumo, pleiteou pela inviabilidade da comunicação a todos os titulares afetados em razão da impossibilidade técnica de levantamento dos nomes dos segurados e da desproporcionalidade da comunicação universal. Solicitou, ainda, prorrogação do prazo até a conclusão do relatório pela AGU para reavaliação da ação a ser executada.

6.1.4. Entretanto, mesmo com o deferimento da prorrogação do prazo de cumprimento da medida preventiva determinada pela CGF, conforme o Despacho (SEI nº 0045861), o INSS não comunicou o incidente de segurança aos titulares de dados pessoais afetados, em claro descumprimento das obrigações legais exaradas no art. 48 da LGPD e do art. 32, §2º, do Regulamento de Fiscalização (Resolução CD/ANPD nº 1/2021).

6.1.5. Restam comprovados, assim, os fatos que ensejaram a instauração deste PAS e a autoria por parte da autuada, nos termos do art. 43, inciso I, da Lei Geral de Proteção Dados Pessoais.

6.2. **Análise da defesa apresentada pelo Autuado**

6.2.1. O INSS, em sede de defesa (SEI nº 0048151), apresentou os argumentos abaixo:

6.2.2. Decisão sobre comunicação do incidente de segurança ao titular deve passar por juízo de pertinência pela Administração Pública.

> "[A] divulgação aos titulares supostamente afetados, quando possível, deve ser avaliada pela Administração Pública Federal e, não havendo comprometimento dos interesses maiores do Estado, as comunicações devem ser realizadas. Isso se dá dessa forma em razão do prevalecimento do interesse público sobre os interesses individuais. No caso, o incidente de segurança que ensejou a abertura do presente processo sancionador foi tempestivamente comunicado à ANPD, que determinou e insistiu na comunicação dos titulares dos dados potencialmente acessados, o que não ocorreu em razão de não se vislumbrar sua pertinência."

6.2.3. A comunicação do incidente de segurança ao titular é medida irrazoável e prejudicial ao interesse público.

> "Por um lado, não foi possível determinar os potenciais dados acessados e seus correspondentes titulares, de modo que comunicações individualizadas seriam materialmente impossíveis. Por outro, uma divulgação ampla e indistinta do incidente cibernético, que teria atingido um percentual ínfimo das milhões de pessoas com as quais o INSS manteve algum tipo de relação ao longo de décadas, contaria apenas com o potencial de gerar pânico e desconfiança em todo o contingente de segurados e beneficiários vinculados ao INSS. Qualquer comunicado a respeito do incidente, antes de proteger efetivamente os segurados e beneficiários, ocasionaria um caos nos canais de atendimento do INSS, que não teria condições sequer de indicar objetivamente se dados foram efetivamente acessados, quais dados e de quais pessoas, caso fosse demandado a fazê-lo. Nesse passo, a determinação para a comunicação dos titulares, além de sobrepujar o princípio da supremacia do interesse público no caso concreto, também

consistiria em medida irrazoável, posto que impossível de execução material em função da indeterminação de dados e seus titulares, e desproporcional, a considerar que impõe obrigação em medida superior àquelas estritamente necessárias ao atendimento do interesse público, que já foram tomadas pelos agentes de tratamento, a saber, o INSS, DATAPREV e AGU, que agiram com total transparência e atenderam aos preceitos legais e normativos da LGPD."

6.2.4. A consequência danosa da comunicação do incidente de segurança ao titular, em vista do art. 20 da LINDB.

"A ampla divulgação aos titulares dos dados que possam ser afetados em incidentes de segurança não é uma consequência legal necessária e automática, dependendo da presença das condições do § 2º do artigo 48 da LGPD, cuja interpretação e aplicação deve ser motivada sob a perspectiva dos princípios da razoabilidade e da proporcionalidade e do consequencialismo."

6.2.5. A determinação que obriga comunicação do incidente de segurança ao titular deve ser motivada pela ANPD.

"No § 2º de tal dispositivo também consta que a ANPD 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 a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente. [...] A ampla divulgação exigiria uma motivação específica por parte da ANPD a respeito das condições estabelecidas em tal dispositivo. Por outro lado, a Coordenação de Fiscalização da ANPD não emprestou qualquer valor às medidas que foram tomadas incontinente no sentido de investigar, comunicar e sanear o problema identificado, num ambiente de absoluta boa-fé e transparência nos processos administrativos. [...] A Coordenação de Fiscalização da ANPD não motivou sua determinação de comunicação do incidente segundo os aspectos contidos no § 2º do artigo 48 da LGPD, nos termos dos artigos 20 a 22 da LINDB. [...] O auto de infração deve ser considerado nulo por falta de motivação, observado o disposto no artigo 2º da Lei nº 4.717, de 29 de junho de 1965, e o disposto no artigo 50, I e II, da Lei nº 9.784, de 1999, ou insubsistente em relação ao mérito, dada a inobservância da supremacia do interesse público, dos princípios da proporcionalidade e da razoabilidade e do consequencialismo tratado na LINDB."

6.2.6. O Decreto 10.748, de 16 de julho de 2021, impede a divulgação de informações sobre incidente de segurança sofrido pela Administração Pública Federal.

"[A] LAI, ao tratar de hipóteses restritivas ao acesso de informações, em seu artigo 23, estabeleceu a possibilidade de serem classificadas

> como sigilosas informações "imprescindíveis à segurança da sociedade ou do Estado". E o Decreto nº 10.748, de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos, considera que as informações sobre incidentes cibernéticos são imprescindíveis à segurança da sociedade e do Estado. Confira-se o disposto em seu artigo 15 [...]. O cotejo entre o artigo 23 da LAI c/c com o artigo 15 do Decreto nº 10.748, de 2021 e o artigo 48 da Lei nº 13.709, de 2018 revelam uma antinomia aparente. Antinomia que não resiste à aplicação do critério da especialidade. Com efeito, o controlador tem o dever de comunicar à ANPD e aos titulares dos dados sobre os incidentes cibernéticos, na presença de riscos ou danos relevantes. E a divulgação aos titulares supostamente afetados, quando possível, deve ser avaliada pela Administração Pública Federal e, não havendo comprometimento dos interesses maiores do Estado, as comunicações devem ser realizadas. Isso se dá dessa forma em razão do prevalecimento do interesse público sobre os interesses individuais."

6.3. ***Das alegações finais apresentadas pelo Autuado***

6.3.1. Foi encaminhado ao Coordenador de Proteção de Dados Pessoais (COPDP) do INSS, por meio do Ofício nº 72/2023/FIS/CGF/ANPD (SEI nº 0048156), intimação para que o autuado apresentasse **alegações finais,** no prazo de 10 (dez) dias úteis, a partir da ciência deste Ofício, perante a Coordenação-Geral de Fiscalização da ANPD, conforme os termos facultados no art. 53 do Regulamento de Fiscalização. O autuado, porém, não respondeu à solicitação, motivo pelo qual foi considerado intimado, em 02/01/2024, por decurso do prazo tácito, conforme Certidão de Intimação Cumprida (SEI nº 0048157).

6.4. ***Subsunção do fato ao tipo infracional correspondente***

<u>I - Da obrigação de comunicar o titular sobre o incidente de segurança em questão: descumprimento do art. 48 da LGPD pelo INSS.</u>

6.4.1. A LGPD inaugurou um sistema jurídico para tutelar os direitos e garantias dos titulares de dados pessoais, a fim de resguardar que qualquer tratamento de dados referente à pessoa natural identificada ou identificável ocorra em acordo com as determinações legais previstas no ordenamento jurídico. Dessa forma, a LGPD estabelece uma série de determinações que devem ser cumpridas pelos agentes de tratamento para que sejam garantidos a autodeterminação informativa, a privacidade, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, entre outros elencados em seu art. 2º.

