

GRUPO II – CLASSE VII – Plenário

TC 039.693/2020-1 [Aposos: 047.560/2020-7; 045.800/2021-9]

Natureza: Representação

Unidades Jurisdicionadas: Conselho de Controle de Atividades Financeiras (Coaf) e Secretaria Especial da Receita Federal do Brasil (RFB)

Representação legal: não há.

SUMÁRIO: REPRESENTAÇÃO. CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). SECRETARIA ESPECIAL DA RECEITA FEDERAL DO BRASIL (RFB). APURAÇÃO DA OCORRÊNCIA DE ACESSO INDEVIDO A DADOS RELATIVOS A PESSOAS EXPOSTAS POLITICAMENTE (PEP) CONTIDOS EM BASES DE DADOS DA RFB E DO COAF. EXAME DO MECANISMO DE COMPARTILHAMENTO DE INFORMAÇÕES ENTRE COAF E RFB. AVALIAÇÃO DE RITOS, PROCEDIMENTOS E CONTROLES DESENHADOS PARA PRESERVAR OS DADOS RELATIVOS A PEP NOS SISTEMAS DO COAF E DA RFB. RECOMENDAÇÕES. DETERMINAÇÕES.

RELATÓRIO

Por registrar as principais ocorrências havidas no processo, resumindo os fundamentos das peças acostadas aos autos, adoto como relatório, com os ajustes necessários, o relatório de fiscalização produzido no âmbito da Secretaria de Controle Externo da Gestão Tributária e Supervisão de Contas (peça 92), a qual contou com a anuência do corpo diretivo da unidade instrutora (peça 93-94):

“I. Apresentação

1. Trata-se de fiscalização realizada pela Secretaria de Controle Externo da Gestão Tributária e Supervisão de Contas (SecexTributária) na Secretaria Especial da Receita Federal do Brasil (RFB), vinculada ao Ministério da Economia, e no Conselho de Controle de Atividades Financeiras (Coaf), vinculado ao Banco Central (e não ao Ministério de Justiça, como constou na capa deste relatório), no período de 1/3/2021 a 30/4/2021.
2. A fiscalização foi motivada por representação apresentada pelo Subprocurador-Geral do Ministério Público junto ao TCU, Lucas Rocha Furtado, em novembro de 2020, após veiculação de matéria jornalística sobre possíveis acessos indevidos a dados de PEPs junto à Receita Federal (peça 1).
3. Este processo foi inicialmente instruído pela Secretaria de Controle Externo da Gestão Tributária, da Previdência e da Assistência Social (SecexPrevidência), que opinou pelo não conhecimento da representação e indeferimento de medida cautelar pleiteada (peça 5). O relator, Ministro Bruno Dantas, discordou do encaminhamento sugerido quanto à primeira parte, decidindo pelo conhecimento da representação, fazendo as seguintes determinações (peça 8):
 - a) conhecer da presente representação, satisfeitos os requisitos de admissibilidade previstos nos arts. 235 e 237, inciso VII, do Regimento Interno deste Tribunal, c/c o art. 81, inciso I, da Lei 8.443/1992;
 - b) indeferir o pedido de concessão de medida cautelar por ausência dos pressupostos;
 - c) determinar à SecexPrevidência que:

- c.1) apure a ocorrência de indevido acesso a dados relativos a pessoas politicamente expostas mantidos em bases da Receita Federal do Brasil e do Conselho de Controle de Atividades Financeiras;
- c.2) avalie os ritos, os procedimentos e o sistema de controle desenhados para preservar os dados de pessoas politicamente expostas mantidos em bases da Receita Federal e do Coaf, bem como o processo de comunicação de fatos entre os dois órgãos, e os controles que existem para inibir, coibir e punir eventuais abusos;
- c.3) avalie a conveniência e a oportunidade de se realizar inspeção no Serpro e na Dataprev, no intuito de verificar os controles e a existência de registros de acesso aos sistemas relacionados ao tema; e
4. Ato contínuo, os autos foram encaminhados para a recém-criada SecexTributária para prosseguimento da instrução.

I. Introdução

I.1. Deliberação que originou o trabalho

5. Em cumprimento aos itens c.1 e c.2 do Despacho emitido em 17/12/2020 pelo Ministro Bruno Dantas (peça 8), considerando a delegação de competência conferida pela Portaria MIN-BD 1/2014 e o disposto no art. 240 do RITCU, a presente inspeção foi autorizada pelo Despacho de 1/3/2021 do Secretário de Controle Externo da Gestão Tributária e Supervisão de Contas (TC 039.693/2020-1, peça 15).

I.2. Visão geral do objeto

II.2.1 Conselho de Controle de Atividades Financeiras (Coaf)

6. O Sistema de Prevenção e Combate à Lavagem de Dinheiro (PCLD) compreende um regime global antilavagem, que engloba instrumentos internacionais que visam a introduzir, no direito interno dos diferentes países, dispositivos para enfrentar crimes de natureza transnacional (lavagem de dinheiro, terrorismo e outros).

7. No contexto do PCLD, o Brasil é signatário de diversas convenções internacionais, com destaque especial para a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), promulgada no Brasil pelo Decreto 5.015, de 12/3/2004. A referida convenção, entre outras medidas, trata das diretrizes para regulamentação e supervisão do sistema financeiro e para a criação das Unidades de Inteligência Financeira (UIF).

8. Nos idos de 1989, com o principal objetivo promover a proteção do sistema financeiro internacional, foi criado o Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (Gafi), a partir de uma ação intergovernamental entre os países membros da Organização para Cooperação e Desenvolvimento Econômico (OCDE).

9. Órgão formulador de políticas destinadas a estimular a realização de reformas legislativas e regulamentares em suas áreas de atuação, o Gafi desenvolveu uma série de recomendações reconhecidas como o padrão internacional para combater a lavagem de dinheiro, o financiamento do terrorismo e a proliferação de armas de destruição em massa. As quarenta Recomendações do Gafi foram revisadas mais recentemente em 2012, para garantir que continuassem relevantes, atualizadas e em condições de serem aplicadas por todos os países do mundo.

10. O Brasil, por ser membro do Gafi, assumiu o compromisso de seguir e implementar as suas recomendações, cujo cumprimento é avaliado periodicamente por meio de processo de avaliação mútua entre as diferentes jurisdições que figuram como membros do Grupo. Como decorrência deste compromisso, foi criada pela Lei 9.613/1998 e reestruturada pela Lei 13.974/2020, a UIF do Brasil, denominada Conselho de Controle de Atividades Financeiras (Coaf).

11. O Coaf é a autoridade central no Brasil do sistema de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa (PLD/FT), especialmente no recebimento, análise e disseminação de informações de inteligência

financeira.

Coaf e a produção de inteligência financeira

12. Vinculado administrativamente ao Banco Central do Brasil, com jurisdição nacional e autonomia operacional, o Coaf é constituído no modelo administrativo, isto é, realiza trabalhos de inteligência financeira, mas não é sua competência realizar investigações, bloquear valores, deter pessoas, realizar interrogatórios e outras atividades dessa natureza (peça 63). Outras informações sobre a estrutura organizacional do Coaf podem ser consultadas no apêndice B deste relatório.

13. O Coaf tem como atribuição legal receber, examinar e identificar as ocorrências de atividades ilícitas previstas na Lei 9.613/1998, que define regras a respeito da prevenção aos crimes de lavagem de dinheiro e ocultação de bens. As ocorrências de atividades suspeitas de ilícitos são comunicadas ao Coaf pelos setores obrigados, pessoas jurídicas e físicas relacionadas no art. 9º da referida Lei (instituições bancárias, joalherias e outras). Contudo, repise-se que o Coaf não investiga pessoas, nem acessa contas bancárias ou qualquer dado fiscal.

14. Os setores obrigados comunicam operações suspeitas com indícios de lavagem de dinheiro, de financiamento do terrorismo, bem como movimentações em espécie (“dinheiro vivo”) acima de determinado valor estabelecido em norma por meio do Sistema de Controle de Atividades Financeiras (Siscoaf).

15. O volume de comunicações tem crescido (atualmente são mais de 25.000 comunicações/dia) e, para auxiliar o seu tratamento, o Coaf utiliza inteligência artificial, por meio da adoção de filtros sistêmicos, conforme apresentação realizada pelo órgão dia 22/2/2021 (peça 53). Assim, critérios de risco orientam a análise ou não do conteúdo da comunicação, a qual pode sofrer o arquivamento automático (Regra de Diferimento Automático) ou ser selecionada para análise individualizada (Modelo Preditivo Supervisionado Classificatório), quando há o preenchimento de matriz de riscos por um analista de inteligência.

16. O Coaf também deve coordenar mecanismos de intercâmbio de informações que viabilizem ações rápidas no combate de ilícitos conforme estabelece § 2º do artigo 14 da Lei 9.613/1998. Dessa forma, as autoridades responsáveis pelas investigações comunicam o Coaf sobre processos investigativos em curso por meio do Sistema Eletrônico de Intercâmbio (SEI-C), que integra o Siscoaf. Em 2020, conforme informado pelo Coaf em resposta ao item a.5 do Ofício 7811/2021-TCU/Seproc (peça 38, p.28 e planilha enviada pelo SEI-C), foram recebidos 12.554 pedidos de intercâmbio de informações de autoridades nacionais, com destaque para Polícia Civil (4.380), Polícia Federal (3.606) e Ministério Público (2.035).

17. Após a abertura do caso e sua distribuição de maneira aleatória, entre os analistas de inteligência, inicia-se a etapa de elaboração do Relatórios de Inteligência Financeira (RIF), que pode seguir dois modelos: (a) RIF sintético - seu conteúdo se restringe às informações das comunicações de operações em espécie ou suspeitas disponíveis na base dados do Coaf sobre pessoas determinadas; (b) RIF analítico - elaborado a partir da conjugação de diferentes fontes de informações disponíveis no Siscoaf, agregando às informações constantes das comunicações de operações financeiras, conhecimento produzido pelos analistas do Coaf, com fundamento em outras bases de dados acessadas, públicas ou não (peça 38, p.21). Em 2020, foram produzidos e disseminados 3.428 RIFs espontâneos, compreendendo relatórios analíticos, sintético automático e não automático (peça 38, p.28 e planilha enviada pelo SEI-C).

18. Após a produção dos RIFs analíticos, estes são submetidos ao Comitê Consultivo que verificará se o relatório tem todas as características necessárias (formais e materiais). Os RIFs sintéticos são liberados pelo Coordenador-Geral. No caso de RIF relativo à movimentação financeira de pessoa com foro especial por prerrogativa de função, a liberação e envio cabem exclusivamente ao Presidente do Coaf. Todos os RIFs são disseminados exclusivamente por meio do Sistema Eletrônico de Intercâmbio do Coaf (SEI-C), que possui os requisitos de segurança na transmissão de dados exigidos pelos padrões internacionais.

(...)

19. Diversos são os controles para se resguardar o sigilo das informações pelo Coaf (Nota Técnica-SEI 14/2021/COAF, peça 38). A Coordenação-Geral de Gestão de Riscos Institucionais (Coris) articula medidas de gestão de riscos, segurança institucional e proteção do conhecimento sensível sob o domínio do órgão. As comunicações somente podem ser enviadas por comunicantes previamente habilitados. O acesso ao conteúdo das comunicações recebidas de forma eletrônica no Siscoaf pelo quadro técnico do Coaf é feito mediante *login* no Siscoaf por certificado digital, ficando registrados os *logs* de acessos. Quanto à disseminação dos RIFs, é feita exclusivamente pelo SEI-C, entre outros controles implementados.

20. Quanto ao tratamento específico de informações referentes a pessoas expostas politicamente, em razão do cargo ou função que ocupam ou ocuparam, a condição de PEP é fator qualificador na matriz de risco do Coaf. No que tange à disseminação dos RIFs, há impedimento da geração de RIF automático apenas para os PEPs que possuem foro por prerrogativa de função em Tribunais Superiores, com subsequente envio para distribuição. Neste caso, há destaque em vermelho no SEI-C que facilita a identificação do PEP com foro, ao qual é aplicado o regime de alçadas, que faz com que os relatórios produzidos necessitem de aprovações adicionais (peça 38).

21. Outras informações sobre o processo de produção de inteligência financeira, o fluxo de produção e disseminação de RIF, os controles para resguardar o sigilo das informações e o tratamento específico de informações referentes a pessoas expostas politicamente podem ser obtidas nos apêndices C a F.

II.2.2 Secretaria Especial da Receita Federal do Brasil (RFB)

22. Segundo o Sistema de Prevenção e Combate à Lavagem de Dinheiro (PCLD), os ilícitos tributários e aduaneiros, a lavagem de dinheiro e demais crimes financeiros são delitos que ameaçam os interesses estratégicos, políticos e econômicos de diversas nações, podendo privar o Estado dos recursos financeiros necessários a seu desenvolvimento de forma sustentável e abalando a confiança dos cidadãos na capacidade de seus dirigentes promoverem a justiça fiscal.

23. Organizações especializadas que tratam do tema como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a Organização Mundial das Aduanas (OMA) e o Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (Gafi), consideram que as autoridades tributárias e aduaneiras têm papel primordial na identificação dos meios mais comuns de movimentação financeira para lavagem de dinheiro, principalmente em função de possuírem ampla gama de atribuições e de instrumentos operacionais em seus campos de atuação (<https://receita.economia.gov.br/sobre/acoes-e-programas/combate-a-ilicitos/lavagem-de-dinheiro>, acesso em maio/2021)

24. Esta visão impõe destacada responsabilidade à RFB – um dos órgãos brasileiros de fiscalização e controle que compõem o sistema nacional de PCLD –, principalmente no que se refere à criação de mecanismos preventivos, ao gerenciamento de riscos e de dados estatísticos, bem como ao aperfeiçoamento de instrumentos de comunicação de indícios dos ilícitos em questão a outras autoridades do sistema.

25. A relevância atribuída pela Receita Federal ao combate a esse delito é traduzida em seu Regimento Interno, que estabelece a repressão ao crime de lavagem de dinheiro como uma de suas finalidades (art. 1º, inciso XX). Neste dispositivo, a RFB institucionaliza o emprego de sua ampla estrutura administrativa, operacional, base de dados e recursos tecnológicos, ativos precipuamente direcionados para o combate de ilícitos tributários e aduaneiros, igualmente para o combate à lavagem de dinheiro.

Copei - a unidade de inteligência fiscal da RFB

26. No âmbito interno da RFB, compete à Coordenação-Geral de Pesquisa e Investigação (Copei), unidade diretamente vinculada à Subsecretaria-Geral da Receita Federal do Brasil, o assessoramento estratégico e as atividades relativas à inteligência fiscal e investigação conjunta com outros órgãos.

27. Na Copei ocorre a análise, a produção e a difusão de conhecimentos de inteligência fiscal para assessorar o processo decisório, em subsídio ao planejamento, à execução e ao aperfeiçoamento das atividades próprias da RFB.

28. Neste sentido, como unidade interna de Inteligência Fiscal da RFB, a Copei é responsável por receber os Relatórios de Inteligência Financeira (RIF) com indícios de ilícitos tributários remetidos pelo Coaf, para fazer o tratamento preliminar e disseminar seu conteúdo para as respectivas unidades de programação e fiscalização na RFB, conforme o caso.

29. Mediante análise preliminar, a Copei verifica se há indícios da prática de ilícito tributário nos fatos relatados, se é competência da RFB e da Copei e se há iminente risco de decadência do crédito tributário. Em caso positivo, há instauração de procedimento administrativo com o objetivo de apurar elementos indiciários e probatórios da prática do ilícito tributário (fase meramente preparatória), para subsidiar a posterior atuação das unidades competentes da RFB (seleção, programação e fiscalização), no regular processo de constituição do crédito tributário (lançamento).

30. No caso específico dos RIF remetidos pelo Coaf, armazenados em repositório seguro da RFB, a Copei, após a análise preliminar, instaura o procedimento administrativo apuratório da prática do ilícito tributário, produzindo, ao final, um Relatório de Inteligência que é encaminhado às unidades internas competentes de seleção, programação ou fiscalização.

(...)

