Tribunal de Contas da União
Secretaria-Geral de Controle Externo
Secretaria de Apoio à Gestão de Processos

OFÍCIO 0856/2025-TCU/Seproc

Brasília-DF, 28/1/2025.

Ao Senhor
LEANDRO BUENO
Coordenador de Comissões Especiais, Temporárias e de Inquérito

Processo TC 023.173/2023-8 Tipo do processo: Solicitação do Congresso Nacional
Relator do processo: Ministro Bruno Dantas
Unidade responsável: Unidade de Auditoria Especializada em Tecnologia da Informação

Assunto: Notificação de acórdão.
Anexos: peças 96, 97 e 98 do processo TC 023.173/2023-8.

Senhor Coordenador,

1. Informo Vossa Senhoria do Acórdão 67/2025-TCU-Plenário, de relatoria do Ministro Bruno Dantas, prolatado na sessão de 22/1/2025, por meio do qual o Tribunal de Contas da União apreciou o processo acima indicado.

2. Encaminho cópia do referido acórdão, cujo inteiro teor pode ser acessado no Portal TCU, endereço eletrônico www.tcu.gov.br/acordaos.

3. Por oportuno, solicito especial atenção às informações complementares que acompanham este ofício, bem assim para a necessidade de utilizar – para resposta a comunicações e envio de documentos – os serviços da plataforma Conecta-TCU ou do protocolo eletrônico, disponíveis no Portal TCU (www.tcu.gov.br), endereço em que também é possível acessar os autos do processo.

4. Esclarecimentos adicionais quanto ao processo indicado ou à presente comunicação podem ser obtidos junto à Secretaria de Apoio à Gestão de Processos (Seproc) pelo e-mail cacidadao@tcu.gov.br, ou pelo telefone 0800-644-2300, opção 2, no horário das 10h às 18h.

Atenciosamente,

Assinado eletronicamente
SIMONE BICALHO FELIX BRAGA
Especialista Sênior II

INFORMAÇÕES COMPLEMENTARES

1) O acesso ao processo indicado nesta comunicação pode ser realizado por meio da plataforma de serviços digitais Conecta-TCU, disponível no Portal TCU (www.tcu.gov.br). A visualização de processos e documentos sigilosos depende de solicitação formal e posterior autorização do relator. Informações detalhadas sobre o uso da plataforma, inclusive para fins de cadastro e credenciamento, podem ser consultadas ao acionar o ícone "Conecta-TCU" do Portal TCU.

2) Nos termos do art. 27, § 3º, da Resolução-TCU 360/2023, havendo necessidade de informar sobre o mesmo conteúdo a diferentes unidades da mesma estrutura organizacional, o TCU encaminhará apenas um expediente, cujo teor deve ser disponibilizado à unidade de controle interno e, quando for o caso, a outros setores dessa instituição que conciliam interesse na matéria.

3) Em se tratando de processo de contas e havendo no acórdão responsáveis com contas julgadas regulares ou regulares com ressalva, incumbe ao dirigente da unidade jurisdicionada, ou a sua unidade de auditoria ou controle interno, dar ciência do teor do acórdão a esses responsáveis, nos termos do art. 4º, § 7º, da Resolução-TCU 360/2023.

4) Nos termos do art. 30 da Resolução-TCU nº 360/2023, quando da apreciação de recurso interposto à deliberação do Tribunal, são expedidas comunicações sobre a deliberação adotada a todas as autoridades, responsáveis e interessados a quem foi dirigida comunicação quando da adoção da deliberação recorrida.

5) No caso de acórdão proferido em processo constante de relação, na forma do art. 143 do Regimento Interno do TCU, não há relatório e voto. A fundamentação de análise de fato e de direito consta da instrução técnica juntada aos autos.

6) A juntada aos autos do instrumento de mandato, quando a parte for representada por procurador, é pressuposto essencial para a atuação do mandatário no processo, nos termos do art. 13, § 2º, da Resolução - TCU 36/1995.

7) Constitui dever das partes, de seus procuradores e de todos aqueles que de qualquer forma participem do processo, uma vez comunicados com êxito, informar e manter atualizadas as informações referentes aos respectivos endereços, não cabendo posterior arguição de nulidade de comunicação em decorrência da alteração de endereço não informada expressamente nos autos, nos termos do art. 5º, *caput* e § 2º, da Resolução-TCU 360/2023.

8) Nos termos dos arts. 31 a 35 da Lei nº 8.443/1992 e 285 a 288 do Regimento Interno do TCU, a parte poderá interpor recurso ao acórdão. A interposição de embargos de declaração é causa de mera suspensão e não de interrupção de prazo para os demais recursos, conforme disposto no art. 34, § 2º, da Lei nº 8.443/1992.

9) A apresentação de petição ou a interposição de recurso deve observar as seguintes orientações:

a) ser dirigida ao relator do processo;

b) indicar, com destaque, o número do processo e deste ofício;

c) utilizar dos serviços da plataforma digital Conecta-TCU ou do protocolo eletrônico disponíveis no Portal TCU;

d) a petição ou o recurso podem ser apresentados diretamente pelo destinatário do ofício ou por intermédio de procurador regularmente constituído nos autos, conforme disciplina o art. 145 do Regimento Interno do TCU;

e) caso haja procurador constituído nos autos, as comunicações processuais subsequentes serão dirigidas a esse representante. Se houver mais de um procurador, pode ser indicado o nome daquele a quem deverão ser encaminhadas as comunicações, conforme o disposto no art. 145, §§ 3º e 4º, do Regimento Interno do TCU, e no art. 38 da Resolução-TCU 360/2023.

10) A informação classificada na origem com restrição de acesso deve ser acompanhada dos seguintes elementos, consoante a Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011), caso contrário será considerada de acesso público pelo Tribunal:

a) indicação objetiva da hipótese de restrição de acesso: informação imprescindível à segurança da sociedade ou do Estado; informação com sigilo atribuído por legislação específica; informação pessoal relativa à intimidade, vida privada, honra e imagem;

b) na hipótese de informação imprescindível à segurança da sociedade ou do Estado, indicar:
b.1) o grau de sigilo da classificação (reservado, secreto ou ultrassecreto);

b.2) o fundamento legal da classificação;

b.3) o prazo de restrição de acesso ou o evento que defina o termo final;

b.4) o assunto sobre o qual versa a informação.

c) na hipótese de informação com sigilo atribuído por legislação específica, indicar o fundamento legal da classificação;

d) na hipótese de informação pessoal relativa à intimidade, vida privada, honra e imagem, indicar o prazo de restrição de acesso e a pessoa a que se refere.

GRUPO I – CLASSE II – Plenário
TC 023.173/2023-8
Natureza: Solicitação do Congresso Nacional
Unidade Jurisdicionada: Polícia Rodoviária Federal
Representação legal: não há

SUMÁRIO: SOLICITAÇÃO DO CONGRESSO NACIONAL. COMISSÃO PARLAMENTAR MISTA DE INQUÉRITO DOS ATOS DE 8 DE JANEIRO. REQUERIMENTO DE FISCALIZAÇÃO PARA VERIFICAR A REGULARIDADE DAS CONTRATAÇÕES REALIZADAS PELA POLÍCIA RODOVIÁRIA FEDERAL (PRF) COM A EMPRESA COGNYTE BRASIL S.A. REGULARIDADE DAS CONTRATAÇÕES ANALISADAS. ADEQUAÇÃO DO USO DO SISTEMA ORBIS ÀS COMPETÊNCIAS DA PRF. AUSÊNCIA DE INDÍCIOS DE DESVIO DE FINALIDADE. OPORTUNIDADES DE MELHORIA NOS CONTROLES INTERNOS E NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, RELACIONADOS AO USO DO SISTEMA. RECOMENDAÇÃO À PRF. CONSIDERAR INTEGRALMENTE ATENDIDA A SOLICITAÇÃO. ENCAMINHAMENTO DE INFORMAÇÕES À COMISSÃO. ARQUIVAMENTO.

RELATÓRIO

Por registrar as principais ocorrências havidas no andamento do processo até o momento, resumindo os fundamentos das peças acostadas aos autos, adoto como relatório, com os ajustes necessários, a instrução da secretaria responsável pela análise da demanda (peça 92), que contou com a anuência do corpo diretivo da unidade (peças 93-94):

> "**INTRODUÇÃO**
>
> 1. Trata-se de Solicitação do Congresso Nacional (SCN), em que a Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito, por meio do Ofício 391/2023 - CPMI8 (peça 2), conforme delegação contida no Ato do Presidente 1/2023 - CPMI8, do Presidente da Comissão Parlamentar Mista de Inquérito dos Atos de 8 de janeiro, encaminhou a este Tribunal o Requerimento 1404/2023 - CPMI - 8 de janeiro, de autoria da Senadora Eliziane Gama (peça 3).
>
> 2. O mencionado requerimento solicitou ao Tribunal de Contas da União (TCU) que realizasse fiscalização para verificar a regularidade das contratações realizadas pela Polícia Rodoviária Federal (PRF) com a empresa Cognyte Brasil S.A. (01.207.219/0001-29) de 2018 até o presente, devendo ser respondidas as seguintes questões (peça 3, p. 1):
>
> a) O objeto de algum contrato refere-se à aquisição de softwares de rastreamento, identificação e interceptação de números de aparelhos celulares de qualquer espécie ou de software de solução de monitoramento de redes sociais? Se sim, quais foram os softwares adquiridos?
>
> b) Qual finalidade da utilização de tecnologias de interceptação de aparelhos telefônicos e de monitoramento de redes sociais, considerando que a PRF não detém competência legal para realizar investigações como a polícia judiciária?

c) Considerando que houve pagamentos à empresa por meio da Ação Orçamentária POLICIAMENTO OSTENSIVO NAS RODOVIAS E ESTRADAS FEDERAIS, como os sistemas da Cognyte são utilizados nas ações de policiamento ostensivo das rodovias federais?

d) Considerando que houve pagamentos à referida empresa por meio da Ação Orçamentária POLICIAMENTO, FISCALIZAÇÃO, COMBATE À CRIMINALIDADE E CORRUPÇÃO, como os sistemas da Cognyte são usados nas ações de policiamento, fiscalização, combate à criminalidade e à corrupção?

e) Haveria desvio de finalidade nas contratações da Cognyte pela PRF?

HISTÓRICO

3. Após consulta aos sistemas disponíveis, o auditor responsável pela instrução inicial (peça 9) identificou a celebração de dois contratos entre a PRF e a empresa Cognyte (peça 8):

a) Contrato 73/2018, firmado entre a então Suntech S.A. e a Superintendência Regional da Polícia Rodoviária Federal no Estado do Rio de Janeiro (PRF/RJ), no valor de R$ 5.000.000,00, com vigência de 28/12/2018 até 28/12/2019 e cujo objeto foi a aquisição de solução integrada denominada Webint; e

b) Contrato 35/2021, firmado com o Departamento de Polícia Rodoviária Federal, no valor de R$ 5.000.000,00, com vigência de 21/9/2021 até 21/3/2024 e cujo objeto é a contratação dos serviços de manutenção, suporte e migração do sistema *verint web intelligence* para o sistema Orbis e realização de treinamento oficial.

4. Assim, em instrução e despachos uniformes, a Unidade de Auditoria Especializada em Contratações (AudContratações) propôs a realização de diligências junto à PRF e à PRF-RJ para obtenção dos elementos necessários para responder as questões postas nesta SCN (peças 9-11).

5. Por meio de despacho, o relator concordou com a unidade técnica (UT) e autorizou a realização dessas diligências (peça 12).

6. Em 18/9/2023, foram encaminhados os Ofícios 45913/2023-TCU/Seproc e 45917/2023-TCU/Seproc (peças 13 e 14), respondidos pelo Ofício 680/2023/CI/CGCI (peça 19), com os documentos às peças 20-28, dentre eles, o Projeto Básico da contratação (peça 20), que prevê a migração do sistema Verint Web Intelligence para o sistema Orbis, em razão da necessidade de atualização tecnológica da busca e coleta de dados em fontes abertas.

7. Em 22/9/2023, o Aviso 791 - GP/TCU foi encaminhado ao Presidente da Comissão Parlamentar Mista de Inquérito dos Atos de 8 de janeiro (peça 18).

8. Em instrução conjunta com a Unidade de Auditoria Especializada em Governança e Inovação (AudGovernança), em que coube à AudContratações analisar a regularidade e a legalidade dos processos de contratação da empresa Cognyte e à AudGovernança examinar a aquisição do sistema da empresa e a contratação de serviços de manutenção, suporte e migração do sistema sob a ótica do desenvolvimento das atividades de negócio - área fim - da PRF, os auditores responsáveis pela análise das respostas encaminhadas apresentaram a seguinte conclusão (peça 30, p. 9-10):

71. As análises desta Unidade Técnica permitiram **responder todos os questionamentos** apresentados no Requerimento 1404/2023 - CPMI (peça 3).

72. Identificaram, ainda, a oportunidade de melhoria dos procedimentos da PRF no que diz respeito à utilização do sistema objeto do Contrato 35/2021, em função disso, será proposta **construção participativa de deliberações**.

73. Por fim, as informações constantes dos autos **não apresentam indícios de irregularidades ou ilegalidades** no processo de contratação ou na gestão dos Contratos 73/2018 e 35/2021.

9. Dessa forma, uma vez que as unidades identificaram oportunidade de melhoria dos procedimentos da PRF no que diz respeito à utilização do sistema objeto do Contrato 35/2021, com a concordância dos dirigentes da AudContratações e da AudGovernança (peça 32), foi proposta a realização de construção participativa de deliberações junto à PRF (peça 30, p. 10).