6.4.2. O artigo 48 da LGPD, nesse sentido, estabelece a obrigação do controlador de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e

ao titular de dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Observe-se abaixo:

> ***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. (Grifo nosso)

6.4.3. Pode-se compreender pela leitura do *caput* do artigo que o controlador não se encontra obrigado a comunicar aos destinatários de direito (ANPD e titulares) a ocorrência de todo e qualquer tipo de incidente de segurança, mas apenas em relação ao *incidente de segurança qualificado*, isto é, aquele cuja ocorrência, em virtude da natureza dos dados pessoais envolvidos ou do número de pessoas naturais afetadas, por exemplo, possa gerar lesões potencialmente danosas aos direitos dos indivíduos afetados[1].

6.4.4. Em caso de ocorrência de incidente de segurança, desse modo, cabe ao controlador avaliar se as consequências do evento podem ocasionar danos materiais ou morais relevantes aos titulares, como discriminação, violação aos direitos à imagem, honra e privacidade, fraudes financeiras e roubos de identidades. É importante destacar, nesse sentido, que o controlador deve sempre agir com cautela ao avaliar as probabilidades de danos a terceiros, de maneira a adotar as medidas preventivas contidas no artigo 48 da LGPD mesmo

nos casos em que houver dúvidas quanto à gravidade dos riscos e danos envolvidos. Isso ocorre uma vez que a comunicação do incidente de segurança qualificado tem como objetivo não apenas o cumprimento do dever de mitigação do prejuízo pelo próprio controlador, mas sobretudo permitir que a pessoa natural afetada possa tomar medidas preventivas para conter os eventuais danos provocados pelo evento[2]. Observe-se, nesse sentido, a conduta defendida por MODENESI (Brasil, 2022):

> "Eventualmente, diante de um caso concreto em que o controlador esteja em dúvida sobre a consumação do incidente de segurança, deve-se, mediante conduta cautelosa e preventiva, **comunicar à autoridade nacional e ao titular** as circunstâncias da ocorrência apurada, o que desvela uma renovada aplicação, no âmbito dos direitos civis, do brocado *in dubio pro societate*, pois proteger dados pessoais e pessoas humanas é, ao fim e ao cabo, proteger toda a sociedade. ***Essa orientação interpretativa induz à criação de uma máxima adequada à sociedade da informação: in dubio pro titular dos dados, que, inclusive, já vem sendo reconhecida como um princípio apto a compensar as assimetrias de poder e de conhecimento entre titular e agentes de tratamento***". (Grifo nosso).

6.4.5. Desse modo, verificado que o incidente de segurança pode gerar risco ou dano relevante aos titulares de dados pessoais, *o controlador não pode se eximir de fazer a devida comunicação do evento adverso*, nos termos do *caput* do art. 48 da LGPD, *tanto para a ANPD quanto para os titulares afetados*. Desse modo, uma vez que a comunicação aos titulares de dados, conforme já destacado, visa a possibilidade de mitigação de eventuais impactos negativos decorrentes do incidente, *ela deve ser feita o mais rapidamente possível*[3].

6.4.6. Assim, além da obrigação de comunicação do incidente aos sujeitos destinatários, a LGPD também estabelece que as informações pertinentes ao evento adverso devem ser prestadas em tempo razoável, nos termos do §1º do art. 48 da LGPD. Ainda que a norma não imponha prazo específico para a comunicação, a demora injustificada na tomada de ação pelo controlador deve ser compreendida como infração ao dever exarado pelo *caput* da norma em comento, pois impede que o titular possa tomar medidas que garantam a segurança de seus dados pessoais, apesar da ocorrência do incidente. É importante ressaltar, nesse sentido, que a ANPD recomenda que o incidente de segurança seja comunicado em até 2 (dois) dias úteis da ciência do fato[4].

6.4.7. Diante do exposto, não há que se falar em exercício do poder discricionário da Administração quando observado que o incidente de segurança ocorrido é potencialmente lesivo aos titulares, por ensejar relevante risco de dano a seus direitos e garantias fundamentais. O poder

discricionário pode ser exercido pela Administração quando o agente administrativo, dentre várias condutas possíveis, pode optar pela ação que traduz maior conveniência e oportunidade para o interesse público[5]. A norma do art. 48 da LGPD *não* confere ao controlador liberdade para fixar juízo de ordem técnica quanto à possibilidade de comunicação do incidente de segurança qualificado aos titulares quando identificado o potencial de ocorrência de danos relevantes decorrentes do avento adverso.

6.4.8. O *caput* do art. 48, na verdade, impõe ao controlador uma atuação vinculada, pois obriga-o a realizar conduta rigorosamente nos termos do parâmetro definido em lei, qual seja, a comunicação tanto à ANPD quanto ao titular de ocorrência do incidente de segurança qualificado que envolva dados pessoais. É importante destacar, nesse sentido, que os sujeitos destinatários da obrigação de comunicação são tanto a Autoridade Nacional de Proteção de Dados quanto os titulares afetados pelo incidente, não cabendo ao controlador optar a quem encaminhará a devida comunicação.

6.4.9. Logo, verificada a ocorrência do incidente de segurança qualificado envolvendo dados pessoais, o controlador deve necessariamente comunicar os titulares sobre a ocorrência do evento, nos termos do *caput* do art. 48 da LGPD. Não há que se falar, desse modo, em exercício legítimo do poder discricionário pelo controlador, uma vez que o agente de tratamento se encontra vinculado à determinação da norma supracitada.

6.4.10. Percebe-se, portanto, conforme destacado no **Auto de Infração nº 1/2023/FIS/CGF/ANPD** (SEI nº 0048146)**, que o INSS** agiu em desconformidade com o disposto no *caput* do art. 48 da LGPD, uma vez que não comunicou aos titulares afetados a ocorrência de incidente de segurança qualificado, consoante verificado por esta Autoridade Nacional de Proteção de Dados no âmbito do Processo de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93.

6.4.11. Conforme verificado durante a tramitação do referido PAI, ademais, o INSS não refutou ou questionou a ocorrência do incidente de segurança ou a possibilidade deste acarretar risco ou dano relevante aos titulares. Na verdade, a própria entidade pública autuada admitiu que o incidente de segurança em comento poderia ensejar riscos e danos aos titulares de dados envolvidos. Tais riscos estão associados ao teor dos dados pessoais contidos na base de dados objeto do incidente, que abrangem dados de comprovação de identidade oficial, bem como dados financeiros e referentes à saúde dos titulares, segundo o Formulário de Comunicação de Incidente de Segurança Complementar - ANPD - Aviso (SEI nº 0045828). O vazamento desses dados pessoais, portanto, pode causar aos titulares tanto danos patrimoniais quanto extrapatrimoniais.

6.4.12. No caso concreto, portanto, caberia ao INSS comunicar as pessoas naturais cujos dados pessoais compunham as bases de dados atingidas pelo incidente de segurança relatado à ANPD, indicando todas as informações referidas no §1º do art. 48 da LGPD. No entanto, a entidade pública regulada resistiu até o momento em cumprir a determinação legal em comento, mesmo após diversas determinações feitas pela Coordenação Geral de Fiscalização (CGF), evidenciando o descumprimento da obrigação legal inserida no art. 48 da Lei Geral de Proteção de Dados Pessoais.

II - Do não atendimento às requisições da ANPD pela entidade autuada:Art. 32, §2º da Resolução CD/ANPD nº 1/2021.