31. Em 2020, a Copei recebeu 740 RIF expedidos pelo Coaf e expediu 21 comunicações (relatórios de inteligência) resultantes de RIF a outras unidades da RFB (Nota-RFB/Copei/Gab GB20210002, peça 32, p.5). De outra banda, foram encerrados 24 procedimentos fiscais acerca de PEP, resultando em lançamentos tributários na ordem de R\$ 90,33 milhões (Nota 92/2021-RFB/Copes/GAB, peça 31, p.12).

32. Com relação aos controles para resguardar o sigilo das informações na RFB, tanto a Copei quanto a Coordenação-Geral de Programação e Estudos (Copes) e a Coordenação-Geral de Fiscalização (Cofis) estão sujeitas à observância do sigilo fiscal estabelecido no art. 198 do Código Tributário Nacional (CTN). Esse dispositivo legal impede o compartilhamento direto das informações custodiadas pela RFB com os demais órgãos fiscalizadores, ressalvadas hipóteses de compartilhamento por força de determinação judicial (art. 198, §1º, inciso I, do CTN), em decorrência de requisição formal do Ministério Público Federal (art. 8º, §§1º e 2º c/c art. 24 da Lei Complementar 75/1993) e as Representações Fiscais para fins Penais (Portaria-RFB 1.750, de 2018) (peça 31, p. 7 e 8; peça 32, p. 3).

33. Entre os controles existentes, podem ser citados: política de segurança da informação; sistema formulário eletrônico de solicitações de acesso de usuários e contas de serviços; registros de eventos (*logs*) e armazenamento dos logs das aplicações da RFB no datacenter do Serpro por um período de oito anos. Em observância aos princípios da impessoalidade, imparcialidade e isonomia tributária, a RFB, na fiscalização de tributos internos, não adota procedimento diferenciado para tratamento de dados referentes a pessoas expostas politicamente (peça 31, p.12).

34. No entanto, o monitoramento do acesso aos dados da Declaração de Imposto de Renda Pessoa Física (DIRPF) é realizado de forma contínua e automática, desde 2013, por meio do sistema Alerta no módulo Midas. Esse sistema é um importante meio que auxilia a RFB na detecção de possível acesso imotivado a informações protegidas por sigilo fiscal e utiliza o cadastro elaborado pela Controladoria-Geral da União (CGU) como parâmetro de acesso aos dados fiscais das PEP.

35. Maiores informações sobre a atuação da Copei, o fluxo interno na RFB das informações dos RIF enviados pelo Coaf, os controles para se resguardar o sigilo das informações na RFB podem ser consultadas nos apêndices G a I.

I.3. Objetivo e questões de auditoria

36. A presente inspeção teve por objetivo apurar a possível ocorrência de indevido acesso a dados relativos a pessoas expostas politicamente (PEPs) nas bases RFB e do Coaf, o seu compartilhamento entre os dois órgãos, bem como avaliar os ritos, procedimentos e controles

desenhados para preservar os dados relativos a PEPs nos sistemas dos órgãos.

37. A partir do objetivo do trabalho, formularam-se as questões adiante indicadas:

- a) Questão 1: Houve ocorrência de indevido acesso a dados relativos a pessoas expostas politicamente em bases da RFB e do Coaf?
- b) Questão 2: Os ritos, os procedimentos e o sistema de controle desenhados são suficientes para preservar os dados de pessoas expostas politicamente mantidos em bases da RFB e Coaf?
- c) Questão 3: O processo de comunicação de fatos entre a RFB e o Coaf é seguro e existem controles para inibir, coibir e punir eventuais abusos?

I.4. Metodologia utilizada

38. Os trabalhos foram realizados em conformidade com as Normas de Auditoria do Tribunal de Contas da União (Portaria-TCU 280, de 8 de dezembro de 2010, alterada pela Portaria-TCU 168 de 30 de junho de 2011) e com observância aos Padrões de Auditoria de Conformidade estabelecidos pelo TCU (Portaria-Segecex 26, de 19 de outubro de 2009).

39. Para a elaboração das matrizes de planejamento e de achados, foram utilizadas as seguintes técnicas de auditoria: exame documental; circularização; comparação com a legislação, jurisprudência e doutrina; entrevistas com os gestores; visitas técnicas para, por meio de pesquisa em sistemas dos órgãos, verificar a regularidade da elaboração de dossiês/relatórios/processos relativos a PEPs produzidos pela RFB e pelo Coaf, bem como avaliação de riscos e controles respectivos.

40. Para verificar o tratamento e utilização dos relatórios de inteligência financeira pela RFB, foi solicitada uma extração de relação de PEPs que tiveram ações fiscais instauradas e concluídas entre os anos de 2015 e 2020, seguida da aplicação de um filtro para verificar quais destes PEPs também foram objeto de RIFs encaminhado pelo Coaf.

41. Ao final da fase de execução do trabalho, foi realizada reunião com gestores da RFB e do Coaf para verificar a coerência da matriz de achados e discutir as principais conclusões da fiscalização, a adequação das análises realizadas e a pertinência das propostas de encaminhamento. A versão validada pelos gestores foi acostada no apêndice A.

I.5. Limitações inerentes à auditoria

42. Como limitação imposta ao trabalho, registra-se que não foi possível verificar os *logs* de acesso aos dados fiscais das PEPs nas bases da RFB, pois, segundo os gestores, o TCU não é competente para controlar resultados de sindicâncias ou de procedimentos administrativos disciplinares instaurados por aquele órgão, consoante a limitação concedida pelo Excelentíssimo Senhor Ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), em 25/10/2019, no âmbito do Mandado de Segurança n. 36.707/DF, que guarda estreita relação com o caso da presente fiscalização (peça 36, p.3-8).

43. Essa limitação não permitiu verificar em quais momentos houve o acesso indevido, mas os processos administrativos abertos pela própria RFB e suas conclusões atestaram tais ocorrências, sendo possível responder à questão 1 de auditoria (Ofício 12/2021–COGER/RFB, peça 52, p.3-4).

I.6. Volume de recursos fiscalizados

44. A mensuração do VRF não se aplica, uma vez que o objeto da inspeção não é quantificável em valores monetários.

I.7. Benefícios estimados da fiscalização

45. Entre os benefícios estimados desta fiscalização, destacam-se o incremento da economia, eficiência, eficácia ou efetividade de órgão, por meio do aperfeiçoamento dos controles desenhados para preservar os dados de pessoas politicamente expostas, além de outros benefícios diretos, como o fornecimento de subsídios para elaboração da relação de PEPs pela Controladoria-Geral da União, em conjunto com o Conselho Nacional de Justiça e o Conselho Nacional do Ministério Público.

II. Achados de auditoria

II.1. Acesso indevido aos dados fiscais de PEPs na RFB

46.O art. 198 do Código Tributário Nacional (CTN) traz a regra do sigilo fiscal, que veda a divulgação, por parte dos servidores da Fazenda Pública, de informação obtida em razão do seu ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades. O sigilo fiscal não se impõe somente à divulgação externa das informações disponíveis no banco de dados do órgão custodiante, mas também se aplica ao acesso interno dessas informações por seus servidores.

47.Neste sentido, todos os atos dos servidores públicos, mesmo os de mero acesso a dados custodiados pelos órgãos a que estão vinculados, devem respeito ao princípio da motivação obrigatória que impõe à Administração Pública o dever de indicação dos pressupostos de fato e de direito que determinaram a prática do ato (art. 2º, inciso VII, da Lei 9.784/1999), a fim de garantir e evidenciar o atendimento do princípio constitucional da impessoalidade que estabelece um dever de **imparcialidade** na defesa do interesse público, **impedindo discriminações (perseguições) ou privilégios (favoritismo)** dispensados a particulares no exercício da função administrativa (MAZZA, Alexandre. *Manual de Direito Administrativo*. 8 ed. São Paulo: Saraiva Educação, 2018. p. 118). Em respeito à regra do sigilo, o servidor deve comprovar a legitimidade do acesso aos dados.

48.Considerando que as pessoas expostas politicamente (PEP) têm maior risco de que seus dados sejam acessados de maneira imotivada devido aos cargos e às funções que ocupam e uma vez que a inspeção foi motivada justamente por um possível acesso aos dados sigilosos dessas pessoas, a RFB foi questionada quanto à ocorrência de acessos indevidos e, se identificados pela RFB, como foram tratados.

49.O órgão informou, conforme Ofício 12/2021-COGER/RFB (peça 52), que, no período de 2018 a 2020, foram instaurados oito processos administrativos disciplinares para apurar possíveis acessos imotivados aos sistemas da RFB, dentre os quais seis são relativos a dados de PEP.

50.Dos oito processos instaurados, quatro encontram-se em andamento e os demais foram concluídos com responsabilização dos servidores que efetuaram os acessos indevidos aos sistemas da RFB. As penalidades aplicadas foram de suspensão, sendo realizadas as devidas comunicações aos gestores de cada unidade de lotação dos servidores apenados.

51.Entre estes processos, um tratou especificamente de apuração correcional de servidor que acessou indevidamente os dados fiscais do Senador Flavio Bolsonaro, concluso pela responsabilização do servidor, sendo aplicada penalidade de suspensão (peça 36, p. 7; peça 52). Ressalta-se que notícia veiculada na Folha de São Paulo sobre esse acesso deu origem à representação (peça 1, p. 2), e que, apesar da limitação imposta ao trabalho em consequência à decisão do STF (parágrafo 42), o acesso indevido foi confirmado pela RFB.

52.Tendo em vista que já estão sendo tomadas medidas para detecção, apuração e penalização de servidores que incorrem em acesso indevido/imotivado a dados fiscais de contribuintes, cabe deixar de determinar à RFB a adoção de medidas para essa finalidade, com fundamento no inciso I do parágrafo único do art. 16 da Resolução-TCU 315, de 2020.

II.2. Necessidade de ampliar a abrangência da base de dados de PEPs mantida pela CGU para contemplar autoridades do Poder Judiciário e do Ministério Público

53.As recomendações do Gafi são reconhecidas como o padrão internacional antilavagem de dinheiro e contra o financiamento do terrorismo (<https://www.gov.br/fazenda/pt-br/centrais-de-conteudos/publicacoes/livros/arquivos/as-recomendacoes-do-gafi.pdf>, p. 195). De acordo com o Gafi, são pessoas expostas politicamente (PEP):

‘indivíduos que ocupam ou já ocuparam funções públicas proeminentes domesticamente, por exemplo, chefes de estado ou de governo, políticos de escalão superior, cargos governamentais de escalão superior, oficiais militares e membros do escalão superior do **Poder Judiciário**, executivos de escalão superior de empresas públicas e dirigentes de partidos políticos.’

(Glossário Geral das Recomendações do Gafi 2012, disponível em <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Portuguese-GAFISUD.pdf>, acesso em 25/5/2021)

54. Cabe ressaltar que, em regra, pela natureza das funções que ocupam, as PEP têm maior risco de que seus dados sejam acessados de maneira imotivada, uma vez que detêm maior poder e/ou tais dados têm grande valor para utilização de eventuais adversários políticos, o que justifica que sejam tomadas precauções adicionais para proteção dos seus dados.

55. Todavia, as recomendações do Gafi têm o propósito de garantir que essas pessoas sejam observadas com mais atenção, em face do maior risco de corrupção ao qual estão sujeitas, devido às posições que ocupam. Nesse sentido é a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31/10/2003, assinada pelo Brasil em 9/12/2003 e promulgada por meio do Decreto 5.687/2006. A convenção dispõe o seguinte no seu art. 52 sobre a prevenção e detecção de transferência de produtos de delito:

‘1. Sem prejuízo ao disposto no Artigo 14 da presente Convenção, cada Estado Parte adotará as medidas que sejam necessárias, em conformidade com sua legislação interna, para exigir das instituições financeiras que funcionam em seu território que verifiquem a identidade dos clientes, adotem medidas razoáveis para determinar a identidade dos beneficiários finais dos fundos depositados em contas vultosas, e **intensifiquem seu escrutínio de toda conta solicitada ou mantida no ou pelo nome de pessoas que desempenhem ou tenham desempenhado funções públicas eminentes e de seus familiares e estreitos colaboradores**. Esse escrutínio intensificado dar-se-á estruturado razoavelmente de modo que permita descobrir transações suspeitas com objetivo de informar às autoridades competentes e não deverá ser concebido de forma que atrapalhe ou impeça o curso normal do negócio das instituições financeiras com sua legítima clientela.

2. A fim de facilitar a aplicação das medidas previstas no parágrafo 1 do presente Artigo, cada Estado Parte, em conformidade com sua legislação interna e inspirando-se nas iniciativas pertinentes de suas organizações regionais, inter-regionais e multilaterais de luta contra a lavagem de dinheiro, deverá:

a) **Estabelecer diretrizes sobre o tipo de pessoas físicas ou jurídicas cujas contas as instituições financeiras que funcionam em seu território deverão submeter a um maior escrutínio**, os tipos de contas e transações às quais deverão prestar particular atenção e a maneira apropriada de abrir contas e de levar registros ou expedientes relativos a elas;’ (grifos nossos)

56. Assim, o Gafi preconiza que as instituições financeiras devem possuir sistemas adequados de gerenciamento de risco para determinar se a pessoa é exposta politicamente, e, em consonância, tanto a RFB quanto o Coaf desenvolveram mecanismos específicos para resguardar e tratar os dados de PEPs: (i) na RFB, foi criado o sistema Alerta, que notifica os supervisores quando ocorrem acessos aos dados de declaração de imposto de renda pessoa física de PEPs; (ii) no Coaf, foram implementados vários mecanismos para prevenir a divulgação indevida de relatórios de inteligência e respectivas comunicações dos setores obrigados que versem sobre PEPs com foro privilegiado.

57. Tais mecanismos têm como uma relevante fonte de informação a base de dados de pessoas expostas politicamente disponibilizado pelo governo federal, que foi implementado pela ação 7/2013 da Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro (Enccla) e é mantido pela Controladoria-Geral da União (CGU).

58. Contudo, constatou-se que a base de dados mantida pela CGU **não inclui** membros do Poder Judiciário ou do Ministério Público (<http://www.portaldatransparencia.gov.br/download-de-dados/pep>), embora alguns deles sejam contemplados na definição de PEPs do Gafi apresentada no parágrafo 53. Isso acaba por onerar o funcionamento dos referidos mecanismos e controles implementados pelos órgãos para salvaguardá-los.

59. Na Receita Federal, uma vez que o sistema Alerta identifica quem é PEP a partir da lista da

CGU, o sistema deixa de cobrir uma parcela significativa de pessoas expostas. Caso ocorram acessos indevidos a dados de membros do Judiciário ou do Ministério Público, não serão emitidos alertas, o que aumenta o risco de que acessos indevidos não sejam detectados.

60.No Coaf, os mecanismos de tratamento de dados de PEPs também são inicialmente baseados na lista da CGU, e posteriormente ocorre inclusão manual de membros do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ). A ampliação da abrangência da base de dados de PEPs mantida pela CGU para contemplar as que integrem o Poder Judiciário e Ministério Público, portanto, contribuiria para facilitar e eventualmente até tornar mais seguro o funcionamento dos mecanismos e controles existentes.

61.Segundo o Coaf (peça 38, p.32), com vistas a completar a lista de PEPs, foi enviado ofício para o Conselho Nacional de Justiça (CNJ) (peça 65) e mantido contato com Conselho Nacional do Ministério Público (CNMP), mas essas duas iniciativas restaram infrutíferas. Pondera-se que os referidos órgãos não tenham compreendido a importância dessa providência para salvaguardar os dados de seus membros.

62.Conclui-se, portanto, que o não envio das informações sobre os seus membros pelo CNJ e pelo CNMP para completar a lista de PEPs organizada pela CGU torna mais oneroso o cumprimento de normas editadas para disciplinar o tratamento de informações relacionadas a PEPs em linha com o disposto no art. 52, item 2, alínea “a”, da Convenção das Nações Unidas Contra a Corrupção, promulgada pelo Decreto 5.687/2006.

63.A CGU se manifestou sobre o achado após recebimento do relatório preliminar de fiscalização (peças 79 e 80), e esclareceu que a consolidação do cadastro de PEPs pelo órgão é resultado da ação 7/2013 da Enccla, que não possui caráter impositivo, e tal atribuição não é mencionada em nenhum outro normativo legal ou infralegal. Assim, embora a relação por ela consolidada não contemple os membros do Ministério Público e do Poder Judiciário, tal fato não configura irregularidade.