10. Após análise da manifestação encaminhada pela PRF em resposta (peças 35-37), a área técnica apresentou seu parecer pronunciando-se de forma conclusiva quanto aos questionamentos formulados na presente SCN (peças 39-42).

11. Entretanto, em seu voto (peça 50), o exmo. Ministro-Relator entendeu que em relação aos itens 'c' e 'd' da SCN, as informações obtidas até então eram insuficientes para responder integralmente à demanda do Congresso Nacional. Entendeu que ainda seria necessário esclarecer: como o sistema Orbis é utilizado, na prática, pela PRF; quais são as funcionalidades do software; como são os registros de *logs* e a auditabilidade da ferramenta; se a previsão do projeto básico de que 'a solução deve acessar dados privados, ou seja, dados que são restritos por credenciais do usuário' representa uma ação intrusiva; e como funcionam as funcionalidades de georreferenciamento de informações e de pesquisa de dados na *Deep* e *Dark* web.

12. Nesse sentido, o Plenário do TCU, no Acórdão 1.228/2024-TCU-Plenário (peça 49), de relatoria do Ministro Vital do Rêgo, decidiu: a) determinar à unidade de auditoria especializada em tecnologia da informação que, se necessário, com apoio da unidade de auditoria especializada em governança, realizasse inspeção na PRF para apurar como tem se dado o efetivo uso da ferramenta objeto do Contrato 35/2021 desde sua assinatura, avaliando eventuais riscos de desvio de finalidade em sua utilização, bem como análise sobre a suficiência dos controles internos e de segurança da informação atualmente empregados na mitigação desses riscos; e b) prorrogar, por cento e oitenta dias, o prazo para atendimento da Solicitação do Congresso Nacional, a partir da data do acórdão (26/6/2024).

13. Assim, a Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) instaurou Inspeção (peça 56), Registro Fiscalis 157/2024, na PRF, visando atender à determinação do Plenário.

EXAME TÉCNICO

14. Conforme determinado pelo Acórdão 1.228/2024-TCU-Plenário (peça 49), foi realizada fiscalização na modalidade inspeção, entre os dias 26/8/2024 e 11/10/2024, com a realização de visitas à sede da PRF. As informações reunidas nas peças 67-79, que subsidiaram o presente exame técnico, foram recebidas via requisição de documentos e durante a execução da inspeção, em que a equipe da unidade técnica pôde executar o procedimento de observação direta sobre todas as funcionalidades da ferramenta Orbis.

15. Tendo em vista os documentos recebidos e os procedimentos realizados, passa-se ao exame e esclarecimento das questões que justificaram à instauração desta inspeção: como tem se dado o efetivo uso da ferramenta Orbis, desde a assinatura do contrato, e eventuais riscos de desvio de finalidade em sua utilização, bem como análise sobre a suficiência dos controles internos e de segurança da informação atualmente empregados na mitigação desses riscos.

I - Efetivo uso da ferramenta Orbis

I.1 - Diferença entre trabalhos de inteligência e trabalhos de investigação

16. Inicialmente, é importante esclarecer a diferença entre as atividades de inteligência e de investigação. Essa diferenciação é importante, sobretudo, porque a PRF não é órgão de polícia judiciária, e, portanto, não realiza investigações formais (*stricto sensu*), mas se vale das atividades de inteligência para cumprir suas atribuições constitucionais de patrulhamento ostensivo das rodovias federais (CF, art. 144, §2º). Ao longo do texto será utilizada a palavra investigação no sentido mais amplo (*lato sensu*) para referir-se às atividades realizadas pela PRF.

17. A investigação policial é feita posteriormente à ocorrência de um suposto crime. A partir do registro inicial de um crime (notícia crime, requisição do Ministério Público ou da Justiça ou representação da vítima), inicia-se uma investigação para apurar os fatos, identificar culpados e obter provas. O procedimento formal de investigação é o inquérito policial, a cargo do Delegado de Polícia. Ao final da investigação, as conclusões obtidas no inquérito são remetidas ao Ministério Público para eventual proposição da ação penal, junto ao Poder Judiciário. Os princípios gerais que embasam a investigação policial derivam dos artigos 4º ao 23 do Código de Processo Penal (CPP).

18. Por sua vez, a atividade de inteligência visa produzir informações e conhecimentos para subsidiar uma tomada de decisão. A Doutrina Nacional de Inteligência de Segurança Pública (DNISP) define

a atividade de inteligência como:

o exercício permanente e sistemático de ações especializadas para a identificação, acompanhamento e avaliação de ameaças reais ou potenciais na esfera de Segurança Pública, orientadas, basicamente, para produção e salvaguarda de conhecimentos necessários à decisão, ao planejamento e à execução de uma política de Segurança Pública e das ações para prever, prevenir e reprimir atos criminosos de qualquer natureza ou atentatórios à ordem pública.

19. Na mesma linha, a Lei 9.883/1999, que institui o Sistema Brasileiro de Inteligência (Sisbin) e cria a Agência Brasileira de Inteligência (Abin), e o Decreto 8.793/2016, que fixa a Política Nacional de Inteligência, definem inteligência como 'atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado'.

20. Nesse contexto, a PRF é órgão integrante do Sisbin e tornou-se órgão permanente do sistema a partir da edição do Decreto 11.693/2023 (art. 7º, § 1º, inciso XI). Ademais, além de compor o Sisbin, a PRF também utiliza da atividade de inteligência para assessorar a tomada de decisão em âmbito interno, buscando aumentar a eficiência da utilização de seus recursos no policiamento ostensivo das rodovias federais. É o que se denomina 'Policiamento Orientado por Inteligência'.

21. Assim, em muitas situações, os indícios preliminares relacionados à preparação de diversas ações criminosas em estradas e rodovias federais podem ser identificados por meio da análise de dados acessíveis em grupos, canais e contas públicas em plataformas de mídias sociais. E a busca em fontes abertas pela atividade de inteligência é parte da Metodologia de Produção de Conhecimento preconizada pela DNISP.

22. Portanto, é normal que a PRF se utilize da ferramenta Orbis para abastecer os sistemas de inteligência dos quais faz parte e para subsidiar o próprio processo decisório interno. Afinal, o software auxilia na coleta e monitoramento de dados de fontes abertas, onde, muitas vezes, ocorrem atos preparatórios e trocas de informações, que o analista de inteligência pode utilizar na produção de conhecimentos que auxiliem o decisor no planejamento e execução de ações de segurança pública, no sentido de prever, prevenir, neutralizar e reprimir atos criminosos que atentem contra a ordem pública, a incolumidade das pessoas, o patrimônio e a livre circulação no âmbito de rodovias e estradas federais.

I.2 - Funcionalidades da ferramenta

23. A equipe de fiscalização realizou observação direta do funcionamento da ferramenta Orbis nos dias 13/9/2024, 16/9/2024 e 18/9/2024 (peças 72, 73 e 74) nas instalações da sede da PRF em Brasília. Durante essa observação foi realizado o levantamento e a verificação de todas as funcionalidades do sistema com a execução em tempo real das operações pelos agentes de inteligência da PRF. Importante ressaltar que, durante a execução da observação direta, as demonstrações de uso da ferramenta foram efetuadas no sistema pelos agentes da PRF, porém conduzidas segundo roteiro elaborado pela equipe de fiscalização.

24. Segundo o manual do usuário, o Orbis é uma ferramenta que extrai informações da internet e disponibiliza recursos para coletar e analisar dados com o objetivo de produzir inteligência útil. O Orbis facilita o processo de produção de conhecimento *online*, seguindo diretrizes e fluxos orientados por inteligência que são integrados ao uso do sistema, ao processamento de dados, ao enriquecimento de informações e à geração de relatórios, criando assim um ambiente dedicado à investigação para os analistas (peça 71, p. 6).

25. O manual dispõe, ainda, que o sistema oferece um espaço seguro para engajamento e investigações mais profundas na rede sobre assuntos de interesse para a inteligência (peça 71, p. 6). Esse documento inclui a descrição de todas as funcionalidades do sistema, ressaltando que algumas delas podem não estar disponíveis caso não façam parte do pacote adquirido pela organização.

26. Assim, a plataforma Orbis utilizada para coleta de dados visando a produção de inteligência na PRF é uma ferramenta complexa e multifuncional, projetada para auxiliar na coleta e análise de

informações a partir de fontes abertas. Esta plataforma é dividida em quatro menus principais que podem ser acessados pelo usuário da ferramenta nas seguintes seções: 'Investigation Dashboard', 'Discovery', 'User Manual' e 'Settings', cada uma com suas funcionalidades específicas (peças 71, p. 9 e 75, p. 4).

Menu 'Investigation Dashboard'

27. O 'Investigation Dashboard' é onde os usuários podem visualizar e filtrar a lista de investigações, além de interagir com funções específicas do painel, sendo uma área da plataforma dedicada à criação e gerenciamento de investigações.

28. Essa área tem, entre suas principais funcionalidades (peças 71, p. 13-14 e 73, p. 2), operações que permitem a visualização gráfica do número de itens coletados em cada investigação ('Collected Data per Investigation'), visualização dos detalhes das solicitações de coleta ('Collection Requests'), consulta aos últimos 20 atores visitados no sistema ('Last Visited Actor') e visualização de gráfico de barras mostrando o *status* dos agentes de coleta do sistema ('OK, Ativo, Bloqueado e Resfriamento') por plataforma web ('Collection Agents Status').

29. Há ainda a opção de visualização da linha do tempo mostrando o número de itens coletados pelo sistema em cada dia ('Data Collection') e visualização do número de arquivos coletados que estão aguardando indexação e enriquecimento com a opção de alerta quando muitos arquivos estiverem esperando ('System Load'). Tais funcionalidades são configuráveis a critério do usuário.

30. Nessa seção é possível a criação de uma investigação (peça 75, p. 4) e a configuração de uma coleta de dados para fornecer informações sobre o ator ou o termo de interesse. Após criada a investigação, é aberto um novo painel com os dados desse caso e com as funcionalidades de coleta de dados (peça 75, p. 9-10).

31. A área de 'Collection Management' permite criar requisições de coleta de três tipos: coleta baseada em atividades por palavra-chave, coleta de ator por URL e coleta de uma lista de atores por parâmetros (peças 71, p. 60-61, 74, p. 1 e 75, p. 9-10).

32. Para buscar atividades, insere-se a palavra-chave e selecionam-se as fontes disponíveis, como Linkedin, Google, Instagram, entre outros, podendo utilizar conectivos e *hashtags* (peças 74, p. 1 e 75, p. 9). A opção 'Advanced Settings' permite ajustar a coleta, definindo o número máximo de resultados, a data limite para os dados coletados, e se republicações serão coletadas, variando conforme a fonte de dados.

33. Após a parametrização, a coleta é nomeada e configurada com opções como execução imediata, prioridade alta, análise de enriquecimento, agendamento e notificações por e-mail (peças 71, p. 61 e 74, p. 1). A coleta configurada aparece no menu 'Collection Management' com detalhes como nome, tipo, fontes, status, entre outros.

34. A coleta por ator segue procedimento similar, mas com URLs em vez de palavras-chave, e a ferramenta identifica automaticamente a fonte baseada na URL (peças 74, p. 1 e 75, p. 10).

35. Para coletas por lista de atores por parâmetros, utiliza-se características dos usuários do Facebook, embora tenha sido relatado que atualizações na plataforma dessa rede social impedem essa funcionalidade de funcionar atualmente (peça 74, p. 1). Os resultados das coletas são acessíveis nos menus 'Actors' e 'Activities', dependendo do tipo de coleta, e podem ser organizados por conteúdo.

36. O menu 'Actors' mostra os resultados das coletas de atores, incluindo detalhes dos perfis, seguidores, atividades e geolocalização. Similarmente, o menu 'Activities' exibe os resultados das coletas de atividades em abas de conteúdo, mídia e geolocalização, permitindo o uso de filtros e a exportação dos dados.

37. O menu 'Artifacts' oferece a visualização de diagramas de vínculos, seleção de informações para análise, *upload* de anexos e geração de relatórios. Foi demonstrado um caso real de uso da ferramenta, incluindo a visualização de relações entre alvos no diagrama de vínculos, a possibilidade de incluir anexos para análise textual e a geração de relatórios automáticos com informações

coletadas, como redes sociais dos alvos e diagrama de vínculos (peça 74, p. 1).

Menu 'Discovery'

38. A seção 'Discovery' facilita a busca rápida por informações específicas e obtém respostas para perguntas simples levantadas sobre um ator ou atividade (peça 71, p. 15), utilizando uma variedade de fontes e permitindo a criação de investigações inteligentes e estruturadas que coletam dados automaticamente sobre alvos selecionados. Esta funcionalidade permite identificar relações entre atores e expandir a coleta de dados com base nessas relações.

39. Dependendo do tipo de informação que se deseja encontrar, apenas certas fontes são consultadas (peça 75, p. 10), sendo possível realizar a busca por nome de usuário, nome, e-mail ou número de telefone, utilizando uma variedade de fontes como Facebook, Instagram, X, LinkedIn, entre outras (peça 74, p. 2). Em resposta à equipe de fiscalização, a PRF reforçou essa informação relatando que as principais fontes de informação do 'Discovery' são possíveis números de telefones, possíveis e-mails e possíveis contas de redes sociais (peça 68, p. 3).

40. Assim, o usuário do Orbis insere a informação desejada (como nome ou telefone) e escolhe as fontes a serem pesquisadas para que a ferramenta retorne possíveis casos positivos.

41. Além disso, existe a funcionalidade de 'Smart Investigation', que permite à ferramenta criar automaticamente um caso e coletar dados sobre o alvo selecionado (peça 75, p. 10).