6.4.13. A comunicação do incidente de segurança é medida preventiva importante, pois, a partir da ação do controlador, o próprio titular pode realizar ações acautelatórias que o protejam de eventuais furtos de identidade, fraudes, assédios comerciais, dentre outros danos que possam o atingir desde a ocorrência do incidente. A Resolução CD/ANPD nº 1/2021, nesse sentido, confere à Coordenação Geral de Fiscalização, no exercício do poder de fiscalização conferido pelo art. 55-J, IV, da LGPD, o poder de determinar ao agente de tratamento medidas preventivas que visem remediar situações que acarretem riscos ou danos aos titulares de dados. Dentre tais medidas, encontra-se a divulgação de informações.

6.4.14. Conforme já relatado nos itens 4.4 e 4.6 do presente Relatório de Instrução, a Coordenação Geral de Fiscalização determinou ao autuado que realizasse a comunicação do incidente de segurança qualificado aos titulares em duas oportunidades. Primeiramente, foi encaminhado o **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825). Posteriormente, a determinação foi exarada por meio do **Despacho Decisório nº 3/2023/CGF/ANPD** (SEI nº 0045840). Em ambas as oportunidades, no entanto, houve a recusa do INSS em cumprir a determinação desta Autarquia Federal, o que implica a subsunção do fato à infração disposta no art. 32, §2º da Resolução CD/ANPD nº 1/2021.

6.4.15. Deve-se, contudo, analisar mais detalhadamente os argumentos trazidos ao conhecimento da CGF pela entidade pública autuada para justificar a sua inércia. Para esse fim, os argumentos apresentados na defesa foram divididos em três blocos: *(i) a comunicação do incidente de segurança qualificado como medida necessária para a proteção dos direitos do titular; (ii) o interesse público subjacente à comunicação do incidente de segurança e da razoabilidade da medida preventiva; e (iii) a inaplicabilidade do art. 15 do Decreto nº 10.748/2021 ao caso concreto.*

(i) A comunicação do incidente de segurança qualificado como medida necessária para a proteção dos direitos do titular:

6.4.16. O INSS, em defesa apresentada no presente processo administrativo sancionador (SEI nº0048151), indicou não haver "como precisar quais dados foram potencialmente acessados, consultados e eventualmente compartilhados, nem as pessoas casualmente afetadas", e que "não foi possível determinar os potenciais dados acessados e seus correspondentes titulares, de modo que comunicações individualizadas seriam materialmente impossíveis". Diante eventual impossibilidade de rastrear os titulares afetados pelo incidente, o autuado arguiu que não seria logicamente possível que a comunicação do incidente fosse realizada de maneira individual, sob pena de não se alcançar o objetivo da medida.

6.4.17. O autuado, desse modo, afirmou não haver conseguido mapear um grupo específico potencialmente atingido pelo incidente, motivo pelo qual a comunicação individual do incidente de segurança ao titular, que seria a solução adequada para a conformidade com o disposto no *caput* da norma, não foi cumprida.

6.4.18. O INSS, além disso, argumentou que eventual "divulgação ampla e indistinta do incidente cibernético (...) **contaria apenas com o potencial de gerar pânico e desconfiança em todo o contingente de segurados e beneficiários vinculados ao INSS**". Desse modo, advertiu que "(q)ualquer comunicado a respeito do incidente, antes de proteger efetivamente os segurados e beneficiários, ocasionaria **um caos nos canais de atendimento do INSS**, que não teria condições sequer de indicar objetivamente se dados foram efetivamente acessados, quais dados e de quais pessoas, caso fosse demandado a fazê-lo" (Grifo original).

6.4.19. Em que pese os argumentos trazidos pelo INSS, compete à entidade, no papel de controladora, empregar todos seus esforços para cumprir a norma de proteção de dados pessoais de forma eficaz. Por conseguinte, a falta de mecanismos de segurança que permitam o rastreio dos dados acessados no incidente ou a impossibilidade técnica de individualização dos titulares afetados pelo incidente, conforme alegado, não deve ser justificativa suficiente para a inaplicabilidade da obrigação legal exarada pelo art. 48 da LGPD, bem como pelo descumprimento da determinação deste órgão fiscalizador.

6.4.20. O objetivo da comunicação ao titular, como já ressaltado neste RI, é garantir ao titular a possibilidade de tomar medidas preventivas para se proteger de eventuais furtos de identidade, fraudes, assédios comerciais, entre outros danos que possam o atingir desde a ocorrência do incidente. Além disso, a inobservância desse dever pelo autuado pode incentivar postura de pouco cuidado com segurança da informação por parte dos agentes de tratamento, uma vez que, não sendo possível a comunicação individualizada ao titular, a obrigação de comunicação não persistiria. Neste cenário, o agente

se valeria do próprio descuido (negligência) para justificar o não cumprimento da lei. Tal conduta, do mesmo modo, exacerba a assimetria informacional existente entre o agente de tratamento e o titular dos dados, ao privar a pessoa natural afetada de receber informações pertinentes quanto ao tratamento de seus dados pessoais pelo controlador, em especial no que se refere aos procedimentos de segurança aos quais os dados são submetidos.

6.4.21. O princípio da boa-fé objetiva, previsto no *caput* do art. 6º da LGPD, nesse sentido, estabelece que as operações de tratamento de dados pessoais devem ser realizadas pelo controlador com observância dos deveres de lealdade e de transparência com o titular, isto é, o controlador precisa orientar as suas ações com base nos interesses legítimos e expectativas razoáveis do titular, no contexto de tratamento que não lhe cause qualquer tipo de abuso, lesão ou desvantagem[6]. Frazão, Prata de Carvalho e Milanez (Brasil, 2022), inclusive, definem que o princípio da boa-fé objetiva possui função limitadora ao restringir, de certa forma, a liberdade de conduta dos agentes de tratamento ao considerar certas práticas como possivelmente abusivas e ao incentivar a transparência e a previsibilidade nas relações jurídicas[7].

6.4.22. A recusa do controlador em comunicar o titular sobre a ocorrência de incidente de segurança qualificado, desse modo, vai de encontro ao princípio da boa-fé objetiva, uma vez que há expectativa razoável do titular em ser devidamente informado sobre incidentes de segurança que possam ensejar resultados danosos para o exercício de seus direitos individuais. Ademais, como um dos objetivos da comunicação é justamente permitir que o titular possa tomar medidas acautelatórias para proteger seus dados pessoais, a falta proposital de comunicação pelo controlador evidencia claro desrespeito ao princípio da prevenção, inscrito no inciso VIII do art. 6º da LGPD. No caso concreto, configura-se uma exacerbação da assimetria informacional entre controlador e titulares de dados, quanto aquele impede que estes tenham todas as informações necessárias para a proteção da tutela de seus direitos e garantias fundamentais.

6.4.23. A impossibilidade técnica de comunicação individual do incidente de segurança qualificado, portanto, não exime o controlador da obrigação legal de comunicação do evento adverso aos titulares, uma vez que a divulgação do incidente pode ser feita por meios indiretos, como uma comunicação individualizada a todos os titulares potencialmente afetados (100% dos titulares cujos dados são tratados no sistema ou na base de dados comprometida), como uma comunicação difusa em seus canais de atendimento e relacionamento (independentemente de ser um titular potencialmente afetado) ou, por fim, como a ampla publicação em meios de comunicação, este último conforme admitido pelo §2º do art. 48 da LGPD.

Nessa transição gradual do mais 'discreto e preciso' ao mais 'exposto e difuso' é possível observar a proporcionalidade entre o ônus que recai sobre o controlador em função de seu preparo e adequação à LGPD: um controlador preparado com sistemas adequados à LGPD (art. 46 e 49) possui governança o suficiente para identificar quem e quando foi afetado e direcionar sua comunicação somente às pessoas efetivamente afetadas, consequentemente reduzindo sua exposição; um controlador que não tomou o devido cuidado em se adequar à LGPD não será capaz de individualizar as pessoas e por conseguinte necessita se expor mais para atingir o comando legal de comunicar às pessoas que seus dados foram potencialmente afetados. Admitir qualquer leitura em sentido oposto constitui uma lógica perversa que estimula o descaso com a segurança da informação, a insensibilidade com o impacto de incidentes nas vidas das pessoas e converte em 'sanção' financeira o investimento realizado pelo controlador que agiu corretamente. Em situações de mercado concorrencial, isso pode até causar abalos significativos no equilíbrio concorrencial entre os agentes econômicos.