64.Informou ainda os esforços que vem conduzindo para honrar o compromisso assumido pelo governo federal, no que se refere ao aprimoramento do cadastro de PEPs, que consta no Plano Anticorrupção do Governo Federal, especificamente do que diz respeito à ação 4, a “Criação do sistema para coleta de informação sobre Pessoas Expostas Politicamente (PEP)” com prazo para 31/12/2021. Nesse sentido, apontou que tem atuado no intuito de melhorar o cadastro de pessoas expostas politicamente para abranger o maior número possível de agentes públicos considerados PEP, e está aprimorando seus procedimentos e sistemas de coleta e consolidação das informações.

65.O Sistema de Transferência de Informação (STI) é um sistema implementado pela CGU originalmente para receber planilhas sobre terceirizados contratados pelos órgãos do Poder Executivo federal. Tal sistema está sendo adaptado para receber os dados de PEPs, primeiramente dos entes municipais (prefeituras e câmaras legislativas) e posteriormente dos governos estaduais e órgãos na esfera federal, e funcionará a partir do encaminhamento mensal, por um usuário cadastrado para representar determinado órgão, de uma planilha padronizada e preenchida sobre dados de PEPs.

66.Contudo, a obrigatoriedade de incluir os membros do Poder Judiciário e do Ministério Público no cadastro para torná-lo mais abrangente só pode ocorrer por força de lei.

67.Assim, cabe dar conhecimento à CGU, ao CNJ e ao CNMP do teor do relatório, no intuito de possibilitar aos órgãos conhecer os riscos identificados pelo TCU em relação à abrangência do atual cadastro de Pessoas Expostas Politicamente e suas consequências nos mecanismos desenhados pela RFB e pelo Coaf para resguardar os dados dessas pessoas, a fim de possibilitar a otimização dos processos de elaboração e consolidação do cadastro.

II.3. Fragilidades nos controles estabelecidos pela RFB para salvaguardar acesso indevido a dados de PEPs pelo Sistema Midas

68.A RFB possui política de segurança da informação, que contempla diversos mecanismos para salvaguardar o acesso aos dados dos contribuintes (peça 34), conforme descrito a seguir.

69. Antes de poder realizar qualquer acesso, o usuário precisa solicitar um perfil de acesso. A política de segurança prevê o fluxo de solicitação e autorização de acesso a dados, vinculados a portarias de acesso elaboradas pelos gestores de cada sistema. As portarias definem o nível de permissão de acesso em função de diferentes perfis, que consideram cargo, carreira, função e lotação do servidor que solicita o acesso.

70. Quando o servidor solicita acesso a determinado sistema, primeiramente ocorre a verificação automática do batimento das informações funcionais com as regras de cada sistema. Caso a solicitação esteja de acordo com as regras, ainda é necessária a aprovação pela chefia da solicitação, e quando a portaria específica do sistema assim definir, ainda pode ser necessária uma aprovação adicional.

71. Os servidores precisam assinar todas as solicitações por meio de certificação digital e são realizadas revisões periódicas (no mínimo, anualmente) dos perfis concedidos em cada sistema. Além disso, existem diversas funcionalidades de controle, como a pesquisa de todas as solicitações realizadas, horários, fluxo com cada passo dos pedidos, além de módulo de desabilitação automática, que avisa as chefias competentes quando ocorrem vacâncias e algum perfil deve ser reavaliado.

72. Após os acessos, os sistemas são sujeitos a registros de eventos (*logs*) que permitem identificar, acompanhar e recuperar evidências nos casos de suspeita de violação de normas e em incidentes de segurança.

73. Em relação aos dados da declaração de imposto de renda da pessoa física (DIRPF) de pessoas expostas politicamente (PEPs), existe ainda o módulo Midas do sistema Alerta, que emite alertas para o superior hierárquico e seu adjunto, com cópia para o gestor regional, sempre que esses dados são acessados por servidor da RFB. Até fevereiro de 2021, essa era apenas uma ferramenta de mensageria, restrita ao envio de alertas. Em março de 2021, entrou em produção nova versão do sistema, o Alerta-Gestor, que passou a permitir o controle dos alertas e o registro das medidas adotadas quanto aos alertas emitidos. Esse sistema agora permite a coleta de informações gerenciais pela Auditoria Interna e Corregedoria, que possuem três perfis de gestor nacional, os quais possibilitam visualizar todos os acessos às DIRPF de PEPs e se estão devidamente motivados (peças 33 e 55).

74. Diante do módulo Midas do sistema Alerta-Gestor, é possível detectar acessos indevidos aos dados das PEPs e tomar as medidas cabíveis sempre que ocorram. Contudo, cabe ressaltar que o sistema Alerta-Gestor não impede o acesso indevido, mas consiste em um mecanismo que pode ajudar na sua detecção. Não há mecanismos automatizados (além do controle de perfis) que previnam tais acessos indevidos, ou que garantam que a Corregedoria do órgão apure e puna eventuais abusos de auditores fiscais.

75. Cabe observar que, sempre que qualquer servidor da RFB acessa o portal da DIRPF, ele deve informar a justificativa para o acesso (programação, outros etc.). Ocorre que essas justificativas são genéricas, o que pode dificultar que o supervisor realize uma supervisão efetiva ao receber o alerta. Por exemplo, se um servidor da área de programação de fiscalizações informar “programação” na justificativa do acesso, esse acesso estará aparentemente correto/motivado, mas tal justificativa não permite ao supervisor verificar a regularidade do acesso, o que poderia ser feito, por exemplo, caso fosse requerido também o registro do número do dossiê/processo que fundamentou a consulta efetuada.

76. Também é relevante destacar que o conceito de **autoridade tributária** pode ser mais um empecilho para a efetivo conhecimento das ações que estão sendo realizadas pelos auditores fiscais, tal qual indicado no relatório originador do Acórdão 2.118/2020-TCU-Plenário (TC 005.576/2019-9):

‘Conforme esse conceito, os atos praticados pelo Auditor-Fiscal da Receita Federal do Brasil na condição de ‘autoridade tributária’ normalmente não são revisados, nem hierarquicamente, nem por pares. Ressalte-se que este conceito não possui previsão legal e deriva-se de uma construção jurídica interna e avalizada por estudos realizados pela Diretoria de Estudos Técnicos do

Sindifisco Nacional.’

77.A edição da Portaria-RFB 11/2021, de 24/2/2021, porém, iniciou um processo de mudança na cultura organizacional de não supervisão dos trabalhos desenvolvidos pelos Auditores Fiscais da RFB, especialmente por meio do seu art. 7º, que estabeleceu a competência dos chefes de equipe de fiscalização de coordenar e supervisionar as atividades de seus subordinados. Ainda assim, como realizar mudanças na cultura organizacional de um órgão normalmente é um processo lento, torna-se ainda mais importante que a RFB crie mecanismos para verificar se a supervisão dos acessos, por meio dos alertas recebidos, está ocorrendo de forma rotineira e efetiva.

78.Em reunião de fechamento da inspeção, ocorrida no dia 30/4/2021, a RFB informou que seria impraticável a implementação de travas automáticas para limitar o acesso ao sistema Midas, que reúne as declarações de imposto de renda de pessoas físicas (DIRPF), uma vez que afetaria e comprometeria outros processos de trabalho como os Centros de Atendimento ao Contribuinte e a Malha Fiscal, que correspondem a um grande volume de acessos neste sistema, além de acarretar em quebra de impessoalidade da administração tributária, por colocar em caráter privilegiado dados de contribuintes com perfil PEP. Contudo, reconheceram que os controles *a posteriori* poderiam ser aperfeiçoados, inclusive para possibilitar a consulta das medidas adotadas pelo supervisor quanto ao alerta recebido (peça 56).

79.Assim, considerando que o sistema Alerta ainda está em desenvolvimento e que o aperfeiçoamento de seus controles *a posteriori* pode contribuir para a efetivação dos princípios da impessoalidade e da motivação (respectivamente, art. 37, *caput*, da Constituição Federal e art. 2º, § único, inciso VII, da Lei 9784/1999), será proposto recomendar à RFB, com fundamento no art. 11 da Resolução-TCU 315, de 2020, que:

- i) aprimore e refine o campo de “justificativa” que deve ser preenchido para acessar o sistema Midas e a base de declarações de imposto de renda de pessoas físicas (DIRPF), para facilitar a detecção de desvios pela supervisão quando do recebimento de alertas referentes a pessoas expostas politicamente;
- ii) avalie a oportunidade e conveniência de incluir ferramentas gerenciais no Sistema Alerta, que permitam avaliar efetivamente ações tomadas pelos supervisores depois de recebidos os alertas, de modo a garantir supervisão efetiva sobre os acessos à base de declarações de imposto de renda de pessoas físicas (DIRPF) de pessoas expostas politicamente.

II.4. Mecanismos de controle no Coaf reservados a PEPs com prerrogativa de foro

80.Conforme informado pelo Coaf, a recomendação 12 do Gafi estabelece que, em razão do cargo ou da função que ocupam ou ocuparam, as pessoas expostas politicamente (PEP) apresentam **maior risco** de envolvimento em operações de lavagem de dinheiro. Por essa razão, os setores obrigados devem realizar monitoramento contínuo e aplicar medidas de devida diligência sobre essas pessoas (peça 38, p. 31).

81.O que pretende a recomendação 12 do Gafi, assim como os normativos internos que a incorporam, não é conferir blindagem extra contra o monitoramento das operações realizadas por essas pessoas. Pelo contrário, o padrão internacional exige que negócios estabelecidos e operações realizadas com PEP sejam submetidas a controles e exames mais rigorosos, em razão do risco intrínseco da função política associada (peça 38, p. 31).

82.Assim, o Coaf aplica às comunicações que versam sobre PEP controles mais rígidos: se a comunicação mencionar PEP, esse fato vai majorar a pontuação de risco calculada pelo órgão (peça 38, p. 31-32).

83.Por outro lado, os Relatórios de Inteligência Financeira (RIF), de caráter indiciário e não probante, podem possuir informações sensíveis para a imagem de PEP e a capacidade de municiar eventuais adversários políticos quando encaminhados a autoridades sem competência investigatória, caso haja foro privilegiado. Esse fato reforça a sensibilidade das informações e justifica a adoção de controles adicionais para evitar sua disseminação equivocada para autoridade incompetente.

84. Desta forma, nos casos em que o RIF envolve pessoas com direito a foro por prerrogativa de função em Tribunal Superior, este é encaminhado exclusivamente ao Procurador-Geral da República (PGR) e ao Diretor-Geral da Polícia Federal, exceto quando outra autoridade competente para investigar apresentar procedimento investigatório devidamente autorizado e instaurado no respectivo Tribunal (peça 38, p. 25-26).

85. Se a pessoa analisada no RIF possuir foro por prerrogativa de função em tribunais de segunda instância de julgamento (instância ordinária), a pasta de difusão para o Ministério Público Federal é substituída por pasta na respectiva Assessoria de Pesquisa e Análise da Procuradoria Regional da República conforme item 16.19 da Parte Geral do Manual da Difin (peça 38, p. 26).

86. Enfim, na entrada de comunicações dos setores obrigados, o sistema identifica quem é PEP para efeito de avaliação de risco, de acordo com as recomendações do Gafi. Já na saída das comunicações (disseminação - envio dos RIFs para autoridades competentes), o Coaf possui mecanismos de controle para mitigar os riscos de envio de RIF para autoridades que não tenham competência para realizar a investigação.

87. Um destes mecanismos é a marcação em vermelho (destaque) das pessoas com foro por prerrogativa de função constantes dos RIFs. No Sistema de Controle de Atividades Financeiras (Siscoaf), os servidores do Coaf têm visualmente esse primeiro alerta. Outro mecanismo é o regime de alçadas e de delegação de competências (item 2 da Parte Geral do Manual da Difin e no POP 2, de 30/07/2020) para atender as regras de disseminação e segundo o qual compete exclusivamente ao Presidente do Coaf liberar RIFs que:

- i) contêm operação financeira de pessoa com foro por prerrogativa de função, no âmbito do Supremo Tribunal Federal (STF) ou do Superior Tribunal de Justiça (STJ);
- ii) destinados a Tribunais Superiores; e
- iii) destinados ao Congresso Nacional (peça 38, p. 26).

88. Assim, esse regime segrega as atividades de acordo com as funções institucionais e define os limites de responsabilidade dos cargos, em que somente o Presidente do Coaf, assessorado pelo comitê consultivo, pode encaminhar às autoridades RIFs nos quais constem pessoas com foro por prerrogativa de função no STF e STJ, destinados a Tribunais Superiores e destinados ao Congresso Nacional (para qualquer comissão ou parlamentar).

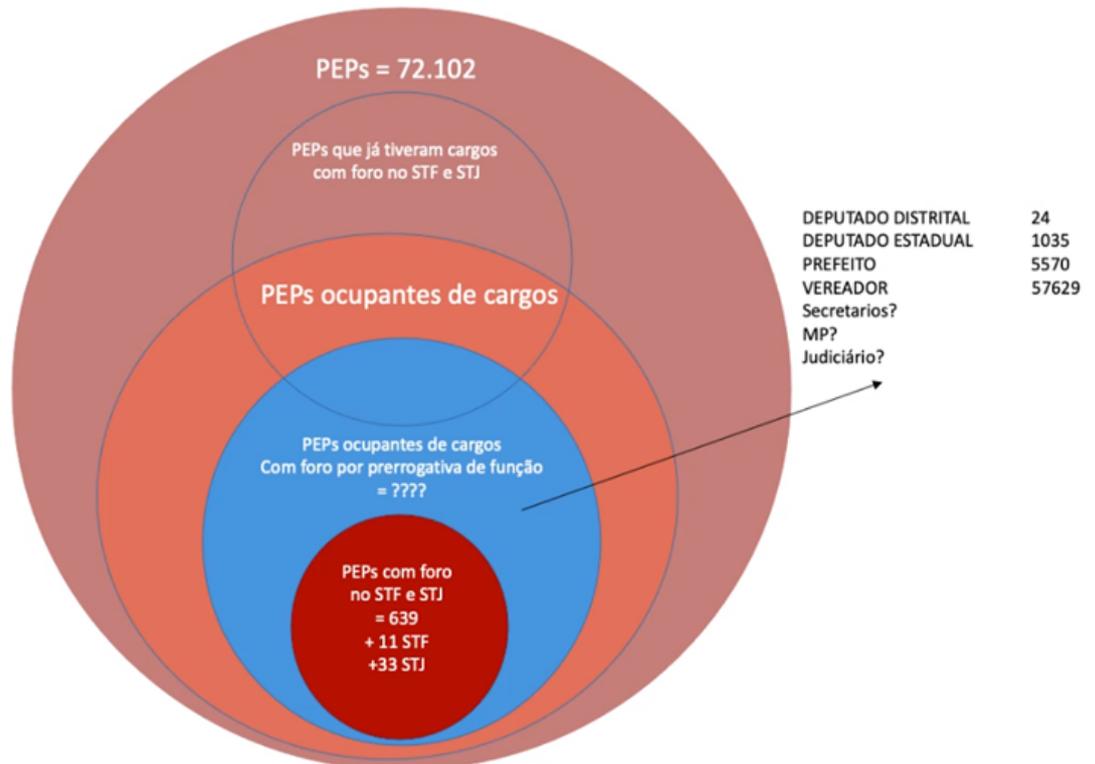
89. Além da marcação no Siscoaf e do regime de alçada, o Coaf tem os seguintes controles específicos para PEPs com foro por prerrogativa de função: bloqueio da geração automática de RIFs pelo sistema; ocultamento da identificação das PEPs no relatório e não envio das comunicações referentes ao PEP anexadas ao RIF.

90. No entanto, conforme Roteiro de Verificação (peça 58), preenchido em inspeção *in loco*, foi verificado o processo de produção do RIF 43648, que continha informações sobre PEP que já não possuía prerrogativa de foro, constatou-se que a PEP não teve marcação em vermelho no Siscoaf, nem foi submetida ao regime de alçada.

91. Desta forma, verificou-se que as PEPs sem foro por prerrogativa de função **não são submetidas** aos mesmos controles aplicados às pessoas com foro, em que pese serem consideradas pessoas expostas politicamente por até cinco anos após terem deixado o cargo.