42. Tal funcionalidade coleta e mapeia os detalhes de um ator, amigos, relações, locais (do mais comum ao menos comum), identificadores, fotos de perfil de conta e outras fotos nas quais ele é identificado por reconhecimento facial, interesses comuns (nuvem de palavras) e se reconhecido em outras investigações no sistema (peça 71, p. 37).

43. Essa opção inicia a investigação, coleta perfis, identifica relações entre os indivíduos envolvidos, expande a coleta com base nas relações mais significativas e produz um relatório resumido com um modelo pré-configurado na ferramenta (peça 74, p. 2).

Menu 'User Manual' e menus superiores

44. O menu 'User Manual' fornece acesso ao manual do usuário, enquanto o menu superior apresenta ícones para notificações, mensagens recebidas, adição de extensões como o Web Engage no navegador, e configurações do perfil do usuário (peça 74, p. 2-3).

Menu 'Settings'

45. No menu 'Settings', encontram-se as configurações globais e as funcionalidades administrativas. As configurações globais permitem a integração com aplicativos externos, a gestão de usuários e grupos, o gerenciamento de agentes de coleta, auditoria, dicionários e configurações avançadas. É possível incluir ícones de aplicativos externos como OMNIX, Luminar, Web Engage, entre outros, cada um com funcionalidades específicas.

46. Verificou-se que a única opção habilitada para aplicativos externos era o módulo Web Engage (peças 73, p. 1 e 75, p. 7). Esse módulo é capaz de realizar uma varredura de textos (com a técnica conhecida como *scrapping*) utilizando um navegador específico, denominado WebInt Browser (peça 71, p. 62-66).

47. Tal coleta de dados é realizada de forma não intrusiva dentro de grupos de conversas públicos ou grupos nos quais o próprio usuário do Orbis está inserido nas redes sociais Whatsapp ou Telegram (peça 74, p. 2-3), conforme previsto no Projeto Básico (PB), item 4.1.1.3 ('Coleta de dados em aplicativos de trocas de mensagens WhatsApp e Telegram, de forma não intrusiva;').

48. Nesse menu ainda é possível gerenciar agentes de coleta para uma ampla gama de fontes de dados, como redes sociais e fontes da *dark* web (peça 75, p. 5-6). Foi esclarecido pela PRF que os agentes de coleta são pré-configurados pela empresa fornecedora e as fontes de coleta selecionadas são as previstas no contrato, podendo haver alteração mediante aditivo contratual e concordância da fornecedora (peça 73, p. 1).

49. O menu 'Settings' apresenta ainda o módulo de auditoria, que oferece funcionalidades como

'History Logs' e 'User Last Activities' (peça 75, p. 7-8), permitindo um acompanhamento detalhado das atividades dos usuários na plataforma (peças 71, p. 83-84 e 73, p. 2). Mais detalhes sobre o funcionamento dos controles de *logs* de atividades serão apresentados ao longo desse relatório em capítulo específico sobre riscos e controles.

50. Na seção, há também a opção 'Dictionary', que são associações de palavras para aprimorar os resultados de consultas e aumentar o número de documentos relevantes recuperados. Entre os dicionários disponíveis na plataforma Orbis, há, por exemplo, o dicionário de acrônimos, que faz associações entre abreviações e suas frases ou palavras associadas. É possível visualizar os dicionários disponíveis e fazer a gestão de novos dicionários por meio da criação, importação, alteração e exclusão (peça 71, p. 73-82). Não foi possível utilizar a funcionalidade durante a observação direta devido à ausência de credenciais necessárias pelos usuários presentes na apresentação (peça 73, p. 2).

51. Por fim, o menu 'Settings' traz algumas ferramentas administrativas denominadas 'Central Log', 'Health Monitor' e 'Central Configuration'. Dessas funcionalidades, foi possível acessar apenas o 'Health Monitor', que apresenta uma plataforma para visualizar métricas e gráficos do uso do Orbis. Não foi possível acessar as demais funcionalidades devido à ausência de credenciais necessárias e foi relatado pela PRF que tais aplicações nunca foram utilizadas pela equipe de inteligência (peça 73, p. 2).

52. Importante ressaltar que as funcionalidades às quais a equipe de fiscalização não teve acesso representam operações de caráter meramente administrativo da ferramenta e são acessadas apenas por funcionários da empresa contratada, conforme foi relatado pela PRF durante a execução dos trabalhos. Assim, tais funcionalidades não estão relacionadas diretamente às atividades fim do software (monitoramento de dados abertos em redes sociais), motivo pelo qual a falta de acesso a esses módulos não afetou a realização da fiscalização e nem as suas conclusões.

I.3 - Pesquisa em *Deep* e *Dark* web

53. Preliminarmente, convém conceituar a superfície da rede, a *deep* web e a *dark* web, bem como apontar as diferenças entre elas. A superfície da internet é a parte da rede acessível ao público geral e inclui qualquer conteúdo público que é indexado por motores de busca padrão, como o Google e o Bing, podendo ser acessada por navegadores web padrão que não requerem nenhuma configuração especial, como Google Chrome, Mozilla Firefox ou Edge. Essa camada da internet inclui *sites* comuns, como *blogs*, lojas virtuais e portais de notícias. Todos esses conteúdos são facilmente encontrados porque são visíveis para o público e podem ser acessados diretamente por meio de um navegador.

54. Por usa vez, a *deep* web refere-se à parte da internet que não é acessível por motores de busca convencionais devido a restrições de acesso, como a necessidade de *login*. Apesar de frequentemente associada a conteúdos ilícitos, a maioria do seu conteúdo é legítimo, incluindo bancos de dados privados, intranets corporativas e registros governamentais. Para acessar esses conteúdos, é necessário autenticação ou conhecer a URL ou endereço IP específicos. A *deep* web representa mais de 90% do conteúdo online e não está disponível ao público geral por ferramentas de busca padrão.

55. Já a *dark* web é uma parte específica da *deep* web e requer softwares especiais, como o navegador Tor, para ser acessada devido ao uso de técnicas de criptografia e roteamento para garantir anonimato. Embora possa ser um espaço para atividades legítimas, como a proteção da privacidade de jornalistas e dissidentes políticos, a *dark* web também é conhecida por hospedar atividades ilegais, incluindo a venda de drogas, armas e outros conteúdos proibidos.

56. Nesse contexto, o PB da contratação previu, dentre os requisitos de negócio, que (peça 23, p. 4):

4.1.1.5. A solução proposta deve fornecer um sistema de coleta capaz de coletar informações de código aberto, sites da *Deep* e *Dark web.*

[…]

4.1.1.20. A solução deve suportar a coleta de websites na *Dark web* (ou seja, com domínio. onion) que são ocultos e inacessíveis em navegadores regulares (websites não indexados no mecanismo de

busca).

57. Tais requisitos foram considerados pelo fiscal técnico do contrato como cumpridos, conforme apresentado em relatório de fiscalização técnica (peça 23, p. 176).

58. O manual do usuário da ferramenta Orbis dispõe que o sistema tem capacidade de coletar dados de todas as camadas da web, incluindo a superfície, a *deep* web e a *dark* web (peça 71, p. 6).

59. Contudo, não foram identificados no manual maiores informações sobre as consultas realizadas na *deep* web e na *dark* web. Tampouco verificou-se no conteúdo dos treinamentos ministrados (peças 69 e 70) orientações sobre esse tipo de busca.

60. Em resposta ao ofício de requisição, a PRF relacionou as fontes mais utilizadas pelos analistas de inteligência no sistema Orbis, dentre as quais não consta referência à pesquisa na *deep* web e na *dark* web.

61. Durante a observação direta realizada pela equipe de fiscalização, a PRF relatou que as pesquisas na *deep* web e na *dark* web são realizadas de maneira subsidiária em relação à outras fontes, como Facebook e Youtube, por fornecerem dados não estruturados (peça 74, p. 1).

62. Os dados não estruturados, nesse contexto, são os oriundos de fontes para os quais a ferramenta não possui um agente de coleta previamente parametrizado, como no caso de Facebook e Youtube, por exemplo, o que dificulta o trabalho de coleta pelos agentes e posterior tratamento e análise pelos agentes de inteligência da PRF (peça 74, p. 1).

63. Importante ressaltar que a PRF reforçou que a busca na *deep* web e na *dark* web, assim como nas demais fontes de dados, limita-se a consultas de dados abertos, não sendo possível a realização de ações intrusivas ou que acessem dados sigilosos ou restritos.

64. Nesse sentido, não foram identificadas evidências de referências a algum tipo de ação que possa ser considerada intrusiva nas coletas de dados na *deep* web e na *dark* web nos documentos relacionados ao processo de contratação, como o PB e o contrato em si, bem como nos documentos referentes à execução contratual e nos materiais fornecidos pela empresa à PRF, incluindo material de treinamento e manual do sistema. Foram obtidas evidências sobre a capacidade da ferramenta de coletar dados na *deep* e *dark* web, porém de dados abertos, sem potencial intrusivo.

I.4 - Funcionalidades aparentemente intrusivas: acesso a dados privados restritos por credenciais de usuários e georreferenciamento/geolocalização

Acesso a dados privados restritos por credenciais de usuários

65. O termo *Open Source Intelligence* (Osint), ou inteligência de fontes abertas na tradução para português, refere-se à inteligência derivada exclusivamente de informações disponíveis publicamente ou comercialmente que atende a prioridades, requisitos ou lacunas específicas de inteligência.

66. Segundo a Doutrina da Atividade de Inteligência, documento publicado pela ABIN e considerado, nos termos do Decreto 8.793/2016, um dos instrumentos essenciais da inteligência nacional, a Osint 'utiliza dados, informações e conhecimentos presentes em insumos disponíveis para qualquer pessoa, ainda que este acesso seja pago'. Assim, essas fontes incluem redes sociais abertas, notícias, publicações acadêmicas, relatórios públicos, entre outros dados que estão disponíveis publicamente ou que podem ser adquiridos comercialmente.

67. O objetivo da Osint é reunir dados que ajudem a preencher lacunas ou responder a perguntas específicas em investigações ou análises de inteligência, sem recorrer a informações sigilosas ou restritas. É amplamente utilizado em áreas como segurança cibernética, monitoramento de mídias e atividades governamentais.

68. Por sua vez, uma intrusão é considerada, segundo o *National Institute of Standards and Technology* (Nist) como 'um evento de segurança, ou uma combinação de múltiplos eventos de segurança, que constitui um incidente de segurança em que um intruso obtém, ou tenta obter, acesso a um sistema ou recurso de sistema sem ter autorização para fazê-lo'. Assim, uma intrusão é um

acesso (ou tentativa de acesso) não autorizado a um ativo por meio da exploração de uma vulnerabilidade.

69. Dessa forma, conceitualmente, a coleta de dados por meio de fontes abertas para posterior análise e processamento em informação e inteligência não se confunde com uma intrusão, uma vez que não utiliza mecanismos de invasão para acesso a dados sigilosos ou protegidos por algum mecanismo de autenticação (como *login* e senha).

70. Nesse contexto, a PRF informou, em resposta à equipe de fiscalização, que o Contrato 73/2018, tratava-se de aquisição de solução integrada de monitoramento de redes sociais, incluindo software e hardware para a coleta, transformação e análise de dados de diversas fontes da web para atender aos requisitos do Osint, englobando informações disponíveis na internet e suporte à *deep* web (peça 22, p. 3).

71. Posteriormente, foi firmado o Contrato 35/2021, que teve como objetivo dar continuidade às atividades realizadas por meio do sistema contratado anteriormente pelo Contrato 73/2018 e previa, em seu PB, a aquisição de sistema de investigação com capacidade de acessar dados obtidos de fontes abertas, conforme consta na descrição da solução de TIC (peça 23 p. 1):

2.2.2 A migração para o Sistema de Investigação Web - ORBIS, se faz necessário considerando o avanço tecnológico de diversas ferramentas utilizadas para a busca e coleta de dados em fontes abertas, bem como a crescente massa de dados disponível em ambiente web, sendo alguns pontos de fundamental importância para o desempenho das atividades de análise de inteligência pela PRF.

72. Além disso, no PB há a justificativa para a contratação (peça 23 p. 2) que cita que '3.1.1 A presente contratação visa otimizar o trabalho de inteligência policial, através do monitoramento de redes sociais e fontes abertas, possibilitando a análise de situações complexas em tempo real'.

73. A PRF também se manifestou sobre as finalidades da contratação, explicando que a aquisição do software de coleta de dados de fontes abertas visa otimizar o tempo dos analistas de inteligência, uma vez que, em um contexto de grande volume de informações disponíveis *online* e em constante expansão, a automação é essencial para a eficiência das operações de coleta de dados e produção de conhecimento de inteligência. Relatou, ainda, que as ferramentas aceleram a identificação e extração de informações relevantes, além de permitir a organização e filtragem automática dos dados, economizando tempo que seria gasto em tarefas manuais (peça 22, p. 3).

74. Assim, no PB e no contrato decorrente da licitação (peça 23, p. 24-45), foram definidos requisitos relacionados à aquisição de sistema de inteligência com foco em fontes abertas, de modo que não foram identificados nos artefatos de planejamento requisitos da contratação que fizessem menção a funcionalidades intrusivas da ferramenta.

75. Contudo, em seu voto (peça 50), o ministro relator Vital do Rêgo, apontou que o seguinte trecho extraído do PB (peça 23, p. 4) sugeriria um potencial intrusivo da ferramenta: '4.1.1.19. A solução deve acessar dados privados, ou seja, dados que são restritos por credenciais do usuário, como por exemplo no Facebook (para acessar os dados, o usuário precisa realizar o *login* no site para recuperar as informações com base no perfil)'.