6.4.24. Não se deve, ademais, impugnar o Auto de Infração nº 1/2023/FIS/CGF/ANPD por falta de transparência quanto à motivação que levou ao referido ato administrativo, conforme alegado pelo autuado. Os motivos determinantes que fundamentaram a medida regulatória foram devidamente informados à entidade autuada no âmbito da Nota Técnica 13/2023/CGF/ANPD (SEI nº 0045838), conforme consta no item 7. da Descrição dos fatos e dos dispositivos infringidos do Auto de Infração nº 1/2023/FIS/CGF/ANPD. Nesse sentido, foi informado ao autuado que "(a) comunicação ao titular deve ser feita em razão do elevadíssimo número de titulares potencialmente afetados, pois trata-se de sistemas que armazenam uma grande quantidade de dados pessoais, tais como Nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes. No mesmo sentido, o próprio INSS informou como critério para comunicação à ANPD que "o incidente de segurança pode acarretar risco ou dano relevante aos titulares"".

(ii) Do interesse público subjacente à comunicação do incidente de segurança e da razoabilidade da medida preventiva:

6.4.25. O princípio da razoabilidade está implícito na Constituição da República Federativa do Brasil e expresso na legislação infraconstitucional, como na Lei nº 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal. De acordo com esse princípio, a Administração Pública deve atuar dentro de certos padrões médios de aceitabilidade pela sociedade, de maneira que será compreendida como razoável a conduta do Estado quando legítima perante o corpo social. Do mesmo modo, não se poderia esperar da Administração a adoção de condutas que resultassem em desacordo

com os princípios gerais do direito.

6.4.26. Pode-se compreender, desse modo, que o princípio da razoabilidade aplicado às atividades de fiscalização da ANPD visaria explicitar a necessidade do uso moderado dos meios administrativos disponíveis para a aplicação da Lei Geral de Proteção de Dados Pessoais. Assim, por meio da observância do princípio da razoabilidade, buscar-se-ia evitar que o atendimento às determinações da ANPD, no exercício das suas atividades fiscalizatória e sancionatória, gerasse encargo excessivamente oneroso para a entidade regulada, especialmente quando o atendimento da determinação estatal se mostrasse em desconformidade com o interesse público preponderante ou os princípios gerais do direito.

6.4.27. Segundo o princípio da supremacia do interesse público, presume-se que a atuação do Estado está pautada pelo interesse geral, consubstanciado nas leis e na Constituição, sendo, desse modo, um resultado da "vontade geral". Decorre deste princípio o fato de que, em havendo conflito entre os interesses privados e o interesse público, representado pelo Estado, prevalecerá este último, resguardando-se os direitos dos particulares.

6.4.28. De acordo com Barroso (Barroso, 2015)[8], ao se analisar a incidência do princípio da supremacia do interesse público em determinada relação jurídica, deve-se primeiramente distinguir o interesse público primário do interesse público secundário. O interesse público primário pode ser compreendido como a própria razão de ser do Estado, ou seja, caracteriza-se como os interesses de toda a sociedade, como a promoção da justiça e do bem-estar social. O interesse público secundário, por sua vez, pode ser entendido como a vontade da pessoa jurídica de direito público exarada em determinada relação jurídica. Para o autor, é o interesse público primário que desfruta de supremacia em um sistema constitucional e democrático, uma vez que ele não é passível de ponderação, uma vez que constitui o próprio parâmetro para a ponderação com outros direitos e garantias fundamentais. O interesse público secundário, por outro lado, ao entrar em aparente colisão com outros valores jurídicos, deve ser ponderado com base nas condições fáticas e de direito presentes no caso concreto.

6.4.29. A avaliação acerca da razoabilidade da ação fiscalizatória da ANPD exige, portanto, uma reflexão qualitativa a respeito da plausibilidade da determinação em análise, ou seja, deve-se avaliar se o objeto da resolução estatal se encontra dentro dos limites impostos pelos princípios gerais do direito e pelo meio social com que o direito à proteção de dados pessoais dialoga. Desse modo, é preciso avaliar as opções disponíveis, no caso concreto, com o objetivo de atingir a solução mais adequada à consecução do interesse público.

6.4.30. Observa-se que no caso em análise a medida determinada pela

ANPD à entidade autuada encontra-se dentro das alternativas legais dispostas em norma jurídica específica, isto é, o art. 48 da LGPD, motivo pelo qual a determinação encontra-se dentro dos limites legais impostos pelo ordenamento jurídico. Conforme já discutido na seção anterior, uma vez identificadas as premissas legais para realização da comunicação do incidente de segurança, não cabe à entidade escolher a qual destinatário irá encaminhar os avisos pertinentes, de maneira que a divulgação aos titulares afetados é obrigatória. Por conseguinte, conforme já destacado, a necessidade de comunicação aos titulares, ainda que de forma indireta, encontra-se amparada pelos princípios gerais de proteção de dados pessoais, especialmente no que se refere à boa-fé e à prevenção. Há, desse modo, legítima expectativa dos titulares de dados em ser devidamente informados sobre incidentes cibernéticos que envolvam seus dados pessoais, sobretudo quando o evento adverso puder provocar riscos e danos relevantes a seus direitos. Assim, é certo que a medida preventiva determinada por esta Autarquia federal encontra-se de acordo com a racionalidade inscrita na Lei Geral de Proteção de Dados Pessoais, motivo pelo qual não se vislumbra ilegalidade ou ilegitimidade na ação fiscalizatória.

6.4.31. Percebe-se, ademais, que as alegações trazidas pelo INSS para indicar a irrazoabilidade da ampla divulgação do incidente de segurança em meios de comunicação, em virtude da impossibilidade técnica de se proceder à comunicação individual dos titulares, baseia-se em eventuais dificuldades administrativas a serem absorvidas pela entidade, como o aumento da sua capacidade de atendimento ao público externo. Trata-se, portanto, de justificativa que visa proteger um interesse público secundário da pessoa jurídica de direito público, o que não se confunde com a aplicação do princípio da supremacia do interesse público no caso concreto.

6.4.32. Ao contrário do que indica o INSS, a comunicação do incidente de segurança, nos termos do inciso I do §2º do art. 48 da LGPD, é, na verdade, medida adequada e proporcional que objetiva a subsunção do interesse público no caso concreto. Primeiramente, deve-se compreender que a tutela do direito à privacidade e o direito à proteção de dados pessoais, ambos valores normativos materializados como garantias fundamentais, nos termos dos incisos X e LXXIX do art. 5º da Constituição Federal, respectivamente, não deve mais ser percebida como o mero exercício de uma garantia individual pelo titular, em que a atuação do Estado ocorreria apenas de maneira negativa. De acordo com essa visão anacrônica, a ação estatal na proteção dos direitos de personalidade, dentre os quais se encontra a privacidade e a proteção de dados pessoais, existiria apenas para salvaguardar um direito individual do cidadão, no contexto de uma tutela remedial.