92. Contudo, na reunião de encerramento da inspeção com o Coaf, realizada em 30/4/2021, questionada a possibilidade de estender o regime de alçadas para todas as PEPs (com ou sem prerrogativa de função), foi informado que, apesar da lista de PEP consolidada pela CGU não estar completa, ela já contempla 72.102 pessoas.

Figura 3- Universo de pessoas expostas politicamente



Fonte: ata de Reunião de Encerramento Coaf de 30/4/2021 (peça 54)

93.Com relação à força de trabalho disponível para elaboração dos RIFs, em reunião realizada no dia 22/2/2021, foi informado que há quarenta servidores na Inteligência do Coaf, dos quais apenas vinte são dedicados à análise de inteligência financeira (peça 53).

94. Considerando que a aplicação dos controles descritos para PEPs com prerrogativa bloqueia a geração automática de RIFs pelo sistema, a partir do qual o relatório precisa ser produzido manualmente por analistas, e que o regime de alçadas cria etapas adicionais que envolvem mais servidores e tempo, fica evidente a impossibilidade de aplicação do regime de alçadas a todas as mais de 70.000 PEPs (incluindo aquelas que já não tem prerrogativa de foro), haja vista limitada capacidade de análise do Coaf frente a quantidade massiva de informações recebidas acerca de PEPs que já tiveram cargos com foro no STF e STJ. Por conseguinte, não será proposta recomendação a respeito deste achado.

II.5. Risco de vazamento ou publicização dos RIF produzidos pelo Coaf por órgãos de destino

95.Inicialmente, destaca-se que não foram identificadas vulnerabilidades no processo de comunicação entre a RFB e o Coaf. A comunicação se dá exclusivamente de forma eletrônica, por meio do sistema SEI-C e somente pode ser enviada por comunicantes previamente habilitados (Nota Técnica-SEI 14/2021/COAF, peça 38, p.29). No caso do recebimento de solicitações de intercâmbio fora do SEI-C, como por e-mail ou pelos correios, as autoridades são orientadas a realizar cadastro no sistema, seguida da inserção da demanda e as respostas também se dão exclusivamente pelo sistema (peça 38, p. 36).

96.As medidas de segurança no compartilhamento das informações pelo Coaf incluem (peça 38, p. 38 e 39):

- i) acesso ao SEI-C com autenticação de dois fatores, por meio de certificação digital e código de autenticação enviado ao e-mail institucional da autoridade quando do seu acesso ao sistema;
- ii) RIF em seu *layout* final (formato pdf) disponível para visualização somente no momento do acesso pela autoridade destinatária;

iii) marca d'água inserida no corpo do RIF, individualizada de acordo com cada instituição e UF de cada uma das autoridades destinatárias;

iv) numeração individualizada do RIF para cada destinatário;

v) código *hash*, QR-Code e elementos de estenografia, que permitem a identificação, a partir do próprio documento .pdf, da autoridade, da data e hora da realização do *download* do documento, que se alteram a cada acesso ao documento, ainda que realizado pela mesma autoridade.

97. Tais mecanismos permitem ao Coaf identificar de modo célere o destinatário do RIF, caso o documento venha a ser divulgado ilegalmente (vazamento) ou publicizado indevidamente (utilização direta pela autoridade para instruir postulação em juízo).

98. A análise de comunicações e todos os atos relacionados, tais como a abertura de casos, vinculação de outras comunicações, geração, tramitação do RIF e vinculação a SEI-C são registrados na própria comunicação, na qual também fica registrado o nome do analista responsável, seguido de despacho eletrônico, no qual consta a motivação de cada ato. A identificação do analista e despacho ficam automaticamente disponíveis no módulo de visualização da comunicação para todos os usuários que acessarem posteriormente a comunicação.

99. O art. 8º, § 2º, da Lei 13.974/2020 exige que o Presidente do Coaf adote as diligências necessárias para apuração de responsabilidade dos servidores e demais pessoas que possam ter fornecido ou divulgado informações conhecidas ou obtidas em decorrência do exercício de suas funções a pessoas que não disponham de autorização legal ou judicial para acessá-las, encaminhando relatório circunstanciado à autoridade policial ou ao Ministério Público para adoção das medidas cabíveis. Conforme informado pelo Coaf, esse procedimento encontra-se disciplinado internamente naquele órgão e foi executado diante de notícias de suposta divulgação indevida de informações do RIF (peça 38, p. 39).

100. No que se refere a divulgação ilegal e/ou publicização indevida de RIFs pelas autoridades destinatárias destes, o Coaf **não** pode fazer nada além de representar às autoridades competentes que apurem eventual abuso cuja natureza pode ser enquadrada em diferentes tipos penais, como os previstos nos art. 10 e 11 da Lei Complementar 105, de 2001, e arts. 153, 299, 313-A, 313-B, 325 e 327 do Código Penal.

101. Verifica-se que, apesar de todos os controles estabelecidos pelo Coaf para rastreamento dos responsáveis pela divulgação/publicização dos RIFs, estes controles têm caráter mitigador, fato que não impede que a autoridade recebedora do RIF, ou pessoa autorizada por esta, o divulgue ilegalmente ou o torne público em procedimentos investigativos/fiscalizatórios, em processos judiciais ou mesmo na imprensa, situação que foge ao controle pelo Coaf, uma vez que os destinatários não são a ele subordinados.

102. Cabe ressaltar que a inserção direta do RIF no processo pode levar a publicização indevida do RIF não somente pela autoridade que as recebeu, mas também pela própria parte investigada como estratégia de defesa de desacreditar as instituições de inteligência e persecução penal.

103. Nesse sentido, o Coaf destacou, em reunião do dia 30/4/2021, que o RIF **não deve ser incluído em autos de processos para efeitos de instrução probatória**, pois tem caráter de mera sinalização de situação atípica, sem força probante, de acordo com a orientação firmada em precedentes da CGU e do STF e com a posição sustentada pelo Coaf quanto à interpretação extensiva do art. 11, inciso II, Lei 9.613, de 1998:

‘Art. 11. As pessoas referidas no art. 9º:

(...)

II - deverão comunicar ao Coaf, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização: (Redação dada pela Lei n. 12.683, de 2012)’

104. Tal interpretação leva em consideração o fato de que o Coaf **não é órgão de investigação**, mas de análise das comunicações, fornecidas pelas pessoas/entidades obrigadas, acerca de movimentações financeiras atípicas, cujo produto é a compilação das informações recebidas,

confrontadas com outras informações contidas na base de dados do Coaf, em **Relatório de Inteligência Financeira, para subsídio das investigações e/ou fiscalizações das autoridades competentes**. Assim, **os RIFs são meios de obtenção de prova** norteadores das investigações e/ou fiscalizações que devem ser aprofundadas para confirmar os indícios apontados nestes relatórios (peça 63, p. 11).

105. Cabe destacar que o voto do Relator, Min. Dias Toffoli, no julgamento do Recurso Extraordinário com Repercussão Geral 1055941 no Supremo Tribunal Federal, que fixou a tese da constitucionalidade do compartilhamento de RIFs com os órgãos de persecução penal para fins criminais, apresentou o estudo do Direito Comparado Espanhol, cuja lei de prevenção ao branqueamento de capitais e ao financiamento do terrorismo naquele país (Lei 10/2010) é expressa ao afirmar, em seu art. 46, que os relatórios de inteligência financeira não têm valor probatório e não podem ser juntados em processos judiciais ou administrativos: “*Artigo 46. Os relatórios de inteligência financeira não devem ter valor probatório e não podem ser incorporados diretamente em processos judiciais ou administrativos*”.

106. O referido voto condutor ressalta ainda que essa percepção está evidenciada nos relatórios disseminados pela Coaf, sendo apresentado o seguinte exemplo de informações contidas em um RIF enviado à Polícia Federal (autoridade competente), transcrito no julgamento de um *habeas corpus* no STJ:

‘1. Em decorrência das atribuições conferidas pelos artigos 14 e 15 da Lei nº 9.613/98, encaminho, em anexo, Relatório de Inteligência Financeira - RIF com informações sobre movimentações que, **embora não sejam necessariamente consideradas ilícitas, evidenciam situações de atipicidade. Essas informações de inteligência destinam-se a subsidiar investigações porventura existentes ou que venham a ser instauradas.**

2. Destaco que as informações constantes do RIF são classificadas como confidenciais, nos termos da Lei 8.159/91, ficando o destinatário responsável pela sua preservação.

3. Com o intuito de resguardar **à integridade das pessoas que, por obrigação legal, devem fornecer informações ao COAF, e do sistema brasileiro de inteligência financeira, o RIF não deve ser exposto aos relacionados, pelo que não é recomendada sua inclusão em inquéritos ou processos**. Informo, por oportuno, que expediente de igual teor foi encaminhado ao Ministério Público Federal e ao Ministério Público Estadual” (STJ. HC 191378/DF 2010/0216887-1, Relator: Ministro Sebastião Reis Júnior, Data de Julgamento: 15/09/2011 - Sexta Turma, Data de Publicação: DJe 05/12/2011 – grifos acrescentados).’

107. No âmbito da RFB, em respeito a esta regra de não disseminação das informações de inteligência produzidas pelo Coaf, a Coordenação-Geral de Pesquisa e Inteligência (Copei), responsável pelo recebimento e tratamento dos RIFs espontâneos, realiza a análise do conteúdo dos RIFs coletando somente as informações úteis para as atividades de programação e fiscalização tributária que passam a compor os relatórios de inteligências elaborados pela Copei, que, por sua vez, são encaminhados para as demais unidades da RFB (programação ou fiscalização). Portanto, não há disseminação dos RIFs entre as unidades internas da RFB, mas tão somente dos dossiês de inteligência produzidos pela Copei.

108. Obviamente que tal interpretação deve ser ponderada pela necessidade de pedido de medida cautelar e/ou medidas assecuratórias (arts. 125 a 144-A e 282, Código de Processo Penal) quando os indícios constantes do RIF apontarem para iminente prática de ato delituoso, em que não há tempo para a produção de provas robustas, exigindo-se ação urgente do órgão jurisdicional. Nestes casos, por critério de razoabilidade, não há óbice para utilização do RIF pelo órgão de persecução penal na instrução do pedido de medida cautelar.

109. A título de exemplo, o Coaf informou o caso de um prefeito investigado que fez um provisionamento para saque de três milhões de reais para comprar um helicóptero, o que provocou a elaboração de um RIF, o qual foi enviado para a autoridade competente que, por sua vez, com base no relatório de inteligência, solicitou medida acauteladora de bloqueio do saque (peça 54).

110. No entanto, mesmo nestes casos de urgência, os RIFs não perdem seu caráter meramente indiciário, posto que o exame de pedidos dessa natureza corresponde à decisão de cognição

sumária e, no curso do processo criminal, será exigida a complementação por provas das práticas delituosas.

111. Apesar de indicado expressamente no corpo do RIF o alerta para a sua não utilização em inquéritos ou processos judiciais, conforme registrado no aludido voto condutor do julgamento do RE 1055941, é comum ser encontrado em procedimentos investigativos (inquéritos policiais e procedimentos investigatórios criminais) ou processos judiciais cópias dos relatórios de inteligência que podem ser geradas pelas autoridades competentes investigativas destinatárias (Ministério Público e autoridade policial), como no caso que chegou ao conhecimento do STJ no Habeas Corpus 191378/DF, citado como exemplo.

112. Ocorre que a interpretação dada por algumas autoridades, de que o RIF se constitui elemento de prova, passível de utilização em procedimentos investigativos ou processos judiciais, fragiliza o sistema de inteligência financeira, pois expõe os agentes e entidades comunicantes, bem como os analistas de inteligência do Coaf, o que pode gerar inclusive prejuízo as investigações das autoridades competentes.

113. Em reunião com o Coaf, no dia 22/2/2021, citou-se o caso de um banco que fez a comunicação de pessoa exposta politicamente, acerca de tentativa de depósito vultoso de dinheiro (tentativas também são comunicadas), e o RIF foi incluído no procedimento investigatório, o que redundou em pedidos de identificação do autor da comunicação pelo banco. Tal situação evidencia grande exposição dos agentes comunicantes quando os RIFs são juntados como elementos probantes nos procedimentos investigatórios ou processos judiciais.

114. Portanto, é preciso estabelecer balizas claras às autoridades destinatárias dos RIFs acerca da possibilidade de sua utilização em seus procedimentos investigatórios/fiscalizatórios e/ou processos judiciais, sob pena de comprometer a eficiência do sistema brasileiro de inteligência.

115. Importante registrar que a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (Enccla) é a principal rede de articulação para o arranjo e discussões em conjunto com diversos órgãos dos Poderes Executivo, Legislativo e Judiciário, principalmente das esferas federal e estadual, bem como do Ministério Público de diferentes esferas, e para a formulação de políticas públicas e soluções voltadas ao combate àqueles crimes. O Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), vinculado à Secretaria Nacional de Justiça do Ministério da Justiça e Segurança Pública, por intermédio da Coordenação-Geral de Articulação Institucional, é a secretaria-executiva da Enccla (<http://enccla.camara.leg.br/quem-somos>, acesso em 20/5/2021).

116. O trabalho da Enccla é realizado por meio de ações elaboradas e pactuadas anualmente pelos seus membros. Para cada ação, é criado grupo de trabalho composto por vários órgãos e instituições, que se reúne mensalmente e realiza diversas atividades como: estudos e diagnósticos legais-normativos e de composição de bancos de dados; elaboração de propostas legislativas; averiguação do estado da arte de sistemas de cadastros; questionamento da necessidades de promover soluções em TI; busca de eficiência na geração de estatísticas; e eventos voltados à evolução dos temas por meio de debates (<http://enccla.camara.leg.br/quem-somos>, acesso em 20/5/2021).

117. Considerando que a divergência de interpretação dada ao art. 11, inciso II, da Lei 9613/1998 fragiliza o sistema de inteligência financeira, cabe, com fundamento no art. 11 da Resolução-TCU 315/2020, recomendar ao Coaf e à Secretaria Nacional de Justiça e Cidadania, por meio de seu Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), que, na condição de Secretaria-executiva da Enccla, suscitem, naquele foro, debate voltado a consolidar orientação técnica às autoridades competentes, destinatárias dos Relatórios de Inteligência Financeira (RIFs), no sentido que esses relatórios não sejam incluídos em autos de processos para efeitos de instrução probatória, por terem caráter de mera sinalização de situação atípica, sem força probante, de acordo com a orientação firmada em precedentes da CGU e do STF e com a adequada interpretação extensiva do art. 11, inciso II, Lei 9.613/1998, a fim de proteger a integridade das pessoas que, por obrigação legal, devem fornecer informações ao Coaf, bem como a efetividade do sistema de PLD/FT.

II.6. Baixo aproveitamento dos RIFs pela RFB

118. Na reunião realizada com a RFB em 31/3/21 (peça 57), foi informado que os Relatórios de Inteligência Financeira encaminhados espontaneamente pelo Coaf agregam pouco valor à atividade de inteligência e programação de fiscalizações do órgão.

119. Até 2019, a Coordenação-Geral de Pesquisa e Investigação (Copei) realizava análises individuais dos RIFs recebidos e tais análises, apesar de consumirem recursos humanos, agregavam pouco valor aos relatórios de inteligência da coordenação. Com isso, os RIFs eram pouco aproveitados pelo setor de programação de fiscalizações (peça 57, p.3-4).

120. Em virtude do baixo aproveitamento, a RFB decidiu modificar, em 2020, a forma de análise dos relatórios. No momento atual, está sendo definida uma estratégia para tratamento dos dados recebidos, que possibilite fazer cruzamentos automatizados dos dados constantes em conjuntos de RIFs recebidos, para posterior desenvolvimento de ferramenta (estratégia contrária à análise individualizada que era realizada até 2019).

121. Para verificar o tratamento e utilização dos RIFs pela RFB, foi solicitada uma extração de relação de PEPs que tiveram ações fiscais instauradas e concluídas entre os anos de 2015 e 2020. A listagem recebida (peça 61) continha 211 procedimentos fiscais instaurados e concluídos nos últimos cinco anos, referentes a 173 pessoas distintas. A seguir, foi solicitado à RFB a aplicação de um filtro para verificar quais destes PEPs também foram objeto de RIFs encaminhado pelo Coaf. A listagem seguinte (peça 62) resultou em apenas 26 PEPs. Dessa listagem, foi selecionado um PEP para verificação do procedimento fiscal instaurado na RFB, assim como para a verificação do processo de produção dos RIFs pelo Coaf.