76. Dessa forma, a equipe de fiscalização enviou ofício de requisição à PRF (peça 65, p. 3) com o objetivo de esclarecer quais outras fontes de dados privados a ferramenta seria capaz de acessar além do Facebook e se seria possível que a ferramenta acessasse, por exemplo, outras redes sociais, sistemas operacionais e aparelhos celulares.

77. Em resposta, a PRF comunicou que a solução foi desenvolvida especificamente para a coleta de dados de fontes abertas, isto é, informações disponíveis ao público (peça 68, p. 3). Assim, não se empregam técnicas intrusivas para obter acesso a dados privados. Nesse sentido, uma vez que plataformas como Facebook, Instagram e X (anteriormente conhecido como Twitter) requerem *login* para acesso, a solução não tem capacidade de acessar dados de perfis privados, podendo apenas acessar informações definidas como públicas.

78. A PRF esclareceu ainda que o item 4.1.1.19 do PB discute o conceito de 'dados privados' dentro do contexto de algumas plataformas que necessitam de *login* para acesso. Nesse sentido, a ferramenta

deve ser capaz de gerenciar essas credenciais para acessar plataformas que exigem *login*, sem que o analista de inteligência precise fazer cadastros nessas plataformas.

79. Foi enfatizado que as consultas de informações sobre pessoas por meio de números de telefone, sejam móveis ou fixos, baseiam-se unicamente em dados disponíveis na internet. A solução não utiliza técnicas intrusivas para acessar dispositivos móveis ou fixos, portanto, não acessa fontes de dados privados que demandem qualquer tipo de ação intrusiva (peça 68, p. 3).

80. Por fim, a PRF informou que as fontes de dados mais utilizadas que necessitam de práticas de *login* para acesso incluem Facebook, Instagram, X e LinkedIn (peça 68, p. 3-4) e que não é viável acessar informações definidas como restritas, a exemplo de contas de redes sociais com configurações de privacidade restritivas (peça 68, p. 6).

81. Assim, os dados privados mencionados no item 4.1.1.19 do PB referem-se aos dados disponíveis nas redes sociais que o usuário optou por tornar públicos. Para coletar essas informações públicas, é necessário criar na ferramenta Orbis um agente de coleta automatizado (robô) que possua um perfil na respectiva rede social e, dessa forma, para que o agente acesse essa rede social é necessário um *login* e senha. Portanto, essa abordagem não envolve o uso da ferramenta para acessar dados restritos ou sigilosos, nem para invadir e controlar sistemas operacionais ou dispositivos móveis, mas para o acesso dos agentes de coleta ao ambiente da rede social, de modo a coletar os dados abertos.

82. A PRF, em nova resposta à equipe de fiscalização, enfatizou mais uma vez que o uso do Orbis ocorre apenas em fontes de dados abertas relatando que: 'A utilização do sistema Orbis ocorre na coleta e análise de dados oriundos de fontes abertas, integrando-se como uma das etapas do conhecimento final a ser produzido em sistema próprio da atividade de inteligência da PRF.' (peça 81 p. 2).

83. Essa afirmação foi feita também em audiência pública realizada pelo Supremo Tribunal Federal em 11/6/2024 para ouvir representantes da sociedade e do governo no âmbito da arguição de descumprimento de preceito fundamental (ADPF) 1143, que aponta a ausência de atuação normativa do Congresso Nacional na regulação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal. Nesse evento, a PRF reafirmou que não adquiriu quaisquer ferramentas tratadas no âmbito dessa ação, ou seja, ferramentas com potencial intrusivo ou invasivo para obter informações sigilosas ou restritas.

84. Conforme relatado no parágrafo 23, a equipe de fiscalização realizou observação direta do funcionamento da ferramenta Orbis com a execução das funcionalidades do sistema por agentes da PRF. Foi solicitado à PRF que demonstrasse o fluxo de criação de um caso e de coleta de dados para verificar a existência de ações potencialmente intrusivas.

85. Inicialmente, a PRF fez uma demonstração e explanação sobre os agentes de coleta da plataforma, que são softwares que automatizam o processo de busca, extração e coleta de informações de fontes públicas e disponíveis na internet. Esses agentes são configurados para monitorar e rastrear uma variedade de fontes.

86. Assim, foi realizado o acesso à função 'Agents management' (peça 75, p. 5-6) demonstrando as fontes de dados, bem como os agentes de coleta disponíveis.

87. Segundo a PRF, tais agentes já vêm pré-configurados pela empresa fornecedora e, no momento da observação direta, estavam disponíveis agentes de coleta apenas para as fontes de dados *dark* web (via navegador Tor), YouTube e Google (peça 73, p. 1), devido ao encerramento do contrato e consequente não renovação dos agentes de coleta para as demais fontes (como Facebook e Instagram).

88. Verificou-se a possibilidade da criação de agentes de coleta para outras fontes de dados. Contudo, a PRF esclareceu que somente a empresa fornecedora tem acesso para criar os agentes de coleta e efetuar a inclusão ou alteração das fontes de coleta, mediante aditivo contratual (peça 73, p. 1).

89. Após a demonstração das fontes de dados, foi criada uma investigação teste (peça 75, p. 9-10) para a visualização do processo de coleta de dados no menu 'Investigation Dashboard'. A plataforma

permite vários tipos de coleta e, para cada um, deve-se inserir um termo (como palavra-chave ou URL) para a busca e selecionar as fontes, dentre as disponíveis para aquele tipo de coleta (peça 74, p. 1).

90. Importante destacar que foi demonstrado um caso real de uso da ferramenta e apresentado o conteúdo dos menus laterais. Nessa demonstração, bem como em todas as etapas anteriores da apresentação feita pela PRF, não foi possível identificar evidências de ação potencialmente intrusiva por meio de acessos indevidos a informações restritas ou sigilosas (peça 74, p. 13). Conforme relatado no parágrafo 23, a equipe de fiscalização conduziu a demonstração solicitando que os agentes da PRF apresentassem as informações requeridas por meio do uso do sistema.

91. Assim, após a realização de observação direta das funcionalidades e da análise dos documentos relacionados ao processo de contratação, como o PB e o contrato em si, bem como dos documentos referentes à execução contratual e dos materiais fornecidos pela empresa à PRF, incluindo material de treinamento e manual do sistema, não foram identificadas evidências que remetam a algum tipo de ação que possa ser considerada intrusiva no uso das funcionalidades do sistema. Foram obtidas evidências sobre a capacidade da ferramenta de realizar coletas de informações diversas, porém de dados abertos, sem potencial intrusivo.

Georreferenciamento e geolocalização

92. Segundo a Doutrina da Atividade de Inteligência[v], a inteligência geoespacial é definida como a 'classificação pela origem do dado da inteligência realizada com base em imagens e dados de geolocalização obtidos para descrever, avaliar e representar visualmente características físicas ou atividades geograficamente referenciadas'.

93. Por sua vez, o georreferenciamento é o processo de relacionar dados, como mapas ou imagens, a coordenadas de um sistema de coordenadas geográficas, como latitude e longitude. Esse processo é essencial para permitir que informações espaciais sejam precisas e possam ser interpretadas em relação à posição real no planeta.

94. Já a geolocalização refere-se à identificação da posição de um dispositivo ou pessoa, em tempo real ou não, por meio de sistemas como GPS, *wi-fi*, torres de celular, entre outros. Diferentemente do georreferenciamento, que é mais utilizado para mapear e associar dados a coordenadas, a geolocalização foca em determinar onde algo ou alguém está.

95. Nesse contexto, o PB da contratação previu que (peça 23, p. 5,7):

4.1.1.30. A solução deve suportar a capacidade de visualização georreferenciada de posts com esta informação.

[…]

4.1.1.67. A solução deve fornecer recursos de geolocalização como: ver a postagem na localização definida, filtrar por Área de interesse, definir novas solicitações de coleta usando Área de interesse.

96. Tais requisitos foram considerados pelo fiscal técnico do contrato como cumpridos, conforme apresentado em relatório de fiscalização técnica (peça 23, p. 176).

97. O manual da ferramenta apresenta algumas funcionalidades relativas ao uso da localização dos alvos como a possibilidade de visualização de mapa para mostrar as localizações geográficas das informações coletadas na investigação. Além disso, é possível definir 'cercas geográficas' ('*geo-fence*'), que são filtros para selecionar apenas os dados coletados que aparecem inseridos em certa delimitação geográfica, podendo indicar concentração de localizações de postagens, por exemplo (peça 71, p. 54).

98. O manual apresenta ainda que 'As informações de localização geográfica podem se originar do texto ou dos metadados da entidade.' (peça 71, p. 58). Assim, a ferramenta Orbis é capaz de fazer a geolocalização e o georreferenciamento a partir de posts em redes sociais utilizando a localidade indicada publicamente pela própria rede social ou pelo usuário; ou por meio da análise e do reconhecimento da localidade de uma imagem disponível publicamente.

99. Tal funcionalidade foi demonstrada à equipe de fiscalização durante observação direta, ocasião em foi apresentado um caso real de uso da geolocalização (peça 74, p. 2).

100. A PRF destacou que entre as principais fontes de dados utilizadas pelos seus analistas de inteligência no sistema Orbis estão o Facebook, Instagram e X (Twitter), onde se empregam dados de georreferenciamento. Esses dados podem ser baseados em postagens, quando disponíveis, em imagens, caso o local seja conhecido, ou em análises textuais, quando a localização é descrita nas postagens. Além disso, no caso do Youtube, a PRF utiliza dados de georreferenciamento que podem ser obtidos a partir de possíveis marcações feitas pelo usuário na publicação do vídeo (peça 68, p. 2-3).

101. Assim, após a realização de observação direta das funcionalidades e da análise dos documentos relacionados ao processo de contratação, como o PB e o contrato em si, bem como dos documentos referentes à execução contratual e dos materiais fornecidos pela empresa à PRF, incluindo material de treinamento e manual do sistema, não foram identificadas evidências que remetam a algum tipo de ação que possa ser considerada intrusiva no uso das funcionalidades de georreferenciamento e geolocalização. Foram obtidas evidências sobre a capacidade da ferramenta de realizar georreferenciamento e geolocalização, porém de dados abertos, sem potencial intrusivo.

I.5 - Recursos abordados no treinamento contratado

102. O objeto da contratação previa, além da contratação do sistema Orbis, a realização de treinamento oficial (peça 23, p. 1), sendo previsto no PB a realização de treinamentos para a operação da solução para até trinta pessoas, totalizando no mínimo sessenta horas-aula por turma. Esses treinamentos seriam destinados à formação de analistas operadores da solução em temas como produção de conhecimento, análises, relatórios, segurança da informação, entre outros aspectos relacionados à solução e aos equipamentos contratados.

103. A PRF comunicou que foram realizados dois treinamentos conforme o acordado, sendo o primeiro de 25 a 29 de outubro de 2021 e o segundo de 22 a 26 de novembro de 2021, capacitando um total de trinta Policiais Rodoviários Federais. Cada policial capacitado atuou como ponto focal para disseminar o conhecimento adquirido aos demais agentes envolvidos na atividade de inteligência nos seus estados de lotação. Foi destacado pela PRF que todos os participantes dos treinamentos são servidores policiais atuando na área de inteligência (peça 68, p. 2).

104. O material utilizado no treinamento foi enviado à equipe de fiscalização (peças 69 e 70) e verificou-se que as capacitações forneceram uma visão abrangente sobre o uso do sistema Orbis e técnicas de inteligência investigativa focadas na coleta de informações de fontes abertas (Osint).

105. O treinamento abordou aspectos como fundamentos da inteligência investigativa, conceito de Osint, uso do sistema ‘Webalert’, o ciclo de vida de uma investigação, o processo de coleta de dados (planejamento e registro), uso da funcionalidade ‘Discovery’, uso da operação assistida, geração de relatórios de inteligência, bem como outras funcionalidades do Orbis (peça 69).

106. Além disso, foi encaminhado material de treinamento complementar produzido pela contratante (peça 70), que aborda dicas para facilitar o uso da ferramenta pelos usuários. Nesse material há orientações sobre uso de operadores, ‘emojis’ e idiomas estrangeiros em buscas, orientações sobre análises de imagens de perfil, uso de células de agrupamento, uso das anotações e dos filtros da proximidade da relação entre os alvos, além de um guia de gestão de avatares.

107. Durante a observação direta realizada pela equipe de fiscalização, foi verificado que houve a criação de perfis específicos para o período de treinamento para cada usuário participante. Posteriormente, esses perfis tiveram seus usuários bloqueados e os respectivos acessos revogados (peça 72, p. 1).

108. Assim, conclui-se que os treinamentos realizados guardam relação com o objeto da contratação e foi demonstrada a necessidade de sua realização para o efetivo uso da ferramenta. Nesse sentido, foi identificada adequação em relação à realização dos treinamentos.

I.6 - Efetivo uso da ferramenta

109. A PRF informou que, de acordo com a DNISP e o Plano Nacional de Inteligência de Segurança Pública (PNI), o analista de inteligência é responsável por produzir conhecimento de inteligência tanto em resposta a um Pedido de Inteligência (PI) quanto por iniciativa própria (peça 81 p. 2).

110. O papel crucial do analista é fornecer conhecimento que apoie o processo decisório, definindo o perfil das ameaças e possibilitando a implementação de medidas preventivas e repressivas para identificar os envolvidos e diminuir sua capacidade de ação.

111. Um PI é um documento confidencial empregado para requisitar dados ou conhecimentos a órgãos afins e outras unidades de inteligência da PRF. Este documento é estruturado em três partes principais: aspectos conhecidos, que detalha os dados disponíveis sobre o tema para orientar a resposta do PI; aspectos solicitados, que lista os dados ou conhecimentos a serem adquiridos ou confirmados; e recomendações especiais, que fornece diretrizes sobre compartimentação, segurança, comunicações, prazos de resposta e outros aspectos relevantes para o trabalho (peça 81 p. 2).

112. Em resposta à equipe de fiscalização, a PRF enviou um exemplo de PI, que gerou uma demanda aos analistas de inteligência, solicitando informações que pudessem identificar pontos ou trechos próximos a rodovias federais que já foram alvos de ataques ou mais suscetíveis aos ataques a torres de distribuição de energia em determinados estados da federação (peça 81 p. 2).

113. Assim, esse exemplo de PI não fez menção explícita a um indivíduo, conforme relatado pela PRF que 'a atividade de inteligência não tem como foco o monitoramento de uma pessoa específica, e sim o contexto em que ela está inserida de acordo com a temática de ameaça' (peça 68, p. 5).

114. Durante a observação direta realizada pela equipe de fiscalização, a PRF apresentou alguns exemplos de PI e foi constatado na amostra analisada que, em alguns casos, foram solicitadas no PI informações relacionadas a determinados alvos específicos (como identificação do nome, CPF, endereço e redes sociais), porém conectadas a um contexto de monitoramento no qual o indivíduo estava inserido e compatíveis com as atribuições da PRF (como bloqueios de rodovia e organizações criminosas), não sendo, portanto, aleatórias ou direcionadas a atividades estranhas às legalmente atribuídas à PRF.

115. Nos relatórios de inteligência, que são gerados após a coleta e a análise de dados abertos, apresentados pela PRF durante a observação direta, foi constatado ainda que o analista de inteligência pode não se limitar a reportar informações apenas dos alvos apontados no PI, caso descubra novas relações relevantes entre os monitorados ou entre grupos diversos.

116. Em manifestação anterior, a PRF havia destacado a importância de reconhecer que, na maioria das vezes, os indícios preliminares de preparação para diversas atividades em estradas e rodovias federais podem ser identificados através da análise de dados disponíveis em grupos, canais e contas públicas em plataformas de mídias sociais. Essas informações são extremamente relevantes e devem ser valorizadas no contexto da produção de conhecimento de inteligência (peça 22, p. 4).

117. A PRF explicou, ainda, que o software adquirido é uma ferramenta de apoio na coleta e monitoramento de dados abertos disponíveis em várias plataformas de mídias sociais. Frequentemente, essas plataformas são palco de atos preparatórios e trocas de informações que podem fornecer subsídios aos analistas de inteligência. Esses dados coletados são essenciais para auxiliar os tomadores de decisão no planejamento e na execução de ações de segurança pública. O objetivo é antecipar, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que possam comprometer a ordem pública, a segurança das pessoas, o patrimônio, e a livre circulação em rodovias e estradas federais (peça 22, p. 5).

118. Importante ressaltar, que por tratar-se de coleta e análise de dados abertos, ou seja, que poderiam ser obtidos por qualquer pessoa, a ferramenta Orbis tem como uma das suas finalidades a otimização do tempo dos analistas de inteligência. A PRF destacou que, diante de um cenário onde a quantidade de informações disponíveis *online* é imensa e continua crescendo, a automação é fundamental para a eficiência na coleta de dados e na produção de conhecimento de inteligência.

119. As ferramentas de automação não só aceleram a identificação e extração de informações relevantes, mas também facilitam a organização e a filtragem automática dos dados, resultando em

uma economia de tempo que, de outra forma, seria gasto em tarefas manuais. Assim, os analistas podem concentrar seus esforços na análise dos dados coletados, tornando o processo de produção de conhecimento de inteligência mais rápido e eficaz (peça 22, p. 3).

120. Dessa forma, a coleta e a análise de dados abertos realizadas pelo Orbis poderiam ser feitas por um agente de inteligência sem apoio de qualquer outra ferramenta de inteligência, porém de forma manual, reduzindo sua eficiência e sua celeridade, aspectos fundamentais no contexto de produção de inteligência.

121. Nesse contexto, o uso do sistema Orbis é parte do processo de coleta e análise de dados de fontes abertas, integrando-se às etapas de produção do conhecimento final no sistema próprio da atividade de inteligência da PRF (peça 81 p. 2).

122. Cabe destacar que o Plano Estratégico 2023-2028 da PRF prevê como um dos seus objetivos estratégicos 'Otimizar o policiamento orientado por inteligência'. Assim, o uso do Orbis guarda relação direta com a estratégia institucional e com o cumprimento desse objetivo.

123. Nesse sentido, a partir da avaliação da metodologia adotada pela PRF para coleta e análise de dados e da avaliação de PI e de relatórios de inteligência gerados, não foram obtidas evidências do uso indevido da ferramenta com desvio de finalidade.

II - Risco de desvio de finalidade e controles do Orbis

124. O desvio de finalidade na utilização de um sistema de informação pode ser conceituado como a utilização da ferramenta tecnológica para propósitos diferentes daqueles para os quais foi originalmente projetado ou destinado, tanto por agentes com permissão concedida para o uso da ferramenta, quanto por terceiros que eventualmente consigam acessá-la indevidamente, sem a necessária permissão.

125. Portanto, no contexto do Orbis, buscou-se identificar quais controles são empregados pela PRF para mitigar o risco de utilização da ferramenta com propósito diverso do interesse da corporação, tanto por usuários com permissão de acesso ao sistema, quanto por usuários não autorizados.

126. Assim, para mitigar os riscos de desvio de finalidade na utilização da ferramenta, verificou-se a adoção dos seguintes controles por parte de PRF:

II.1 - Solução *on premises* (peças 78 e 79)

127. Manter os servidores e os dados fisicamente no *datacenter* da própria corporação (modelo *on premises*) oferece maior controle sobre a segurança, privacidade e integridade das informações.

128. Essa abordagem reduz a exposição a riscos externos, como violações de segurança em serviços de terceiros, e permite a implementação de políticas de segurança personalizadas, incluindo criptografia, controle de acesso e monitoramento físico do hardware.

129. A centralização dos dados críticos no próprio *datacenter* também facilita a conformidade com normas de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados), uma vez que a corporação tem controle direto sobre quem acessa as informações e onde elas estão armazenadas.

130. No âmbito do procedimento de observação direta, fez-se uma visita ao *datacenter* da PRF, restando verificada a presença física do equipamento que operacionaliza a plataforma Orbis, bem como os controles de acesso lógico ao servidor do Orbis e de perímetro (de acesso físico ao *datacenter*) implementados (peças 72, p. 2, 78 e 79).

II.2 - Política de concessão e revogação de acessos (peça 72, p. 1)

131. De acordo com a norma ABNT NBR ISO/IEC 27002, 'convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios'.

132. Assim, uma política eficaz de concessão e revogação de acessos é crucial para garantir a segurança e a integridade de sistemas.

133. Essa política estabelece critérios claros para a atribuição de permissões de acesso com base nas

funções e responsabilidades dos usuários, garantindo que apenas pessoas autorizadas possam acessar dados sensíveis ou realizar ações críticas.

134. Isso minimiza o risco de violações de segurança, acesso não autorizado ou uso indevido de informações estratégicas.

135. A revogação de acessos de forma tempestiva, especialmente quando um colaborador muda de função ou deixa a organização, é igualmente importante para prevenir o acesso indevido.

136. Além disso, a implementação de uma política bem definida atende a requisitos de conformidade com normas de proteção de dados, como a LGPD, e ajuda a mitigar o risco de ameaças internas e externas, promovendo um ambiente de segurança contínua e controlada.

137. Em resposta ao Ofício de Requisição 987/2024 - AudTI, foi relatado pela PRF (peça 68, p. 4-5) que a aprovação inicial para o acesso ao Orbis é realizada pelo chefe da unidade local de inteligência.

138. Esta etapa envolve uma avaliação criteriosa da necessidade de uso do sistema, baseada nas demandas locais. Após a indicação pelo chefe da unidade, o pedido de acesso é encaminhado ao Serviço de Inteligência Cibernética, acompanhado da anuência do responsável pela unidade local.

139. A concessão do acesso ao sistema é temporária, limitando-se ao período em que o usuário permanece ativo na atividade de inteligência. O procedimento para a revogação do acesso é iniciado automaticamente com o desligamento do agente de inteligência, conforme protocolos estabelecidos em um manual interno.

140. Este processo envolve a colaboração de diversas áreas da PRF, responsáveis por garantir a execução das medidas necessárias para o efetivo desligamento do agente, incluindo a revogação de acessos a sistemas restritos.

141. Também foi relatado que o sistema Orbis possuía, no momento da observação direta, um total de 286 usuários cadastrados. Destes, 32 tinham o acesso bloqueado devido ao desligamento da atividade de inteligência, enquanto 254 usuários mantinham o acesso ativo.

142. Entre os usuários ativos, três são servidores do Serviço de Inteligência Cibernética com perfil de administrador, e um usuário integra a equipe de suporte técnico da empresa responsável pela plataforma, encarregado de realizar correções e solucionar problemas.

143. Adicionalmente, foi mencionado que todos os usuários do sistema Orbis, sem exceção, assinam um Termo de Compromisso e Manutenção de Sigilo com a Polícia Rodoviária Federal.

144. Por fim, a PRF assevera que todos os usuários cadastrados no sistema são servidores policiais rodoviários federais expressamente designados para atuar na área de inteligência.

145. Sobre esse ponto convém destacar que, também em atendimento ao Ofício de Requisição 987/2024 - AudTI a PRF enviou lista de presença de treinamentos ministrados sobre o Orbis (peça 80).

146. A partir de consulta ao portal do Diário Oficial da União e em outros *sites* com informações de servidores públicos, verificou-se que todos os integrantes da lista de presença são ou já foram servidores policiais rodoviários federais (peça 86).

147. Além disso, no âmbito do procedimento de observação direta, foi relatado pela PRF que foram criados até então 286 usuários para a plataforma, incluindo usuários criados para fins de treinamento e usuários bloqueados (ou seja, que tiveram seu acesso revogado) (peça 72, p. 1).

148. Foi informado que cada regional da PRF possui cerca de 3 usuários habilitados e a sede possui usuários habilitados para a Coordenação de Contrainteligência, Coordenação de Análise de Inteligência, Coordenação de Gestão de Operações de Inteligência, Serviço de Inteligência Cibernética, Serviço de Soluções de Inteligência e Central Nacional de Inteligência. A área de Inteligência possui cerca de setecentos Policiais Rodoviários Federais alocados (ou seja, nem todos com acesso à plataforma Orbis) (peça 72, p. 1).

149. Por fim, verificou-se que o processo de concessão e revogação de acesso mencionado pela PRF

está efetivamente previsto no Manual de Procedimentos de Inteligência (MPI) - 006 - Recrutamento (peça 82), com disposição específica apontando para a necessidade de que seja assinado um termo de compromisso de manutenção de sigilo quando da admissão do novo servidor da Atividade de Inteligência (peça 82, p. 10 e 14), bem como de que sejam realizadas as exclusões dos acessos aos sistemas e redes sociais inerentes à Atividade de Inteligência (peça 82, p. 11).

II.3 - Credenciais de acesso (*login* e senha) e permissões distintas a usuários (peça 72, p. 1-2. peça 75, p. 2-4)

150. A implementação de credenciais de acesso (*login* e senha) e permissões distintas para usuários em um software é essencial para garantir a segurança e o controle adequado do sistema.

151. Credenciais de acesso servem como a primeira linha de defesa, assegurando que apenas usuários autorizados possam acessar o sistema, enquanto o uso de permissões diferenciadas garante que cada usuário tenha acesso apenas aos recursos necessários para desempenhar suas funções.

152. A definição de diferentes níveis de acesso é uma prática fundamental para mitigar riscos, como o acesso indevido a dados confidenciais ou a execução de ações críticas por usuários sem a devida autorização.

153. Isso também promove a integridade do sistema, impede o abuso de privilégios e facilita a conformidade com normas de proteção de dados, como a LGPD e outras normas de segurança da informação.

154. No âmbito do sistema Orbis, em resposta ao Ofício de Requisição 987/2024 - AudTI, a PRF relatou a existência de dois perfis: usuário comum e usuário administrador (peça 68, p. 4).

155. O usuário comum tem acesso às funções de coleta e análise de dados, enquanto o usuário administrador tem acesso a funcionalidades de configurações globais, de gerenciamento de usuários e de auditoria, além das funcionalidades habilitadas ao usuário comum.

156. Cada usuário tem permissão para visualizar apenas os casos que criou ou aqueles para os quais recebe permissões específicas de leitura ou escrita de outros usuários. Apenas os administradores têm a capacidade de visualizar todo o conteúdo coletado (peça 68, p. 7).

157. Além disso, para prevenir acesso indevido e tentativa de invasão ao sistema e outros incidentes de segurança da informação, a solução efetua o bloqueio de usuário após três tentativas de *login* com o uso de senha errada (peça 68, p. 7).

158. Ainda segundo a PRF (peça 68, p. 7), o procedimento de controle de uso indevido da ferramenta consiste, em caso de suspeita, na notificação imediata à Corregedoria Geral que é então envolvida para conduzir a apuração necessária.

159. Usuários com privilégios de administrador têm a capacidade de monitorar as ações dos demais usuários mediante notificação sobre uso suspeito da ferramenta, além de gerar relatórios detalhados das atividades realizadas no sistema.

160. Em esclarecimento adicional (peça 91, p. 2), a PRF explicou o conceito de 'uso suspeito da ferramenta', expondo que 'a Doutrina de Inteligência da PRF prima pelo uso rigorosamente alinhado aos princípios éticos e legais, garantindo que sua aplicação seja exclusivamente voltada à finalidade institucional considerando como uso suspeito qualquer manipulação ou aplicação que não esteja conforme a finalidade da ferramenta como fora demonstrado *in locu* durante a inspeção, a exemplo de a) Consultas pessoais; b) Uso para interesses políticos; c) Criação de dossiês.'.

161. Os *logs* de atividades são mantidos armazenados, sendo analisados quando provocados pela Corregedoria.

162. A PRF destaca, por fim, que esse procedimento ainda não foi formalizado.

163. A partir do exame do Manual do Usuário do Orbis (peça 71), restaram confirmadas as informações relatadas pela PRF acerca dos perfis de usuários do sistema e do bloqueio de usuário após tentativas de acesso com senha incorreta (peça 71, p. 69-71).

164. Além disso, por meio de observação direta, confirmou-se a exigência de *username* e respectiva senha para efetuar o *login* na plataforma, bem como que a plataforma não permite o acesso às funcionalidades caso seja inserida uma senha incorreta (peça 71, p. 1).

165. Ainda, criou-se um usuário para testes, sem perfil de administrador, tendo restado confirmado que o referido usuário, após seu *login*, não possui acesso à área de configurações da plataforma e só consegue acessar os casos cujo acesso foi concedido pelo administrador (peça 71, p. 1. Peça 75, p. 3-4).

166. Verificou-se que é possível criar grupos de usuários com os mesmos acessos, divididos apenas para organização dos casos. Confirmou-se que cada usuário só visualiza os casos produzidos pelos grupos aos quais pertence, bem como que o administrador pode visualizar todos os casos de todos os grupos (peça 71, p. 1; peça 75, p. 4).

167. Além disso, foi demonstrado que, na revogação, é efetuado o bloqueio do usuário (não a sua exclusão, embora seja possível), a partir da inserção incorreta de sua senha por três vezes na tela de *login* da plataforma (o Orbis não possui uma funcionalidade de bloqueio direto de usuários por parte do administrador) (peça 72, p. 2).

II.4 - Rede virtual privada (peça 72, p. 1. Peça 75, p. 1-2)

168. A VPN (Virtual Private Network) é uma tecnologia que cria uma conexão segura e criptografada entre o dispositivo do usuário e a internet.

169. A VPN atua como um túnel protegido, permitindo que os dados trafeguem de maneira privada e segura, mesmo quando o usuário está conectado a redes públicas, como Wi-Fi.

170. Ela é amplamente utilizada para proteger informações sensíveis, garantir a privacidade *online* e permitir o acesso a redes corporativas de forma segura por meio de uma rede pública.

171. No âmbito da PRF (peça 68, p. 7), em resposta ao Ofício de Requisição 987/2024 - AudTI a corporação informou a utilização de VPN para acessar a plataforma.

172. Além disso, por meio de observação direta, verificou-se que é utilizada a ferramenta FortiClient VPN para acessar a plataforma (peça 72, p. 1. Peça 75, p. 1-2).

173. Com efeito, constatou-se que, para acessar a plataforma por meio do roteamento de rede 4G/5G de telefonia celular ou a partir da rede WiFi interna da PRF, se faz necessária a utilização daquela ferramenta de VPN (peça 72, p. 1).

174. Também foi realizado o teste de conexão ao sistema Orbis via rede interna cabeada da PRF, tendo restado verificado que não foi possível estabelecer conexão com a plataforma nem por meio da ferramenta de VPN tampouco pela inserção direta do endereço IP do Orbis diretamente no navegador (peça 74, p. 3).

II.5 - *Firewall* (peça 72, p. 2. Peça 78, p. 4)

175. Um *firewall* é um sistema de segurança que monitora e controla o tráfego de rede, filtrando pacotes de dados com base em regras de segurança predefinidas.

176. Ele atua como uma barreira entre redes internas confiáveis e redes externas, como a internet, com o objetivo de bloquear tentativas de acessos não autorizados e proteger os sistemas contra ameaças, como ataques cibernéticos.

177. *Firewalls* podem ser implementados como hardware, software ou uma combinação de ambos, e são amplamente utilizados para garantir a segurança de redes corporativas e pessoais.

178. Um *firewall* trabalha analisando o tráfego de entrada e saída da rede e comparando-o com um conjunto de regras definidas, permitindo ou bloqueando pacotes de dados de acordo com essas regras.

179. Isso protege contra invasões e acessos indesejados, enquanto permite o tráfego legítimo.

180. No âmbito da PRF (peça 68, p. 7), em resposta ao Ofício de Requisição 987/2024 - AudTI foi informado que a corporação utiliza *firewall* com regras restritivas para proteger o acesso ao Orbis.

181. Além disso, no âmbito do procedimento de observação direta, restou verificada a presença física do equipamento de firewall Fortinet FortiGate na arquitetura da rede que contempla o sistema Orbis (peça 78, p. 4-5. Peça 79, p. 1-2).

II.6 - Segmentação de redes locais virtuais (peça 72, p. 2. Peça 77. Peça 78, p. 5-6)

182. A segmentação de redes locais virtuais (*virtual local area networks* - VLANs) na arquitetura de um software desempenha um papel crucial na segurança e no gerenciamento eficiente da rede.

183. Ao dividir uma rede física em várias sub-redes lógicas (VLANs), é possível isolar diferentes grupos de usuários ou dispositivos, limitando a propagação de tráfego indesejado e vulnerabilidades de segurança. Essa estratégia minimiza o risco de ataques laterais, em que invasores podem se mover lateralmente dentro da rede após comprometer um ponto específico.

184. Além disso, a segmentação por VLANs facilita o gerenciamento da rede, permitindo que administradores apliquem políticas específicas de segurança, controle de acesso e qualidade de serviço (QoS) a diferentes grupos, o que é particularmente importante em ambientes que hospedam sistemas críticos ou informações sensíveis.

185. Ao controlar o fluxo de tráfego e restringir o acesso com base nas funções e necessidades dos usuários, VLANs contribuem significativamente para a segurança e o desempenho do software auditado.

186. No âmbito da PRF (peça 68, p. 7), em resposta ao Ofício de Requisição 987/2024 - AudTI, foi informado que a corporação utiliza arquitetura de rede separada em VLANs segmentadas.

187. Além disso, no âmbito do procedimento de observação direta, restou verificada a segmentação em VLANs exposta no aplicativo de gerência do *firewall* aplicado à rede do sistema Orbis (peça 78, p. 5).

188. Por fim, a PRF disponibilizou o mapa de arquitetura geral de rede da plataforma Orbis, bem como a lista de IPs e VLANs, evidenciando a implementação da segmentação em VLANs bem distribuídas (peças 76 e 77).

II.7 - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (peça 72, p. 2)

189. Uma equipe de tratamento e resposta de redes computacionais, frequentemente denominada como CSIRT (*Computer Security Incident Response Team*), é essencial para a segurança de uma organização, pois atua na detecção, análise e resposta a incidentes de segurança, como ataques cibernéticos, violações de dados e outros incidentes de redes.

190. Essa equipe é responsável por adotar ações rápidas e coordenadas para mitigar ameaças e restaurar as operações normais da rede, minimizando danos, custos e interrupções aos negócios.

191. A presença de uma equipe especializada é fundamental para estabelecer processos claros de prevenção e resposta, além de assegurar conformidade com padrões de segurança e regulamentações legais, como a LGPD.

192. Uma CSIRT bem treinada e preparada permite uma abordagem proativa na gestão de riscos, ajudando a prevenir ataques futuros e garantindo uma recuperação eficiente e eficaz de incidentes.

193. No âmbito da PRF (peça 68, p. 7), em resposta ao Ofício de Requisição 987/2024 - AudTI, foi relatada a existência da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (Etri), regulamentada pela Instrução Normativa 45, de 22 de junho de 2021, da PRF (IN - PRF 45/2021) e designada pela Portaria 1, de 14 de fevereiro de 2023, também da PRF.

194. Importa mencionar que, durante o procedimento de observação direta, foi relatado pela PRF que nunca fora detectada uma tentativa de acesso indevido à plataforma Orbis (peça 72, p. 2).

195. Verificou-se que a mencionada Instrução Normativa trata, com efeito, da Política de Segurança da Informação da PRF (Posin), a qual detalha a composição e as atribuições da Etri nos seguintes termos (peça 84, p. 15-16):

Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETRI

Art. 15. A ETRI será formada por integrantes da Diretoria de Tecnologia da Informação e Comunicação (DTIC) e da Diretoria de Inteligência (DINT), ou suas congêneres, sendo composta por dois representantes indicados de cada unidade a seguir:

I - Área de Contrainteligência;

II - Área de Infraestrutura e Aplicações; e

III - Área de Integração, Segurança e Ciência de Dados.

Parágrafo único. Os representantes da equipe e seus suplentes serão designados mediante ato conjunto do Diretor de Tecnologia da Informação e Comunicação e do Diretor de Inteligência, respectivamente.

Art. 16. Compete à ETRI:

I - receber, analisar e responder de forma tempestiva às notificações relacionadas a problemas e ou incidentes de segurança em redes computacionais da PRF;

II - comunicar sobre a ocorrência de todos os incidentes de segurança da informação;

III - gerar estatísticas sobre incidentes de segurança da informação;

IV - trabalhar em conjunto com outras equipes;

V - fazer gestão de riscos de segurança da informação;

VI - apoiar na definição de políticas e normas de segurança da informação no âmbito da PRF;

VII - realizar monitoramentos visando a prevenção de atividade maliciosa contra os ativos institucionais de informação;

VIII - desenvolver e melhorar soluções de segurança, com análise preventiva dos equipamentos e de sistemas de redes e internet;

IX - ajudar na disseminação da cultura de segurança da informação no âmbito da PRF;

X - investigar as causas dos incidentes no ambiente computacional; e

XI - elaborar e implementar o plano de resposta a incidentes de segurança da informação.

Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETRI-(UF)

Art. 17. A ETRI das unidades desconcentradas será formada por integrantes da área de Tecnologia da Informação e Comunicação e da área de Inteligência, sendo composta por um representante indicado de cada unidade e substitutos.

Parágrafo único. Os representantes da equipe e seus suplentes serão designados mediante ato do Superintendente Regional e terão as mesmas competências da ETRI nacional, porém relacionadas aos eventos locais.

196. Atualmente, os componentes da Etri estão designados na Portaria DTIC/PRF 1, de 14 de fevereiro de 2023 (peça 83).

II.8 - Registros de uso (*logs*): armazenamento e política de gestão (peça 73, p. 2)

197. O armazenamento de *logs* em sistemas de inteligência é essencial para garantir a segurança, conformidade e integridade operacional. *Logs* são registros detalhados de atividades que ocorrem no sistema, incluindo acesso de usuários, eventos de rede e operações realizadas.

198. Manter esses registros permite detectar, analisar e responder a incidentes de segurança, fornecer evidências para auditorias e garantir a conformidade com regulamentos de proteção de dados.

199. A auditabilidade dos *logs* é igualmente importante, pois assegura que as informações armazenadas sejam precisas, completas e imutáveis.

200. A capacidade de revisar e auditar os *logs* de forma eficiente ajuda a identificar padrões de

comportamento, rastrear alterações não autorizadas e fornecer transparência nas operações do sistema.

201. Isso possibilita ações corretivas imediatas e a criação de políticas de segurança mais robustas para proteger os dados e recursos críticos da organização.

202. No âmbito da PRF (peça 68, p. 7), em resposta ao Ofício de Requisição 987/2024 - AudTI, foi relatado que foi publicada em 29 de maio de 2024, pela Diretoria de Tecnologia da Informação e Comunicação (DTIC) em conjunto com as demais diretorias, a Instrução Normativa - PRF 130, de 29/5/2024, que institui a Política de Gestão de Registros (*logs*) de Auditoria no âmbito da Polícia Rodoviária Federal (PGRA/PRF).

203. O referido normativo institui prazo de 120 dias a partir de sua publicação para os devidos ajustes internos. Sendo assim, os dados do sistema Orbis/Webint estão atualmente armazenados em servidores específicos da PRF, aguardando os devidos ajustes em relação a nova norma.

204. A PRF dá conta, ainda, de que o sistema possui um módulo de auditoria, onde somente usuários com credenciais de administrador possuem acesso (peça 68, p. 8).

205. O módulo de *logs* registra os seguintes dados: Data; Nome do Usuário; Primeiro Nome; Último Nome; E-mail; *User Group*; Atividade; Tipo; Nome do caso; ID do caso; ID do objeto; Notas; ID do sistema; Endereço IP.

206. A partir do exame do Manual do Usuário do Orbis (peça 71), restou confirmada a existência da funcionalidade que permite a auditoria dos *logs* do sistema (peça 71, p. 83-84).

207. Além disso, no âmbito do procedimento de observação direta, restou confirmada a presença da funcionalidade de auditoria, que exibe os registros de atividades realizadas pelos usuários (*logs*) (peça 73, p. 2; peça 75, p. 7-8).

208. Convém destacar, ainda, que a recente PGRA/PRF prevê premissas e responsabilidades pela gestão dos *logs*, bem como os requisitos mínimos para o registro de eventos, além de disposições sobre coleta, armazenamento, uso e exclusão dos *logs* (peça 85).

209. Por fim, é importante mencionar que o art. 19, *caput*, da PGRA/PRF prevê que ‘os registros de eventos devem ser armazenados por um período mínimo de 2 (dois) anos, sem prejuízo de outros prazos previstos em referências legais e normativas específicas’ (peça 85, p. 4).

210. Em que pese ter sido verificado que o Orbis mantém armazenado o histórico de *logs* de até um ano antes da data da consulta (peça 73, p. 2), o fim da vigência da contratação ocorreu anteriormente à instituição da PGRA/PRF, não havendo de se falar em impropriedade, portanto.

II.9 - Análise sobre a suficiência dos controles internos

211. O item 9.1 do Acórdão 1.228/2024-TCU-Plenário determina que a unidade técnica efetue análise sobre a suficiência dos controles internos e da segurança da informação empregados pela PRF para mitigar os riscos de desvio de finalidade na utilização do Orbis.

212. Como se sabe, a gestão de riscos é um processo contínuo de identificação, avaliação, mitigação e monitoramento de riscos, visando reduzi-los a um nível aceitável, mas reconhecendo que a eliminação total do risco é geralmente impraticável, em função dos custos envolvidos, a não ser que a organização opte por evitar ou transferir o risco.

213. Em todo caso, em que pese terem sido verificados uma série de controles que têm o condão de mitigar o risco de desvio de finalidade na utilização da ferramenta sob análise, entende-se que ainda há espaço para o aperfeiçoamento desses controles por meio da realização de análises dos registros de uso (*logs*) do Orbis.

214. Com efeito, trata-se de medida que já foi diligentemente iniciada pela PRF com a recente instituição da PGRA/PRF por meio da Instrução Normativa 130, de maio de 2024, especialmente em seu art. 27, o qual dispõe que ‘análises de logs de auditoria devem ser realizadas pelo menos 2 (duas) vezes ao ano para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial’.

215. É preciso, porém, que a periodicidade da auditoria preconizada no dispositivo acima seja claramente definida para o caso do Orbis, para que haja o efetivo cumprimento de seu comando, inclusive em razão de nunca ter sido realizado um trabalho de auditoria para analisar os *logs* com o intuito de identificar desvio de finalidade na utilização da ferramenta (peça 73, p. 2).

216. Além de facilitar o planejamento da auditoria, a definição de uma periodicidade evita que cada auditoria ocorra injustificadamente muito próxima uma da outra, deixando um período extenso do ano sem passar por uma fiscalização.

217. Assim, a critério da PRF, por exemplo, pode ser definida uma periodicidade semestral, quadrimestral, trimestral etc. para a realização da auditoria dos *logs* prevista no art. 27 da PGRA.

218. Além dessa auditoria periódica, a implementação de um procedimento formal de monitoramento contínuo para detectar em tempo real (ou com pouco atraso) o uso do sistema com potencial desvio de finalidade poderia figurar, em tese, como um controle a ser adotado pela PRF, evitando que potenciais desvios de finalidade sejam detectados apenas nos trabalhos de auditoria periódicos.

219. Sobre tal aspecto, atualmente, a PRF conta apenas com um procedimento informal de controle de uso indevido da ferramenta, que consiste em notificar a Corregedoria Geral quando da detecção da irregularidade (parágrafos 156 a 159).

220. O fato de o procedimento não ser formalizado traz um risco, pois o procedimento pode ser interrompido a qualquer momento a depender de mudanças no comando da PRF, ou com a saída dos agentes que atualmente executam tal procedimento.

221. Em outras palavras, a formalização permite que o conhecimento sobre o procedimento seja documentado e preservado, facilitando a continuidade operacional e a transmissão de conhecimento, independentemente das mudanças de pessoal.

222. Um outro controle possível, também em tese, seria a previsão de uma auditoria periódica dos *logs* do Orbis a ser realizada por uma instância externa à Área de Inteligência, que teria mais isenção para efetuar as análises dos registros de uso do sistema.

223. Obviamente, a viabilidade dos controles adicionais acima sugeridos depende de análise da PRF quanto à conveniência e à oportunidade de sua adoção, em razão dos custos envolvidos e dos eventuais impactos no devido andamento das atividades de inteligência.

224. Vale destacar que a PRF relatou que está em andamento a construção de uma política de atuação voltada para a coleta e análise de dados provenientes de fontes abertas, bem como de um manual de procedimentos para utilização de soluções de inteligência de fontes abertas (peça 68, p. 6).

225. Portanto, entende-se pertinente recomendar à unidade jurisdicionada, com o fito de mitigar o risco de desvio de finalidade na utilização do sistema Orbis, que inclua, na referida política, previsões relativas à definição da periodicidade da auditoria de *logs* prevista no art. 27 da PGRA.

ANÁLISE DOS COMENTÁRIOS DOS GESTORES

226. De acordo com o procedimento previsto no art. 14, § 2º, II da Resolução - TCU 315/2020, foi dada a oportunidade aos gestores de se manifestarem sobre a recomendação sugerida pela equipe de fiscalização na reunião de encerramento do trabalho, realizada em 21/11/2024 na sede da PRF.

227. A PRF informou que os gestores da Diretoria de Inteligência concordaram com a recomendação preliminar feita pela equipe de auditoria (peça 89) e destacaram a importância de realizar auditorias regulares de *logs* para melhorar os controles internos e reduzir riscos, o que ajudará na governança e na eficiência das ferramentas de inteligência.

228. Além disso, a PRF enfatizou que essa avaliação é crucial para melhorar as contratações com a empresa Cognyte Brasil S.A e afirmou que o processo de fiscalização é essencial para corrigir problemas e planejar futuras aquisições, 'visando ao desenvolvimento de ferramentas confiáveis que subsidiem o processo decisório estratégico da Alta Gestão'.

229. Por fim, a PRF informou que 'as ações necessárias já estão em curso, conforme acordado na mencionada reunião, e nosso compromisso é de concluir a implementação das medidas no prazo

estipulado pelo TCU.'.

230. Portanto, não havendo objeção por parte da PRF acerca da recomendação preliminar, propõe-se sua manutenção.

CONCLUSÃO

231. Conforme o planejamento da Inspeção, a equipe de fiscalização realizou observação direta sobre todas as funcionalidades da ferramenta Orbis, nas instalações da sede da PRF. A ferramenta extrai informações da internet, a partir de fontes abertas, e disponibiliza recursos para investigar e analisar dados com o objetivo de produzir conhecimentos de inteligência.

232. Em relação à pesquisa em *deep* web e em *dark* web, foram obtidas evidências sobre a capacidade da ferramenta de coletar dados nessas camadas da internet, porém apenas dados abertos, sem potencial intrusivo.

233. O Projeto Básico aparentemente sugere um potencial intrusivo da ferramenta quando prevê que ela deve acessar dados privados, ou seja, dados que são restritos por credenciais do usuário, como por exemplo no Facebook (para acessar os dados, o usuário precisa realizar o *login* no *site* para recuperar as informações com base no perfil). Porém, o que ocorre é que algumas plataformas, como Facebook, Instagram e X (anteriormente conhecido como Twitter), requerem *login* para acesso, e a Orbis deve ser capaz acessar essas plataformas, sem que o analista de inteligência precise fazer um cadastro. Isso, entretanto, não envolve o uso da ferramenta para acessar dados restritos ou sigilosos, mas apenas os dados que o usuário optou por tornar públicos para os demais usuários da rede social. Portanto, não se trata de uma intrusão.

234. Ademais, constatou-se que a ferramenta Orbis é capaz de realizar geolocalização e georreferenciamento a partir de *posts* em redes sociais utilizando a localidade indicada publicamente pela própria rede social ou pelo usuário; ou por meio da análise e do reconhecimento da localidade de uma imagem disponível publicamente. Assim como nos demais casos, a capacidade da ferramenta de realizar georreferenciamento e geolocalização se restringe a dados abertos, sem potencial intrusivo.

235. Além disso, foram capacitados trinta Policiais Rodoviários Federais, e cada um deles atuou como ponto focal para disseminar o conhecimento adquirido aos demais agentes envolvidos na atividade de inteligência em seus estados de lotação. Observou-se que todos os participantes dos treinamentos são servidores policiais atuando na área de inteligência.

236. Sobre o efetivo uso da ferramenta pela PRF, muitas vezes, os indícios preliminares de preparação para diversas atividades em estradas e rodovias federais podem ser identificados por meio da análise de dados disponíveis em grupos, canais e contas públicas em plataformas de mídias sociais, e essas informações são extremamente relevantes no contexto da produção de conhecimento de inteligência. O objetivo é antecipar, prevenir, neutralizar e reprimir atos criminosos de qualquer natureza que possam comprometer a ordem pública, a segurança das pessoas, o patrimônio, e a livre circulação em rodovias e estradas federais.

237. Durante a observação direta, a PRF apresentou alguns exemplos de Pedido de Inteligência (PI) e foi constatado na amostra analisada que, em alguns casos, foram solicitadas no PI informações relacionadas a determinados alvos específicos (como identificação do nome, CPF, endereço e redes sociais), porém conectadas a um contexto de monitoramento no qual o indivíduo estava inserido e compatíveis com as atribuições da PRF (como bloqueios de rodovia e organizações criminosas), não sendo portanto aleatórias ou direcionadas a atividades estranhas às legalmente atribuídas à PRF.

238. Importante ressaltar que, por tratar-se de coleta e análise de dados abertos, ou seja, que poderiam ser obtidos por qualquer pessoa, a ferramenta Orbis tem como uma das suas finalidades a otimização do tempo dos analistas de inteligência. A PRF destacou que, diante de um cenário onde a quantidade de informações disponíveis *online* é imensa e continua crescendo, a automação é fundamental para a eficiência na coleta de dados e na produção de conhecimento de inteligência. Ressalte-se que não foram encontradas evidências de uso indevido da ferramenta Orbis pela PRF.

239. Em relação ao risco de desvio de finalidade no uso da Orbis, identificou-se a existência de

diversos controles empregados pela PRF para mitigar o risco de utilização da ferramenta com propósito diverso do interesse da corporação, tanto por usuários com permissão de acesso ao sistema, quanto por usuários não autorizados, entre os quais se destacam a manutenção dos servidores e dados fisicamente no *datacenter* da própria corporação; a existência de política de concessão e revogação de acessos; criação de grupos de usuários em que cada usuário só visualiza os casos produzidos pelos grupos aos quais pertence; utilização de VPN para acessar a plataforma; utilização de firewall com regras restritivas para proteger o acesso ao Orbis; segmentação de redes locais virtuais (*virtual local area networks* - VLANs) na arquitetura do software; existência de Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (Etri), entre outros.

240. Além disso, há mecanismos de auditabilidade e responsabilização quanto ao uso da ferramenta. O sistema possui um módulo de auditoria, onde somente usuários com credenciais de administrador possuem acesso. Esses usuários têm a capacidade de monitorar as ações dos demais usuários mediante notificação sobre uso suspeito da ferramenta, além de gerar relatórios detalhados das atividades realizadas no sistema. Também há um módulo de *logs*, que registra diversos tipos de dados dos usuários e das atividades do sistema.

241. Por fim, sobre a determinação do Acórdão 1.228/2024-TCU-Plenário para que a unidade técnica efetuasse análise sobre a suficiência dos controles internos e da segurança da informação empregados pela PRF para mitigar os riscos de desvio de finalidade na utilização do Orbis, importa ressaltar que a gestão de riscos é um processo contínuo de identificação, avaliação, mitigação e monitoramento de riscos, visando reduzi-los a um nível aceitável, mas reconhecendo que a eliminação total do risco é geralmente impraticável.

242. Nesse sentido, a avaliação realizada pela equipe de inspeção trouxe uma nova percepção de risco mais baixo de desvio de finalidade do uso da ferramenta Orbis em relação ao que foi inicialmente suscitado no âmbito da SCN, tendo em vista que ela não dispõe de potencial intrusivo por trabalhar apenas com a coleta e com o processamento de dados provenientes de fontes abertas.

243. Assim, em que pese terem sido verificados uma série de controles que têm o condão de mitigar o risco de desvio de finalidade na utilização da ferramenta sob análise, entende-se que ainda há espaço para o aperfeiçoamento desses controles por meio da realização de análises dos registros de uso (*logs*) do Orbis, medida que já foi diligentemente iniciada pela PRF com a recente instituição da PGRA por meio da Instrução Normativa 130. É preciso, porém, que a periodicidade da auditoria preconizada no dispositivo acima seja claramente definida para o caso do Orbis.

244. Também seria recomendável a implementação de um procedimento formal de monitoramento contínuo para detectar em tempo real (ou com pouco atraso) o uso do sistema com potencial desvio de finalidade. Um outro controle possível, também em tese, seria a previsão de uma auditoria periódica dos *logs* do Orbis a ser realizada por uma instância externa à Área de Inteligência, que teria mais isenção para efetuar as análises dos registros de uso do sistema.

245. Por fim, considerando a possibilidade de construção participativa das deliberações deste Tribunal, nos termos do art. 14 da Resolução-TCU 315/2020, bem como o previsto nas Normas de Auditoria (NAT) aprovadas pela Portaria-TCU 280/2010, referente aos comentários dos gestores, foi oportunizado aos gestores da PRF, em reunião de encerramento realizada em 21/11/2024, a apresentação de comentários quanto às consequências práticas da implementação das medidas aventadas no parágrafo 239.3, bem como eventuais alternativas à recomendação. Os comentários foram registrados e levados em consideração na proposta final de recomendação endereçada à PRF.

PROPOSTA DE ENCAMINHAMENTO

246. Em virtude do exposto, encaminhe-se os autos ao gabinete do relator Ministro Vital do Rêgo com as seguintes propostas:

246.1. **encaminhar** cópia da decisão que vier a ser adotada ao presidente da Comissão Parlamentar Mista de Inquérito dos Atos de 8 de janeiro, mediante aviso do Presidente do Tribunal, nos termos do art. 19 da Resolução - TCU 215/2008;

246.2. **considerar** a presente solicitação **integralmente atendida**, nos termos do art. 17, II, da

Resolução - TCU 215/2008; e

246.3. **recomendar** à Polícia Rodoviária Federal, com fundamento no art. 11 da Resolução - TCU 315/2020, com o fito de mitigar o risco de desvio de finalidade na utilização do sistema Orbis (ou do que vier a sucedê-lo), que inclua na política em construção para regulamentar a coleta e a análise de dados provenientes de fontes abertas previsões relativas (i) à definição da periodicidade da auditoria de *logs* prevista no art. 27 da Política de Gestão de Registros (*logs*) de Auditoria instituída pela Instrução Normativa 130, de maio de 2024;

246.4. **fazer constar**, na ata da sessão em que estes autos forem apreciados, nos termos do art. 8º da Resolução - TCU 315/2020, comunicação do Relator ao colegiado no sentido de não ser monitorada pela unidade técnica a recomendação contida no parágrafo 246.3, por ser uma oportunidade de melhoria pontual em um controle já implementado pela PRF (auditoria de *logs*); e

246.5. **arquivar** o presente processo, nos termos dos arts. 169, II, do Regimento Interno/TCU e 14, IV, da Resolução - TCU 215/2008."

É o relatório.

VOTO

Trata-se de Solicitação Congresso Nacional, encaminhada pela Comissão Parlamentar Mista de Inquérito (CPMI) dos Atos de 8 de janeiro, de autoria da Senadora Eliziane Gama, na qual requer a fiscalização das contratações realizadas pela Polícia Rodoviária Federal (PRF) com a empresa Cognyte Brasil S.A. de 2018 até a presente data.

2. O objetivo principal foi verificar a regularidade dessas contratações e o uso das tecnologias adquiridas, considerando as competências legais da PRF, devendo ser respondidas as seguintes questões:

a) O objeto de algum contrato refere-se à aquisição de softwares de rastreamento, identificação e interceptação de números de aparelhos celulares de qualquer espécie ou de software de solução de monitoramento de redes sociais? Se sim, quais foram os softwares adquiridos?

b) Qual finalidade da utilização de tecnologias de interceptação de aparelhos telefônicos e de monitoramento de redes sociais, considerando que a PRF não detém competência legal para realizar investigações como a polícia judiciária?

c) Considerando que houve pagamentos à empresa por meio da Ação Orçamentária POLICIAMENTO OSTENSIVO NAS RODOVIAS E ESTRADAS FEDERAIS, como os sistemas da Cognyte são utilizados nas ações de policiamento ostensivo das rodovias federais?

d) Considerando que houve pagamentos à referida empresa por meio da Ação Orçamentária POLICIAMENTO, FISCALIZAÇÃO, COMBATE À CRIMINALIDADE E CORRUPÇÃO, como os sistemas da Cognyte são usados nas ações de policiamento, fiscalização, combate à criminalidade e à corrupção?

e) Haveria desvio de finalidade nas contratações da Cognyte pela PRF?

3. Registro que o presente processo teve sua primeira instrução a cargo da Unidade de Auditoria Especializada em Contratações (AudContratações), cujo auditor responsável identificou dois contratos principais: o Contrato 73/2018, relacionado à aquisição de uma solução integrada para monitoramento, e o Contrato 35/2021, destinado à manutenção e migração tecnológica para o sistema Orbis.

4. Após essa identificação, o então Relator do feito, Min. Vital do Rêgo, autorizou diligências junto à PRF para obter informações sobre os contratos e sua execução. Documentos como projetos básicos, notas fiscais e registros financeiros foram solicitados e analisados pela referida unidade instrutora, em conjunto com a então Unidade de Auditoria Especializada em Governança e Inovação (AudGovernança).

5. As análises preliminares da unidades não identificaram indícios de ilegalidades nos contratos, mas apontaram a necessidade de esclarecimentos adicionais quanto à aplicação prática do sistema Orbis nas atividades operacionais da PRF.

6. Dessa forma, o Plenário, por meio do Acórdão 1.228/2024-TCU-Plenário, conheceu da presente Solicitação e determinou a realização de inspeção *in loco* na PRF pela Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI), para apurar o efetivo uso da ferramenta Orbis e avaliar a adequação dos controles internos de segurança da informação, bem como eventuais riscos de desvio de finalidade.

7. A inspeção, realizada entre agosto e outubro de 2024, envolveu visitas à sede da PRF e procedimentos de observação direta das funcionalidades da ferramenta. A unidade verificou que o software é utilizado para atividades de inteligência baseadas em fontes abertas, isto é, disponíveis ao público (OSINT - *Open Source Intelligence*), sem potencial intrusivo, com foco na produção de

inteligência voltada ao planejamento estratégico do policiamento ostensivo em rodovias federais e alinhadas às atribuições da PRF como órgão integrante do Sistema Brasileiro de Inteligência (Sisbin).

8. Não foram constatados indícios de desvio de finalidade ou práticas incompatíveis com as atribuições da PRF, mas identificaram-se oportunidades de melhoria nos controles internos e na política de segurança da informação, relacionados ao uso do sistema.

9. A análise dos comentários dos gestores reforçou que a ferramenta Orbis é empregada exclusivamente para subsidiar atividades de inteligência policial, com foco na coleta de dados de fontes abertas, em consonância com as atribuições da PRF. Os gestores também forneceram informações sobre os procedimentos adotados para garantir a conformidade com as normas legais e técnicas, além de destacar os benefícios operacionais da ferramenta.

10. Paralelamente, a PRF trabalha na construção de uma política de atuação para coleta e análise de dados de fontes abertas e um manual de procedimentos para o uso de ferramentas de inteligência.

11. Isso posto, a AudTI concluiu pela regularidade das contratações analisadas e pela adequação do uso do sistema Orbis às competências da PRF, não havendo evidências de práticas incompatíveis com os normativos vigentes.

12. Assim, propõe considerar a SCN integralmente atendida, bem como recomendar à PRF que inclua, na política em construção para regulamentar a coleta e a análise de dados provenientes de fontes abertas, previsões relativas à definição da periodicidade da auditoria de *logs* prevista no art. 27 da Política de Gestão de Registros (*logs*) de Auditoria, instituída pela Instrução Normativa PRF 130, de maio de 2024.

13. Manifesto minha integral concordância com o encaminhamento alvitrado pela AudTI, cujos fundamentos adoto como minhas razões de decidir, sem prejuízo dos breves comentários que tecerei a seguir.

14. A ferramenta Orbis, plataforma avançada de pesquisa e correlação de informações, utilizada para subsidiar operações estratégicas e táticas, com foco na prevenção e repressão a crimes, além de outras missões institucionais da PRF, mostrou-se essencial para otimizar a análise de grandes volumes de informações disponíveis na *internet*, oferecendo suporte à produção de conhecimento estratégico.

15. Vale ressaltar que sua aplicação prática abrange o monitoramento de redes sociais, análise de conteúdos disponíveis publicamente na *internet* e identificação de padrões que possam indicar ameaças ou irregularidades em rodovias federais e áreas sob jurisdição da corporação. Concordo com a conclusão da unidade instrutora de que tais atividades são conduzidas pela PRF de maneira a respeitar os limites impostos pela legislação brasileira e as diretrizes de proteção de dados pessoais, garantindo que não se ultrapassem os direitos fundamentais dos cidadãos.

16. Além disso, os controles implementados, a exemplo da infraestrutura local *on premises* (operação em servidores próprios da PRF), políticas rigorosas de concessão e revogação de acessos, credenciais de *login* com permissões diferenciadas e monitoramento de atividades, se mostraram robustos e eficazes para mitigar riscos de uso inadequado. Os treinamentos específicos para operação do sistema recebidos pelos agentes também reforçam a segurança e a governança na utilização da ferramenta.

17. Em que pese terem sido verificados que tais controles têm o condão de mitigar o risco de desvio de finalidade na utilização da ferramenta, entende-se que ainda há espaço para aperfeiçoamento por meio da realização de análises periódicas dos registros de uso (*logs*) do Orbis.

18. Portanto, não há dúvidas de que a proposta de recomendação direcionada à PRF reflete a preocupação com a governança e a transparência no uso da referida plataforma. Entendo que tal medida busca assegurar que a corporação adote critérios claros e objetivos para a realização de auditorias regulares.

19. Importante ressaltar que já existe previsão, no art. 27 da Política de Gestão de Registros (*logs*) de Auditoria (instituída pela Instrução Normativa PRF 130/2024), acerca da periodicidade de realização das análises de *logs* de auditoria (pelo menos duas vezes ao ano), para a detecção de anomalias ou eventos anormais que possam indicar uma ameaça potencial.

20. Assim, enalteço a importância do mencionado normativo. É, de fato, exemplo claro de um esforço institucional inicial para garantir a rastreabilidade e a auditoria das atividades realizadas na esfera de suas ferramentas de inteligência.

21. No entanto, anuo ao entendimento da unidade instrutora de que é imprescindível que a periodicidade da auditoria seja claramente determinada para o caso do Orbis, para que haja o efetivo cumprimento de seu comando, inclusive em razão de nunca ter sido realizado um trabalho de auditoria para analisar os *logs* com o intuito de identificar desvio de finalidade na utilização da ferramenta.

22. Além de facilitar o planejamento das auditorias, a definição exata de sua periodicidade evita que elas ocorram injustificadamente muito próximas uma da outra, enquanto períodos extensos possam transcorrer sem qualquer fiscalização dessa natureza. Essa frequência, devidamente fixada, permitirá maior controle sobre o uso das informações coletadas e analisadas, além de garantir que eventuais desvios sejam detectados tempestivamente.

23. Dessa forma, a corporação poderá fortalecer sua atuação no campo da inteligência policial, assegurando que suas operações sejam conduzidas com transparência e respeito às normas vigentes, reforçando o seu compromisso com os princípios da legalidade, eficiência e *accountability*. Essa recomendação, portanto, não apenas contribui para a melhoria contínua dos processos institucionais, como também alinha a atuação da PRF aos padrões de excelência esperados de um órgão integrante do Sisbin.

Ante o exposto, voto por que o Tribunal adote o Acórdão que ora submeto à deliberação deste Colegiado.

TCU, Sala das Sessões, em 22 de janeiro de 2025.

Ministro BRUNO DANTAS
Relator

ACÓRDÃO Nº 67/2025 – TCU – Plenário

1. Processo nº TC 023.173/2023-8.
2. Grupo I – Classe de Assunto: II – Solicitação do Congresso Nacional.
3. Interessados/Responsáveis: não há.
4. Unidade Jurisdicionada: Polícia Rodoviária Federal.
5. Relator: Ministro Bruno Dantas.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI).
8. Representação legal: não há

9. Acórdão:

VISTOS, relatados e discutidos estes autos de Solicitação do Congresso Nacional para que este Tribunal realize fiscalização das contratações realizadas pela Polícia Rodoviária Federal (PRF) com a empresa Cognyte Brasil S.A., de 2018 até a presente data;

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, ante as razões expostas pelo Relator, em:

9.1. considerar a presente solicitação integralmente atendida, nos termos do art. 17, II, da Resolução - TCU 215/2008;

9.2. recomendar à Polícia Rodoviária Federal, com fundamento no art. 11 da Resolução TCU 315/2020, com o objetivo de mitigar o risco de desvio de finalidade na utilização do sistema Orbis (ou do que vier a sucedê-lo), que inclua na política em construção para regulamentar a coleta e a análise de dados provenientes de fontes abertas previsões relativas à definição da periodicidade exata das análise de *logs* de auditorias, previstas no art. 27 da Política de Gestão de Registros (*logs*) de Auditoria, instituída pela Instrução Normativa PRF 130, de 29 maio de 2024;

9.3. dispensar o monitoramento da determinação supra, com fundamento no art. 17, § 2º, da Resolução 315/2020;

9.4. encaminhar cópia deste acórdão, bem como do relatório e voto que o fundamentam, à Comissão Parlamentar Mista de Inquérito (CPMI) dos Atos de 8 de janeiro;

9.5. arquivar estes autos, com fundamento no art. 14, inciso IV, da Resolução TCU 215/2008 c/c art. 169, inciso V, do RITCU.

10. Ata n° 1/2025 – Plenário.
11. Data da Sessão: 22/1/2025 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-0067-01/25-P.
13. Especificação do quórum:
13.1. Ministros presentes: Vital do Rêgo (Presidente), Walton Alencar Rodrigues, Benjamin Zymler, Augusto Nardes, Bruno Dantas (Relator), Jorge Oliveira e Antonio Anastasia.
13.2. Ministros-Substitutos convocados: Marcos Bemquerer Costa e Weder de Oliveira.

(Assinado Eletronicamente)
VITAL DO RÊGO
Presidente

(Assinado Eletronicamente)
BRUNO DANTAS
Relator

Fui presente:

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

TRIBUNAL DE CONTAS DA UNIÃO

TERMO DE CIÊNCIA DE COMUNICAÇÃO

(Documento gerado automaticamente pela Plataforma Conecta-TCU)

Comunicação: Ofício 000.856/2025-SEPROC

Processo: 023.173/2023-8

Órgão/entidade: SF - Coordenação de Comissões Especiais, Temporárias e de Inquérito - Coceti

Destinatário: COORDENAÇÃO DE COMISSÕES ESPECIAIS, TEMPORÁRIAS E DE INQUÉRITO - SF

Informo ter tomado ciência, nesta data, da comunicação acima indicada dirigida à/ao COORDENAÇÃO DE COMISSÕES ESPECIAIS, TEMPORÁRIAS E DE INQUÉRITO - SF pelo Tribunal de Contas da União, por meio da plataforma Conecta-TCU.

Data da ciência: 17/03/2025

(Assinado eletronicamente)

LEANDRO AUGUSTO DE ARAUJO CUNHA TEIXEIRA BUENO

Usuário habilitado a receber e a acessar comunicações pela plataforma Conecta-TCU.