6.4.33. Tal acepção da proteção do direito à privacidade, no entanto, não mais encontra guarida no arcabouço jurídico de sociedades democráticas, pois

ignora o desenvolvimento das premissas que permeiam a tutela da privacidade nas últimas décadas, em especial, no contexto da digitalização crescente das relações sociais[9], o que resultou no desenvolvimento de um novo direito a proteção de dados pessoais. Observe-se, nesse sentido, lição de Danilo Doneda[10]:

> "A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva da tutela da pessoa quanto a sua progressiva adequação às novas tecnologias de informação. **Não basta pensar na privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma "predileção" individual, associada basicamente ao conforto e comodidade.** A própria noção da privacidade como algo de que um cidadão respeitável poderia abrir mão (ou que ao menos se esperasse isto de um cidadão honesto e de bons costumes), a presumida "transparência de quem não tem nada a temer", deixa de fazer sentido dada a crescente complexidade das situações que tais arroubos podem desencadear e das suas consequências para os cidadãos. Uma esfera privada, dentro da qual a pessoa tenha condições de desenvolver a própria personalidade, livre de ingerências externas, ganha hoje ainda mais importância: passa a ser pressuposto para que a pessoa não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada (para tocar em um conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade.
>
> **A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos.**
>
> (...)
>
> **A tutela remedial**, típica do direito subjetivo, não é mais do que um instrumento entre outros que podem ser utilizados para a tutela da privacidade, e de forma alguma é a estrutura na qual deva necessariamente se concretizar. **A ela faltam os instrumentos adequados à realização da função promocional da tutela da privacidade como meio de proteção da pessoa humana e da atuação da cláusula geral da proteção da personalidade; nela igualmente não é concebida a dimensão coletiva na qual se insere a problemática da privacidade.** Nesse sentido, deve ser entendida a tutela da privacidade através da responsabilidade civil que, se é uma perspectiva que não deve de forma alguma ser descartada como opção em uma série de situações, por si só não promove o avanço necessário na tutela da privacidade. Nessa perspectiva, ela continuaria a ser encarada como mera liberdade negativa, isto é, desconsiderando tanto a evolução da matéria como o alcance da norma constitucional, que, ao considerar a privacidade em seu aspecto positivo, destaca sua função promocional – para o que deve lançar mão de outros institutos".

6.4.34. Tem-se, desse modo, que o INSS, ao entender que a determinação da ANPD, no âmbito do PAI nº 00261.002177/2022-93, iria de encontro ao

interesse público, por supostamente trazer ônus elevado a sua atuação administrativa, em favor de interesses de particulares, desconsidera completamente a evolução doutrinária e jurisprudencial dos Tribunais Superiores no que se refere ao sentido conferido à proteção de dados pessoais no ordenamento jurídico pátrio e o seu papel instrumental para o livre desenvolvimento da personalidade dos indivíduos e, portanto, da dignidade humana.

6.4.35. A proteção de dados pessoais, a partir de uma evolução do direito à privacidade[11], possui como razão de ser a salvaguarda de um valor normativo que irradia direitos a toda a coletividade, para além da mera tutela individual, visto que possui fundamento direto com o princípio da dignidade da pessoa humana, de maneira que não se pode mais separar o interesse público primário da proteção da garantia fundamental em comento. Essa concepção já foi, inclusive, reconhecida pelo Supremo Tribunal Federal, no âmbito do julgamento da ADI 6.649, quanto à ADPF 695, que analisou a constitucionalidade do Decreto nº 10.046/2019, que instituiu normas para o compartilhamento de dados pessoais pelo Poder Público. O Ministro Gilmar Mendes, em seu voto seminal, asseverou que[12]:

> "(...) Todavia, diferentemente do que assevera o ente público, **a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais.**
>
> Como bem destacado por Gillian Black e Leslie Stevens, pesquisadores britânicos dedicados a essa temática, "se a privacidade for tratada simplesmente como um direito ou interesse individual, sempre será possível para o setor público controlar dados para suas finalidades públicas, já que isso será sempre reputado como necessário e proporcional" (tradução livre) (BLACK, Gillian e STEVENS, Leslie. "Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest". In: Scripted. Vol. 10, n. 1, 2013, p. 95).
>
> Nesse sentido, **assentam os autores a necessidade de se conferir uma abordagem comunitária e institucional ao direito à proteção de dados pessoais, evitando-se que este valor sempre sucumba diante da invocação do interesse público.**
>
> A consciência de que os governos devem tratar o regime jurídico de privacidade como um objetivo coletivo de estruturação dos regimes democráticos, e não como um valor contraposto de proteção de interesses individuais, é corolário do próprio reconhecimento da autonomia do direito fundamental à proteção de dados pessoais.
>
> Sobre esse ponto, destaca-se mais uma vez o escólio de Miriam Wimmer:
>
> 'A aplicação da legislação de proteção de dados no tratamento de dados pelo Poder Público – tanto no caso de atos individuais e concretos como também na edição de atos normativos –

> traz, portanto, o desafio de conciliação entre os princípios tradicionalmente aplicáveis à Administração Pública e aqueles contidos na própria LGPD, sem que se determine a precedência prima facie de um interesse público abstratamente caracterizado e reconhecendo também a importância da proteção de dados pessoais para além da sua dimensão individual. A eficiência demandada da Administração Pública e o interesse público tutelado pelo Estado devem, portanto, ser compreendidos no contexto de um conjunto mais amplo de princípios e com elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais". (WIMMER, Miriam. "Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público". In: DONEDA, Danilo; SARLET, Ingo Wolgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional. Rio de Janeiro, Editora Forense, 2021, pp. 271-288)'". (Grifo meu)

6.4.36. Acredita-se, portanto, que a realização do interesse público primário ocorre, ao contrário do que fora alegado pelo INSS, com a comunicação do incidente de segurança aos titulares afetados, seja por meio direto, seja por meio indireto, por se tratar de procedimento que visa a garantia do direito fundamental de proteção de dados pessoais, insculpido no art. 5º, inciso LXXIX, da Constituição Federal.

(iii) Da inaplicabilidade do art. 15 do Decreto nº 10.748/2021 ao caso concreto:

6.4.37. A entidade pública autuada afirma que o disposto no artigo 15 do Decreto nº 10.748, de 16 de julho de 2021, impediria a divulgação de informações sobre incidente de segurança sofrido pela Administração Pública Federal. De acordo com o dispositivo, as informações sobre os incidentes cibernéticos são consideradas imprescindíveis à segurança da sociedade e do Estado, sendo classificadas como informações sigilosas, segundo o art. 4º, III, e o art. 23 e 24, da Lei de Acesso à Informação (LAI). Argumenta-se, desse modo, que as informações relativas aos comunicados de incidentes de segurança seriam informações classificadas, nos termos do art. 23 da Lei nº 12.527/2011, Lei de Acesso à Informação – LAI. Tal interpretação, no entanto, não pode prosperar.

6.4.38. O artigo 23 da Lei nº 12.527/2011 dispõe de modo exaustivo as informações que podem ser classificadas pela Administração Pública, por serem consideradas imprescindíveis à segurança da sociedade ou do Estado. Desse modo, consideram-se informações classificadas aquelas submetidas temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, as informações que se enquadrem nos incisos do referido dispositivo legal:

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
>
> III - pôr em risco a vida, a segurança ou a saúde da população;
>
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
>
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
>
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
>
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
>
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

6.4.39. Observa-se, inicialmente, que o art. 23 da LAI não constitui hipótese autônoma de sigilo, ou seja, o enquadramento de determinada informação ou documento em uma das hipóteses descritas no artigo não é suficiente para se determinar a restrição de acesso. Para que seja feita a devida restrição de acesso à informação, por meio de procedimento de classificação, a autoridade classificadora competente (art. 27 da LAI) deve estabelecer o prazo de restrição de acesso ao documento salvaguardado no ato de produção do Termo de Classificação de Informação (TCI), documento formal que oficializa esse ato administrativo. É a partir da produção do TCI que a Administração Pública pode determinar a restrição de acesso a documento classificado[13].