122. Nesse caso, verificou-se que o PEP selecionado (peças 58 e 59) teve uma ação fiscal iniciada pela RFB em 07/12/2014 e distribuída para execução em 16/3/2015, no âmbito de um programa especial para fiscalizar os contribuintes envolvidos na operação Lava a Jato. Já o RIF 43648 do Coaf, sobre essa mesma pessoa, foi elaborado em 2016, ou seja, posterior à ação de fiscalização pela RFB, e com isso não foi aproveitado pela RFB.

123. Foi verificado que o encaminhamento de RIFs pelo Coaf sofre algumas restrições. Na visita técnica ao Coaf, constatou-se que, quando o PEP tem prerrogativa de função, o RIF normalmente só pode ser encaminhado para o Procurador-Geral da República, para que ele tome as providências que julgar necessário. Na reunião de encerramento da inspeção com o Coaf, em 30/4/2021, foi complementado que, se houver indícios de ilícitos tributários o RIF poderá ser enviado para RFB, ainda que uma das pessoas reportadas tenha foro por prerrogativa de função (é o denominado “encaminhamento concorrente” previsto no Manual da Difin (peça 38, p.25).

124. Segundo o Coaf, o “encaminhamento concorrente depende da clara identificação de indícios de sonegação e outros crimes tributários no teor das comunicações analisadas. Em geral comunicações com esse tipo de suspeição reportam apenas a incompatibilidade entre renda/patrimônio/faturamento cadastrado(a) com a movimentação financeira apresentada. Também é comum ser reportada a utilização da conta dos sócios para a movimentação financeira de suas empresas. Todavia, nesses dois tipos de situações mais recorrentes de suspeição de crimes tributários, a RFB já possui, por meio do recebimento da e-financeira, as informações necessárias para identificar autonomamente as suspeições nas movimentações, não havendo a dependência de informações enviadas pelo Coaf. Acrescentou ainda que, entre outras situações corriqueiramente reportadas, os setores obrigados identificam indícios de desvio de recursos públicos, mas que não necessariamente estariam associados também a suspeições de sonegação fiscal” (peça 81, p. 1-2).

125. Nessas verificações *in loco*, constatou-se, ademais, que o intercâmbio de informações entre os dois órgãos foi restrito ao encaminhamento de RIFs (solicitados ou espontâneos) pelo Coaf e à solicitação de RIFs por auditores da RFB, quando já existia procedimento fiscal instaurado.

126. Importante destacar que o Grupo de Ação Financeira contra a Lavagem de Dinheiro e o financiamento do Terrorismo (Gafi) estabelece que um sistema de inteligência financeira efetivo é o que as autoridades competentes têm acesso tempestivo a informações de inteligência financeira e outras informações relevantes e elas são utilizadas adequadamente nas investigações de lavagem de

dinheiro e financiamento do terrorismo. Em outras palavras, “as autoridades competentes têm os recursos e as habilidades para usar as informações de modo a conduzir suas análises e investigações financeiras, identificar e rastrear os bens, e desenvolver análises operacionais”.

127. Nesse sentido é que foi firmado o ‘Resultado Imediato 6 da Avaliação de Efetividade’, constante da Metodologia do Gafi, que estabelece o padrão internacional antilavagem de dinheiro e contra o financiamento do terrorismo (disponível em <https://www.gov.br/fazenda/pt-br/centrais-de-conteudos/publicacoes/livros/arquivos/as-recomendacoes-do-gafi.pdf>, p. 295. Acesso em 10/6/2021).

128. Segundo o Gafi, as seguintes questões centrais devem ser consideradas para determinar se o sistema de inteligência financeira de cada país membro está alcançando o resultado esperado:

‘6.1 Até que ponto a inteligência financeira e outras informações relevantes são acessadas e usadas em investigações para desenvolver provas e rastrear produtos do crime relacionados a lavagem de dinheiro, crimes antecedentes a ela associados e financiamento do terrorismo?’

6.2 Até que ponto as autoridades competentes estão recebendo ou solicitando relatórios (por exemplo, comunicações de operações suspeitas, comunicações sobre numerário e instrumentos negociáveis ao portador) que contenham informações relevantes e exatas que as assistam no desempenho de suas funções?

6.3 Até que ponto a análise e a disseminação da Unidade de Inteligência Financeira apoiam as necessidades operacionais das autoridades competentes?’

(Resultado imediato 6 da Avaliação de Efetividade do Gafi – disponível em <https://www.gov.br/fazenda/pt-br/centrais-de-conteudos/publicacoes/livros/arquivos/as-recomendacoes-do-gafi.pdf>, p. 296. Acesso em 10/6/2021).

129. Portanto, a situação verificada na RFB demonstra que, para melhorar a efetividade do sistema de inteligência financeira brasileiro, é necessário melhorar o tratamento dado aos RIFs encaminhados pelo Coaf, assim como alargar o compartilhamento de informações custodiadas por ambos os órgãos, de modo a dar efetividade aos trabalhos de inteligência financeira na ceara de combate a ilícitos tributários, em consonância com o Resultado Imediato 6 da Avaliação da Efetividade do Gafi.

130. Assim, propõe-se:

i) recomendar à RFB, com fundamento no art. 11 da Resolução-TCU 315, de 2020, que continue com os esforços para estabelecer os cruzamentos na base de dados de RIFs de geração espontânea encaminhados pelo Coaf para agregar valor à programação de ações fiscais;

ii) recomendar à RFB e ao Coaf, com fundamento no art. 11 da Resolução-TCU 315/2020, que estudem medidas que possibilitem um maior compartilhamento de informações entre os dois órgãos, para melhor subsidiar os trabalhos de inteligência financeira e combate à ilícitos tributários por ambos, em atenção ao Resultado Imediato 6, item 6.2 da Avaliação da Efetividade, constante das recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o financiamento do Terrorismo (Gafi).

III. Análise dos comentários dos gestores

131. Após encaminhamento do relatório preliminar de fiscalização aos destinatários das deliberações contidas no relatório, foram recebidos comentários do Conselho de Controle de Atividade Financeira e da Controladoria-Geral da União.

132. Em relação ao Coaf, não houve discordância entre o teor do relatório e os comentários, que versavam, em sua maioria, sobre ajustes pontuais nos textos, a fim de conferir maior clareza e objetividade ao relatório. Nesse sentido, foram realizados pequenos ajustes ao longo do texto, aos títulos dos achados III.2 e III.4, e às propostas de encaminhamento dos achados III.5 e III.6.

133. Quanto à CGU, os esclarecimentos e sugestões apresentadas resultaram na inclusão dos parágrafos 63 a 66 no relatório e no ajuste da proposta de encaminhamento do achado III.2.

134. A análise detalhada dos comentários consta na peça 82.

IV. Análise dos comentários do Ministério Público junto ao TCU

135. Conforme despacho da peça 85, o ministro relator Bruno Dantas determinou à SecexTributária a análise das contribuições do subprocurador-geral do MPTCU ao relatório preliminar da fiscalização, consignadas à peça 84.

136. Em sua manifestação, o MPTCU concorda com as análises e propostas contidas no relatório preliminar e, adicionalmente, traz uma abordagem sobre repercussões penais do acesso indevido a informações e bases de dados dos órgãos objeto desta representação, propondo novos encaminhamentos.

137. Cita dispositivos introduzidos pela Lei 9.983/2000 no Código Penal (CP), tendentes a penalizar a conduta de acesso indevido a bases de dados criadas e mantidas pelo Estado: art. 313-A, crime de inserção de dados falsos em sistema de informações; art. 313-B, crime de modificação ou alteração não autorizada de sistema de informações; art. 325, crime de violação de sigilo profissional, cujos §§ 1º e 2º dizem respeito a quaisquer formas de acesso indevido a bases de dados (inserções, alterações, exclusões ou consultas); art. 153, crime de divulgação de segredo, cujos §§ 1º-A e 2º se prestam a coibir a divulgação indevida de dados sigilosos mantidos em bases de dados mantidas pelo Estado. Menciona, ainda, o art. 154-A do CP, referente ao crime de invasão de dispositivo informático.

138. Em vista da legislação criminal tendente a coibir acessos indevidos a bases de dados informatizadas estatais, o MPTCU propõe (peça 84, p. 4-5):

a. determinação para que as ocorrências de acesso indevido àquelas bases sejam tratadas não apenas na instância administrativa, mas também, quando for o caso, levadas a conhecimento do Ministério Público, para fins de persecução penal;

b. recomendação para adoção de medidas de salvaguarda do sigilo de informações sigilosas extraídas das bases da RFB quando essas informações são enviadas aos em cumprimento a disposições legais ou a ordens de autoridades competentes para tanto, identificando-se, nessas transferências, a pessoa física destinatária das informações sigilosas e que essa pessoa, antes de ter acesso às informações que lhe estão sendo transmitidas, assumo formalmente, mediante certificação digital, o compromisso de zelar pelo sigilo e de se responsabilizar pelo uso da informação recebida. Essa proposta é feita com respaldo na Constituição (artigo 5º, inciso X) e nas diversas normas infraconstitucionais que cuidam da matéria, a exemplo da Lei 12.527, de 18/11/2011 (Lei de Acesso à Informação), da Lei 13.709, de 14/8/2018 (Lei Geral de Proteção de Dados Pessoais) e do Decreto 9.637, de 26/12/2018, que trata da Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da Administração Pública federal;

c. o exame da possibilidade de se incluir, pelo Tribunal, nas normas voltadas à organização dos processos de contas anuais de órgãos e entidades integrantes da Administração Pública federal, a exigência de que sejam informadas as ocorrências de acessos indevidos às bases de dados informatizadas mantidas sob suas responsabilidades, bem como as providências tomadas para fins de apuração administrativa daquelas ocorrências e para fins de persecução penal, se for o caso.

139. Em apertada síntese, repisa-se que a representação inicial tratou de provocar este Tribunal a fim de que se apurasse a ocorrência de acesso indevido a dados relativos a pessoas politicamente expostas mantidos em bases da RFB e do Coaf, avaliando os controles desenhados para a preservação do sigilo destes dados, seja de maneira interna a cada órgão ou no intercâmbio específico entre estes dois órgãos (RFB e Coaf) (peça 1), que contou com a concordância do ministro relator, conforme despacho à peça 8.

140. Quanto à proposta constante na alínea “a” do parágrafo 138, a equipe concorda que seria interessante que as ocorrências de acesso indevido fossem levadas ao conhecimento do Ministério Público, para fins de persecução penal. Porém, conforme visto acima, a verificação do envio de notícia crime ao respectivo órgão de persecução penal para apuração da ocorrência de crimes

conexos ao acesso indevido às bases de dados estatais não foi objeto de análise na presente inspeção, e com isso, determinação à RFB nesse sentido, além de não constar do escopo desta fiscalização, não foi discutida com o gestor, tampouco constou do relatório preliminar que foi encaminhado aos gestores para manifestação.

141. De igual forma, a proposta constante na alínea “b”, que aborda o risco de vazamento de informações da RFB, quando essas informações são enviadas aos destinatários em cumprimento a disposições legais ou a ordens de autoridades competentes, que podem ser dos mais diversos (Polícia Federal, Justiça Federal, Ministérios Públicos etc.) extrapola a abrangência do escopo da presente inspeção, uma vez que foi objeto de análise o fluxo das informações exclusivamente entre RFB e Coaf. Embora a equipe concorde com a proposta do Ministério Público, tal análise não foi realizada ao longo da inspeção, discutida com o gestor ou apresentada no relatório preliminar.

142. Cabe ressaltar que esta modalidade de fiscalização tem escopo restrito, utilizada para suprir lacunas de informações do processo a que se vincula conforme dispõe o art. 240 do RITCU.

143. A Portaria-Segecex 29/2010, que disciplina a realização de inspeções, em seu art. 2º, deixa claro o seu escopo restrito e a necessidade de ser apresentada nova proposta de fiscalização para tratar de matérias extrapolem o escopo da ação de controle:

‘Art. 2º A inspeção é planejada e executada no âmbito de processo de controle externo pré-existente e vincula-se à ação de controle objeto do referido processo.

§ 1º O escopo da inspeção limita-se ao da ação de controle à qual ela se vincula.

§ 2º O titular da unidade técnica avaliará a conveniência e a oportunidade de apresentar proposta de realização de auditoria quando houver indícios de irregularidades cuja apuração extrapole o escopo da ação de controle.

§ 3ª A portaria de fiscalização referente à inspeção poderá deixar de contemplar prazo para a fase de relatório nas situações em que o relato dos fatos investigados e apurados coincidir com a própria instrução do processo.’

144. Assim, com fundamento no art. 2º da Portaria-Segecex 29/2010, entende-se que, na presente inspeção, não devem ser acolhidos os encaminhamentos adicionais propostos pelo MPTCU, referidos nas alíneas “a” e “b” do parágrafo 138 deste relatório, uma vez que tais apurações não foram mencionadas na representação inicial ou no despacho do ministro relator que determinou a ação de controle, e com isso, extrapolaram o escopo previamente fixado.

145. Todavia, considerando a relevância das sugestões dos encaminhamentos propostos pelo MPTCU e com fundamento no art. 14 da Resolução-TCU 315/2020, propõe-se, adicionalmente, que seja realizada diligência à RFB, para que, no prazo de quinze dias, os gestores apresentem informações quanto às consequências práticas da implementação das medidas aventadas nas alíneas “a” e “b” do parágrafo 138 do presente relatório (ou eventuais alternativas), incluindo na diligência a peça 84 do presente processo, que contém as considerações do subprocurador-geral do MPTCU, a fim de subsidiar as manifestações a serem apresentadas.

146. Quanto à proposta de inclusão nas normas de contas de informação sobre ocorrências de acessos indevidos às bases de dados (alínea “c”), também não pode ser acolhida pela equipe de inspeção, por considerá-la incompatível com novo modelo de processo de contas inaugurado pela IN-TCU 84/2020, pautado nos princípios da racionalização e da simplificação, e que tem como base a auditoria financeira integrada com conformidade para o exame da regularidade da gestão.

V. Conclusão

147. Em relação à ocorrência de acessos indevidos a dados de PEPs no Coaf e na RFB, restou constatada a ocorrência de acesso indevido aos dados fiscais de pessoas expostas politicamente (PEP) na RFB (parágrafos 46 a 52). Com efeito, os sistemas da RFB são sujeitos a registros de eventos (*logs*) que permitem identificar, acompanhar e recuperar evidências nos casos de suspeita de violação de normas e em incidentes de segurança. Em certos casos, a recuperação dos *logs* de acesso depende de apuração especial pelo Serpro (com custos). No período de 2018 a 2020, a RFB

detectou oito acessos indevidos aos dados de contribuintes nas bases do órgão, sendo seis desses acessos relativos a PEPs. A RFB informou que foram instaurados processos administrativos para todos os casos, sendo que quatro ainda estão em andamento. Nos quatro casos concluídos, houve responsabilização dos servidores que efetuaram os acessos indevidos e aplicadas penalidades de suspensão. Assim, cabe deixar de determinar à RFB a adoção de medidas para essas finalidades.

148. No que tange aos ritos, procedimentos e sistemas de controle, constatou-se: necessidade de ampliar a abrangência da base de dados de PEPs mantida pela CGU para contemplar autoridades do Poder Judiciário e do Ministério Público (parágrafos 53 a 67); fragilidades nos controles estabelecidos pela RFB para salvaguardar acessos indevidos a dados de PEPs pelo Sistema Midas (parágrafos 68 a 79); e mecanismos de controle do Coaf reservados a PEPs com prerrogativa de foro (parágrafos 80 a 94).

149. Os principais mecanismos implementados tanto pela RFB quanto pelo Coaf para preservar os dados de PEPs têm como uma relevante fonte de informação a base de dados de pessoas expostas politicamente disponibilizado pelo governo federal, mantida pela Controladoria-Geral da União (CGU). Ocorre que esse cadastro **não inclui** membros do Judiciário ou do Ministério Público, o que acaba por onerar o funcionamento dos referidos mecanismos e controles implementados pelos órgãos para salvaguardá-los. De igual forma, impede que seja lida a atenção requerida pelo Convenção das Nações Unidas contra a Corrupção (art. 52, itens 1 e 2, alínea “a”), promulgada pelo Decreto 5.687/2006.

