Comissão Mista de Reavaliação de Informações

140ª Reunião Ordinária

Decisão CMRI nº 526/2024/CMRI/CC/PR

NUP: 09002.002067/2022-57
Órgão: MRE – Ministério das Relações Exteriores
Requerente: B.S.M .

Resumo do Pedido

O Requerente solicitou informações sobre o sistema intratec, de currículos profissionais do MRE, quais sejam:
1) Dicionário de dados;
2) Esquema relacional do banco de dados;
3) Volume do banco de dados;
4) Tecnologia de armazenamento do banco de dados.

Resposta do órgão requerido

O Órgão considerou inviável a divulgação de informações a respeito das especificações e paradigmas dos sistemas de informática que regem os bancos de dados da rede interna do MRE ("Intratec"), pois considerou o pedido desarrazoado, com base no art. 13, inciso II do Decreto nº 7.724/2012, e nos termos do art. 12.2 da Portaria/MRE nº 43, de 26 de janeiro de 2015, cumulado com o art. 45 do Decreto nº 7.845, de 2012 e dos resguardos previstos pela Lei Geral de Proteção de Dados Pessoais (LGPD). Ressaltou, ainda, a existência de precedentes Controladoria-Geral da Uniãoque correlacionam a definição de pedido desarrazoado a questões atinentes a informações sobre o funcionamento do banco de dados, que desdobram na governança de tecnologia e segurança de informação (a exemplo do processo 03005.071987/2021-28).

Recurso em 1ª instância

O Requerente reiterou o pedido, relacionando o interesse nas informações sobre: 1) o volume em megabytes ou gigabytes que os dados do sistema ocupam, alegando se tratar apenas do espaço que os dados ocupam no servidor – algo que, segundo o próprio, não colocaria o sistema em risco; 2) a tecnologia de armazenamento; 3) o dicionário de dados, por se tratar de um documento que atribuiria contexto semântico aos dados.

Resposta do órgão ao recurso em 1ª instância

O Órgão reiterou a resposta anterior e acrescentou que o recurso trouxe elemento estranho à matéria do pedido original, configurando inovação em fase recursal, conforme Súmula CMRI nº 2/2015. Assim, orientou o Requerente para um novo pedido de acesso à informação, para apreciação da matéria pelas instâncias administrativas iniciais, caso fosse de interesse.

Recurso em 2ª instância

O Requerente contestou a resposta do Órgão quanto a alegação de ter sido o pedido em 1ª Instância considerado inovação recursal e reiterou o acesso às informações requeridas.

Resposta do órgão ao recurso em 2ª instância

O MRE reiterou a resposta inicial, negando o acesso às informações com no art. 13, II do Decreto nº 7.724, de 2012. Ademais, esclareceu os seguintes pontos: a divulgação das informações solicitadas poderia colocar em risco a guarda de dados sob responsabilidade do MRE; a divulgação de informações sobre o volume de dados e sobre o sistema Intratec, se divulgadas, poderiam comprometer a segurança da informação, uma vez que poderiam contribuir para o planejamento de exfiltração de dados e para o planejamento de ataque cibernético, respectivamente; o fornecimento de informações sobre dicionário de dados, poderia, igualmente, contribuir para ataque do tipo "injeção", pois o atacante conheceria certos padrões e tamanhos de texto aceitos pelo banco de dados, identificando eventuais vulnerabilidades.

Recurso à Controladoria-Geral da União (CGU)

Em recurso à CGU, o Requerente alegou que, de acordo com o art. 29, §1º, III da Lei Federal 14.129, de 2021 é direito do cidadão obter acesso às informações fornecidas, as quais seriam corriqueiramente fornecidas por órgãos públicos. Concluiu reiterando que o fornecimento das informações solicitadas não apresentaria risco.