6.4.40. Verifica-se, desse modo, que a hipótese de restrição de acesso com fundamento no art. 23 da LAI guarda diferenças com a hipótese presente no art. 22 da norma de transparência. A restrição de acesso a informações protegidas por hipótese de sigilo prevista em lei, por sua vez, encontra-se prevista no artigo 22 da Lei nº 12.527/2011, bem como é regulamentada no Poder Executivo Federal por meio do artigo 6º, inciso I do Decreto nº 7.724/2012, abaixo:

> Lei nº 12.527/2011:
>
> Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.
>
> Decreto nº 7.724/2012:
>
> Art. 6º O acesso à informação disciplinado neste Decreto não se aplica: I - às hipóteses de sigilo previstas na legislação, como fiscal, bancário, de operações e serviços no mercado de capitais,

comercial, profissional, industrial e segredo de justiça.

6.4.41. Ao contrário do que ocorre com as informações classificadas, a restrição de acesso a informações cuja publicidade se encontra limitada por legislação específica prescinde da produção de ato administrativo subsequente para produzir os seus efeitos. Outra característica que difere esta base legal daquela relacionada às informações classificadas é que o termo final da restrição de acesso em leis específicas não depende necessariamente de um lapso temporal pré-definido pela Administração Pública. Há restrições decorrentes de lei específica cujo termo final é um evento ou a cessação de uma condição, assim como há hipóteses de restrição sem evento claro que a defina.

6.4.42. O art. 15 do Decreto nº 10.748, de 16 de julho de 2021, nesse sentido, estabelece que as informações específicas sobre os incidentes cibernéticos e sobre as configurações e características técnicas de ativos de informação de cada órgão ou entidade da administração pública federal direta, autárquica e fundacional são consideradas imprescindíveis à segurança da sociedade e do Estado. Desse modo, o §1º do Decreto determina que as informações supramencionadas somente poderão ser acessadas por profissionais autorizados pelas autoridades responsáveis pelos ativos de informação dos órgãos ou das entidades da administração pública federal direta, autárquica e fundacional.

6.4.43. Observa-se, portanto, que o artigo 15 do Decreto nº 10.748, de 16 de julho de 2021 possui como finalidade precípua determinar que a Administração tome as medidas técnicas e administrativas necessárias para que as informações específicas relacionadas a incidentes cibernéticos sejam acessadas somente por agentes públicos devidamente autorizados, de modo a se resguardar dos olhos públicos informações estratégicas sobre o evento adverso. Nesse sentido, como medida mitigadora, seriam disponibilizados ao público em geral apenas dados estatísticos gerais relativos aos incidentes cibernéticos.

6.4.44. A restrição de acesso a tais informações, assim, ao ser considerada como imprescindível à segurança da sociedade e do Estado, encontra seu fundamento de validade infraconstitucional nos termos do inciso VI do artigo 23 da LAI. Desse modo, a restrição de acesso à informação exarada pelo artigo 15 do Decreto nº 10.748, de 16 de julho de 2021 não constitui hipótese autônoma de sigilo nos termos do art. 22 da LAI, motivo pelo qual a reserva das informações somente poderá ser considerada legal se adotado pelo órgão ou entidade pública o correto procedimento de classificação a que essas informações se submetem.

6.4.45. Isso é o que se depreende da inteligência do artigo 19 do Decreto nº 7.845/2012, que regulamentou no âmbito do Poder Executivo Federal os

procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo. De acordo com a norma, a decisão de classificação, desclassificação, reclassificação ou redução do prazo de sigilo de informação classificada em qualquer grau de sigilo observará os procedimentos previstos nos artigos 31 e 32 do Decreto nº 7.724 de 16 de maio de 2012, que regulamentou a aplicação da LAI no Poder Executivo Federal[14].

6.4.46. Tem-se, finalmente, que a decisão administrativa que resolver pela classificação de informações específicas envolvendo incidentes cibernéticos, nos termos do art. 23, inciso VI da Lei nº 12.527/2011 c/c o artigo 15 do Decreto nº 10.748/ 2021, deverá necessariamente ser formalizada em decisão consubstanciada em Termo de Classificação de Informação, conforme determinado pelo artigo 31 do Decreto nº 7.724/12, respeitando-se a previsão de apenas três níveis de restrição de acesso por classificação de informações: reservado, secreto e ultrassecreto. É importante enfatizar, nesse sentido, que, em nenhum momento deste processo sancionador - ou no processo de fiscalização que deu ensejo à confecção do Auto de Infração nº 01/2023/CGF/ANPD –, o INSS indicou a existência de TCI que comprovasse a classificação das informações específicas envolvendo o incidente de segurança objeto da medida sancionatória em análise.

6.4.47. Deve-se enfatizar, ademais, que o artigo 15 do Decreto nº 10.748/2021 limita a restrição de acesso apenas a *informações específicas* relacionadas a eventuais incidentes cibernéticos. Isso significa que a opacidade informacional temporária se refere somente a dados e informações de caráter técnico e administrativo cuja divulgação geral puder fragilizar a segurança do próprio sistema que se pretende salvaguardar, o que geraria prejuízos para a sociedade e o Estado.

6.4.48. Assim, a partir de uma interpretação sistemática da norma, compreende-se que a comunicação das informações constantes do §1º do artigo 48 da LGPD aos titulares afetados por incidentes de segurança qualificados não seria passível de restrição de acesso por classificação, seja por sua generalidade, seja por se tratar de um dos objetivos da Rede Federal de Gestão de Incidentes Cibernéticos, qual seja, divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos, presente no I do art 3º do Decreto nº 10.748/ 2021.

7. DOSIMETRIA DA(S) SANÇÃO(ÕES)

7.1. *Classificação da infração.*

7.1.1. Conforme já relatado, a autuada incorreu em violação à obrigação estabelecida no art. 48 da LGPD. Além disso, a entidade autuada deixou de realizar medida preventiva determinada Autoridade Nacional de Proteção de Dados Pessoais, no âmbito de Processo de Apuração de Incidente de Segurança, conforme o disposto no artigo 32 do Regulamento de Fiscalização, sendo

observada, portanto, a circunstância agravante do inciso II, § 2º do art. 32 do Regulamento de Fiscalização.

7.1.2. Diante do exposto, cabe, inicialmente, realizar a classificação da infração cometida pela entidade autuada (leve, média ou grave), conforme indica o art. 8º da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, doravante Regulamento de Dosimetria:

> 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.

7.1.3. O art. 48 da LGPD, caput e incisos, determina que o controlador deve apresentar CIS adequada, tanto à ANPD quanto ao titular, em prazo

razoável, sempre que o incidente de segurança puder acarretar risco ou dano relevante aos titulares. Conforme visto nos itens 6.4.1 a 6.4.12, a entidade pública autuada não realizou a comunicação do incidente de segurança qualificado aos titulares afetados, mesmo após as determinações exaradas pela Coordenação-Geral de Fiscalização.

7.1.4. A falta de CIS ao titular, especialmente quando resulta na exposição de dados pessoais em espaço não controlado de acesso, inclusive de dados de saúde e de benefícios previdenciários, pode afetar significativamente interesses e direitos fundamentais dos titulares. Isso porque o titular não sabe que seus dados foram expostos e, com isso, se encontra impossibilitado de tomar por conta própria medida preventivas que possam evitar o uso indevido de identidade, fraudes financeiras e 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.