150. Ressalta-se que a obrigatoriedade de incluir os membros do Poder Judiciário e do Ministério Público no cadastro da CGU só pode ocorrer por força de lei, por isso não há que se falar em irregularidade pela ausência da inclusão dessas PEPs no referido cadastro. Assim, a proposta de encaminhamento contempla dar conhecimento à CGU, ao CNJ e ao CNMP do teor do relatório, no intuito de possibilitar aos órgãos conhecer os riscos identificados pelo TCU, a fim de possibilitar a otimização dos processos de elaboração e consolidação do cadastro.

151. O sistema Alerta-Gestor da RFB, com base no cadastro de PEPs da CGU, envia mensagens para o superior hierárquico e seu adjunto sempre que dados de declaração de imposto de renda de pessoa física referentes a PEPs são acessados por meio do sistema Midas e tem por objetivo possibilitar a detecção dos acessos indevidos. Contudo, por se tratar de controle *a posteriori* e não prévio, o sistema não impede a ocorrência do acesso indevido. Por outro lado, a implementação de travas automáticas para acesso ao sistema Midas foi considerada impraticável, pois isso iria afetar outros processos de trabalho da RFB. Como o sistema Alerta ainda está em desenvolvimento, há espaço para aperfeiçoamento dos controles *a posteriori*.

152. Em relação ao tratamento dos dados de PEPs com prerrogativa de foro pelo Coaf, constatou-se que são sujeitos a mecanismos mais rigorosos que aqueles aplicados aos PEPs que deixaram suas funções até cinco anos, apesar destes também serem considerados politicamente expostos, ainda que não possuam mais prerrogativa de função (parágrafos 80 a 94).

153. Com relação ao processo de comunicação entre a RFB e o Coaf, detectou-se risco de vazamento ou publicização dos Relatórios de Inteligência Financeira (RIF) produzidos pelo Coaf por órgãos de destino (parágrafos 95 a 117) e baixo aproveitamento dos RIFs pela RFB (parágrafos 118 a 130).

154. Cabe destacar que não foi possível detectar vulnerabilidades no processo de comunicação entre a RFB e o Coaf, haja vista toda a comunicação ser feita pelo Sistema de Intercâmbio de Informações do Coaf (SEI-C) e, conforme detalhado no relatório, existem controles para inibir, coibir e punir eventuais abusos (parágrafos 95 a 98). Quanto ao tratamento dos RIFs, foi constatada uma boa prática na RFB: os RIFs são utilizados apenas como insumos para produzir relatórios de inteligência da Coordenação-Geral de Pesquisa e Investigação (Copei) e estes últimos relatórios é que são disseminados internamente, e não os documentos originais do Coaf (parágrafo 107).

155. Todavia, em relação às demais autoridades competentes, constatou-se “Risco de vazamento ou publicização dos RIF produzidos pelo Coaf por órgãos de destino”. Apesar de todos os controles estabelecidos pelo Coaf para rastreamento dos responsáveis pela divulgação/publicização dos RIFs, os

órgãos destinatários têm interpretação distinta do Coaf sobre o sigilo dos relatórios estabelecido pelo art. 11, inciso II, da Lei 9.613/1998.

156. Finalmente, a análise do processo de comunicação entre a RFB e o Coaf resultou na constatação “Baixo aproveitamento dos RIFs pela RFB” (parágrafos 118 a 130). Verificou-se que as análises individuais que eram realizadas no RIFs recebidos pela Copei (até 2019) agregavam pouco valor aos relatórios de inteligência, e, por isso, a própria RFB está estudando uma forma de tornar as análises de RIFs mais efetivas.

157. Entre os benefícios estimados desta fiscalização, destaca-se o incremento da economia, eficiência, eficácia ou efetividade de órgão ou entidade da administração, por meio do aperfeiçoamento dos controles desenhados para preservar os dados de pessoas expostas politicamente, além de outros benefícios diretos, como o fornecimento de subsídios para elaboração da relação de PEPs pela Controladoria-Geral da União, em conjunto com o Conselho Nacional de Justiça e o Conselho Nacional do Ministério Público.

158. As principais propostas do relatório constituem-se na realização de recomendações para aprimoramento das situações apontadas nos achados.

VI. Proposta de encaminhamento

159. Ante todo o exposto, considerando as análises efetuadas na presente inspeção, submetem-se os autos à consideração superior, sugerindo o seu encaminhamento ao gabinete do Ministro Bruno Dantas, nos termos do art. 157 do RITCU, com as seguintes propostas:

a) conhecer da presente representação, satisfeitos os requisitos de admissibilidade previstos nos arts. 235 e 237, inciso VII, do Regimento Interno deste Tribunal c/c art. 103, § 1º, da Resolução TCU 259/2014, para, no mérito, considerá-la procedente;

b) recomendar à Secretaria Especial da Receita Federal do Brasil (RFB), com fundamento no art. 11 da Resolução-TCU 315/2020, que:

b.1) aprimore e refine o campo de “justificativa” que deve ser preenchido para acessar o sistema Midas e a base de declarações de imposto de renda de pessoas físicas (DIRPF), para facilitar a detecção de desvios pela supervisão quando do recebimento de alertas referentes a pessoas expostas politicamente por meio do sistema Alerta-Gestor;

b.2) avalie a oportunidade e conveniência de incluir ferramentas gerenciais no sistema Alerta-Gestor, que permitam avaliar efetivamente as ações tomadas pelos supervisores depois de recebidos os alertas, de modo garantir uma supervisão efetiva sobre os acessos à base de declarações de imposto de renda de pessoas físicas (DIRPF) de pessoas expostas politicamente;

b.3) continue com os esforços para estabelecer os cruzamentos na base de dados de Relatórios de Inteligência Financeira (RIFs) de geração espontânea encaminhados pelo Coaf para agregar valor à programação de ações fiscais;

c) recomendar à Secretaria Especial da Receita Federal do Brasil (RFB) e ao Conselho de Controle de Atividades Financeiras (Coaf), com fundamento no art. 11 da Resolução-TCU 315/2020, que estudem medidas que possibilitem um maior compartilhamento de informações entre os dois órgãos, para melhor subsidiar os trabalhos de inteligência financeira e combate à ilícitos tributários por ambos, em atenção ao Resultado Imediato 6, item 6.2 da Avaliação da Efetividade, constante das recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o financiamento do Terrorismo (Gafí);

d) recomendar, com fundamento no art. 11 da Resolução-TCU 315/2020, ao Conselho de Controle de Atividades Financeiras e à Secretaria Nacional de Justiça e Cidadania, por meio de seu Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), que, na condição de secretaria-executiva da Enccla, suscitem, naquele foro, debate voltado a consolidar orientação técnica às autoridades competentes, destinatárias dos Relatórios de Inteligência Financeira (RIFs), no sentido de que esses relatórios não sejam incluídos em autos de processos para efeitos de instrução probatória, por terem caráter de mera sinalização de situação atípica, sem força probante,

de acordo com a orientação firmada em precedentes da CGU e do STF e com a adequada interpretação extensiva do art. 11, inciso II, Lei 9.613/1998, a fim de proteger a integridade das pessoas que, por obrigação legal, devem fornecer informações ao Coaf, bem como a efetividade do sistema de PLD/FT.

e) encaminhar o acórdão que vier a ser proferido à Secretaria Especial da Receita Federal do Brasil, ao Conselho de Controle de Atividades Financeiras, à Secretaria Nacional de Justiça e Cidadania, à Controladoria-Geral da União, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público, destacando que o relatório e o voto que fundamentam a deliberação encaminhada podem ser acessados por meio do endereço eletrônico www.tcu.gov.br/acordaos e que, caso tenham interesse, o Tribunal pode encaminhar-lhes cópia desses documentos sem quaisquer custos;

f) nos termos do art. 8º da Resolução-TCU 315/2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do relator ao colegiado no sentido de monitorar as deliberações propostas nos itens “b” a “d”;

g) considerando as contribuições do MPTCU à peça 84, realizar diligência junto à Secretaria Especial da Receita Federal do Brasil (RFB), com fundamento no art. 14 da Resolução-TCU 315/2020, para que os gestores apresentem informações quanto às consequências práticas da implementação das medidas aventadas itens "a" e "b" do parágrafo 138 deste relatório, enviando-se cópia da peça 84 do presente processo, a fim de subsidiar as manifestações a serem apresentadas, restituindo os autos à SecexTributária para realizar as devidas análises.”

2. Tendo em vista os ajustes de escopo e abrangência ocorridos na fiscalização após a representação inicial, determinei o envio dos autos ao autor da representação, o Subprocurador-geral Lucas Rocha Furtado, para que se manifestasse sobre o relatório e os encaminhamentos preliminares sugeridos e eventualmente indicasse linhas complementares a serem examinadas (peça 83).

3. Sobreveio então parecer com ponderações baseadas no relatório de fiscalização ainda preliminar, isto é, antes da manifestação dos gestores (peça 66). Na ocasião, foram sugeridas novas propostas em relação à primeira análise da unidade instrutora (peça 84):

a) determinar aos órgãos e entidades que administram as bases de dados objeto deste trabalho para que adotem as providências necessárias para que as ocorrências de acesso indevido às informações constantes dessas bases sejam levadas ao conhecimento do Ministério Público, para fins de persecução penal;

b) recomendar a adoção de medidas de salvaguarda da confidencialidade de informações sigilosas extraídas das bases da RFB quando essas são enviadas a outros destinatários por imposição legal, tal como a identificação do destinatário e a assunção de compromisso de zelar pelo sigilo, estabelecendo uma trilha rastreável do compartilhamento desses dados.

4. A SecexTributária, conquanto tenha concordado com o teor das medidas, registrou que não haviam sido submetidas a considerações pelos gestores dos órgãos eventualmente atingidos pelas propostas. Diante do quadro, determinei a realização de diligência à Secretaria Especial da Receita Federal do Brasil (RFB) e ao Conselho de Controle de Atividade Financeira (Coaf) para que se manifestassem quanto às consequências práticas acerca das propostas, bem como eventuais alternativas a essas medidas (despacho de peça 98).

5. Em atendimento e após as manifestações pertinentes dos órgãos jurisdicionados, a unidade instrutora se manifestou pela manutenção da proposta de encaminhamento originária contida no relatório de fiscalização de peça 93, *in verbis* (peças 114-116):

“Em atenção ao Despacho do Ministro Relator Bruno Dantas (peça 98), vem para análise os comentários do Conselho Nacional de Justiça (CNJ), acostados aos autos após a conclusão do relatório de fiscalização (peças 96-97), bem como do Conselho de Controle de Atividades Financeiras (Coaf) (peças 103-107) e da Secretaria Especial da Receita Federal do Brasil (RFB)

(peças 108-111), acerca das consequências práticas das propostas de determinações formuladas pelo Subprocurador-Geral Lucas Rocha Furtado (peça 84), bem como eventuais alternativas a essas medidas.

2. Ao serem notificados mediante Ofícios 6128/2021-TCU/Seproc e 6129/2021-TCU/Seproc (peças 99-100), com ciência em 29/10/2021 (peças 101-102), o Coaf e a RFB encaminharam os seus comentários (peças 103-107 e 108-111, respectivamente), os quais serão tratados no item II desta instrução, logo após a análise da manifestação do CNJ (peças 96-97) sobre o achado III.2 do relatório preliminar de fiscalização (peça 66).

I. CNJ sobre o achado III.2 - Utilização pela RFB e pelo Coaf de relação de PEPs que não resguarda o sigilo dos dados dos membros do Poder Judiciário e do Ministério Público

3. Em relatório preliminar, a equipe de auditoria identificou risco de que eventuais acessos indevidos aos dados de membros do Poder Judiciário e do Ministério Público não fossem detectados e coibidos pela RFB e pelo Coaf, uma vez que os mecanismos específicos de resguardo e tratamento dos dados destas pessoas são baseados na lista de PEPs, administrada pela CGU, e, por sua vez, os aludidos membros não estão contemplados nesta listagem (peça 66, p. 12-14).

4. Diante do achado III.2, foi proposto inicialmente a seguinte determinação:

b) determinar à Controladoria-Geral da União (CGU), como órgão responsável pela manutenção da relação de pessoas expostas politicamente (PEPs), com fundamento no art. 4º da Resolução-TCU 315, que, em conjunto com o Conselho Nacional de Justiça (CNJ) e o Conselho Nacional do Ministério Público (CNMP), no prazo de 180 dias, implementem mecanismos para que a relação de PEPs passe a incluir os membros do Poder Judiciário e do Ministério Público, de modo a dar cumprimento ao art. 52, item 2, alínea “a”, da Convenção das Nações Unidas contra a Corrupção, promulgada por meio do Decreto 5.687/2006; (peça 66, p. 25)

5. Por meio do Despacho SEI/CNJ-11145402 (peça 97), o CNJ se manifestou acerca da citada proposição informando, em síntese:

a) o banco de dados do CNJ não alcança os membros do Supremo Tribunal Federal (STF) nem os membros do Conselho Superior da Justiça do Trabalho (CSJT) e do Conselho da Justiça Federal (CJF);

b) inexistente normativo no âmbito do Poder Judiciário que indique quem são Pessoas Expostas Politicamente (PEPs) daquele poder;

c) nem a Lei 9.613/98, nem os Decretos 5.640/2005 e 5.687/2006, que recepcionaram no Brasil as convenções internacionais contra o terrorismo e a corrupção, têm previsão sobre o conceito de pessoa politicamente exposta;

d) a Circular 3.461/2009 do Banco Central do Brasil (Bacen), no que se refere aos órgãos do Poder Judiciário, considera PEPs somente os membros do CNJ, do STF e dos Tribunais Superiores;

e) a Resolução 29/2017 do Coaf informa que são PEPs os membros do STF, dos Tribunais Superiores e dos Tribunais Regionais Federais, do Trabalho e Eleitorais, relativamente ao Poder Judiciário;

f) tanto a Resolução Coaf quanto a Circular Bacen extrapolam as limitações legais ao definirem as PEPs;

g) o TCU não tem competência para tecer a referida determinação.

6. Verifica-se que os comentários do CNJ se coadunam com os comentários apresentados pela Controladoria-Geral da União (CGU), no sentido de que a obrigatoriedade de inclusão dos membros do Poder Judiciário e do Ministério Público no cadastro de PEPs, para torná-lo mais abrangente, somente pode ocorrer por meio de lei, de modo que não caberia determinação à CGU neste sentido, sendo sugerido, alternativamente, que fosse dado conhecimento do teor do relatório, no intuito de possibilitar-lhe conhecer os riscos identificados por este Tribunal em relação à

abrangência do atual cadastro de PEPs, a fim de possibilitar a otimização dos seus processos internos (Análise dos Comentários dos Gestores - peça 82, parágrafos 14 a 20).

7. Anuindo com tais comentários, a equipe de auditoria excluiu a referida proposta de determinação e propôs, alternativamente, dar conhecimento à CGU, ao CNJ e ao CNMP do teor do relatório, no intuito de possibilitar aos órgãos conhecer os riscos identificados pelo TCU em relação à abrangência do atual cadastro de pessoas expostas politicamente e suas consequências nos mecanismos desenhados pela RFB e pelo Coaf para resguardar os dados dessas pessoas, possibilitando ainda a otimização dos processos de elaboração e consolidação do cadastros (peça 93, parágrafo 67).

8. Assim, os comentários ofertados pelo CNJ somente corroboram com a análise já realizada, não repercutindo nas propostas constantes do relatório final de fiscalização (peça 93, parágrafo 139, item “e”).

II. Coaf e RFB sobre as propostas adicionais feitas pelo MPTCU

9. Em sua manifestação (peça 84), o MPTCU concorda com as análises e propostas contidas no relatório preliminar e, adicionalmente, traz uma abordagem sobre repercussões penais do acesso indevido às informações e bases de dados dos órgãos fiscalizados nesta representação, propondo novos encaminhamentos. Tais propostas foram objeto de comentários do Coaf e da RFB, que serão examinados nos subitens subsequentes.

