Comissão Mista de Reavaliação de Informações

131ª Reunião Ordinária

Decisão CMRI nº 173/2024/CMRI/CC/PR

NUP: **03005.157212/2023-19**
Órgão: **INSS – Instituto Nacional do Seguro Social**
Requerente: **V. A. S. M** .

Resumo do Pedido

O Requerente fez referência a uma sentença proferida no processo 5000086- 03.2021.4.03.6345, pelo Juizado Especial Federal (JEF) de Marília, que teria reconhecido vazamento de dados de beneficiária do INSS para instituições financeiras, e solicitou:

A) O motivo detalhado do vazamento;
B) Servidores envolvidos e suas matrículas;
C) Se existem indícios de ações criminosas e quais;
D) Documentos internos que eventualmente tenham sido produzidos no intento de apurar o devido vazamento, bem como documentos com conclusões sobre o incidente.

Foi anexado ao NUP aparente cópia da sentença referida pelo Requerente.

Resposta do órgão requerido

O INSS alegou que o pedido não versaria sobre solicitação de informação pública e que se trataria de consulta, situação na qual o cidadão deseja obter do Poder Público um pronunciamento acerca de uma condição hipotética ou concreta. Ademais, por se tratar de processo judicial, o Órgão sugeriu que o Requerente buscasse informações adicionais diretamente no Juízo prolator da sentença e acrescenta que o SIC não substitui os canais de atendimento do INSS e foi criado como ferramenta para obtenção de informações públicas com base na LAI.

Recurso em 1ª instância

O Requerente reiterou o pedido e refutou a resposta do Órgão em 1ª instância, ao alegar que: o pedido do item D teria sido claro ao solicitar documentos que estariam sujeitos à apreciação enquanto informação pública; o item C teria questionado se existiriam indícios de atividade criminosa nos vazamentos, o que destinaria a questão à documentos de auditoria ou fiscalização do órgão; o item B teria solicitado, caso tenha havido falha ou irregularidade de servidor constatada documentalmente, que fosse informado nome e matrícula deles; e, por fim, que o item A seria presumível, uma vez que o trabalho de correção das falhas de segurança se destinaria à apurar dos detalhes do vazamento dos dados em questão. O Requerente incluiu em seu recurso link de notícia na qual o então presidente do INSS admitiria a existência de um "pente-fino interno para combater o vazamento de dados" e anexou ao processo parecer da CGU no NUP 00077.000553/2019-97, possivelmente como exemplo de precedente que justificaria a concessão de seu pedido.

Resposta do órgão ao recurso em 1ª instância

O Requerido ratificou a resposta inicial e referiu que a parte autora do processo judicial citado pelo Requerente, devidamente representada por seu advogado, poderia solicitar ao Juízo da sentença que expeça ofício ao INSS solicitando informações que entender necessárias, se for do seu interesse. O Órgão também alegou que as informações sobre dados cadastrais (constantes nos sistemas do INSS), bem como suposto vazamento de tais dados, seriam informações pessoais, nos termos dos arts. 55 a 60 do Decreto nº 7.724/2012. Portanto, a beneficiária do INSS citada na sentença poderia, também, solicitar informações sobre seus dados pessoais diretamente ao Órgão, com os devidos elementos que comprovassem sua identidade.

Recurso em 2ª instância

O Requerente reiterou o pedido e alegou que: apesar dos indícios do vazamento terem sido obtidos em processo judicial, o pedido formulado referir-se-ia a caso geral, em que a vítima em questão fora uma das afetadas; que os casos de vazamento não seriam pontuais, visto que amplamente divulgados em sites jornalísticos; que não pretende obter detalhes sobre o caso específico, mas acesso a informações públicas sobre eventos e documentos do qual este acontecimento específico faz parte.