7.1.5. 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. No entanto, no presente caso, a infração de falta de comunicação aos titulares versa sobre quantidade significativa de dados sensíveis relacionados à saúde e benefícios previdenciários, conforme item 4.3 da Nota Técnica 54/2023 (SEI nº 0048148). Essas características elevam o grau de classificação da infração que, por esse motivo, passa a ser considerada como **grave,** segundo art. 8º, §3º, “a” e "d", do Regulamento de Dosimetria:

> Art. 8º
>
> § 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;
>
> (...)

d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos

7.2. ***Definição do tipo de sanção administrativa.***

7.2.1. O art. 52 da LGPD define as sanções administrativas aplicáveis pela ANPD aos agentes de tratamento de dados que cometerem infrações às normas previstas na lei. Nesse sentido, a LGPD estabelece que a Autoridade de Proteção de Dados Pessoais, após o devido processo administrativo que possibilite o contraditório e a ampla defesa, poderá aplicar os seguintes tipos de sanção administrativa:

> I) advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III) multa diária, observado o limite total a que se refere o inciso II;
>
> IV) publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V) bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI) eliminação dos dados pessoais a que se refere a infração;
>
> VII) (VETADO);
>
> VIII) (VETADO);
>
> IX) (VETADO);
>
> X) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e
>
> XII) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

7.2.2. O Regulamento de Dosimetria, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, por sua vez, regulamentou a aplicação das sanções administrativas previstas na LGPD, assim como os parâmetros e critérios para a dosimetria das eventuais sanções aplicadas. As penalidades, conforme os preceitos indicados tanto na LGPD quanto no Regulamento de Dosimetria, devem ser aplicadas de forma gradativa, levando-se em consideração critérios específicos dispostos na norma.

7.2.3. A sanção de advertência, regulamentada no art. 9º do Regulamento de Dosimetria, nesse sentido, será aplicada quando a infração observada for considerada de natureza leve ou média e não caracterizar reincidência específica ou quando houver a necessidade de imposição de medida corretiva que tenha como finalidade corrigir a infração e reconduzir o infrator à plena conformidade à LGPD e aos regulamentos aplicados por esta Autarquia federal.

7.2.4. Observou-se, no entanto, que as infrações cometidas pela entidade autuada foram consideradas de natureza grave, por envolver o tratamento de dados pessoais em larga escala e dados pessoais sensíveis. Além disso, a ocorrência de uma circunstância agravante, nos termos do art. 32, §2º, II, do Regulamento de Fiscalização, ou seja, o não atendimento de medida preventiva determinada pela autoridade fiscalizatória, indica a necessidade de aplicação de medida sancionatória mais grave. Assim, em virtude da circunstância agravante, compreende-se que não se aplica ao caso concreto a sanção de advertência.

7.2.5. O Regulamento de Dosimetria, por sua vez, define, em seu art. 20, que a ANPD poderá aplicar sanção administrativa de publicização da infração ao autuado, considerando a relevância e o interesse público da matéria. A sanção de publicização consiste na divulgação da infração pelo próprio infrator, após devidamente apurada e confirmada sua ocorrência. Considerando que a realização do interesse público primário, no caso concreto, ocorre com a devida comunicação do incidente de segurança aos titulares afetados, ainda que por meio indireto, conforme consta nos itens a 7.31 a 7.43 deste RI, bem como a natureza grave da infração, acredita-se que a sanção de publicização da infração seja mais adequada à inobservância pelo autuado da conduta do art. 48 da LGPD e do dever de comunicação aos titulares afetados.

7.2.6. Deve-se ressaltar, nesse sentido, que a sanção de publicização deverá indicar o teor, o meio, a duração e o prazo para o seu cumprimento, nos termos do art. 20, §2º do Regulamento de Dosimetria. Além disso, conforme o disposto no art. 21 do Regulamento de Dosimetria, é importante enfatizar que a sanção de publicização da infração não se confunde com a publicação de decisão de aplicação de sanção administrativa no Diário Oficial da União ou com os demais atos realizados pela ANPD, para fins de atendimento ao princípio da publicidade administrativa. Nesse sentido, o ônus relacionado à publicização da infração deve ser suportado exclusivamente pelo infrator. Assim, de acordo com as normas que regulamentam a matéria, sugere-se o seguinte texto de comunicação ao titular a ser adotado pelo infrator:

> O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto

de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.

Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: encarregado@inss.gov.br."

7.2.7. Para se atingir o objetivo da comunicação, sugere-se que o comunicado fique disponível por 180 (cento e oitenta) dias corridos contados a partir da data do cumprimento da intimação da decisão que determinar a sanção administrativa, ou seja, contados a partir do início da publicização do comunicado. Igualmente, sugere-se que a comunicação esteja disponível:

- na primeira página do sítio do INSS (https://www.gov.br/inss/pt-br) ou até, no máximo, a um clique de distância da página inicial, sob pena da comunicação não atingir seu objetivo de informar o titular sobre o incidente de segurança; e
- no menu de 'notificações' do aplicativo Meu INSS, com indicação visual de que há mensagem pendente de leitura/visualização.

7.2.8. Em relação às demais sanções previstas na norma, percebe-se que não deve ser aplicação ao caso concreto a sanção de multa simples, prevista no art. 10, incisos I e II, do Regulamento de Dosimetria. Ainda que esta sanção administrativa seja prevista em caso de descumprimento pelo infrator de medidas preventivas a ele impostas, 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, motivo pelo qual deixa-se de se aplicar tal sanção. Igualmente, muito embora seja uma infração grave, as outras sanções previstas na LGPD (no caso, os incisos V a XII do art. 52) tampouco são adequadas para a infração ora analisada, em função do interesse público que justifica a necessidade do tratamento dos dados, bem como necessidade de aplicação proporcional da medida sancionatória. Igualmente, muito embora seja uma infração grave, as outras sanções

previstas na LGPD (no caso, os incisos V a XII do art. 52) tampouco são adequadas para a infração ora analisada, em função do interesse público que justifica a necessidade do tratamento dos dados, bem como necessidade de aplicação proporcional da medida sancionatória

7.2.9. Fica, portanto, cominada a **sanção de publicização da infração**, exarada nos termos do art. 20 da Resolução CD/ANPD nº 4/2023, para a infração ao art. 48 da LGPD, considerando-se como circunstância agravante a falta de atendimento pela autuada de determinação exarada pela ANPD, nos termos do art. 32, §2º, II, da Resolução CD/ANPD nº 1/2021

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 1/2023/CGF/ANPD (4411917), conclui-se pela seguinte recomendação:

8.1.1. Por violação ao art. 48 da LGPD, com circunstância agravante nos termos do art. 32, §2º, II, da Resolução CD/ANPD nº 1/2021, a aplicação da sanção de PUBLICIZAÇÃO DA INFRAÇÃO ao INSS. A entidade pública autuada, assim, deverá, em até 10 dias úteis, contados a data da intimação:

a) Publicar comunicado, na primeira página do sítio (https://www.gov.br/inss/pt-br), que deverá permanecer acessível pelo prazo de 60 dias, contados a partir da intimação da decisão que determinar a sanção administrativa, com o seguinte teor:

> O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.
>
> Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada

no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: encarregado@inss.gov.br."

b) Enviar mensagem, via recurso de notificação, a todos os usuários do aplicativo Meu INSS, para que fique disponível no menu de 'notificações' do aplicativo Meu INSS, com indicação visual de que há mensagem pendente de leitura/visualização, com o seguinte teor:

"O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica a ocorrência de incidente de segurança entre agosto e setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS, saiba mais no link:" [apontar para o link criado para atender a determinação 8.1.1.a]

8.2. Por fim, é importante registrar 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 em concreto. Tais decisões não vinculam, naturalmente, a análise e o posicionamento da CGF em futuros processos sancionadores.

8.3. Caso a entidade pública autuada não cumpra a referida decisão nos termos definidos pela Autoridade Nacional de Proteção de Dados, recomenda-se que o presente processo administrativo sancionador seja encaminhado para os órgãos de controle interno competentes, nos termos do art. 55-J, XXII, da LGPD, para que sejam tomadas as medidas administrativas necessárias em relação aos agentes públicos que deram causa ao descumprimento do disposto na legislação de proteção de dados pessoais.

9. ENCAMINHAMENTOS

9.1. Este Relatório de Instrução encerra a fase de instrução da atuação repressiva prevista no Art. 54, parágrafo único, do Regulamento de Fiscalização.

9.2. O presente Relatório de Instrução deve ser encaminhado à CGF para decisão, de acordo com Art. 55 do Regulamento de Fiscalização.

9.3. Após a decisão, o autuado deverá ser intimado para cumprimento da sanção e/ou apresentação de recurso, em até 10 dias, em consonância com o Art. 44, da Lei nº 9.784/99, e o Art. 58, do Regulamento de Fiscalização. Em caso de sanção de multa, o autuado deverá pagá-la no prazo de até 20 (vinte) dias úteis, contados a partir da ciência oficial da decisão de aplicação de sanção.

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

9.5. Por derradeiro, deve-se informar que a entidade autuada, mesmo após consultada, nos termos do Ofício nº 72/2023/FIS/CGF/ANPD (SEI nº 4836919), não indicou eventuais informações constantes no presente processo administrativo sancionatório que pudessem estar protegidas por hipótese de sigilo exaradas pela Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI).

9.6. Encaminho, por fim, o presente Relatório de Instrução para aprovação superior.

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA
Auditor federal de finanças e controle

De acordo.

ULLIANA CERVIGNI MARTINELLI
Coordenadora de Fiscalização, Substituta

---

[1] MODENESI, Pedro; Art. 48. In *Comentários à lei geral de proteção de dados pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 452.

[2] MODENESI, Pedro; Art. 48. In *Comentários à lei geral de proteção de dados pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 455.

[3] SOMBRA, Thiago Luís.Planos de resposta a incidentes de segurança com dados pessoais e a construção de uma governança responsiva. In *Compliance e políticas de proteção de dados [livro eletrônico]*, 1º. ed. São Paulo: Thomson Reuters Brasil, 2021. RB-25.5

[4] ANPD. Qual o prazo para comunicar um incidente de segurança? Comunicação de Incidentes de Segurança, 2022. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acessado em 22/01/2024.

[5] RITA TOURINHO, *Discricionariedade administrativa*, Juruá, 2º ed. 2009, p 127. In CARVALHO FILHO, José dos Santos, *Manual de direito administrativo*, 31º ed., atual. E ampl. – São Paulo: Atlas, 2017. p 53.

[6] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de proteção de dados pessoais, fundamentos da LGPD*. 1º ed. Rio de Janeiro: Forense, 2022. p. 72.

[7] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de proteção de dados pessoais, fundamentos da LGPD*. 1º ed. Rio de Janeiro: Forense, 2022. p. 73.

[8] BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 5. ed. São Paulo: Saraiva, 2015. P. 94-97.

[9] MEJIAS, U.A.; COULDRY, N. *Datafication.* Internet Policy Review, 8 (4), 2019.

[10] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados pessoais*. 2º ed. -- São Paulo: Thomson Reuters Brasil, 2021.

[11] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.* (Saraiva 2014).

[12] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 6.649 e Arguição de Descumprimento de Preceito Fundamental n. 695.** Lei nº 13.709/2018 e Decreto nº 10.046/2019. Controvérsia relativa aos limites, ao âmbito de proteção e à dimensão axiológica dos direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade, especificamente no que diz respeito ao uso compartilhado de dados pessoais pelo Estado brasileiro. ReQte(s). Conselho Federal da Ordem dos Advogados do Brasil e Partido Socialista Brasileiro (PSB). Intdo. Presidente da República. Rel. Min. Gilmar Mendes, em 15 de setembro de 2022. Disponível em https://portal.stf.jus.br/. Acessado em 19/01/2024.

[13] BRASIL. Controladoria-Geral da União. *Parecer sobre acesso à informação para atender ao Despacho Presidencial de 1° de janeiro de 2023*. Disponível em https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-conclui-revisao-dos-sigilos-impostos-a-documentos-de-acesso-publico/copy_of_PARECERFINALSOBREACESSOINFORMAO_CGU_FEV2023.pdf. Acessado em 23/01/2024. Pgs 59-60.

[14] Art. 31. A decisão que classificar a informação em qualquer grau de sigilo deverá ser formalizada no Termo de Classificação de Informação - TCI, conforme modelo contido no Anexo, e conterá o seguinte:

I - código de indexação de documento;

II - grau de sigilo;

III - categoria na qual se enquadra a informação;

IV - tipo de documento;

V - data da produção do documento;

VI - indicação de dispositivo legal que fundamenta a classificação;

VII - razões da classificação, observados os critérios estabelecidos no art. 27, com a justificativa para o grau de sigilo adotado; (Redação dada pelo Decreto nº 11.527, de 2023)

VII-A - assunto a que se refere a informação, com a descrição de elementos mínimos que permitam a identificação do tema de que trata a classificação; (Incluído pelo Decreto nº 11.527, de 2023)

VIII - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 28;

IX - data da classificação; e

X - identificação da autoridade que classificou a informação.

§ 1º O TCI seguirá anexo à informação.

§ 2º As informações previstas no inciso VII do **caput** deverão ser mantidas no mesmo grau de sigilo que a informação classificada.

§ 3º A ratificação da classificação de que trata o § 5º do art. 30 deverá ser registrada no TCI.

Art. 32. A autoridade classificadora ou outro agente público que classificar a informação deverá enviar, no

prazo de trinta dias, contado da data da decisão de classificação ou de sua ratificação, as informações previstas no **caput** do art. 31 à: (Redação dada pelo Decreto nº 11.527, de 2023)

I - Comissão Mista de Reavaliação de Informações, no caso de informações classificadas no grau ultrassecreto ou secreto; ou (Incluído pelo Decreto nº 11.527, de 2023)

II - Controladoria-Geral da União, no caso de informações classificadas em qualquer grau de sigilo, ressalvado o envio das informações de que trata o inciso VII do **caput** do art. 31. (Incluído pelo Decreto nº 11.527, de 2023) Vigência

§ 1º Na hipótese de que trata o inciso II do **caput**, quando identificar, no desempenho das competências previstas no art. 68, a partir do exame dos elementos públicos que compõem o TCI, indícios de erro na classificação da informação, a Controladoria-Geral da União deverá: (Incluído pelo Decreto nº 11.527, de 2023)

I - notificar a autoridade classificadora, que decidirá sobre a reavaliação da classificação no prazo de trinta dias; e (Incluído pelo Decreto nº 11.527, de 2023)

II - informar a Comissão Mista de Reavaliação de Informações, no caso de informações classificadas no grau ultrassecreto ou secreto, para fins do disposto no inciso I do **caput** do art. 47. (Incluído pelo Decreto nº 11.527, de 2023)

§ 2º Os indícios de erro a que se refere o § 1º serão considerados quanto: (Incluído pelo Decreto nº 11.527, de 2023)

I - ao não enquadramento do assunto de que trata o inciso VII-A do **caput** do art. 31 nas hipóteses legais de sigilo; e (Incluído pelo Decreto nº 11.527, de 2023)

II - a não adequação do grau de sigilo. (Incluído pelo Decreto nº 11.527, de 2023)

Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima**, **Assessor(a)**, em 25/01/2024, às 15:00, 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 **Ulliana Cervigni Martinelli**, **Coordenador(a), Substituto(a)**, em 25/01/2024, às 17:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

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 **0053354** e o código CRC **1E8C7722**.

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