II. 1. Determinação aos órgãos e entidades que administram as bases de dados objeto deste trabalho para que adotem as providências necessárias para que as ocorrências de acesso indevido às informações constantes dessas bases sejam levadas ao conhecimento do Ministério Público, para fins de persecução penal.

Comentários

10. Em relação a essa determinação, o Coaf, mediante Nota Técnica-SEI 71/2021/COAF, informa que já existem disposições legais no mesmo sentido, a exemplo do art. 66 da Lei de Contravenções Penais, art. 116, XII, da Lei 8.112/1990, e art. 8º, inciso IV e §2º, da Lei 13.974/2020 (peça 104, p. 2).

11. O Coaf encaminha, ainda, por meio do Despacho Coaf 17179379, fluxogramas dos procedimentos que vinham sendo adotados em face de denúncias, inclusive em decorrência de acessos indevidos às informações constantes das bases de dados custodiadas pelo órgão de inteligência financeira (peças 104, p. 2; peças 105-107).

12. Em tais fluxogramas, são mencionadas as hipóteses de comunicação às autoridades competentes, como o Ministério Público, a exemplo das seguintes: “Avaliar a pertinência de eventual comunicação antecipada à autoridade competente”; “Verificar se pode haver indício de fornecimento ou divulgação indevida de informação do Coaf”; “Verificar se há indícios de envolvimento de integrantes do Coaf”; “Avaliar a pertinência do proposto, inclusive eventual comunicação a outra(s) autoridade(s)”; e “Adotar a providência proposta” (peça 104, p. 2; peças 106-107).

13. Assim sendo, o Coaf entende que já se encontra implementada a rotina de encaminhar os casos de acessos indevidos às bases de dados ao conhecimento do Ministério Público (peça 104, p. 3).

14. De qualquer modo, ressalta que a redação da determinação deve ser direcionada a órgão específico, a fim de evitar eventual ambiguidade de determinar providências que já se encontram implementadas (peça 104, p. 3).

15. Por sua vez, a RFB, por meio do Parecer Coger/GNP 573/2021(peça 111), informa que sua Corregedoria, inclusive por força da Lei 8.112/1990 (arts. 154, parágrafo único, e 171), quando do desenvolvimento dos procedimentos administrativos disciplinares (PAD), realiza as pertinentes representações penais (peça 111, p. 2).

16. Ressalta que, em regra, a representação penal ao Ministério Público ocorre após a conclusão do PAD, em observância ao entendimento contido no Manual de Processo Administrativo da CGU (peça 111, p. 3).

Análise

17. Conforme comentários dos gestores, já existem mecanismos implementados para que as ocorrências de acesso indevido sejam levadas ao conhecimento do Ministério Público, para fins de persecução penal, o que torna dispensável a determinação proposta pelo MPTCU.

18. Ressalte-se também que é dever legal dos servidores e autoridades da RFB e do Coaf representar contra ilegalidades, inclusive crimes, conforme arts. 116, XII, 154, parágrafo único, 171 da Lei 8.112/1990; e art. 8º, inciso IV e §2º, da Lei 13.974/2020.

19. Neste sentido, por força do art. 7º, inciso II, da Resolução TCU 315/2020, a determinação proposta pelo MPTCU, para que o Coaf e a RFB representem criminalmente quem devassar as suas bases de dados de forma indevida, não deve ser acolhida, haja vista a vedação da formulação de determinações para mera observância de normativos ou legislação.

II. 2. Recomendação para a adoção de medidas de salvaguarda do sigilo de informações sigilosas extraídas das bases da RFB quando essas são enviadas a outros destinatários por imposição legal, tal como a identificação do destinatário e a assunção de compromisso de zelar pelo sigilo, estabelecendo uma trilha rastreável do compartilhamento desses dados.

Comentários

20. Quanto a esta recomendação, o Coaf destaca que a proposta trata apenas da salvaguarda de informações extraídas das bases de dados da RFB, não lhe afetando (peça 104, p. 4).

21. Acrescenta que, caso a recomendação proposta abrangesse as informações extraídas das bases do Coaf, ter-se-ia uma recomendação de medidas já adotadas pelo Coaf, haja vista que este já vinha adotando importantes medidas de salvaguarda de informações sigilosas extraídas de suas bases de dados, tais como: a) identificação de destinatários; b) exigência de certificação digital; c) mecanismos de autenticação em dois fatores; e d) assunção de compromisso de zelo pelo sigilo.

22. Tais medidas são confirmadas nos parágrafos 149 a 160 da Nota Técnica 14/2021/COAF (peça 38, p. 38-160), Ofício SEI 500/2020/COAF (peça 46) e verificação *in loco* da equipe de auditoria (peça 58).

23. Ressalta as seguintes medidas convergentes com a proposta de recomendação alvitrada:

a) atualização do Plano Estratégico do Coaf, ciclo 2020/2023, incluindo os seguintes objetivos estratégicos: aumentar a qualidade da produção de inteligência financeira e promover seu uso adequado pelas autoridades competentes; ampliar a compreensão da sociedade e de atores institucionais sobre o sistema de PLD/FTP e sobre os papéis do Coaf; buscar a excelência em padrões de governança e de segurança da informação;

b) eventos voltados a ampliar a conscientização de autoridades em relação a melhores práticas no uso de elementos de inteligência financeira veiculados em Relatórios de Inteligência Financeira (RIFs);

c) avaliação de riscos exclusivamente dedicada à temática de segurança da informação no âmbito da Política de Gestão de Riscos (Prisc) de que trata a Portaria Coaf 11, de 12 de julho de 2021, e em linha com a Política de Segurança da Informação e Comunicação (Posic) do Coaf;

d) ampliação das ações de disseminação da Posic do Coaf, inclusive mediante reformulação do pacote de Treinamento Básico para Ingressantes no Coaf (TBI);

e) desenvolvimento de versão atualizada do Sistema Eletrônico de Intercâmbio (SEI-C), inclusive com a incorporação de mecanismos adicionais de segurança.

24. A RFB, por meio da Nota 625/2021-RFB/Copes/GAB/2021, informa que a Portaria-RFB 551/2013 dispõe sobre o tratamento de expedientes oriundos de outros órgãos, entidades,

autoridades ou cidadãos utilizados para solicitar dados econômico fiscais de contribuintes, análise de situação fiscal ou instauração de procedimento fiscal no âmbito daquele órgão fazendário (peça 109, p. 1). Trata também da preservação do caráter sigiloso de informações protegidas por sigilo fiscal e prevê três alternativas de fornecimento de dados protegidos por sigilo fiscal: entrega em meio físico (art. 13), documento eletrônico em formato digital (art. 14) e acesso on-line pelo requisitante (art. 15) (peça 109, p. 1).

25. Registra que, mesmo antes do advento da Portaria em questão, medidas de salvaguarda de sigilo já estavam sendo tomadas pela RFB, nos termos da Portaria SRF 580/2001 (peça 109, p. 1).

26. Paralelamente, a Portaria-RFB 551/2013 contém regras específicas para o fornecimento de dados em meio físico, prevendo o uso de dois envelopes: o primeiro, lacrado, contendo os dados sigilosos e informações adicionais; e o segundo contendo o recibo de entrega que deve ser assinado preferencialmente pela autoridade requisitante ou funcionário responsável pelo recebimento de correspondências no órgão solicitante (peça 109, p. 2).

27. Acrescenta, por meio do Despacho n. 00.076/Cotec/Sucor/RFB/2021, que a entrega de documento eletrônico em formato digital é feita por destinatário identificado, e o acesso à informação está condicionado à utilização do certificado digital do destinatário, conforme arts. 5º, 6º, 7º, 11, 12 e 14 da Portaria-Cotec 21/2020 (peça 110, p. 2).

28. Quanto ao acesso on-line da informação pelo requisitante (art. 15 da Portaria-RFB 551/2013), ele é realizado somente com certificado digital e, previamente ao acesso, o requisitante assina termo de responsabilidade (peça 110, p. 2).

Análise

29. Conforme comentários do Coaf e da RFB já existem mecanismos implementados de salvaguarda do sigilo de informações sigilosas extraídas das suas bases: parágrafos 149 a 160 da Nota Técnica 14/2021/COAF (peça 38, p. 38-160), Ofício SEI 500/2020/COAF (peça 46) e verificação *in loco* da equipe de auditoria (peça 58), relativamente ao Coaf; e Portaria-RFB 551/2013 e Portaria-Cotec 21/2020, no que se refere à RFB. Assim, mostra-se dispensável a proposta de recomendação sugerida pelo MPTCU.

30. Portanto, não deve ser acolhida a proposta de recomendação para que se adote medidas de salvaguarda do sigilo de informações sigilosas extraídas das bases da RFB, quando essas são enviadas a outros destinatários por imposição legal, haja vista já existirem mecanismos implementados com este fim.

Conclusão e proposta de encaminhamento

31. Os comentários apresentados pelo CNJ são convergentes com a análise já realizada no relatório final de fiscalização e não repercutem nas propostas de deliberação feitas pela equipe de auditoria de modo a alterá-las (parágrafos 3-8).

32. Considerando que é dever legal dos servidores e autoridades da RFB e do Coaf representar contra ilegalidades e que já existem mecanismos implementados para que as ocorrências de acesso indevido às bases de dados desses órgãos sejam levadas ao conhecimento do Ministério Público para fins de persecução penal, não deve ser acolhida a proposta de determinação do MPTCU nesse sentido (parágrafos 9-19).

33. Considerando que tanto o Coaf quanto a RFB vêm implementando medidas de salvaguarda do sigilo de informações sigilosas extraídas de suas bases, inclusive quando enviadas a outros destinatários por imposição legal, não deve ser acolhida a proposta de recomendação apresentada pelo MPTCU no sentido de se implementar tais medidas (parágrafos 20 a 30).

34. Após avaliar a manifestação do CNJ, do Coaf e da RFB, em cumprimento ao despacho da peça 93, conclui-se que não há qualquer repercussão na proposta de mérito constante do relatório de fiscalização, remanescendo inalteradas as propostas apresentadas pela equipe de auditoria constantes dos itens “a” a “f” do parágrafo 159 do relatório de fiscalização (peça 93), devendo-lhe-

ser acrescentada, ainda, proposta de arquivar os presentes autos, nos termos do art. 250, inciso I, do Regimento Interno do TCU.

35. Ante todo o exposto, submetem-se os autos à consideração superior, a fim de que seja apreciado o relatório de fiscalização (peça 93) e as propostas apresentadas pela equipe de auditoria constantes dos itens “a” a “f” do parágrafo 159 do referido relatório, às quais deve ser acrescentada a proposta de arquivar os presentes autos, nos termos do art. 250, inciso I, do Regimento Interno do TCU.”

É o Relatório.

VOTO

Tratam os autos de Representação ofertada pelo Ministério Público junto ao TCU acerca de possíveis ocorrências de acessos indevidos a dados relativos a pessoas expostas politicamente (PEPs) contidos em bases de dados custodiadas pela Secretaria Especial da Receita Federal do Brasil (RFB) e do Conselho de Controle de Atividades Financeiras (Coaf), em decorrência da veiculação de matéria jornalística a esse respeito. Foi analisada ainda a sistemática de compartilhamento de informações entre os dois órgãos, bem como avaliados ritos, procedimentos e controles desenhados para preservar os dados relativos a pessoas expostas politicamente nos sistemas dos órgãos.

2. O trabalho contemplou inspeção realizada pela Secretaria de Controle Externo da Gestão Tributária e Supervisão de Contas (SecexTributária) na RFB e no Coaf com o objetivo de elucidar três pontos adiante indicados:

2.1. Questão 1: Houve ocorrência de indevido acesso a dados relativos a pessoas expostas politicamente em bases da RFB e do Coaf?

2.2. Questão 2: Os ritos, os procedimentos e o sistema de controle desenhados são suficientes para preservar os dados de pessoas expostas politicamente mantidos em bases da RFB e do Coaf?

2.3. Questão 3: O processo de comunicação de fatos entre a RFB e o Coaf é seguro e existem controles para inibir, coibir e punir eventuais abusos?

3. A fiscalização constatou: (i) acesso indevido a dados fiscais de pessoas expostas politicamente na RFB; (ii) necessidade de ampliar a abrangência da base de dados de pessoas expostas politicamente mantida pela Controladoria-Geral da União (CGU) de modo a contemplar autoridades do Poder Judiciário e do Ministério Público; (iii) fragilidades nos controles estabelecidos pela RFB para salvaguardar acessos indevidos a dados de pessoas expostas politicamente por meio do Sistema Midas; (iv) mecanismos de controle no Coaf reservados a pessoas expostas politicamente com prerrogativa de foro; (v) risco de vazamento ou publicização de Relatórios de Inteligência Financeira (RIFs) produzidos pelo Coaf por órgãos de destino; e (vi) baixo aproveitamento dos Relatórios de Inteligência Financeira pela RFB.

4. Tendo em vista os ajustes de escopo e abrangência ocorridos no processo após a representação inicial, determinei o envio dos autos ao autor da representação, o Subprocurador-Geral Lucas Rocha Furtado, para que se manifestasse sobre o relatório e encaminhamentos preliminares sugeridos e eventualmente indicasse linhas complementares a serem examinadas (peça 83).

5. Sobreveio então parecer do representante do *Parquet* com ponderações baseadas em relatório de fiscalização ainda preliminar, isto é, antes da manifestação dos gestores (peça 66). Na ocasião, foram sugeridas novas propostas em relação à primeira análise da unidade instrutora (peças 84 e 98):

5.1. determinar aos órgãos e entidades que administram as bases de dados objeto deste trabalho para que adotem as providências necessárias para que as ocorrências de acesso indevido às informações constantes dessas bases sejam levadas ao conhecimento do Ministério Público, para fins de persecução penal;

5.2. recomendar a adoção de medidas de salvaguarda da confidencialidade de informações sigilosas extraídas das bases da RFB quando essas são enviadas a outros destinatários por imposição legal, tal como a identificação do destinatário e a assunção de compromisso de zelar pelo sigilo, estabelecendo uma trilha rastreável do compartilhamento desses dados.

6. A unidade instrutora, conquanto tenha concordado com o teor das medidas, registrou que elas não haviam sido submetidas a considerações pelos gestores dos órgãos eventualmente atingidos pelas propostas. Diante do quadro, determinei a realização de diligência à Secretaria Especial da

Receita Federal do Brasil e ao Conselho de Controle de Atividade Financeira para que se manifestassem quanto às consequências práticas das propostas adicionais do MPTCU, bem como eventuais alternativas a essas medidas (despacho de peça 98).

7. Em atendimento e após as manifestações pertinentes dos órgãos jurisdicionados, a unidade instrutora se manifestou pela manutenção da proposta de encaminhamento originária contida no relatório de fiscalização de peça 93, conforme transcrito no relatório precedente (peças 114-115).

8. Em exame do feito, anuo aos exames empreendidos pela unidade instrutora e à proposta de mérito final, que referenda o encaminhamento contido no relatório (peças 93-95, c/c peças 114-116), incorporando seus fundamentos às minhas razões de decidir, exceto nos pontos em que dou encaminhamento diverso, na forma deste Voto.

9. Passo a comentar as principais constatações, que trouxeram à tona importantes aspectos relativos à qualidade e ao cuidado quanto à custódia e ao acesso a informações sigilosas relativas a pessoas expostas politicamente no âmbito da Secretaria Especial da Receita Federal do Brasil e do Conselho de Controle de Atividades Financeiras.

10. Em relação à primeira questão, de fato restou constatada a ocorrência de acesso indevido aos dados fiscais de pessoas expostas politicamente na RFB.

11. No período de 2018 a 2020, a RFB detectou oito acessos indevidos a dados de contribuintes nas bases do órgão, sendo seis desses acessos relativos a pessoas expostas politicamente. A RFB informou que foram instaurados processos administrativos para todos os casos, sendo que quatro ainda estão em andamento. Nos quatro casos concluídos, houve responsabilização dos servidores que efetuaram os acessos indevidos e aplicadas penalidades de suspensão.

12. Como detalhado no relatório, os sistemas da RFB são sujeitos a registros de eventos (*logs*) que permitem identificar, acompanhar e recuperar evidências nos casos de suspeita de violação de normas e em incidentes de segurança. Em certos casos, a recuperação dos *logs* de acesso depende de apuração especial pelo Serpro (com custos).

