TRIBUNAL SUPERIOR ELEITORAL

RESOLUÇÃO Nº 23.650

PROCESSO ADMINISTRATIVO Nº 0600343-06.2021.6.00.0000 – BRASÍLIA – DISTRITO FEDERAL

Relator: Ministro Luís Roberto Barroso
Interessado: Tribunal Superior Eleitoral

Institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.

O TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e

CONSIDERANDO a entrada em vigor da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e a necessidade de sua regulamentação para a adequada implementação de suas diretrizes no âmbito da Justiça Eleitoral;

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece o marco civil da Internet (Lei do Marco Civil da Internet), e a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso à informação (Lei de Acesso à Informação – LAI);

CONSIDERANDO a Resolução CNJ nº 363, de 12 de janeiro de 2021, que estabelece medidas para o processo de adequação dos tribunais à LGPD, em especial o dever de disponibilizar informação ao titular de dados por meio de política geral de privacidade e proteção de dados pessoais (art. 1º, VI, *c*);

CONSIDERANDO que a Justiça Eleitoral trata os dados pessoais de forma colaborativa para o desempenho de suas atribuições constitucionais, legais e regulamentares;

CONSIDERANDO que o direito à informação deve ser garantido de forma harmoniosa com a privacidade, intimidade, honra e imagem dos titulares de dados pessoais cadastrados nos bancos de dados da Justiça Eleitoral, bem como com os direitos fundamentais de liberdade e de livre desenvolvimento da personalidade da pessoa natural; e

CONSIDERANDO a relevância da proteção à autonomia informativa dos cidadãos para a democracia;

RESOLVE:

Art. 1º Instituir a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.

§ 1º Esta Política tem por objetivo estabelecer diretrizes para as ações de planejamento e de execução das obrigações funcionais e de gestão administrativa.

§ 2º Esta Política se aplica a qualquer operação de tratamento de dados pessoais realizada pela Justiça Eleitoral, independentemente de o meio ser físico ou eletrônico, ou do país onde estejam localizados os dados.

§ 3º Os magistrados, servidores, colaboradores internos e externos e quaisquer outras pessoas que realizam tratamento de dados pessoais em nome da Justiça Eleitoral se sujeitam às diretrizes, às normas e aos procedimentos previstos nesta resolução e são responsáveis por garantir a proteção de dados pessoais a que tenham acesso.

§ 4º Inclui-se na condição de colaborador o estagiário, o terceirizado e todo aquele que preste serviço ou desenvolva, na Justiça Eleitoral, qualquer atividade de natureza permanente, temporária ou excepcional, mesmo que sem retribuição financeira direta ou indiretamente por parte desta Justiça Especializada.

Art. 2º Os termos, as expressões e as definições utilizados nesta Política são aqueles conceituados na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), sendo complementares as disposições estabelecidas nesta Resolução.

CAPÍTULO I

DOS PRINCÍPIOS

Art. 3º O tratamento de dados pessoais pela Justiça Eleitoral deverá ser pautado pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da LGPD, a saber: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Parágrafo único. De modo a tutelar o direito à proteção de dados pessoais e à autodeterminação informativa das pessoas naturais, a Justiça Eleitoral deverá conciliar os princípios da publicidade e da eficiência com a proteção da intimidade e da vida privada da pessoa natural, em consonância com as Leis nºs 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), 12.965/2014 (Lei do Marco Civil da Internet) e 12.527/2011 (Lei de Acesso à Informação – LAI).

CAPÍTULO II

DAS DIRETRIZES

Art. 4º Para conformar as ações de tratamento de dados pessoais no âmbito da Justiça Eleitoral, deverão ser consideradas as seguintes diretrizes:

I – definição de procedimentos que garantam os princípios da segurança da informação dos dados pessoais em todo o seu fluxo de tratamento e durante todo o seu ciclo de vida;

II – padronização do modo de tratamento de dados pessoais, com a adoção de anonimização ou pseudonimização, sempre que necessário;

III – elaboração ou adequação das políticas de privacidade e termos de uso;

IV – adequação dos normativos, formulários, sistemas e aplicativos informatizados à legislação de referência;

V – adequação dos sítios eletrônicos dos Tribunais Eleitorais, para que disponibilizem as informações exigidas pelos arts. 9º e 23, I, da LGPD;

VI – adequação de contratos, acordos de cooperação técnica, convênios ou atos similares;

VII – capacitação de magistrados e servidores, bem como conscientização do público interno e externo, acerca desta Política e das boas práticas e governança dela decorrentes; e

VIII – promoção dos registros de tratamento de dados pessoais, nos termos do art. 37 da LGPD, para que sejam informados ao titular quando solicitado (art. 18 da LGPD e 14 desta Resolução).

Parágrafo único. Cabe ao Tribunal Superior Eleitoral a coordenação da adequação dos sistemas informatizados comuns à Justiça Eleitoral e de seus respectivos normativos aos princípios e regras previstos na LGPD e nesta Política.

CAPÍTULO III

DAS HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

Art. 5º O tratamento de dados pessoais pela Justiça Eleitoral deve ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas atribuições normativas.

Art. 6º Em atendimento às suas atribuições, a Justiça Eleitoral poderá, no estrito limite de suas atividades, tratar dados pessoais sem o consentimento dos titulares, desde que observados os princípios estabelecidos pelo art. 6º da LGPD e respaldada a sua atuação nas hipóteses elencadas no art. 7º, incisos II a X, art. 10, incisos I e II, art. 11, inciso II, art. 23 *caput*, e arts. 26 e 27, todos da LGPD.

§ 1º Eventuais tratamentos que não estejam contemplados nas hipóteses previstas no *caput* estarão sujeitos à obtenção de consentimento dos interessados.

§ 2º O consentimento para tratamento de dados pessoais de criança deverá ser dado de forma específica e em destaque por ao menos um dos pais ou pelo responsável legal.

Art. 7º Os contratos, convênios e instrumentos congêneres mantidos pela Justiça Eleitoral deverão estar disponíveis para consulta pelos interessados, nos termos da LAI, observada a proteção dos dados pessoais que não sejam essenciais ao cumprimento da referida lei e ao interesse público, de acordo com a LGPD, de modo a se evitar a exposição indevida de dados pessoais que não precisem ser publicizados.

Parágrafo único. Para o cumprimento do disposto no *caput*, os Tribunais deverão adotar medidas tais como a aposição de tarjas sobre dados pessoais ou a supressão parcial de números cadastrais.

Art. 8º A Justiça Eleitoral pode requisitar informações acerca do adequado tratamento dos dados pessoais confiados a pessoas físicas ou jurídicas com quem mantenha contratos, convênios ou instrumentos congêneres.

Parágrafo único. As pessoas físicas ou jurídicas mencionadas no *caput* deverão observar os regramentos estabelecidos por esta resolução, além de cumprir os deveres legais e contratuais respectivos, dentre os quais se incluirão os seguintes:

I – firmar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais requeridas pela Justiça Eleitoral;

II – apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança para a proteção dos dados pessoais, segundo a legislação, normas regulamentares da Justiça Eleitoral, padrões técnicos definidos pela Autoridade Nacional de Proteção de Dados (ANPD) e instrumentos contratuais;

III – manter os registros de tratamento de dados pessoais que realizar, com condições de rastreabilidade e de fornecimento de prova eletrônica;

IV – seguir as diretrizes e instruções transmitidas pela Justiça Eleitoral;

V – facultar acesso a dados pessoais somente para o pessoal autorizado, naquilo que for estritamente necessário, e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo tal compromisso estar disponível em caráter permanente para exibição à Justiça Eleitoral, mediante solicitação;

VI – permitir a realização de auditorias, incluindo inspeções da Justiça Eleitoral ou de auditor independente por ela autorizado, e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII – auxiliar, em toda providência que estiver ao seu alcance, no atendimento pela Justiça Eleitoral de obrigações perante titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII – comunicar formal e imediatamente à Justiça Eleitoral a ocorrência de incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções; e

IX – descartar de forma irrecuperável, ou devolver para a Justiça Eleitoral, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

Art. 9º A transferência internacional de dados somente poderá ser feita nas hipóteses do art. 33 da LGPD.

CAPÍTULO IV

DO CICLO DE VIDA DOS DADOS PESSOAIS

Art. 10. Os dados pessoais tratados pela Justiça Eleitoral devem ser:

I – mantidos disponíveis, íntegros e confidenciais, nos termos da Resolução TSE nº 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

II – tratados somente quando diante de hipótese legal autorizativa; e

III – eliminados, quando cabível, aqueles que já não forem necessários por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção, nos termos da tabela de temporalidade, conforme classificação, avaliação e destinação das informações e documentos de cada Tribunal.

CAPÍTULO V

DOS DIREITOS DO TITULAR DE DADOS PESSOAIS

Art. 11. A Justiça Eleitoral deve tomar as providências necessárias para que o titular do dado pessoal possa usufruir dos direitos assegurados pelos arts. 18 e 19 da LGPD.

Art. 12. Deverá ser divulgada no portal de cada Tribunal Eleitoral informação ostensiva, adequada e clara sobre a aplicação da LGPD, incluindo:

I – identificação do controlador e do encarregado e suas respectivas informações de contato;

II – as hipóteses em que a instituição realiza o tratamento de dados pessoais, contendo a previsão legal, a finalidade específica, a forma e duração do tratamento, os procedimentos e as práticas utilizadas para a execução desses tratamentos, bem como informações acerca do uso compartilhado de dados pelo controlador e a respectiva finalidade;

III – as responsabilidades dos agentes que realizam o tratamento;

IV – os direitos dos titulares, com menção explícita àqueles contidos no art. 18 da LGPD;

V – aviso de coleta de dados pessoais em navegação pela Internet (inclusive por meio de *cookies*), política de privacidade para navegação na página da instituição e política geral de privacidade e proteção de dados pessoais; e

VI – a disponibilização de formulário para o exercício do direito de solicitação de informações pessoais ou de reclamações pelo titular dos dados pessoais, bem como de orientações quanto ao procedimento para o seu encaminhamento.

Art. 13. As informações sobre o tratamento de dados pessoais de crianças e adolescentes deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Art. 14. O titular dos dados pessoais tem direito a obter do controlador, em relação aos seus dados tratados, em linguagem clara e simples, mediante requerimento, as seguintes informações:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com esta Resolução ou com o disposto na LGPD;

V – portabilidade dos dados, de acordo com a regulamentação da Autoridade Nacional de Proteção de Dados (ANPD);

VI – eliminação dos dados pessoais tratados com fundamento em seu consentimento, exceto nas hipóteses necessárias de conservação para adimplemento a princípios e normas da atividade administrativa, caso em que deverá ser informado acerca do prazo da conservação de seus dados; e

VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

§ 1º Além dos direitos arrolados no *caput*, caso o tratamento seja baseado no consentimento, o titular dos dados deve ser expressamente informado sobre a possibilidade de não o fornecer, bem como sobre as consequências da negativa e sobre a possibilidade de revogação do consentimento a qualquer tempo, nos termos do § 5º do art. 8º da LGPD.

§ 2º A formulação da requisição prevista nos arts. 18 e 19 da LGPD e a correspondente resposta serão feitas por meio seguro e idôneo, o qual deverá conter funcionalidades de segurança que garantam a inequívoca identificação do requisitante.

§ 3º No caso de a coleta dos dados pessoais não haver sido realizada de forma direta pela Justiça Eleitoral, deverá ser disponibilizada ao titular dos dados, em caso de solicitação, informação acerca da origem primária dos dados.

§ 4º Os Tribunais Eleitorais deverão padronizar meios de comunicação para o atendimento de solicitações ou dúvidas de titulares de dados pessoais, e demais procedimentos organizacionais, visando a assegurar celeridade na prestação da informação.

§ 5º A informação prevista nos incisos I e II do *caput* deverá ser prestada no prazo de 15 (quinze) dias, contados da data do protocolo do requerimento do titular.

§ 6º As informações previstas nos incisos III e seguintes do *caput* deverão ser prestadas no prazo de até 20 (vinte) dias, contados da data do protocolo do requerimento do titular, prorrogável, justificadamente, por mais 10 (dez) dias.

CAPÍTULO VI

DOS REQUISITOS DE SEGURANÇA PARA O TRATAMENTO DE DADOS PESSOAIS

Art. 15. O tratamento de dados pessoais deverá observar as normas expressas na Política de Segurança da Informação (PSI) da Justiça Eleitoral e, ainda, os seguintes cuidados:

I – cada ativo de informação que envolva o tratamento de dados pessoais deverá ter tal característica destacada na ferramenta de inventário em que estiver arrolado, devendo constar, ainda, no relatório de impacto à proteção de dados pessoais;

II – o tratamento de informações produzidas ou custodiadas pela Justiça Eleitoral que envolvam dados pessoais deverá ser objeto de registro (art. 37 da LGPD);

III – a necessidade de manutenção da guarda dos dados pessoais deverá estar fundamentada na tabela de temporalidade de cada Tribunal; e

IV – diante de incidente de segurança que possa acarretar risco ou dano relevante a titular de dados pessoais, o controlador deverá comunicar, em prazo de até 72 (setenta e duas) horas úteis, à ANPD e ao titular, nos termos do art. 48, § 1º, da LGPD.

§ 1º O relatório de impacto a que se refere o inciso I do *caput* deverá observar as exigências contidas no art. 38, parágrafo único, da LGPD e ainda:

I – obedecer ao padrão mínimo estabelecido pelo Comitê Gestor de Proteção de Dados Pessoais do TSE (Resolução CNJ nº 363/2021), que será aprovado pela Direção-Geral do TSE e comunicado aos TREs, observadas recomendações que advenham das autoridades competentes;

II – sofrer revisão bianual ou sempre que houver alteração relevante no tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos das pessoas que tenham dados tratados por quaisquer instâncias da Justiça Eleitoral; e

III – ser consolidado pelo Tribunal competente e encaminhado ao CGPD do TSE para compilação e posterior envio à Autoridade Nacional de Proteção de Dados (ANPD).

§ 2º O registro de que trata o inciso II do *caput* deverá identificar a finalidade e a pessoa ou o processo responsável pela efetivação do tratamento de dado pessoal e estar acessível ao titular do dado nos termos do art. 19 da LGPD, bem como para eventual responsabilização, nos termos do art. 42 da mesma lei.

§ 3º Nas atualizações e na aplicação da tabela de temporalidade de cada Tribunal, o tempo de armazenamento dos dados pessoais deverá levar em consideração os direitos à eliminação, à privacidade e à autodeterminação informativa, cabendo a manutenção de dados que possam constranger seu titular apenas durante o período em que essas informações possam ter consequências no gozo de direitos.

§ 4º A comunicação ao titular de dados pessoais a que se refere o inciso IV do *caput* deverá ser feita por meio seguro e idôneo, o qual deverá conter funcionalidades de segurança que garantam a inequívoca identificação do titular.

CAPÍTULO VII

DA ESTRUTURA DA GESTÃO DE DADOS PESSOAIS

Art. 16. Cada Tribunal Eleitoral deverá manter estrutura administrativa interna para o atendimento das diretrizes estabelecidas na presente resolução e para o tratamento de dados pessoais, compreendida, no mínimo, pelo Encarregado e pelo Comitê Gestor de Proteção de Dados Pessoais (CGPD), bem como pelas unidades incumbidas de efetivar tratamentos de dados pessoais e daquelas incumbidas da segurança da informação.

Art. 17. Deverão ser identificadas as unidades administrativas da Justiça Eleitoral (cartórios eleitorais, seções, coordenadorias ou secretarias) que, pela natureza de suas funções, efetivem o tratamento de dados pessoais.

§ 1º Às unidades mencionadas no *caput* incumbe:

I – providenciar registro (art. 37 da LGPD) das operações de tratamento de dados pessoais que efetivarem;

II – efetivar o tratamento em consonância com as normas sobre a matéria e segundo as instruções fornecidas pelo TSE ou pelo respectivo TRE;

III – prestar as informações necessárias ao desenvolvimento dos trabalhos do CGPD e ao desempenho das atribuições do Encarregado;

IV – informar à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), na forma e nos termos da PSI e da LGPD, acerca de incidentes de segurança que representem risco ou dano relevante aos titulares de dados pessoais de que tomem conhecimento; e

V – informar diretamente ao Encarregado violações a esta Política que não estejam abrangidas pela hipótese do inciso IV.

§ 2º Para cumprimento do disposto no inciso I do § 1º deste artigo, o TSE e os TREs deverão munir as unidades mencionadas no *caput* de instrumentos normativos e operacionais que possibilitem a identificação da realização de tratamento em registros dos titulares dos dados.

§ 3º Apenas usuários credenciados poderão realizar tratamento de dados, o que será feito de acordo com níveis de acesso estipulados pela Justiça Eleitoral.

§ 4º Na hipótese do inciso IV, a ETIR, verificando que o incidente representa risco ou dano relevante aos titulares de dados pessoais, deverá comunicar o fato ao Encarregado.

Art. 18. Para os fins de compreensão das normas de proteção de dados pessoais na Justiça Eleitoral, em complemento às definições constantes da LGPD, considera-se:

I – Controlador: o Tribunal Superior Eleitoral e o Tribunal Regional Eleitoral, a quem competem as decisões referentes ao tratamento de dados pessoais;

II – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

III – Encarregado: unidade indicada pelo respectivo Tribunal Eleitoral, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); e

IV – Controlador conjunto: o Tribunal Eleitoral que, por força de lei, convênio ou contrato, determinar as finalidades e os meios de tratamento de dados pessoais em conjunto com outra pessoa natural ou jurídica, de direito público ou privado.

§ 1º O Juízo Eleitoral, embora tenha atribuições e competência para decidir a respeito do tratamento de dados pessoais, nas hipóteses assim definidas em Leis e Resoluções, não se equipara à figura do Controlador.

§ 2º O Tribunal Eleitoral, quando realiza o tratamento de dado pessoal em nome do Tribunal Controlador, atua na função de operador.

§ 3º Não se consideram controladores conjuntos, mas apenas controladores, aqueles que, apesar de decidirem a respeito do mesmo conjunto de dados pessoais, o fazem para finalidades diversas.

Art. 19. Caberá ao Encarregado:

I – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;

III – orientar as partes envolvidas no tratamento de dados pessoais a respeito das práticas a serem tomadas em relação à sua proteção;

IV – encaminhar, quando houver necessidade de providências por parte do CGPD, demandas, proposições e orientações a seu exame; e

V – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 1º Aqueles que exercerem as atividades de atribuição do Encarregado deverão ter conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como as habilidades necessárias para desempenhar as funções das quais serão incumbidos.

§ 2º O representante do Encarregado deverá ter acesso direto à alta administração do Tribunal, para o adequado desempenho de suas funções.

Art. 20. O Comitê Gestor de Proteção de Dados Pessoais (CGPD) terá caráter multidisciplinar e será composto, no mínimo, por representantes da Presidência, da Diretoria-Geral, do Gestor de Segurança da Informação e, no caso dos Tribunais Regionais, de Cartório Eleitoral.

§ 1º Os representantes indicados pelas unidades citadas no *caput* devem ser preferencialmente servidores da Justiça Eleitoral ou servidores públicos cedidos à Justiça Eleitoral.

§ 2º O CGPD deliberará por maioria.

§ 3º Havendo conflito de interesses entre a unidade de origem de qualquer membro do CGPD e a deliberação a ser tomada, tal membro não participará da respectiva deliberação.

Art. 21. Ao CGPD de cada Tribunal Eleitoral incumbe:

I – elaborar propostas de regulamentação da LGPD;

II – sugerir providências a serem adotadas com vistas à implementação da LGPD;

III – monitorar e avaliar o cumprimento da LGPD;

IV – propor diretrizes para o aprimoramento contínuo de mecanismos de proteção a dados pessoais no âmbito da Justiça Eleitoral, inclusive nos campos do planejamento, da governança, administração de processos e procedimentos, elaboração de normas, rotinas operacionais, práticas organizacionais, desenvolvimento e gestão de sistemas de informação e relações com a imprensa; e

V – atuar colaborativamente, quanto à proteção de dados pessoais, junto às unidades responsáveis pela capacitação e pela conscientização.

Parágrafo único. Os Tribunais Eleitorais poderão conferir outras atribuições ao CGPD, consideradas as especificidades locais.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 22. A Justiça Eleitoral deverá reforçar e aprimorar constantemente esta Política, empreendendo estudos a fim de verificar a necessidade de sua revisão, no máximo a cada 3 (três) anos, atentando à evolução tecnológica e aos novos paradigmas de boas práticas.

Parágrafo único. As boas práticas adotadas para a proteção de dados pessoais e a governança implantada deverão ser objeto de campanhas informativas, visando a disseminar a cultura protetiva, com conscientização e sensibilização dos interessados.

Art. 23. Situações fáticas, procedimentais ou normativas que impactem no tratamento de dados pessoais, ainda que não previstas expressamente nesta Política, deverão observar os princípios e diretrizes aplicáveis para o tratamento de dados pessoais.

Art. 24. A fim de estruturar dados pessoais para uso compartilhado, nos termos da LGPD, os Tribunais Eleitorais, tal qual os demais órgãos públicos com os quais a Justiça Eleitoral vier a firmar acordos de cooperação, deverão desenvolver e sustentar soluções capazes de garantir a interoperabilidade entre seus sistemas.

Art. 25. Caso a ANPD, no exercício de suas competências legais, preveja prazos diversos dos estabelecidos nesta Resolução, prevalecerão aqueles definidos pela Autoridade.

Art. 26. Os órgãos da Justiça Eleitoral deverão abordar as questões que permeiam a proteção de dados pessoais em seus planos estratégicos, bem como nos documentos e nas práticas deles decorrentes.

Art. 27. A Política Geral de Privacidade e Proteção de Dados Pessoais e a Política de Segurança da Informação da Justiça Eleitoral são complementares, devendo ser interpretadas em conjunto.

Art. 28. Os Tribunais Eleitorais terão até 31 de dezembro de 2021 para adaptar seus atos normativos às regras previstas nesta Resolução, respeitada a regra da anualidade eleitoral, quando aplicável.

Art. 29. Os casos omissos serão resolvidos pela Presidência de cada Tribunal Eleitoral, no âmbito de sua competência.

Art. 30. Esta Resolução entra em vigor na data da sua publicação.

Brasília, 9 de setembro de 2021.

MINISTRO LUÍS ROBERTO BARROSO – RELATOR

RELATÓRIO

O SENHOR MINISTRO LUÍS ROBERTO BARROSO: Senhores Ministros, trata-se de minuta de resolução que institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral.

2. O tema foi objeto de estudo do grupo de trabalho instituído por meio da Portaria TSE nº 162/2021, para o fim específico de propor regulamentação sobre a aplicação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) no âmbito da Justiça Eleitoral.

3. Constam dos autos, dentre outros documentos, a minuta de resolução (ID 144194988), o parecer emitido pela Assessoria Jurídica da Secretaria do TSE (ID 144195188) e o despacho conclusivo da Secretaria-Geral da Presidência (ID 144195488).

4. O trâmite administrativo se deu nos autos do Procedimento Administrativo SEI nº 2021.00.000002332-9, autuado como Processo Administrativo, conforme despacho ID 144195538.

5. Os autos vieram-me conclusos em 20.7.2021.

6. É o relatório.

VOTO

O SENHOR MINISTRO LUÍS ROBERTO BARROSO (relator): Senhores Ministros, trata-se de minuta de resolução que institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral, e regulamenta os preceitos estabelecidos na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

2. O processo de adequação à LGPD foi iniciado pela Secretaria do Tribunal a partir da instituição de grupo de trabalho para aquele fim específico (Portaria TSE nº 162/2021), bem como seguindo recomendação do Conselho Nacional de Justiça, que, por meio da Resolução CNJ nº 363/2021, estabeleceu medidas a serem adotadas pelos tribunais para facilitar o processo de implementação da LGPD no contexto do sistema judicial. Uma dessas providências consiste em disponibilizar informação adequada sobre o tratamento de dados pessoais, por meio de **política geral de privacidade e proteção de dados pessoais** a ser aplicada internamente no âmbito de cada Tribunal e supervisionada pelo Comitê Gestor de Proteção de Dados Pessoais (art. 1º, VI, *c*).

3. Cumpre informar que o Comitê Gestor de Proteção de Dados Pessoais (CGPD) do TSE foi instituído por meio da Portaria TSE nº 98/2021, com o objetivo de funcionar como órgão consultivo e responsável pelo processo de implementação da LGPD no âmbito deste Tribunal Superior.

4. Esta Política se aplica a qualquer operação de tratamento de dados pessoais realizada pela Justiça Eleitoral, independentemente de o meio ser físico ou eletrônico, ou do país onde estejam localizados os dados (art. 1º, § 2º, da minuta). O tratamento de dados pessoais pela Justiça Eleitoral deverá ser pautado pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da LGPD, a saber: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (art. 3º da minuta).

5. Ao analisar a minuta, a Assessoria Jurídica da Secretaria do TSE, além de sugerir algumas alterações no texto, elaborou um breve histórico da proteção de dados sob um panorama mundial, tendo em vista o avanço tecnológico, o aumento contínuo do processamento de dados pessoais, o advento da Internet,

as mídias sociais, dentre outras razões, que “tornaram impositiva a adoção de medidas regulatórias eficazes e padronizadas para garantir não só a intimidade das pessoas, como o fluxo seguro de informações, a economia e a própria democracia” (ID 144195188). Confira-se:

> “**Breve histórico da proteção de dados**
> 5. A lei brasileira de proteção de dados pessoais espelha-se no Regulamento Geral sobre a Proteção de Dados (GDPR) europeu, primeiramente publicado em 27 de abril de 2016 e implementado em 25 de maio de 2018. A primeira norma de proteção de dados que se tem notícia também tem origem naquele continente: a Lei de Proteção de Dados do estado alemão de Hesse, datada de 1970[3].
> 6. Esse esforço normativo mundial é uma reação ao avanço tecnológico das últimas décadas, principalmente no campo do processamento de dados, que trouxe o tema da proteção de dados para o centro das preocupações da sociedade e a privacidade para o centro do debate democrático.
> 7. Nas palavras de Stefano Rodotà[4], a novidade introduzida pelos computadores é a transformação de informação dispersa em informação organizada.
> 8. Vivemos hoje na chamada sociedade da informação[5], com massivos bancos de dados cuja sistematização e processamento são capazes de gerar uma quantidade e qualidade de informação sem precedentes na história da humanidade.
>
> > Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos a respeito das informações pessoais e, consequentemente, sobre a própria pessoa. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo. (Doneda, D. A Proteção dos Dados Pessoais como um Direito Fundamental. Op. cit., pág. 93)
>
> 9. O Tribunal Constitucional alemão, no emblemático julgamento da lei federal regedora do censo alemão de 1982, descreveu bem o problema:
>
> > Hoje, com a ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. (*in* Doneda. Panorama Histórico da Proteção de Dados Pessoais. Tratado de Proteção de Dados Pessoais. Coordenadores Danilo Doneda... (et. al), Rio de Janeiro: Forense. 2021, pág. 9)
>
> 10. Entre nós, em 1995, o Superior Tribunal de Justiça proferiu o seguinte posicionamento por meio do voto do Ministro Ruy Rosado, relator do REsp nº 22.337-8/RS.
>
> > *A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de pronto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, algumas providências já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível das garantias fundamentais, com o direito de autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do ombudsman, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação (Hassemer, “Proteção de Dados”,*

palestra proferida na Faculdade de Direito da UFRGS, 22.11.93). No Brasil, a regra do art. 5º, inc. X, da Constituição de 1988, é um avanço significativo: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". (DJ 20/3/1995).

11. Contemporaneamente, entende-se que o maior risco não reside no conteúdo dos dados, mas nas possibilidades e finalidades do seu tratamento, de maneira que não cabe mais falar em dados irrelevantes. A esse respeito, Danilo Doneda[6] registra:

A utilização sempre mais ampla de dados pessoais para as mais variadas atividades – identificação, classificação, autorização e tantas outras – torna tais dados elementos essenciais para que a pessoa possa se mover com autonomia e liberdade nos corredores do que hoje costumamos denominar de Sociedade da Informação. Os dados pessoais chegam a fazer às vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável.
O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.

12. O aumento contínuo do processamento de dados pessoais, o advento da *internet,* as mídias sociais, o *big data*[7] e o incessante incremento da tecnologia tornaram impositiva a adoção de medidas regulatórias eficazes e padronizadas para garantir não só a intimidade das pessoas, como o fluxo seguro de informações, a economia e a própria democracia.

A Lei nº 13.709/2018 – LGPD

13. Daí o advento da Lei Brasileira de Proteção de Dados Pessoais – LGPD, a disciplinar o tratamento de dados pessoais, em meio digital ou físico, por pessoa física ou jurídica, de direito público ou privado, e estabelecer, entre outros aspectos, os fundamentos do regime (art. 2º), os princípios gerais (art. 6º) e requisitos de tratamento dos dados pessoais (arts. 7º a 10) e dos dados pessoais sensíveis (arts. 11 a 13), os direitos dos titulares de dados (arts. 18 a 22), responsabilidades dos controladores e operadores de dados (arts. 42 a 45), com o consequente sancionamento no caso de descumprimento (arts. 52 a 54), além da criação do órgão regulador, a Agência Nacional de Proteção de Dados - ANPD (arts. 55-A a 57) e do Comitê Nacional de Proteção de Dados (arts. 58-A e 58- B).

14. A LGPD, na esteira do GDPR, adotou o paradigma de controle pautado na confiança no controlador, com foco na sua responsabilização, um dos pilares da proteção de dados. Segundo Leonardo Parentoni[8], s*aiu-se de um paradigma de controle prévio por instituições públicas para o de confiança no controlador – presumindo-se sua boa-fé e conformidade jurídica, de modo que eventual fiscalização será feita posteriormente.*

15. Esse esquema normativo demanda dos agentes de tratamento (controladores e operadores de dados) o exaurimento do protocolo legal para garantia da integridade e segurança dos dados pessoais dos titulares de forma a eximirem-se de futura responsabilização.

16. Com relação ao tratamento de dados pessoais pelo Poder Público, ademais das normas de aplicação geral, há dispositivos específicos, como os arts. 23 a 30.

17. Miriam Wimmer[9], ao examinar a proteção de dados no setor público sob a perspectiva dos princípios, ressalta a necessidade de que a aplicação das normas observe a harmonização entre os princípios consagrados da Administração Pública e aqueles trazidos pela LGPD, partindo-se da compreensão de que não há antagonismo entre privacidade e interesse público:

O que tanto o princípio da eficiência como o da supremacia do interesse público têm em comum é o fato de remeterem a ideias como interesse geral e bem comum, conceitos jurídicos dotados de elevado grau de indeterminação e que por vezes são apresentados de maneira a confrontar direitos e princípios que tutelam de maneira mais direta o indivíduo. Essa crítica tem sido feita por parte da doutrina, de maneira bastante enfática, no tocante ao princípio da supremacia do interesse público, especialmente em face do amplo rol de direitos fundamentais plasmados na Constituição. Nos últimos anos, diversos autores têm vindo a problematizar a ideia de que o interesse público se beneficiaria de uma prevalência a priori, em abstrato, em face dos direitos fundamentais dos particulares. O mesmo argumento pode ser invocado com relação

ao princípio da eficiência, que deve ser ponderado, nos casos concretos, com os princípios e direitos fundamentais eventualmente em jogo.

(...)

O deslinde de tal questão deve necessariamente passar por uma compreensão mais alargada da privacidade e da proteção de dados pessoais, que levem em consideração o seu valor social para além de sua perspectiva individualista. Nessa linha, autores como Raab (2012:129) e Solove (2008:80-93) desenvolvem argumentos para que se abandone a formulação na qual privacidade individual e interesse público são apresentados como valores contrapostos, enfatizando o papel da privacidade e da proteção de dados pessoais para a própria democracia e para a vida em sociedade, ao encorajar a autonomia moral do cidadão e viabilizar direitos políticos, como a liberdade de associação e a criação de espaços de discussão cívica sem temor de represálias.

Tal compreensão permite colocar a proteção de dados pessoais e o interesse público em posições não contrapostas, mas como elementos que se reforçam mutuamente.

(...) A questão a ser enfrentada, portanto, é de assegurar que no desempenho de suas missões, inclusive na dimensão de normatização, a atuação do Poder Público se dê de maneira a buscar a concordância prática entre princípios como os da eficiência, do interesse público e da publicidade, e os princípios constantes da LGPD, como os da finalidade, da adequação e da necessidade, orientados pela ideia de autodeterminação informativa do cidadão.

18. Trata-se, portanto, de um novo regime jurídico no campo do Direito Administrativo, trazendo novos parâmetros para a relação entre o Estado e os cidadãos.

Análise da questão pelo Supremo Tribunal Federal

19. Em maio de 2020, o STF examinou a questão da proteção de dados à luz da Constituição Federal na ocasião do julgamento, pelo Plenário, das Ações Diretas de Constitucionalidade nºs 6.387, 6.388, 6.389, 6.390 e 6.393.

20. Por meio da análise da constitucionalidade da transferência de dados pessoais de consumidores por empresas de telefonia ao IBGE, durante o período da pandemia da Covid-19, para a realização da Pesquisa Nacional por Amostra de Domicílios – PNAD, nos termos da MP nº 954/2020, o STF estabeleceu o âmbito de proteção e os limites constitucionais à intervenção estatal sobre a garantia à proteção de dados e autodeterminação informativa e reconheceu o direito à proteção de dados como um direito fundamental, autônomo, extraído a partir da leitura sistemática da Constituição Federal[10].

21. Ao longo dos votos da extensa maioria que referendou a cautelar concedida pela Ministra Rosa Weber, restou assentado que, embora o princípio da convivência das liberdades públicas limite os direitos e garantias fundamentais – tais como a vida privada, a intimidade e o sigilo de dados –, a privacidade somente pode ceder diante de justificativa consistente e legítima.

22. Assim, o interesse público legítimo capaz de autorizar o compartilhamento de dados dos cidadãos define-se pela necessidade, adequação e proporcionalidade da medida e essa avaliação exige que sejam reveladas a forma e a finalidade da utilização dos dados, além da limitação do tratamento ao mínimo possível.

23. Ademais, registrou-se a necessidade de adoção de mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida.

24. Para o STF, a mera previsão de que os dados serão utilizados com exclusividade por determinado órgão não é suficiente. É necessário garantir que o tratamento ocorrerá de forma segura.

25. Segundo Laura Schertel[11], na decisão liminar, a Ministra Rosa Weber trouxe *o conceito de dado pessoal e sua tutela constitucional de modo ampliado*, de forma que, *aparentemente, a interpretação constitucional conferida foi a de que qualquer dado que leve à identificação de uma pessoa pode ser usado para a formação de perfis informacionais de grande valia para o mercado e para o Estado e, portando, merece proteção constitucional*.

26. Em 24 de junho do mesmo ano, foi concedida pelo Ministro Gilmar Mendes medida cautelar, *ad referendum* do Plenário, na Arguição de Descumprimento de Preceito Fundamental nº 695 do Distrito Federal (ADPF 695), em que era requerido o reconhecimento e reparação de grave lesão a preceitos fundamentais pelo poder público em razão de compartilhamento de dados pessoais pelo Serpro com a Agência Brasileira de Inteligência (ABIN), com base no Decreto nº 10.046, de 9 de outubro de 2019.

27. Esse julgado, após detida análise da evolução dos direitos à privacidade e à proteção de dados, com ênfase na nova perspectiva da privacidade como indutora da cidadania e da democracia à força da realidade decorrente do processamento dos dados pessoais, conclui que *o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e inciso X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea*".

6. A coordenadora dos estudos, ao encaminhar a minuta de resolução à Presidência, apresentou considerações relevantes para a análise deste Plenário, a saber (ID 144195488):

> "Em atenção ao despacho GAB-DG 1707261, trago as seguintes considerações trazidas no Parecer ASJUR nº 327/2021 (1686028), que trata sobre a minuta de resolução que institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral (1664316):
>
> *a) nos considerando, acrescentar: CONSIDERANDO a relevância da proteção à autonomia informativa dos cidadãos para a democracia;*
>
> Trata-se de um 'considerando' adicional importante, que pode ser acrescentado e torna a Minuta mais completa.
>
> *b) no art. 8º, V, substituir 'que tenha estrita necessidade' por 'estritamente necessário';*
>
> Trata-se de alteração de redação que traz mais clareza ao texto.
>
> *c) no art. 10, I, informar a resolução que instituiu a PSI-JE, Res. TSE nº 23.644/2021;*
>
> De acordo.
>
> *d) com relação ao art. 14, IV, sugere-se estabelecer na norma o processo e os critérios mínimos para o reconhecimento de que os dados são desnecessários, excessivos ou tratados em desconformidade;*
>
> Não vejo necessidade em se alterar a redação proposta na Minuta. A Administração Pública é quem deve fazer um primeiro exame acerca da finalidade, necessidade e adequação do tratamento de dados por ela feito. O cidadão, avaliando que o exame foi incorreto, tem o ônus de explicitar as razões de sua compreensão diversa, pelos motivos dispostos na LGPD e que poderão vir a ser estabelecidos em normas mais específicas.
>
> *e) no que diz respeito ao inciso V, questionamos a pertinência da portabilidade no que diz respeito aos dados custodiados pela Justiça Eleitoral, à luz das ponderações de Miriam Wimmer[12]: 'Não faria sentido conceber que um cidadão pudesse requerer ao Poder Público a portabilidade de seus dados constantes de determinada base de dados governamentais,...';*
>
> A previsão contida na Minuta deu-se diante da possibilidade, ainda que potencial apenas, de que venha a existir alguma situação em que a aplicabilidade se aplique.
>
> *f) no § 1º do mesmo artigo, onde se lê 'sendo o tratamento baseado no consentimento', alterar para 'caso o tratamento seja baseado no consentimento';*
>
> Caso a avaliação da Corte seja a de que a redação proposta melhora a compreensibilidade do texto, não há oposição.
>
> *g) com relação ao Capítulo VI, indaga-se, preliminarmente, se as políticas e salvaguardas estão embasadas em processo de avaliação sistemática de impactos e riscos à privacidade, conforme a previsão do art. 50, I, d, da LGPD;*
>
> A formulação de regras explícitas de boas práticas é uma faculdade no caput do art. 50 da LGPD e ainda é preciso amadurecer institucionalmente para sua elaboração.
>
> *h) com relação ao relatório de impacto à proteção de dados pessoais, sugere-se previsão específica para este artefato, esclarecendo se deverá ser elaborado sempre que houver tratamento de dados pela Justiça Eleitoral ou em quais situações, bem como os seus requisitos mínimos. Sugere-se, como referência, o Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD)[13], elaborado pelo Comitê Central de Governança de Dados do Poder Executivo;*

O inciso II do parágrafo 1º do art. 15 da Minuta estabelece que o RIPD deverá ser revisto a cada dois anos ou, ainda, sempre que houver alteração relevante no tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos das pessoas. Quanto ao seu conteúdo, o inciso I deste mesmo parágrafo estabelece que será estabelecido pelo CGPD, o que tem a virtude de permitir um RIPD mais enxuto e mais factível diante da realidade da Justiça Eleitoral ou das necessidades que venham a surgir.

i) no art. 18, IV, substituir 'em conjunto' por 'em comum acordo'[14];

Não nos parece a melhor redação, pois o controlador conjunto pode ter essa condição como resultado de previsão legal, de modo que não se tratará de tratamento de dados por 'acordo'.

j) no art. 21, incluir inciso contemplando a elaboração de programa de governança, nos termos do art. 50, I, da LGPD.

Novamente, a formulação de regras explícitas de boas práticas é uma faculdade no caput do art. 50 da LGPD e ainda é preciso amadurecer institucionalmente para sua elaboração. Assim, não nos parece oportuna a formulação de uma tal exigência já na primeira Política Geral de Privacidade e Proteção de Dados Pessoais da Justiça Eleitoral.

Feitas essas considerações, sugiro a distribuição do presente Processo Administrativo para deliberação pelo Pleno do TSE".

7. Quanto a essas observações, manifesto-me favorável à sugestão apresentada pela Assessoria Jurídica quanto ao art. 14, § 1º, da minuta. A redação "sendo o tratamento baseado no consentimento" dá a entender que se trata de conjunção explicativa, contudo, a razão desse trecho é restringir a uma determinada hipótese, qual seja, o caso de o tratamento ser baseado no consentimento.

8. Ainda, em relação à minuta de resolução, dois pontos merecem destaque. *Em primeiro lugar*, uma das hipóteses que autoriza o tratamento de dados pessoais é o consentimento do titular, nos termos dos arts. 7º, I, e 11, I, da LGPD. Contudo, conforme dispõe o art. 6º da minuta, a Justiça Eleitoral poderá, no estrito limite de suas atividades, tratar dados pessoais sem o consentimento dos titulares, desde que observados os princípios estabelecidos pelo art. 6º da LGPD[1] e respaldada a sua atuação nas hipóteses elencadas nos arts. 7º, II a X, 11, II, 23, *caput*, 26 e 27, da LGPD[2].

9. *Em segundo lugar*, destaco que algumas regras concernentes ao "programa de governança em privacidade" ou ao "processo de avaliação sistemática de impactos e riscos à privacidade", providências mencionadas no art. 50, § 2º, I, da LGPD, não foram contempladas na presente proposta. Isso porque, conforme explicado pela coordenadora dos trabalhos, "a formulação de regras explícitas de boas práticas é uma faculdade no *caput* do art. 50 da LGPD e ainda é preciso amadurecer institucionalmente para sua elaboração", de modo que serão tratadas em futuras atualizações desta Política Geral. Nesse sentido, o art. 22 da minuta estabelece que a Justiça Eleitoral deverá reforçar e aprimorar constantemente a Política Geral de Privacidade e Proteção de Dados Pessoais, empreendendo estudos a fim de verificar a necessidade de sua revisão, no máximo a cada 3 (três) anos, atentando à evolução tecnológica e aos novos paradigmas de boas práticas. A par disso, nada impede que, embora não abordados nesta primeira Política Geral de Privacidade e Proteção de Dados Pessoais, sejam estabelecidas pelos Tribunais Eleitorais regras e programas de boas práticas em gestão de dados pessoais.

10. Com essas considerações, proponho a aprovação da presente minuta pelo Plenário desta Corte.

11. É como voto.

---

[1] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[2] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

II – para o cumprimento de obrigação legal ou regulatória pelo controlador;

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – apoio e promoção de atividades do controlador; e

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

(...)

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I – em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II – (VETADO);

III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV – quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)

V – na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades. (Incluído pela Lei nº 13.853, de 2019)

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:

I – nas hipóteses de dispensa de consentimento previstas nesta Lei;

II – nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do *caput* do art. 23 desta Lei; ou

III – nas exceções constantes do § 1º do art. 26 desta Lei.

Parágrafo único. A informação à autoridade nacional de que trata o *caput* deste artigo será objeto de regulamentação. (Incluído pela Lei nº 13.853, de 2019)

EXTRATO DA ATA

PA Nº 0600343-06.2021.6.00.0000/DF. Relator: Ministro Luís Roberto Barroso. Interessado: Tribunal Superior Eleitoral.

Decisão: O Tribunal, por unanimidade, aprovou a minuta de resolução que institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral, nos termos do voto do relator.

Composição: Ministros Luís Roberto Barroso (presidente), Edson Fachin, Alexandre de Moraes, Luis Felipe Salomão, Mauro Campbell Marques, Sérgio Banhos e Carlos Horbach.

Vice-Procurador-Geral Eleitoral: Paulo Gustavo Gonet Branco.

SESSÃO DE 9.9.2021.

Assinado eletronicamente por: LUÍS ROBERTO BARROSO
13/09/2021 14:50:14
https://pje.tse.jus.br:8443/pje-web/Processo/ConsultaDocumento/listView.seam
ID do documento: 154886838

21091314501411900000153603234

IMPRIMIR GERAR PDF