Resposta do órgão ao recurso em 2ª instância

O Órgão reiterou as respostas anteriores e alegou que houve inovação recursal pelo Requerente, ao solicitar informação no recurso distinta daquela pedida inicialmente. O INSS alegou, também, que não fornece informações sobre benefícios previdenciários às instituições financeiras e que, em caso de suspeita de vazamento de dados, deve ser analisado o caso concreto, por meio de solicitação feito ao encarregado do tratamento dos dados pessoais. Acrescentou que os empréstimos consignados seriam operacionalizados diretamente pela instituição financeira conveniada e a DATAPREV, sendo que o INSS se restringiria apenas à consignação dos valores autorizados pelo beneficiário e o repasse à instituição financeira conveniada. Informou, ainda, que o INSS é responsável pelo credenciamento das instituições financeiras, através da celebração de Acordo de Cooperação Técnica, desde que atendidos os requisitos legais e técnicos exigidos, e que o INSS não celebra Acordo de Celebração Técnica para fins de operacionalização de empréstimo consignado diretamente com representantes/correspondentes bancários por ausência de previsão legal, visto que tais entidades não constituiriam instituição financeira segundo os critérios do Banco Central. O Órgão expôs que a contratação de correspondentes seria de responsabilidade da instituição financeira contratante, e que deve ser comunicada ao Banco Central pela contratante mediante registro no sistema de Informações sobre Entidades de Interesse do Banco Central (Unicad). Por fim, o INSS alegou que, em decorrência da assinatura de Acordo de Cooperação Técnica entre o Instituto Nacional do Seguro Social (INSS) e a Secretaria Nacional do Consumidor, vinculada ao Ministério da Justiça, as reclamações referentes a Empréstimo Consignado deverão ser resolvidas no Portal do Consumidor, através do endereço eletrônico http://www.consumidor.gov.br/.

Recurso à Controladoria-Geral da União (CGU)

O Requerente refuta a alegação de inovação ao afirmar que houvera equívoco na interpretação de seu pedido pelo INSS, e que mencionara o processo judicial em questão *"apenas por tratar-se 1) de indício inconteste de vazamento generalizado, uma vez que é inimaginável o vazamento de apenas uma linha de cadastro; 2) de referência, afim (sic) de que o incidente fosse localizado em sua data"*. O Requerente reiterou seu pedido, acompanhado dos seguintes esclarecimentos:

> *A) O motivo detalhado do vazamento; - observe-se que não se trata de detalhamento do caso concreto da parte autora da ação, mas do incidente de segurança de um modo geral, em seus motivos (se falha técnica, qual falha técnica? se irregularidade, qual irregularidade?)*
>
> *B) Servidores envolvidos e suas matrículas; - Observe-se que não é solicitado, mais uma vez, nenhum dado ou informação pessoal da parte autora do processo judicial de referência, mas tão somente o nome de servidores públicos envolvidos em um incidente de interesse público;*
>
> *C) Se existem indícios de ações criminosas e quais; - Novamente, não se trata de ação criminosa com relação a uma pessoa apenas. Seria impensável, repito, a articulação de um esquema criminoso com objetivo de obter um único número de telefone para uso em telemarketing. Há que se pensar, por lógica, em vazamento ilegal de nada menos do que uma massa de dados de diversos contribuintes;*
>
> *D) Documentos internos que eventualmente tenham sido produzidos no intento de apurar o devido vazamento, bem como documentos com conclusões sobre o incidente - Por fim, o item D é claro ao registrar que não se tratam (sic) dos documentos pessoais da autora do processo judicial, tampouco dos autos do mesmo processo, mas de documentos de auditoria.*

Por fim, o Requerente solicitou que, nos termos da LAI, caso não fosse concedido acesso integral à informação por ser ela parcialmente sigilosa, fosse assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

Análise da CGU

A partir dos esclarecimentos prestados pelo Requerente em seu recurso, a CGU concluiu que as informações solicitadas seriam de interesse público, cabendo, portanto, a análise do direito de acesso a esse tipo de documentação. Por isso, a Controladoria decidiu realizar interlocução junto ao Órgão, a fim de obter esclarecimentos adicionais sobre a existência de auditorias ou outros procedimentos apuratórios ou, mesmo, acerca de simples providências documentadas, para apurar eventuais vazamentos de dados sobre benefícios previdenciários, suas causas e responsáveis e, em caso afirmativo, para que fosse informado o status dos procedimentos e avaliar a possibilidade de disponibilizá-los ao requerente, tarjando-se eventuais informações pessoais sensíveis ou protegidas por sigilo legal. Na interlocução, o INSS ressaltou que tem mantido contato com o Banco Central, Dataprev e, principalmente com a Coordenação-Geral de Inteligência Previdenciária (COINP) da Secretaria Especial de Previdência e Trabalho, do Ministério do Trabalho e Previdência, a fim de identificar as fontes e possíveis falhas nos fluxos internos e externos, que contribuem para um possível vazamento de dados de segurados. Esclareceu, também, que trabalhando com o setor de inteligência, responsável pelas apurações, que atua junto às Delegacias da Polícia Federal no combate a essa prática criminosa, além de estar buscando meios de fortalecer os mecanismos de prevenção aos vazamentos de dados. O Órgão argumentou que a divulgação de detalhes das apurações poderia comprometer gravemente as atividades de inteligência, investigação e fiscalização em andamento, bem como aquelas que já foram concluídas. Asseverou que a preservação da confidencialidade dessas informações é vital para garantir a eficácia e eficiência dos esforços de segurança cibernética. Esclareceu que todas as fases da gestão de incidentes cibernéticos são conduzidas de forma a assegurar a cadeia de custódia de evidências forenses (art. 154-A, do Código Penal). Salientou que toda a documentação afeta ao tema é armazenada em conformidade com as legislações vigentes (LGPD, LAI e CP) e com a devida preservação dos dados pessoais e sigilosos envolvidos. O Órgão declarou que não realizou trabalhos de auditoria ou apuração relacionados diretamente com vazamentos de dados de benefícios previdenciários a instituições bancárias ou financeiras. Entretanto, o Órgão afirmou que conduzira procedimentos apuratórios relacionados aos vazamentos/roubo de credenciais de acesso aos sistemas previdenciários, seja de servidores ou de terceiros. A CGU expôs que a temática de incidentes cibernéticos, que incluem os vazamentos de dados, fora tratada pela instituição no âmbito do precedente 00077.000814/2019-79. No citado precedente, a CGU decidiu por manter a negativa de acesso em face de dados detalhados (quantitativo, origem e alvo do ataque) de incidentes cibernéticos sofridos por órgãos e entidades da administração pública federal, em função do risco em potencial de que essas informações pudessem vulnerabilizar os avanços alcançados no combate aos ataques e fundamentou a negativa de acesso, na desarrazoabilidade do pedido, nos termos do art. 13, inciso II do Decreto nº 7.724/2012. A CGU avaliou, no presente caso, que fornecer os documentos e o detalhamento requerido pelo cidadão nos pedidos de letras "A" a "D" seria, igualmente, desarrazoado, porque violaria o próprio interesse público, uma vez que exporia o INSS e os usuários de serviços públicos a riscos de sofrerem novos ataques cibernéticos. Portanto, a CGU corroborou o entendimento da entidade recorrida de que a divulgação de motivos, dados e documentos sobre as apurações envolvendo o vazamento de dados de beneficiários do INSS pode comprometer as atividades de inteligência, investigação e fiscalização em andamento, pois poderiam prejudicar e frustrar as próprias apurações em curso. Quanto aos procedimentos já concluídos, a Controladoria vislumbrou que também poderiam ocorrer prejuízos decorrentes da sua divulgação, porque poderiam demonstrar os métodos utilizados para invadir ou vazar dados dos sistemas eletrônicos da entidade e, ainda, a metodologia que foi empreendida para investigar os incidentes cibernéticos. A CGU ponderou que os avanços tecnológicos dos incidentes cibernéticos estão cada vez mais automatizados, sendo potencializados por diretivas de inteligência artificial, e que informações relativas ao tema podem ser utilizadas como insumo para a exploração de novas vulnerabilidades por meio de engenharia social e pela análise de tendências e padrões de ataques realizados.

Decisão da CGU

A CGU decidiu pelo indeferimento do recurso interposto, devendo ser mantida a restrição de acesso em face dos requerimentos de letras "A" a "D", com fundamento no art. 13, inciso II do Decreto nº 7.724/2012, por se tratar de pedidos desarrazoados, cujo atendimento não encontra amparo nos objetivos da Lei nº 12.527/2011.

Recurso à Comissão Mista de Reavaliação de Informações (CMRI)

Em seu recurso à CMRI, o Requerente reiterou o pedido e o argumento do recurso à CGU, de concessão de acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

Admissibilidade do recurso à CMRI

Recurso conhecido. Cumpridos os requisitos de legitimidade, tempestividade, cabimento e regularidade formal.

Análise da CMRI

A análise do processo permitiu verificar, após os esclarecimentos realizados pelo Requerente nas instâncias recursais, que o pedido, subdividido inicialmente em quatro itens, versa, como um todo, sobre informações integrantes de quaisquer procedimentos apuratórios acerca de vazamento de dados de beneficiários do INSS para instituições financeiras. Da resposta do Órgão à interlocução feita pela CGU, é possível inferir que tais vazamentos constituem incidentes cibernéticos. O INSS argumentou, ainda que a divulgação de detalhes dessas apurações poderia comprometer gravemente as atividades de inteligência, investigação e fiscalização em andamento, bem como aquelas que já foram concluídas. É digno de nota que, no NUP 00077.001295/2017-02, a CMRI analisou questão semelhante. Naquele processo, o requerente solicitou relatório com o teor de invasões a sites de domínio estatal, qual foi o site atingido e qual o prejuízo. O pedido teria sido feito com base em relatório recebido do GSI, que informaria que teria ocorrido registro de 797 ocorrências de vazamento de informações sigilosas nos sites dos domínios .gov.br, leg.br, jus.br, mil.br, mp.br e def.br. Após análise do tema, a CMRI decidiu pelo desprovimento do pedido, com fundamento no art. 13, inciso II do Decreto nº 7.724/2012, visto compreender a desarrazoabilidade do pedido, em função dos riscos potenciais de disponibilização da informação requerida. O Manual de Aplicação da LAI na Administração Pública Federal (4ª edição), define pedido desarrazoado como "*aquele que não encontra amparo para a concessão de acesso solicitado nos objetivos da LAI e tampouco nos seus dispositivos legais, nem nas garantias fundamentais previstas na Constituição. É um pedido que se caracteriza pela desconformidade com o interesse público, segurança pública, celeridade e economicidade da Administração Pública*." No caso em tela, é possível verificar que o atendimento do pedido do Requerente, com a divulgação de motivos, dados e documentos sobre as apurações envolvendo o vazamento de dados de beneficiários do INSS, pode comprometer as atividades de inteligência, investigação e fiscalização, além de demonstrar os métodos utilizados para invadir ou vazar dados dos sistemas eletrônicos da entidade e, ainda, a metodologia que foi empreendida para investigar os incidentes cibernéticos. Portanto, a concessão da informação solicitada pelo Requente contraria o interesse público, podendo ser caracterizada como desarrazoada.

Decisão da CMRI

A Comissão Mista de Reavaliação de Informações, por unanimidade, decide pelo conhecimento do recurso e, no mérito, pelo indeferimento, com fundamento no art. 13, inciso II, do Decreto nº 7.724/2012, por ser desarrazoado o fornecimento dos dados pois pode comprometer as atividades de inteligência, investigação e fiscalização, bem como os métodos utilizados para invadir ou vazar dados dos sistemas eletrônicos da entidade e, ainda, a metodologia que foi empreendida para investigar os incidentes cibernéticos.

Documento assinado eletronicamente por **Miriam Aparecida Belchior**, **Secretário(a)-Executivo(a)**, em 09/04/2024, às 21:19, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Jorge Luiz Mendes de Assis**, **Usuário Externo**, em 10/04/2024, às 09:09, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **CARLOS AUGUSTO MOREIRA ARAUJO**, **Usuário Externo**, em 10/04/2024, às 11:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **RONALDO ALVES NOGUEIRA registrado(a) civilmente como RONALDO**, **Usuário Externo**, em 10/04/2024, às 19:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Míriam Barbuda Fernandes Chaves**, **Usuário Externo**, em 12/04/2024, às 19:02, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Rogério Brito de Miranda**, **Assessor(a) Especial**, em 15/04/2024, às 09:43, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Caroline Dias dos Reis**, **Usuário Externo**, em 15/04/2024, às 21:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida informando o código verificador **5086706** e o código CRC **E8F7927E** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00131.000008/2024-66 SUPER nº 5086706