Análise da CGU

A CGU entendeu ser desarrazoada a entrega das informações solicitadas, pois a concessão de acesso exporia não apenas potenciais informações privadas contidas nesse banco, mas também as estratégias de agregação, produção e armazenamento de informações do Ministério, visto que o sistema, além de outras funcionalidades, também serviria de portal de acesso a dezenas de outros sistemas internos. A CGU esclareceu que o entendimento do MRE estaria em consonância com a maior parte da jurisprudência administrativa da CGU, que tem entendido que o acesso a informações sobre a estrutura de sistemas de informação de órgãos públicos constitui pedido desarrazoado, apesar de que a desarrazoabilidade de pedidos de acesso a informações relacionadas à tecnologia de armazenamento de dados não ser uma regra absoluta, devendo ser analisada caso a caso. Acrescentou, ainda, a necessidade de se realizar uma análise casuística em pedidos análogos, e o desprovimento dos pedidos dependeria de comprovação pelo órgão requerido quanto a exposição de sua tecnologia informacional e possíveis prejuízos em termos de exposição de dados pessoais ou em termos de exposição da lógica interna de produção de dados de um órgão público. Sendo assim, ainda que não se descarte que no futuro a CGU venha a desenvolver uma maior compreensão institucional acerca do tema específico (funcionamento tecnológico de sistemas informatizados), no presente momento não haveria elementos ou argumentos para refutar a análise do próprio MRE no que diz respeito à sensibilidade e segurança dos dados envolvidos.

Decisão da CGU

A CGU indeferiu o recurso, com fundamento no art. 13, inciso II, do Decreto nº 7.724, de 2012, por entender que a divulgação do dicionário de dados, do esquema relacional do banco de dados; do volume do banco de dados; e da tecnologia de armazenamento do banco de dados do sistema INTRATEC, do MRE, seria desarrazoada.

Recurso à Comissão Mista de Reavaliação de Informações (CMRI)

O Requerente recorreu à CMRI questionando a caracterização do pedido como desarrazoado, alegando que negar acesso à informação teria, como consequência jurídica, a criação de uma nova hipótese de sigilo eterno, em contrária violação ao disposto pela Lei nº 12.527, de 2011. Acrescentou que, para os casos em que o acesso à informação puder afetar a segurança das atividades e colocar em risco o funcionamento regular da Administração Pública, a referida Lei é clara em determinar que o órgão deve classificar a informação nos termos do art. 23, caput, e, ato contínuo, estabelecer restrição de acesso por prazo certo e determinado, conforme o art. 24, §1º. Assim, asseverou que ao negar fornecer a informações a pedidos “desarrazoados”, o órgão estaria indiretamente induzindo o cidadão a ter que explicitar as razões do seu pedido. Considerou o Requerente que o art. 10, §3º da LAI se apresentaria claro em vedar qualquer tipo de exigência relacionada aos motivos da solicitação e, sendo assim, não seria possível, sob o ponto de vista jurídico, aceitar o raciocínio utilizado para negar acesso à informação, sob pena de violação à disposição legal expressa que, sob aspecto normativo, se encontraria hierarquicamente acima do que dispõe o Decreto Federal 7.724, de 2012. Subsidiariamente, solicitou que fossem fornecidas apenas as informações sobre o módulo de currículos do Intratec.

Admissibilidade do recurso à CMRI

Recurso parcialmente conhecido. Conforme o art. 24 do Decreto nº 7.724, de 2012, e os arts. 19 e 20 da Resolução CMRI nº 6, de 6 de junho de 2022, o recurso cumpre os requisitos de legitimidade, tempestividade e regularidade formal. O requisito de cabimento não foi atendido quanto à parcela do recurso que configura demanda de ouvidoria, que está fora do escopo do direito de acesso à informação.

Análise da CMRI

Inicialmente cumpre registrar que, no que diz respeito a parcela do recurso que versa sobre a definição do conceito de "pedido desarrazoado" e suas aplicações, o mérito não foi analisado em decorrência do não conhecimento, uma vez que se verificou não se tratar de pedido de acesso nos termos do art. 4º e 7º da Lei nº 12.527, de 2011, pois tem teor de questionamento sobre a aplicação da legislação em caso concreto, o que caracteriza manifestação de ouvidoria, regradas pela Lei nº 13.460, de 2017, e devem ser registradas em campo específico na Plataforma Fala.BR para seu devido tratamento, não podendo, portanto, ser conduzido por meio da ferramenta de acesso à informação ora utilizada. Passando a análise da parcela do recurso que versa sobre o acesso ao dicionário de dados; o esquema relacional, o volume e tecnologia de armazenamento do banco de dados do módulo de currículos do Intratec, foi feito interlocução com o MRE que informou:

> *"1 – Favor informar se há um único banco de dados para o "módulo de currículos" e Sistema Intratec.*
> *Resposta: Trata-se do mesmo banco de dados. Apesar do uso de esquemas diferentes, há compartilhamento de tabelas.*
>
> *2 – Considerando que um esquema de banco de dados pode representar a configuração lógica da totalidade ou de parte de uma base de dados relacional, é possível disponibilizar somente a parte do esquema que se refere as tabelas/exibições correspondente ao módulo de currículos?*
> *Resposta: O "esquema relacional de um banco de dados" é coleção de metadados que descreve os relacionamentos entre objetos e informações em um banco de dados. Ainda que possa ser tecnicamente viável a sua disponibilização, avalia-se que a eventual divulgação de dados técnicos que podem subsidiar ações passíveis de representar risco para a segurança da informação do Ministério das Relações Exteriores contraria, entre outros, a Política Nacional de Segurança da Informação e a Política Nacional de Cibersegurança.*
>
> *2.1 – Em caso negativo favor informar com detalhes técnicos o porquê da negativa (se houver amparo legal, favor informar para resguardar a restrição)*
> *Resposta: O Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR Nº 93, de 2021, define "ameaça" como "conjunto de fatores externos com o potencial de causar dano para um sistema ou organização". O conhecimento de informações atinentes ao funcionamento de banco de dados, que desdobram na governança de tecnologia e segurança de informação, poderá facilitar a identificação por terceiros de possíveis vulnerabilidades a ataques.*
> *Conforme o Art. 2º do Decreto 9.637/2018, a proteção de dados organizacionais é abrangida pela segurança da informação. O referido Decreto, em seu artigo 3º, elenca entre os princípios da Política Nacional de Segurança da Informação a prevenção de incidentes de segurança da informação (IX) e o dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas (XI). Por sua vez, figura entre os objetivos da Política Nacional de Cibersegurança (PNCiber) "estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos", conforme disposto no Art. 3º do Decreto 11.856/2023.*
> *Ressalta-se, ainda, que a hipótese de franquear informações e dados que poderão subsidiar ações passíveis de representar risco para a segurança da informação choca com as normas internas para o tratamento das informações produzidas, processadas, transmitidas ou armazenadas no âmbito deste Ministério. A Política de Segurança da Informação e Comunicações do Ministério das Relações Exteriores (POSIC), aprovada pela Portaria Nº 43, de 26 de janeiro de 2015, determina, em seu artigo 4.2, que "O acesso aos serviços de TIC do MRE é limitado a servidores com vínculo estatutário e funcionários com vínculo contratual com a SERE ou com os postos no exterior.". Ademais, o artigo 12.2 da POSIC prevê que "Os dados, as informações e os sistemas de informação devem ser protegidos contra ameaças e ações*

não autorizadas, acidentais ou não, com vistas a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses dados e ativos.".
A sensibilidade de tais informações também pode ser aferida pela cláusula de sigilo presente no Termo de Referência do contrato de prestação de serviços Nº 5/2022, de administração, manutenção e operação de dados e de bancos de dados, firmado entre o Ministério e a empresa Datainfo Soluções de Tecnologia da Informação LTDA. Conforme pactuado, a Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos."

A fim de compreender melhor os riscos no fornecimento das informações nova interlocução com o Recorrido foi feita conforme segue:

Deve-se ter presente que o conhecimento prévio sobre o tamanho de um banco de dados pode auxiliar significativamente na exfiltração de dados, permitindo que um atacante planeje e execute o ataque de forma mais eficiente. A título ilustrativo, seguem sete maneiras pelas quais essa informação pode ser utilizada com esse intuito:

1) Otimização da Estratégia de Exfiltração: Saber o tamanho do banco de dados permite ao atacante escolher o método mais eficiente para a exfiltração.
Por exemplo:
- Bancos de Dados Pequenos: Podem ser exfiltrados em uma única operação ou por meio de canais discretos, minimizando o risco de detecção.
- Bancos de Dados Grandes: Exigem segmentação ou extração incremental para evitar levantar suspeitas ou acionar sistemas de monitoramento de rede.

2) Evasão de Detecção: Sistemas de segurança frequentemente monitoram picos incomuns no tráfego de dados. Se o atacante conhece o tamanho do banco de dados, pode garantir que a exfiltração se alinhe aos padrões normais de tráfego, dificultando a detecção.

3) Seleção de Meio de Armazenamento Apropriado: O atacante pode preparar métodos de armazenamento ou transmissão capazes de lidar com o volume de dados, garantindo que a extração não falhe no meio da operação.

4) Estimativa do Tempo Necessário: A exfiltração de um banco de dados grande pode levar tempo significativo, especialmente se a largura de banda for limitada ou se for necessário restringir a velocidade para evitar detecção. Conhecer o tamanho do banco de dados permite ao atacante calcular o tempo necessário e planejar adequadamente.

5) Planejamento de Engodo e Ofuscação: Se o banco de dados for grande, atacantes podem exfiltrar apenas partes específicas ou introduzir tráfego de distração para mascarar suas atividades. Conhecer o tamanho total ajuda a decidir quais dados devem ser priorizados e a quantidade de tráfego fictício a ser gerada.

6) Ajuste de Compressão ou Criptografia: Para conjuntos de dados grandes, atacantes podem usar compressão para reduzir o volume de dados a ser exfiltrado. O conhecimento prévio do tamanho do banco de dados ajuda na escolha das ferramentas adequadas de compressão e métodos de criptografia para uma extração segura e eficiente.

7) Foco em Dados Específicos: O conhecimento do tamanho ajuda atacantes a inferir a escala de subconjuntos de dados específicos que desejam (por exemplo, registros de clientes, dados financeiros). Essa informação permite priorizar dados críticos, minimizando o impacto do processo de exfiltração.

A "tecnologia de armazenamento de banco de dados" refere-se ao modelo tecnológico utilizado para o armazenamento, organização e processamento das informações em um banco de dados. Não são utilizadas tecnologias distintas para os diferentes módulos de um sistema. Informações sobre o módulo de

currículos podem ser aplicáveis a sistemas sensíveis, nos quais são armazenados dados sigilosos. Deve-se ter presente, portanto, que a divulgação pública da tecnologia de armazenamento de banco de dados utilizada por um sistema interno governamental pode expor a infraestrutura do Ministério das Relações Exteriores a diversos riscos de segurança da informação, aumentando a superfície de ataque e facilitando ações maliciosas. Os principais riscos associados incluem:

1) Facilitação de Ataques Direcionados: Informações sobre a tecnologia utilizada (como o tipo de banco de dados, versão, ou fornecedor) podem permitir que atacantes explorem vulnerabilidades conhecidas específicas daquela solução.
Por exemplo:
- Se for revelado que um sistema utiliza versão desatualizada de um banco de dados, atacantes podem usar "exploits" documentados para comprometer o sistema. A esse respeito, deve-se ter presente que sistemas tradicionais de banco de dados, a exemplo de MySQL, PostgreSQL e MongoDB, divulgam publicamente histórico de vulnerabilidades conhecidas e que podem ser exploradas. Ressalta-se, ainda, que, devido à complexidade da operação e aos impactos na disponibilidade de sistemas corporativos, atualizações de bancos de dados demandam a mobilização de diversas equipes técnicas, de modo que precisam ser planejadas com antecedência. Não se pode assegurar, portanto, que sempre serão realizadas imediatamente após a disponibilização de alguma atualização de segurança, o que permite antever a existência de janelas de vulnerabilidade.

2) Reconhecimento e Planejamento de Ataques: Com essas informações, um atacante pode realizar reconhecimento detalhado (fase inicial de ataques cibernéticos) e planejar ataque direcionado. Adicionalmente, ferramentas automatizadas de teste de vulnerabilidades de segurança podem ser configuradas especificamente para o tipo de tecnologia utilizada pelo Ministério, identificando fraquezas adicionais.

3) Aumento do Risco de Engenharia Social: A divulgação pode ajudar a criar ataques de engenharia social mais convincentes. Por exemplo:
- Enviar e-mails de "phishing", para que solicitações fraudulentas de suporte técnico pareçam legítimas, na tentativa de enganar administradores do sistema, induzindo-os a instalar códigos maliciosos ("malwares") como sendo legítimos ou fornecer credenciais de acesso.

4) Escalabilidade de Ataques por Meio de Automação: Conhecendo a tecnologia utilizada, um atacante pode criar scripts automatizados para explorar vulnerabilidades específicas, aumentando a eficiência e o alcance do ataque.

5) Possibilidade de Exfiltração ou Corrupção de Dados: Tecnologias de armazenamento específicas podem apresentar falhas relacionadas a permissões mal configuradas, autenticação fraca ou exposição de interfaces de gerenciamento. Conhecendo o tipo de banco de dados, atacantes podem buscar atalhos para comprometer a confidencialidade, a integridade e a disponibilidade dos dados armazenados.

6) Dependência de Tecnologias Terceirizadas: Caso a tecnologia divulgada dependa de um provedor de serviços terceirizado, a exposição pública pode levar a ataques à infraestrutura do próprio fornecedor ("supply chain attack"), comprometendo a segurança dos dados governamentais.

7) Exploração de Configurações Padrão: Não raro, sistemas de banco de dados são implantados com configurações padrão do fornecedor, que podem conter vulnerabilidades, como: credenciais de acesso pré-definidas e portas abertas para acesso remoto.
A divulgação da tecnologia pode incentivar atacantes a explorar essas configurações caso não tenham sido devidamente modificadas.

8) Risco de Ataques de "Ransomware": Informações sobre o tipo de banco de dados podem facilitar a execução de ataques de "ransomware" para criptografar dados, exigindo pagamento para restauração. Esse risco é ampliado se a tecnologia for amplamente utilizada e documentada.

Conforme dados divulgados em transparência ativa pelo Centro de Prevenção, Tratamento e Resposta a

Incidentes Cibernéticos de Governo (CTIR Gov), órgão do Gabinete de Segurança Institucional (GSI), nos dez primeiros meses de 2024 foram registrados cerca de 6.700 episódios de vazamento de dados, dos quais 1236 apenas no mês de outubro. O claro sinal de incremento desse tipo de incidente reforça a necessidade de medidas que evitem a ampliação de riscos.

O Ministério das Relações Exteriores entende, em suma, que o fornecimento de dados relacionados às especificações e paradigmas dos sistemas de informática aumentaria, por diferentes meios, a vulnerabilidade dos sistemas internos de gestão da informação, com possíveis efeitos deletérios à segurança institucional, ao sigilo das comunicações diplomáticas e à manutenção das redes de comunicação utilizadas pelo Ministério das Relações Exteriores.

Do exposto no processo em voga, verificou-se estar comprovados os riscos de ocorrência de eventos de ataques de segurança e vazamento de dados, e assim entende-se ser desarrazoada a solicitação de acesso nos termos do inciso II do art. 13 do Decreto nº 7.724, de 20121. Nesse sentido, sobre a matéria os normativos vigentes dispõem:

Decreto nº 10.748, de 16 de julho de 2021

Art. 15. 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****.*

§ 1º As informações de que trata o caput ***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. (Grifos nosso)***

Portaria GSI/PR nº 93, de 18 de outubro de 2021

ATIVOS DE INFORMAÇÃO - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

Dito isto, importa registrar que a Lei nº 12.527, de 2011 (Lei de Acesso à Informação - LAI), em seu art. 22, *in verbis*, reconhece a existência de outras hipóteses de sigilo além daquelas por ela previstas:

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.

Com base nos dispositivos acima mencionados, entende-se que, no presente caso, os dados de interesse do Requerente constituem-se características técnicas de ativos de informação, que precisam ser restritos pois poderia colocar em risco a guarda de dados sob responsabilidade do MRE, devendo o seu acesso ser permitido somente aos profissionais autorizados e agentes públicos especificados na norma.

Decisão da CMRI

A Comissão Mista de Reavaliação de Informações decide, por unanimidade, pelo conhecimento parcial do recurso, uma vez que parte é demanda de ouvidoria, não se tratando de pedido de acesso nos termos do art. 4º e 7º da Lei nº 12.527, de 2011. Na parte que conhece, decide pelo indeferimento com fulcro no art. 15 do Decreto nº 10.748, de 2021 c/c art. 22 da Lei nº 12.527, de 2011, em razão de os dados solicitados consistirem em características técnicas de ativos de informação do órgão, cuja divulgação integral pode gerar a ocorrência de eventos de ataques de segurança e vazamento de dados, comprometendo o funcionamento de um sistema crítico para a Administração Pública Federal, sendo desarrazoada a concessão de acesso, nos termos do inciso II do art. 13 Decreto nº 7.724, de 2012.

Documento assinado eletronicamente por **Pedro Helena Pontual Machado**, **Secretário(a)-Executivo(a) Adjunto(a)**, em 30/12/2024, às 19:09, 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 **Eveline Martins Brito**, **Usuário Externo**, em 02/01/2025, às 17:00, 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 03/01/2025, às 10:16, 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 03/01/2025, às 12:11, 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 **PAULO ROCHA CYPRIANO**, **Usuário Externo**, em 06/01/2025, às 15:24, 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 07/01/2025, às 09:25, 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 **6327130** e o código CRC **3F030151** no site:
https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Referência: Processo nº 00131.000032/2024-03 SEI nº 6327130