13. Trata-se do Sistema Alerta-Gestor da RFB, com base no cadastro de pessoas expostas politicamente da CGU, o qual envia mensagens para o superior hierárquico e seu adjunto sempre que dados de declaração de imposto de renda referentes a pessoas expostas politicamente são acessados por meio do sistema Midas, mecanismo que tem por objetivo possibilitar a detecção de acessos indevidos.

14. Ou seja, os mecanismos de controle estabelecidos permitem identificar acessos indevidos e imotivados e viabilizar a consequente persecução disciplinar, porém não evitam a ocorrência desses eventos que, seguramente, representam violação do dever de sigilo fiscal – o qual se impõe não somente à divulgação externa de informações disponíveis no banco de dados do órgão custodiante, mas também ao acesso interno indevido por seus servidores.

15. Adicionalmente, as pessoas expostas politicamente têm maior risco de que seus dados sejam acessados de maneira imotivada e eventualmente vazados, devido aos cargos e às funções que ocupam, cuja repercussão alcança não apenas a esfera pessoal, mas também a funcional e a institucional dos ocupantes de cargos-chave na Administração.

16. Indagada a respeito, a RFB informou que o módulo Midas do sistema Alerta-Gestor permite detectar acessos indevidos aos dados das pessoas expostas politicamente e tomar as medidas cabíveis sempre que ocorram, o que consubstancia mecanismo de auxílio à detecção. Não há, contudo, mecanismos automatizados (além do controle de perfis) que previnam tais acessos indevidos, ou que garantam que a Corregedoria do órgão apure e puna eventuais abusos de auditores fiscais.

17. A RFB informou ainda que seria impraticável a implementação de travas automáticas para limitar o acesso ao sistema Midas, que reúne as declarações de imposto de renda de pessoas físicas (DIRPF), uma vez que afetaria e comprometeria outros processos de trabalho como os Centros de Atendimento ao Contribuinte e a Malha Fiscal, que correspondem a um grande volume de acessos neste sistema, além de possível quebra de impessoalidade da administração tributária, por colocar em caráter privilegiado dados de contribuintes com perfil de pessoa exposta politicamente. Reconheceram, contudo, que os controles *a posteriori* poderiam ser aperfeiçoados.
18. Entendeu a unidade instrutora, considerando todas as informações prestadas pelo fisco federal, que já estariam sendo tomadas medidas para detecção, apuração e penalização de servidores que incorrem em acesso indevido/imotivado a dados fiscais de contribuintes, motivo pelo qual entendeu despidendo determinar à RFB a adoção de medidas para essa finalidade.
19. Embora concorde que haja instrumentos capazes de promover as medidas corretivas em caso de falhas dessa natureza, retorno ao ponto de que não há mecanismos para evitar a ocorrência de eventos que representam violação do dever de sigilo fiscal, especialmente em relação a pessoas expostas politicamente, ocupantes de cargos de relevo na República.
20. Nesse ponto, sem prejuízo das pertinentes recomendações na forma sugerida pela unidade instrutora, dissinto da conclusão quanto à impossibilidade de o TCU determinar a adoção de providências com vistas a assegurar o cumprimento do devido sigilo fiscal.
21. Entendo que eventuais limitações de sistema não devem servir como justificativa para não implementar controles necessários ao cumprimento de dever legal de resguardo do sigilo fiscal, de qualquer cidadão que seja. É dizer, o sistema deve se amoldar ao cumprimento do dispositivo legal, e não o contrário.
22. Tendo em vista o disposto no art. 198 do Código Tributário Nacional (CTN), em conjunto com os arts. 14 e 52 da Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31/10/2003, assinada pelo Brasil em 9/12/2003 e promulgada por meio do Decreto 5.687/2006, deveria a RFB estabelecer mecanismo que efetivamente impedisse o acesso indevido e imotivado a dados sigilosos de pessoas expostas politicamente.
23. Considerando, porém, a discricionariedade do gestor e que a medida mais acertada pode demandar estudos para fins de adequação de procedimentos e sistemas às demais rotinas de trabalho do fisco federal, é razoável **determinar** à RFB que, no prazo de 120 dias, em atenção aos dispositivos acima, avalie e apresente a este Tribunal possíveis providências acerca de controles internos a serem implantados que sejam capazes de impedir acesso indevido e imotivado a dados sigilosos de pessoas expostas politicamente.
24. No que se refere aos ritos, procedimentos e sistemas de controle, observou-se que os principais mecanismos implementados tanto pela RFB quanto pelo Coaf para preservar os dados de pessoas expostas politicamente têm como relevante fonte de informação a base de dados de pessoas expostas politicamente disponibilizado pelo governo federal, mantida pela Controladoria-Geral da União (CGU).
25. Ocorre que esse cadastro não inclui membros do Judiciário ou do Ministério Público em razão de dificuldades de articulação institucional, o que acaba por onerar o funcionamento dos referidos mecanismos e controles implementados pelos órgãos para salvaguardá-los.
26. Na Receita Federal, uma vez que o sistema Alerta identifica quem é pessoa exposta politicamente a partir da lista da CGU, esse controle deixa de abarcar parcela significativa de agentes públicos nessa condição. Caso ocorram acessos indevidos a dados de membros do Judiciário ou do Ministério Público, não serão emitidos alertas, o que aumenta o risco de que acessos impróprios não sejam detectados.

27. No Coaf, os mecanismos de tratamento de dados de pessoas expostas politicamente também são inicialmente baseados na lista da CGU, e posteriormente ocorre inclusão manual de membros apenas do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ).
28. Nesse cenário, é evidente que a ampliação da abrangência da base de dados de pessoas expostas politicamente, mantida pela CGU, de maneira a contemplar as que integrem o Poder Judiciário e Ministério Público, contribuiria sobremaneira para facilitar e eventualmente tornar mais seguro o funcionamento dos mecanismos e controles internos existentes.
29. A Controladoria-Geral da União informou que a consolidação do cadastro de pessoas expostas politicamente pelo órgão é resultado da ação 7/2013 da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (Enccla), que não possui caráter impositivo. Ademais, tal atribuição não é mencionada em nenhum outro normativo legal ou infralegal, de modo que, se a relação por ela consolidada não contempla os membros do Ministério Público e do Poder Judiciário, tal fato não configura irregularidade.
30. Dito de outra forma, a obrigatoriedade de incluir os membros do Poder Judiciário e do Ministério Público no cadastro da CGU só poderia ocorrer por força de lei. Reconheço, portanto, que do ponto de vista da Controladoria-Geral da União, não configura irregularidade a ausência da inclusão dessas pessoas expostas politicamente no referido cadastro, mas uma falha ou deficiência de governança.
31. Sob esses fundamentos, estou de acordo com a proposta de dar conhecimento à CGU, ao CNJ e ao CNMP dessa fragilidade, no intuito de possibilitar aos órgãos melhor entenderem os riscos identificados pelo TCU que incidem sobre seus membros e titulares, a fim de possibilitar a otimização dos processos de elaboração e consolidação do cadastro.
32. Por outro lado, isso em nada afasta a responsabilidade e o dever legal da RFB em assegurar o sigilo fiscal com cuidado especial sobre absolutamente todas as pessoas expostas politicamente. Assim, não havendo completude no cadastro da CGU, deveria o fisco dispor de outros mecanismos para salvaguardar os acessos indevidos, uma vez que a limitação do sistema do órgão central de controle interno não a exime de cumprir na íntegra suas atribuições legais.
33. Por outro lado, como já ponderei acima, deve-se resguardar a discricionariedade do gestor em avaliar a medida mais acertada para solucionar essa relevante deficiência, motivo pelo qual é razoável **determinar** à RFB que, no prazo de 120 dias, em atenção aos dispositivos legais já mencionados, avalie e apresente a este Tribunal possíveis providências acerca de controles internos a serem implantados capazes de assegurar que o rol de completo de pessoas expostas politicamente inclua membros do Ministério Público e do Poder Judiciário.
34. Por fim, em relação ao processo de comunicação entre a RFB e o Coaf, detectou-se risco de vazamento ou publicização dos Relatórios de Inteligência Financeira (RIFs) produzidos pelo Coaf por órgãos de destino.
35. Apesar do risco, não foi possível detectar vulnerabilidades no processo de comunicação entre a RFB e o Coaf, haja vista todo o trâmite ser feito pelo Sistema de Intercâmbio de Informações do Coaf e, conforme detalhado no relatório, existirem controles para inibir, coibir e punir eventuais abusos.
36. Finalmente, a análise do processo de comunicação entre a RFB e o Coaf resultou na constatação de baixo aproveitamento dos Relatórios de Inteligência Financeira pela RFB. Verificou-se que as análises individuais realizadas sobre os relatórios recebidos pela área competente do fisco federal agregam pouco valor aos relatórios de inteligência, e, por isso, a própria RFB estaria estudando uma forma de tornar as análises desses relatórios mais efetivas.
37. Quanto a essas duas questões, entendo que as providências em curso pelos órgãos

jurisdicionados e informadas no relatório precedente tendem a suprir as lacunas de governança identificadas, em especial a recomendação dirigida ao Conselho de Controle de Atividades Financeiras e à Secretaria Nacional de Justiça e Cidadania, por meio de seu Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), para que, na condição de Secretaria-Executiva da Enccla, suscitem, naquele foro, debate voltado a consolidar orientação técnica às autoridades competentes, destinatárias dos Relatórios de Inteligência Financeira, no sentido de que esses não sejam incluídos em autos de processos para efeitos de instrução probatória, por terem caráter de mera sinalização de situação atípica, sem força probante, de acordo com os fundamentos legais apontados no acórdão.

38. Diante do exposto, com os ajustes acima propostos, acompanho a essência das constatações da unidade instrutora.

39. Feitas essas considerações, voto por que o Tribunal adote o Acórdão que ora submeto à deliberação deste Colegiado.

TCU, Sala das Sessões, em 7 de dezembro de 2022.

Ministro BRUNO DANTAS
Relator

ACÓRDÃO Nº 2710/2022 – TCU – Plenário

1. Processo nº TC 039.693/2020-1.
- 1.1. Apensos: 047.560/2020-7; 045.800/2021-9.
2. Grupo II – Classe de Assunto: VII – Representação.
3. Interessados/Responsáveis: não há.
4. Unidades Jurisdicionadas: Conselho de Controle de Atividades Financeiras; Secretaria Especial da Receita Federal do Brasil.
5. Relator: Ministro Bruno Dantas.
6. Representante do Ministério Público: Subprocurador-Geral Lucas Rocha Furtado.
7. Unidade Técnica: Secretaria de Controle Externo da Gestão Tributária e Supervisão de Contas (SecexTributária).
8. Representação legal: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos de Representação do Ministério Público junto ao TCU com o objetivo de apurar a ocorrência de acesso indevido a informações de pessoas expostas politicamente contidos em bases de dados da Secretaria Especial da Receita Federal do Brasil (RFB) e do Conselho de Controle de Atividades Financeiras (Coaf) e a forma como se dá o compartilhamento de informações entre esses órgãos, bem como avaliar os ritos, procedimentos e controles desenhados para preservar os dados relativos a pessoas expostas politicamente nos sistemas dos aludidos órgãos,

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em Sessão do Plenário, diante das razões expostas pelo Relator, em:

9.1. conhecer da representação, satisfeitos os requisitos de admissibilidade previstos nos arts. 235 e 237, inciso VII, do Regimento Interno deste Tribunal, c/c o art. 103, § 1º, da Resolução-TCU 259/2014 e considerá-la procedente;

9.2. determinar à Secretaria Especial da Receita Federal do Brasil (RFB), com fundamento no art. 250, inc. II, do Regimento Interno do TCU, c/c o art. 4º da Resolução-TCU 315/2020, que, no prazo de 120 dias, em atenção ao art. 198 do Código Tributário Nacional (CTN), c/c os arts. 14 e 52 da Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31/10/2003, assinada pelo Brasil em 9/12/2003 e promulgada por meio do Decreto 5.687/2006, avalie e apresente a este Tribunal:

9.2.1. providências em termos de possíveis controles internos, a serem implantados, capazes de impedir acesso indevido e imotivado a dados sigilosos de pessoas expostas politicamente contidos em bases de dados custodiadas pela Secretaria Especial da Receita Federal do Brasil (RFB);

9.2.2. providências em termos de possíveis controles internos, a serem implantados, capazes de assegurar que suas bases de dados sejam alimentadas com o rol completo de pessoas expostas politicamente, o que deve incluir membros do Ministério Público e do Poder Judiciário;

9.3. recomendar à Secretaria Especial da Receita Federal do Brasil (RFB), com fundamento no art. 250, inc. III, do Regimento Interno do TCU, c/c o art. 11 da Resolução-TCU 315/2020, que:

9.3.1. aprimore e refine o campo de “justificativa” que deve ser preenchido para acessar o sistema Midas e a base de declarações de imposto de renda de pessoas físicas (DIRPF), para facilitar a detecção de desvios pela supervisão quando do recebimento de alertas referentes a pessoas expostas politicamente por meio do sistema Alerta-Gestor;

9.3.2. avalie a oportunidade e conveniência de incluir ferramentas gerenciais no sistema Alerta-Gestor, que permitam avaliar efetivamente as ações tomadas pelos supervisores depois de recebidos os alertas, de modo a garantir uma supervisão efetiva sobre os acessos à base de declarações de imposto de renda de pessoas físicas (DIRPF) de pessoas expostas politicamente;

9.3.3. continue com os esforços para estabelecer os cruzamentos na base de dados de Relatórios de Inteligência Financeira (RIFs) de geração espontânea encaminhados pelo Coaf para agregar valor à programação de ações fiscais;

9.4. recomendar à Secretaria Especial da Receita Federal do Brasil (RFB) e ao Conselho de Controle de Atividades Financeiras (Coaf), com fundamento no art. 250, inc. III, do Regimento Interno do TCU, c/c o art. 11 da Resolução-TCU 315/2020, que estudem medidas que possibilitem maior compartilhamento de informações entre os dois órgãos, para melhor subsidiar os trabalhos de inteligência financeira e combate a ilícitos tributários por ambos, em atenção ao Resultado Imediato 6, item 6.2 da Avaliação da Efetividade, constante das recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o financiamento do Terrorismo (Gafi);

9.5. recomendar, com fundamento no art. 250, inc. III, do Regimento Interno do TCU, c/c o art. 11 da Resolução-TCU 315/2020, ao Conselho de Controle de Atividades Financeiras e à Secretaria Nacional de Justiça e Cidadania, por meio de seu Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), que, na condição de Secretaria-executiva da Enccla, suscitem, naquele foro, debate voltado a consolidar orientação técnica às autoridades competentes, destinatárias dos Relatórios de Inteligência Financeira (RIFs), no sentido de que esses relatórios não sejam incluídos em autos de processos para efeitos de instrução probatória, por terem caráter de mera sinalização de situação atípica, sem força probante, de acordo com a orientação firmada em precedentes da Controladoria-Geral da União e do Supremo Tribunal Federal e com a adequada interpretação extensiva do art. 11, inciso II, Lei 9.613/1998, a fim de proteger a integridade das pessoas que, por obrigação legal, devem fornecer informações ao Coaf, bem como a efetividade do sistema de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa (PLD/FT);

9.6. encaminhar cópia deste acórdão à Secretaria Especial da Receita Federal do Brasil, ao Conselho de Controle de Atividades Financeiras, à Secretaria Nacional de Justiça e Cidadania, à Controladoria-Geral da União, ao Conselho Nacional de Justiça e ao Conselho Nacional do Ministério Público;

9.7. nos termos do art. 8º da Resolução-TCU 315/2020, autorizar o monitoramento das deliberações contidas nos itens 9.2, 9.3, 9.4 e 9.5.

10. Ata nº 46/2022 – Plenário.

11. Data da Sessão: 7/12/2022 – Ordinária.

12. Código eletrônico para localização na página do TCU na Internet: AC-2710-46/22-P.

13. Especificação do quórum:

13.1. Ministros presentes: Walton Alencar Rodrigues (na Presidência), Benjamin Zymler, Bruno Dantas (Relator) e Antonio Anastasia.

13.2. Ministros-Substitutos convocados: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e Weder de Oliveira.

(Assinado Eletronicamente)
WALTON ALENCAR RODRIGUES
na Presidência

(Assinado Eletronicamente)
BRUNO DANTAS
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral