VOTO

Trata-se de relatório de auditoria, de natureza de conformidade, realizada para diagnosticar os controles implementados por organizações públicas federais para adequação à Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), e induzir iniciativas para o pleno cumprimento da Lei, contribuindo para a diminuição dos riscos relativos à privacidade dos cidadãos e à segurança dos dados custodiados pela Administração Pública Federal (APF).

Após o transcurso de 1 (um) ano da entrada em vigor da LGPD, o Tribunal verificou que 76,7% das organizações públicas federais permaneciam nos graus inexpressivo ou inicial de adequação (Acórdão 1.384/2022-TCU-Plenário, relator E. Ministro Augusto Nardes).

Dada a relevância da matéria, esta segunda ação de controle foi autorizada para verificar a evolução do cumprimento da legislação por 387 órgãos e entidades, a partir da aplicação do questionário de autoavaliação de controles internos (*Control Self-Assessment* – CSA) e da exigência de documentos comprobatórios das informações prestadas (Apêndice D – p. 76, peça 949).

Para permitir a comparação entre os órgãos/entidades auditados, a partir das respostas das organizações, foi criado o "indicador de adequação à LGPD" (iLGPD) e foram definidos quatro níveis de adequação: "Inexpressivo" (< 15%), "Iniciando" (entre 15% e 40%), "Intermediário" (entre 40% e 70%) e "Aprimorado" (> 70%).

Cabe registrar que Tribunais de Contas Estaduais (TCEs) de oito estados da federação (AM, BA, CE, PA, PE, PR, RJ e RN) também fiscalizaram organizações públicas estaduais e municipais sob suas respectivas jurisdições, por meio de ação coordenada no âmbito da Rede Integrar.

Passo a tratar dos achados de auditoria.

Inicialmente, registro discreta evolução nas organizações públicas federais, em relação aos resultados obtidos na auditoria realizada em 2021, com a diminuição das quantidades de órgãos e entidades que figuram nos primeiros níveis ("Inexpressivo" e "Inicial") o aumento dos números de entes que se enquadram nos níveis "Intermediário" e "Aprimorado".

Comparação entre o iLGPD 2021 e o iLGPD 2024.

Nível de adequação à LGPD	Auditoria 2021	Auditoria 2024
Inexpressivo	68 (17,8%)	52 (13,44%)
Inicial	225 (58,9%)	174 (44,96%)
Intermediário	78 (20,4%)	128 (33,07%)
Aprimorado	11 (2,9%)	33 (8,53%)
Totais	**382 (100%)**	**387 (100%)**

Ao analisar as respostas aos questionários de forma mais detalhada, observa-se grande disparidade entre a situação dos diversos órgãos/entidades nos vários aspectos auditados e é possível concluir que ainda existem grandes lacunas a serem preenchidas para atendimento integral da LGPD por boa parte da Administração.

A seguir, relaciono as falhas e lacunas mais relevantes identificadas na fiscalização, para as quais considero necessário o endereçamento de medidas pelo Tribunal.

II

A preparação da organização para atendimento à LGPD envolve diversas ações, como instituição de grupo de trabalho, elaboração de estudos, definição de políticas de proteção de dados pessoais, de capacitação, de privacidade e até a adoção de programa de governança em privacidade de dados implementado, amplamente divulgado e periodicamente avaliado e revisado, no nível mais maduro em relação ao tema.

A auditoria evidenciou que 278 das 387 (71,84%) organizações federais auditadas identificaram e planejaram as medidas necessárias de adequação à LGPD, sendo que 171 (44,19%) já publicaram um ou mais normativos relacionados ao tema e 13,70% das organizações têm programa de governança em privacidade de dados implementado e com monitoração periódica.

Passados quase sete anos de publicação da Lei, no entanto, 109 (28,16%) das organizações ainda não concluíram a identificação e planejamento das medidas necessárias para adequação à LGPD, sendo que 11 delas sequer iniciaram trabalhos nesse sentido.

A ausência ou fragilidade das ações de planejamento coloca em risco a privacidade dos titulares de dados envolvidos e pode causar prejuízos aos próprios órgãos/entidades, como condenação ao pagamento de indenizações e danos à imagem.

Por isso, acolho a proposta de recomendar a essas entidades que realizem ações para identificar, planejar e implementar medidas de preparação necessárias à adequada dos dispositivos da LGPD.

III

O alcance dos resultados pretendidos pelas iniciativas de adequação à LGPD depende de providências relativas ao contexto organizacional específico de cada órgão/entidade, como identificação das partes interessadas, análises dos diferentes tipos de dados pessoais tratados e dos processos organizacionais que realizam o tratamento desses dados.

Restou demonstrado que 40 (10,34%) das organizações ainda não conduziram nenhuma iniciativa para identificar os normativos que lhe são aplicáveis e os elementos mínimos relacionados aos dados tratados, como as categorias de titulares, operadores, controladores conjuntos (no caso de tratamento de dados em conjunto com outros órgãos/entidades), processos de negócio, responsáveis e locais de armazenamento dos dados. Essas entidades também não analisaram a necessidade de adequar instrumentos contratuais e não avaliaram os riscos associados aos processos de tratamento de dados.

A ausência dessas medidas denota que esses órgãos não conhecem de forma detalhada os dados que devem proteger, colocando em risco a qualidade da segurança que devem prover e prejudicando a adoção de contratos e normas que definam claramente papéis e responsabilidades sobre dados pessoais compartilhados.

Portanto, recomendo a esses 40 órgãos/entidades que adotem providências quanto ao aprimoramento de seus contextos organizacionais.

IV

A alta direção da organização deve demonstrar claramente liderança e comprometimento com a iniciativa de adequação à LGPD. Nesse sentido, a elaboração e a ampla divulgação de políticas relacionadas à proteção de dados pessoais (Política de Segurança da Informação - PSI, Política de Classificação da Informação - PCI e Política de Proteção de Dados Pessoais – PPDP), bem como a nomeação de um encarregado pelo tratamento de dados pessoais (*Data Protection Officer* - DPO), são ações fundamentais para o processo de adequação à LGPD.

Na contramão dessa orientação, estão 24 organizações que não realizaram nenhuma dessas ações, o que demonstra a falta de priorização do processo de adequação à LGPD por parte da alta administração.

Adicionalmente, as respostas aos questionários informam que 80 (20,87%) organizações não possuem Política de Segurança da Informação, documento obrigatório, segundo o art. 15, inciso II, do Decreto 9.637/2018, c/c a IN - GSI/PR 1/2020; 48 órgãos/entidades (12,4%) ainda não indicaram ou nomearam o encarregado pelo tratamento de dados pessoais, em descumprimento ao art. 41 da Lei 13.709/2018; e 250 organizações não padronizaram a comunicação sobre incidentes de segurança que

possam acarretar risco ou dano relevante à Associação Nacional e Proteção de Dados e aos titulares, em afronta ao artigo 48 da Lei 13.709/2018.

Por se tratar de medidas básicas e imprescindíveis à adequada proteção de dados, deixo de acolher a proposta de dar mera ciência das irregularidades aos órgãos/entidades que não estão cumprindo a legislação para, em vez disso, exarar determinações, com definição de prazo, para que comprovem a correção das irregularidades tratadas nesta seção.

V

Quanto à capacitação dos agentes para atendimento da LGPD, somente 98 órgãos/entidades (25,32%) estabeleceram essa temática no respectivo plano de capacitação e já treinaram a maioria dos seus colaboradores nessa área.

Outras 161 organizações ou não possuem plano de capacitação ou ainda não incluíram no existente a necessidade de realizarem treinamento específico relacionado à proteção de dados pessoais, apesar de 118 delas terem afirmado a participação de alguns agentes em cursos sobre o tema.

A ausência de ações em Plano de Capacitação formalizado indica que a instituição não mapeou o conjunto de conhecimentos, competências e habilidades necessárias aos seus colaboradores. Nesse contexto, a realização de cursos sem tal planejamento pode resultar na ineficácia das iniciativas, além de prejudicar a conscientização e a sensibilização das equipes quanto à necessidade de preparação para lidar com a proteção de dados e os diversos impactos e prejuízos que as violações relacionadas podem causar ao órgão/entidade.

Ainda sobre a dimensão “capacitação”, registro que esta auditoria inovou em relação ao trabalho anterior ao incluir questões sobre a relação entre a LGPD e a Lei de Acesso à Informação.

A princípio, a aplicação dessas leis pode parecer conflituosa ou, no mínimo, desafiadora, tendo em vista a necessidade de buscar o melhor equilíbrio entre o direito ao acesso à informação e à proteção da privacidade dos indivíduos e segurança dos dados pessoais.

Nesse sentido, as organizações devem capacitar seus agentes para que sejam capazes de harmonizar, nas suas atividades do dia a dia, os dois diplomas legais. No entanto, apenas 46 (13,53%) organizações afirmaram ter capacitado em LAI mais da metade dos colaboradores que receberam treinamento em proteção de dados pessoais, enquanto somente 57 (16,77%) orientaram seus colaboradores em relação à existência de normativos correlatos emitidos pela CGU, como a Portaria Normativa - CGU 71/2023, e apenas 44 (12,94%) divulgaram o “Parecer sobre acesso à informação para atender ao Despacho Presidencial de 1º de janeiro de 2023”.

Pelo exposto, acolho a proposta de recomendar a elaboração de plano de capacitação relacionado à proteção de dados, ajustando-a no sentido de que os órgãos/entidades avaliem a inclusão de ações para capacitar os agentes quanto à necessária harmonização das disposições da LGPD e da LAI nas atividades relacionadas à proteção de dados e à disponibilização do devido acesso à informação.

VI

A organização deve ser capaz de provar que os tratamentos de dados pessoais que realiza são lícitos e os titulares de dados devem compreender claramente as finalidades para as quais seus dados pessoais são tratados.

Para tal, é salutar que órgãos e entidades identifiquem e documentem as finalidades de todas as suas principais atividades de tratamento de dados pessoais, avaliem se coletam apenas os dados estritamente necessários para cumprir com suas finalidades e se esses dados são retidos durante o tempo estritamente necessário, identifiquem as bases legais que fundamentam suas atividades de tratamento de dados pessoais e mantenham registro das operações de tratamento de dados., elaborem

Relatório de Impacto à Proteção de Dados Pessoais (LGPD, art. 5º, inciso XVII) e implementem controles para mitigar os riscos identificados nesse relatório.

A auditoria verificou, no entanto, que, à exceção da documentação das bases legais, todas as demais práticas relativas à conformidade dos tratamentos de dados pessoais com a LGPD foram atendidas apenas pela minoria dos órgãos/entidades, com destaques negativos para a falta de manutenção de registro das operações de tratamento em 270 das 387 organizações auditadas (69,77%) e a ausência de elaboração de qualquer Relatório de Impacto à Proteção de Dados Pessoais – RIPD – (LGPD, art. 5º, inciso XVII) por 280 (72,35%) organizações (Tabela 6 peça 949, p. 20).

Tendo em vista os elevados percentuais de respostas negativas obtidas, que ultrapassaram 50% para todas as questões relativas ao tema, expeço recomendação aos órgãos/entidades auditados para que adotem medidas para aprimoramento da conformidade do tratamento dos dados pessoais coletados, considerando os critérios previstos na Lei 13.709/2018, art. 5º, inciso XVII, art. 6º, em especial incisos I, II e III, e arts. 7º, 37, 38 e 40, bem como na norma ABNT NBR ISO/IEC 27701:2019, itens 7.2.1 (Identificação e documentação do propósito), 7.2.2 (Identificação de bases legais), 7.2.5 (Avaliação de impacto de privacidade), 7.2.8 (Registros relativos ao tratamento de dados pessoais), 7.4.1 (Limite de coleta) e 7.4.7 (Retenção).

VII

A organização deve assegurar que os titulares tenham acesso a informações relacionadas ao tratamento de seus dados pessoais por meio da publicação, de maneira clara e concisa, de informações relativas a esses tratamentos. A organização também deve estar preparada para atender todos os direitos dos titulares que são elencados na LGPD (arts. 9º e 17-22).

A Política/Aviso de Privacidade é um documento endereçado aos usuários de um sítio, serviço ou sistema (titulares de dados – público externo), com o propósito de dar visibilidade ao tratamento de dados pessoais e demonstrar que os princípios da LGPD são atendidos.

De acordo com as respostas fornecidas à equipe de fiscalização, 146 (37,73%) organizações não elaboraram Política de Privacidade e 90 (23,26%) não implementaram mecanismos para atender direitos dos titulares previstos nos arts. 9º e 18 da LGPD, falhando em relação aos seus deveres de transparência e na regular obtenção de consentimento do titular para tratamento de seus dados.

Do exposto, acolho as propostas de recomendação para que essas entidades aprimorem suas atividades de proteção de dados, disponibilizando Política de Política de Privacidade (ou instrumento similar) e implementando mecanismos para comprovarem o atendimento dos direitos dos titulares.

VIII

O compartilhamento de dados pessoais demanda a adoção de controles adequados com vistas a mitigar os riscos que possam comprometer a segurança e a proteção desses dados.

Das 387 organizações, 170 (43,93%) ainda não avaliaram se compartilham dados pessoais com terceiros ou ainda não realizaram a devida identificação dos dados eventualmente compartilhados.

O desconhecimento sobre os compartilhamentos implica na incapacidade de assegurar a segurança e a proteção dos dados, pois ao não identificar os compartilhamentos e ao não manter o devido registro de quais dados são compartilhados, o órgão/entidade não tem como adotar controles adequados para mitigar os riscos associados, por exemplo, o de um possível vazamento de dados pessoais.

Nesse sentido, pertinente a proposta de recomendação para que essas entidades avaliem se compartilham dados pessoais com terceiros e identifiquem os dados eventualmente compartilhados.

IX

Importante achado desta fiscalização é relativo à atuação das unidades de controle interno dos órgãos e entidades auditados.

Restou evidente que o controle interno de 250 organizações não realizou avaliação relacionada à proteção de dados pessoais e 194 não trataram de aspectos atinentes à LAI nos últimos 3 anos.

A atuação dessas unidades é fundamental para assegurar que as leis, as normas gerais e as normas internas sejam efetivamente observadas, bem como para avaliar riscos em relação aos processos de trabalho da organização.

Destaco, por fim, que órgãos com jurisdição ou supervisão administrativa sobre outros (*e.g.* CNJ, CNMP, SGD/MGI, Sest/MGI e ANPD) também devem atuar com vistas a induzir o aprimoramento dos controles relativos à proteção de dados.

Por isso, recomendo que essas unidades e esses órgãos acompanhem e induzam a implementação dos controles necessários para adequação à LGPD, em especial quanto às fragilidades identificadas nesta auditoria.

Adicionalmente, acolho as propostas da equipe de auditoria de disponibilizar "Painel Nacional de Implementação da LGPD" e relatórios individuais de *feedback* sobre os achados de auditoria, por consistirem em importantes ferramentas de incentivo à implementação das melhorias pretendidas, além de o Painel permitir que a sociedade civil acompanhe e cobre dos gestores e organizações a execução das providências para adequação à Lei.

Por fim, agradeço as valiosas contribuições apresentadas pelo E. Ministro Bruno Dantas, incorporando-as às minhas razões de decidir, no sentido de garantir o equilíbrio entre a LGPD e a LAI, com vistas a salvaguardar tanto a proteção dos dados pessoais quanto à transparência pública.

Feitas essas considerações, voto para que o Tribunal adote a minuta de acórdão que submeto ao Colegiado.

TCU, Sala das Sessões, em 25 de junho de 2025.

WALTON ALENCAR RODRIGUES
Relator