



COLÉGIO DOS ENCARREGADOS PELO TRATAMENTO DE DADOS PESSOAIS
DO MINISTÉRIO PÚBLICO

ESTUDO TÉCNICO

A PROTEÇÃO DE DADOS PESSOAIS E O USO DE REGISTRO DE CONEXÃO, DE ACESSO A APLICAÇÕES E DE GEOLOCALIZAÇÃO PELOS ÓRGÃOS DA ADMINISTRAÇÃO SUPERIOR DO MINISTÉRIO PÚBLICO

Agosto/2025

ENCARREGADOS PELO TRATAMENTO DE DADOS PESSOAIS DO MINISTÉRIO PÚBLICO

ALBERTO VINICIUS CARTAXO DA CUNHA
Encarregado MPPB

ANA PAULA MACHADO FRANKLIN
Encarregada CNMP

ANDERSON BATISTA DE SOUZA
Encarregado MPAP

ANTONIO IRAN COELHO SÍRIO
Encarregado MPCE

AUGUSTO CÉSAR LEITE DE RESENTE
Encarregado MPSE

CARLOS RENATO SILVY TEIVE
Encarregado MPSC

CLEBER COUTO
Encarregado MPMG

CLEY BARBOSA MARTINS
Encarregada MPAM

DANILO ELIAS PEREIRA
Encarregado MPGO

ERICKSON GIRLEY BARROS DOS SANTOS
Encarregado MPRN

FELIPE MAGNO SILVA FONSECA
Encarregado MPRO

FERNANDA WEIAND
Encarregada MPRS

GUILHERME MAGALHÃES MARTINS
Encarregado MPRJ

HUGO EVO MAGRO CORRÊA URBANO
Encarregado MPPR

JANAÍNA DO SACRAMENTO BEZERRA
Encarregada MPPE

JORGE AUGUSTO CAETANO DE FARIAS
Encarregado MPM

JORGE LUIZ DA COSTA PESSOA
Encarregado MPPI

JOSÉ FERNANDO RUIZ MATURANA
Encarregado Titular MPT

DIEGO JIMENEZ GOMES
Encarregado Adjunto MPT

JOSÉ MARIANO DE ALMEIDA NETO
Encarregado MPMT

LAURO FRANCISCO DA SILVA FREITAS
JÚNIOR
Encarregado MPPA

LEONARDO ANDRADE MACEDO
Encarregado MPF

LINCOLN ZANIOLO
Encarregado MPRR

LUIS HENRIQUE CORRÊA ROLIM
Encarregado MPAC

MARIA CRISTINA ROCHA PIMENTEL
Encarregada MPES

NATÁLIA MACEDO LUNA TAVARES
Encarregada MPMA

PAULO ROBERTO GONÇALVES
ISHIKAWA
Encarregado MPMS

RODRIGO FOGAGNOLO MAURICIO
Encarregado MPDFT

RUI GOMES SANCHES JUNIOR
Encarregado MPBA

TARSO RIZO OLIVEIRA RIBEIRO
Encarregado MPTO

TIAGO CINTRA ZARIF
Encarregado MPSP

VICENTE JOSÉ CAVALCANTE
PORCIÚNCULA
Encarregado MPAL

GRUPO DE TRABALHO PARA O ESTUDO TÉCNICO

ANDERSON BATISTA DE SOUZA
Encarregado MPAP

CARLOS RENATO SILVY TEIVE
Encarregado MPSC

GUILHERME MAGALHÃES MARTINS
Encarregado MPRJ

GRUPO DE TRABALHO**“A PROTEÇÃO DE DADOS PESSOAIS E O USO DE REGISTRO DE CONEXÃO, DE
ACESSO A APLICAÇÕES E DE GEOLOCALIZAÇÃO PELOS ÓRGÃOS DA
ADMINISTRAÇÃO SUPERIOR DO MINISTÉRIO PÚBLICO”****ESTUDO TÉCNICO****1. APRESENTAÇÃO**

Ab initio, cumpre ressaltar que a vigência da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709/18) e a promulgação da Emenda Constitucional n. 115, respectivamente em 18/9/2020 e em 10/2/2022, trouxeram ao cenário nacional substanciais alterações quanto ao tratamento de dados pessoais.

É bem verdade que o ordenamento jurídico brasileiro já tutelava a proteção de dados pessoais por meio de leis esparsas – Lei n. 12.527/2011 (Lei de Acesso à Informação, art. 4º, inciso IV e art. 31); Lei n. 8.078/90 (Código de Defesa do Consumidor, arts. 43 e 44); Lei n. 12.965/2014 (Marco Civil da Internet, art. 7º, incisos VII a X), apenas para citar alguns exemplos.

Contudo, as alterações legislativas mais recentes acima mencionadas, além de haverem erigido a proteção de dados pessoais ao *status* de direito fundamental expresso (art. 5º, LXXIX, da CF/1988), introduziram um novo paradigma quanto à coleta, armazenamento, acesso e difusão de dados pessoais, instituindo um sistema protetivo, proporcionando uma isonomia em relação a outros direitos fundamentais, fundamental para a proteção de liberdades fundamentais, como a privacidade, o direito à informação e à transparência.¹

Especificamente em relação ao Ministério Público, é importante destacar que – considerando suas particularidades institucionais e a dupla responsabilidade de, ao mesmo tempo, observar a proteção de dados pessoais como agente de tratamento e tutelar esse direito fundamental por meio de seus órgãos de execução – foi aprovada, em 12 de dezembro de 2023, a Resolução CNMP n. 281. Essa norma estabelece diretrizes substanciais para orientar esse processo, instituindo a Política Nacional de Proteção de

¹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2.ed. São Paulo: Revista dos Tribunais, 2020. p.264.

Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no âmbito do Ministério Público.

É certo que as referidas construções normativas estão em consonância com as melhores normas internacionais que regem a matéria, notadamente o Regulamento Geral Europeu (RGPD), bem como que visam proteger a pessoa natural em uma sociedade na qual, diante do avanço tecnológico, o tratamento de dados pessoais é massivo.

Nesse contexto, no 5º Encontro Nacional de Encarregados pelo Tratamento de Dados Pessoais dos Ministérios Públicos dos Estados, da União e do CNMP, realizado em 03 de abril de 2025, na sede do Ministério Público do Estado do Espírito Santo na cidade de Vitória/ES, veio à baila, a partir de discussões realizadas entre os Encarregados, a importância de se analisar, sob a perspectiva da proteção de dados pessoais, o monitoramento, pela Corregedoria-Geral do Ministério Público, de endereços de IP de membros com a finalidade de verificar o cumprimento da obrigação de residência na comarca de lotação e/ou de estarem comparecendo fisicamente nas Promotorias de Justiça.

Como decorrência da necessidade de se aprofundar a análise do tema, foi deliberado, na oportunidade, pela criação de um Grupo de Trabalho formado pelos seguintes Encarregados: Anderson Batista de Souza (MPAP), Carlos Renato Silvy Teive (MPSC) e Guilherme Magalhães Martins (MPRJ).

Nessa senda, após reuniões e trabalhos realizados, apresenta-se, em 22 de agosto de 2025, no 6º Encontro Nacional de Encarregados pelo Tratamento de Dados Pessoais dos Ministérios Públicos dos Estados, da União e do CNMP, o presente estudo técnico para discussão e deliberação.

2. INTRODUÇÃO

É indubitável que, no cumprimento de suas obrigações legais², a Corregedoria-Geral do Ministério Público é o órgão orientador e fiscalizador da conduta dos membros do Ministério Público, incumbindo-lhe, dentre outras atribuições, a fiscalização da obrigação imposta a todos os membros do Ministério Público, tanto pela Constituição

² Lei n. 8.625/93. Art. 17. A Corregedoria-Geral do Ministério Público é o órgão orientador e fiscalizador das atividades funcionais e da conduta dos membros do Ministério Público, incumbindo-lhe, dentre outras atribuições:

[...]

V- instaurar, de ofício ou por provocação dos demais órgãos da Administração Superior do Ministério Público, processo disciplinar contra membro da instituição, presidindo-o e aplicando as sanções administrativas cabíveis, na forma da Lei Orgânica;

Federal³, quanto pela Lei Orgânica Nacional⁴, de residir na comarca de lotação, salvo autorização do chefe da instituição. Além disso, incumbe-lhe também fiscalizar, por exemplo, conforme Recomendação do CNMP⁵, a presença física dos membros do Ministério Público em audiências e atos judiciais presenciais.

Entretanto, não há dúvidas de que, mesmo no cumprimento de suas obrigações legais, a atividade orientadora e fiscalizadora da Corregedoria-Geral do Ministério Público deverá ser exercida observando o direito fundamental à proteção de dados pessoais.

A propósito, dispõe o art. 108, *caput*, e §1º, da Resolução CNMP n. 281:

Art. 108. No exercício do dever de monitoramento e supervisão administrativa, decorrentes da relação legal, estatutária, empregatícia ou contratual, o CNMP, os ramos e as unidades do Ministério Público, o quanto possível, deverão balancear e proteger a privacidade de seus membros, servidores, estagiários e prestadores de serviços em cotejo com o necessário tratamento de dados pessoais.

§1º Para a finalidade institucional indicada no caput deste artigo, o exercício de ponderação anteriormente referido deverá levar sempre em conta os princípios da necessidade, legitimidade, proporcionalidade e transparência e/ou comunicação ao titular dos dados pessoais.

Assim, o presente estudo se propõe a analisar se os registros de conexão (endereço de IP) e de acesso a aplicações, bem como a geolocalização, sob a perspectiva da proteção de dados pessoais, podem ser utilizados não só por Corregedorias-Gerais, mas também pelos demais órgãos da Administração Superior e, em caso positivo, em que medida, no exercício do poder disciplinar.

No que se refere à geolocalização, embora não tenha sido objeto de discussão inicial e nem haja indícios de sua utilização por órgãos correcionais no âmbito do Ministério Público, sua relação direta com o tema em análise justifica sua inclusão como elemento a ser examinado também no presente estudo.

³ Art. 129, §2º. As funções do Ministério Público só podem ser exercidas por integrantes da carreira, que deverão residir na comarca da respectiva lotação, salvo autorização do chefe da instituição.

⁴ Art. 43. São deveres dos membros do Ministério Público, além de outros previstos em lei:

[...]

X- residir, se titular, na respectiva Comarca;

⁵ Recomendação de Caráter Geral n. 1/2024. Art. 1º Recomendar às Corregedorias-Gerais das unidades e ramos dos Ministérios Públicos da União e dos Estados que promovam a fiscalização regular da presença física dos(as) membros(as) do Ministério Público em audiências e atos judiciais presenciais, salvo em situações justificadas.

3. OS REGISTROS DE CONEXÃO E DE ACESSO A APLICAÇÕES E A GEOLOCALIZAÇÃO SÃO DADOS PESSOAIS?

Inicialmente, para verificar a aplicabilidade das normas de proteção de dados pessoais à situação em análise, é necessário avaliar se os dados referentes aos registros de conexão, de acesso a aplicações e de geolocalização dos membros do Ministério Público caracterizam-se como dados pessoais.

Com efeito, o art. 1º da Lei Geral de Proteção de Dados Pessoais (LGPD)⁶ delimita expressamente seu campo de aplicação ao tratamento de dados pessoais. Dessa forma, um amplo conjunto de informações que não se enquadra nessa categoria permanece fora do escopo de incidência da norma.

Comentando aludida questão, trazem-se à colação os ensinamentos de Rony Vainzof⁷:

A Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) se preocupa e versa apenas e tão somente sobre o tratamento de dados pessoais. Ou seja, não atinge diretamente dados de pessoa jurídica, documentos sigilosos ou confidenciais, segredos de negócio, planos estratégicos, algoritmos, fórmulas, *softwares*, patentes, entre outros documentos ou informações que não sejam relacionadas a pessoa natural identificada ou identificável. Toda essa miríade de outros tipos de informações ou documentos podem encontrar tutela em distintos diplomas legais, como a Lei de Proteção Industrial (Lei 9.279/1996), a Lei de Direitos Autorais (Lei 9.610/1998) e a Lei de Software (Lei 9.609/1998), apenas para citar alguns exemplos, mas não na LGPD.

Feita essa consideração inicial, passa-se, doravante, a analisar cada um dos dados em questão e a sua classificação como dado pessoal ou não.

Ressalta-se que não é o propósito do presente estudo aprofundar a análise técnica acerca dos “registros de conexão” e de “acesso a aplicações” e tampouco de “geolocalização”, até mesmo porque diferentes aplicações e redes são utilizados pelos ramos e unidades do Ministério Público brasileiro e seria inviável analisá-los com a amplitude necessária neste estudo, mas apenas verificar a categorização desses dados como pessoais ou não, bem como a tutela jurídica que lhes é conferida⁸.

⁶ Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

⁷ LGPD: Lei Geral de Proteção de Dados comentada. Coordenada por Viviane Nóbrega Maldonado e Renato Opice Blum. 4 ed. Ver. E atual. São Paulo: Thomson Reuters Brasil, 2022. P. 21-22.

⁸ Reconhece-se que, devido à diversidade de sistemas e/ou redes utilizados pelos diferentes ramos e unidades do Ministério Público, pode haver situações em que os dados gerados a partir do uso de uma aplicação voltada à atividade-fim não se enquadrem, de forma estrita, como registros de conexão ou de acesso a aplicações, conforme definidos pelo Marco Civil da

Como ponto de partida, o art. 5º, incisos VI e VII, da Lei n. 12.965/2014 (Marco Civil da Internet), define o que se considera “registros de conexão” e “acesso a aplicações”:

Art. 5º Para efeitos desta Lei, considera-se:

[...]

VI- registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII- aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

Em complemento, tem-se o art. 14, inciso I, do Decreto n. 8.771/2016, que, ao regulamentar o Marco Civil da Internet, dispõe sobre o que se considera dado pessoal:

Art. 14. Para os fins do disposto neste Decreto, considera-se:

I- dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;

No mesmo sentido, o art. 5º, inciso I, da LGPD, define dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”, isto é, a norma brasileira de proteção de dados pessoais adotou um critério expansionista para considerar como tal não apenas aquilo que identifica diretamente a pessoa natural, mas também aquele conjunto de dados que permite identificar a pessoa, a depender da situação em concreto.

Sobre o conceito de dado pessoal previsto na LGPD, tem-se o escólio de Arthur Pinheiro Basan⁹:

Portanto, em linhas gerais, a compreensão do conceito de dado pessoal, essencial para o entendimento da LGPD, parte de uma definição flexível e fluida, em razão da ampla possibilidade de informações que, por meio do tratamento de dados, são capazes de tornar o titular identificável ou mesmo capazes de formar um perfil a seu respeito, interferindo no livre desenvolvimento da sua personalidade, enquanto pessoa humana. Por isso, **é possível afirmar que um dado ser considerado pessoal ou não demanda uma análise contextual**, ou seja, depende da informação que, após passar pelo devido tratamento, pode ser extraída de um determinado banco de dados. (Grifou-se)

Internet. No entanto, essa circunstância não descaracteriza, por si só, a natureza desses dados como pessoais ou não. Por essa razão, optou-se por tratá-los sistematicamente como registros de conexão e de aplicação, mesmo ciente dessa particularidade. Além disso, essa variação de sistemas utilizados poderá implicar maiores restrições de acesso, nas hipóteses em que o ramo ou a unidade, na qual a respectiva Corregedoria esteja vinculada, não possuir os registros de conexão e de aplicação, conforme será melhor abordado no tópico 5.

⁹ Comentários à lei geral de proteção de dados pessoais / Alexandre Pereira Bonna ... [et al.]; coordenado por Guilherme Magalhães Martins, João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior. Indaiatuba, SP: Editora Foco, 2022. p. 41.

Nessa senda, embora se reconheça que se possa, a depender da situação em concreto, admitir a existência em tese de “registros de conexão” e de “acesso a aplicações”¹⁰ que excepcionalmente não se enquadrem como dados pessoais, não há dúvidas de que, em regra, serão considerados pessoais, máxime quando tratados pelos órgãos correccionais com a finalidade de apurar a conduta de um servidor, estagiário, prestador de serviço ou membro específico do Ministério Público.

Quanto à geolocalização, aplica-se o mesmo critério utilizado para definição de dado pessoal. Se, na situação concreta, o dado permitir a identificação de uma pessoa natural – seja por sua precisão ou por sua vinculação a outras informações (como identificadores técnicos previamente associados ao titular) – ele deverá ser classificado como dado pessoal. Por outro lado, se a identificação da pessoa natural não for possível, nem direta nem indiretamente, o dado não será considerado pessoal, e, portanto, não estará submetido ao regime jurídico de proteção de dados.

Em síntese, os dados de conexão e de acesso a aplicações de internet serão considerados dados pessoais, assim como os de geolocalização, quando utilizados por órgãos correccionais. Isso porque, na prática, esses dados só terão utilidade quando, no caso concreto, for possível identificar um determinado membro do Ministério Público.

4. EXISTE HIPÓTESE LEGAL QUE AUTORIZA ESSE TRATAMENTO?

É importante destacar que a classificação de tais dados como pessoais não significa, por si só, que não possam ser utilizados pelos órgãos correccionais. Contudo, em razão dessa classificação, balizas mais restritivas deverão ser observadas, sob pena de afronta ao direito fundamental à proteção de dados pessoais.

Dessa forma, considerando que os dados pessoais em tela são considerados comuns e não sensíveis¹¹, para ser considerado regular esse tratamento, primeiro, ele deve ser embasado em, pelo menos, uma hipótese legal, prevista no art. 7º da LGPD.

¹⁰ Por exemplo, compartilhamento de IPs (IPv4) entre mais de um usuário de internet, de forma a ser inviável no caso específico identificar quem seja o responsável.

¹¹ Art. 5º Para os fins desta Lei, considera-se:

[...]

II- dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

In casu, a base legal para o tratamento em questão encontra respaldo no art. 7º, II, c/c art. 23, ambos da LGPD, que autoriza o tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatório pelo controlador.

Sobre o cumprimento de obrigação legal ou regulatória, extrai-se do Guia Orientativo da ANPD, que aborda o Tratamento de dados pessoais pelo Poder Público¹²:

Conforme o art. 7º, II, da LGPD, o tratamento de dados pessoais pelo Poder Público poderá ser realizado “para o cumprimento de obrigação legal ou regulatória pelo controlador”. A mesma hipótese está prevista no art. 11, II, a, que rege o tratamento de dados sensíveis.

De forma geral, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, que se diferenciam em razão da espécie de norma jurídica que estabelece a obrigação a ser cumprida. É o caso, em especial, das normas de conduta e das **normas de organização**.

[...]

Já na segunda hipótese, a obrigação legal decorre de normas de organização, assim entendidas **as normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições. Nesse contexto normativo, o tratamento de dados pessoais é parte essencial do exercício de prerrogativas estatais típicas, uma vez que necessário para viabilizar a própria execução das atribuições, competências e finalidades públicas da entidade ou do órgão público.**

Assim, diferentemente das normas de conduta, que estabelecem obrigações de forma direta e expressa, prevendo uma consequência específica em caso de descumprimento, as normas de organização estabelecem obrigações que estão associadas, de forma mais geral, ao próprio cumprimento e à execução de atribuições legais típicas da entidade ou do órgão público responsável pelo tratamento de dados pessoais. (Grifou-se)

Ora, conforme já destacado acima, nos termos do art. 17 da Lei Orgânica Nacional do Ministério Público (Lei n. 8.625/93), incumbe à Corregedoria-Geral do Ministério Público orientar e fiscalizar as atividades funcionais e a conduta dos membros do Ministério Público, e, em alguns Estados, o de servidores da Instituição, sendo certo que, para cumprir esse seu mister, invariavelmente terá que tratar dados pessoais dos membros ou de servidores do Ministério Público, inclusive esses que não são considerados dados pessoais sensíveis. Nesses termos, tornam-se prescindíveis maiores digressões nesse ponto.

¹² Guia Orientativo: Tratamento de dados pessoais pelo Poder Público, versão 2.0, Brasília: 2023, p. 15-16. Disponível em: <<https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf/view> >

5. DOS PRINCÍPIOS DE PROTEÇÃO

É cediço que para que um tratamento de dados pessoais seja considerado regular, não basta que esteja calcado numa hipótese legal, ele deve observar também os princípios previstos no art. 6º da LGPD e, no caso específico do Ministério Público, ainda ao disposto no art. 3º da Resolução CNMP n. 281/2023.

Assim, embora seja necessária a observância de todos os princípios lá previstos, considerando as especificidades da situação em análise – dados pessoais de membros do Ministério Público tratados por órgãos correccionais – mostra-se especialmente relevante abordar os seguintes: finalidade, adequação, necessidade (proporcionalidade), transparência, segurança e qualidade dos dados.

A propósito, extrai-se do art. 6º, incisos I, II, III, VI e VII da LGPD:

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;

[...]

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;

No tocante aos princípios da finalidade, adequação e necessidade, cabe destacar que eles preconizam a menor quantidade de dados pessoais necessária para se atingir uma finalidade pretendida de forma adequada.

Ou seja, se para aferir a presença física de um determinado membro do Ministério Público numa comarca, é suficiente para o órgão de controle a informação de que ele acessou o sistema, utilizado para o trabalho na área-fim da instituição, a partir de uma rede da própria instituição, não se mostra consentâneo com a proteção de dados pessoais a

utilização de outros dados pessoais mais invasivos ou desnecessários, como por exemplo, a geolocalização precisa por meio de um celular funcional.

Da mesma forma, se a finalidade pretendida pelo órgão correcional é apurar, por exemplo, o exercício irregular de atividade político-partidária de um determinado membro, não se mostra em consonância com a proteção de dados pessoais a utilização de dados desnecessários a essa finalidade, como por exemplo dados pessoais para aferir a presença física na comarca pelo membro.

Nesse aspecto, cabe ainda especial destaque ao art. 3º, I, da Resolução CNMP n. 281/2023, que aponta como princípios vetores para a promoção da proteção de dados pessoais pelo Ministério Público a proporcionalidade e a razoabilidade.

Além disso, abordando especificamente a questão do dever de monitoramento e supervisão administrativa, decorrente da relação estatutária, o art. 108 da referida resolução, já citado acima, reitera que o CNMP, os ramos e as unidades do Ministério Público, na medida do possível, deverão balancear e proteger a privacidade de seus membros, em cotejo com o necessário tratamento de dados pessoais. E ainda, em seu §1º, dispõe que para tanto deverá “levar sempre em conta os princípios da necessidade, legitimidade, proporcionalidade e transparência e/ou comunicação ao titular dos dados pessoais”.

Nesses termos, a Política Nacional de Proteção de Dados Pessoais do Ministério Público reitera, com especial ênfase, a importância de se observar os princípios da proporcionalidade e da razoabilidade – os quais estão intimamente ligados aos da finalidade, adequação e necessidade já abordados – na utilização de dados pessoais para fins de monitoramento e supervisão administrativa, o que por certo se insere a atividade correcional em questão.

O conceito jurídico de proporcionalidade, ensina Jane Reis Pereira¹³, traduz uma estrutura de pensamento consistente em avaliar a correlação entre os fins visados e meios empregados nos atos do poder público. Para a autora, possui como subprincípio a necessidade, que tem por conteúdo a noção de que, dentre várias medidas restritivas de direitos fundamentais igualmente aptas para atingir o fim perseguido, a Constituição impõe que o legislador opte por aquela menos lesiva para os direitos.

Para Luis Roberto Barroso, a proporcionalidade se tornou um mecanismo de controle dividido em três etapas, na qual se vai verificar: (i) a adequação de uma medida

¹³ PEREIRA, Jane Reis. Os imperativos de razoabilidade e proporcionalidade. In: BARROSO, Luís Roberto (organizador). A reconstrução democrática do Direito Público no Brasil. Rio de Janeiro: Renovar, 2007. p.162-163 e 183.

para produzir determinado resultado (idoneidade do meio para realizar o fim visado); (ii) a necessidade da providência, sendo vedado o excesso (se houver meio menos gravoso para atingir o mesmo fim é ilegítimo o meio mais gravoso); e (iii) a proporcionalidade em sentido estrito, pela qual se afere se o fim justifica o meio, vale dizer, se o que se ganha é mais valioso do que o que se sacrifica.¹⁴

Essa especial observância não tem o condão de obstar à utilização desses dados pelos órgãos correccionais, pois, a depender da situação em concreto, mostrar-se-á mais razoável o emprego, por exemplo, de um registro de aplicação de um membro no sistema utilizado pela própria instituição para o trabalho na atividade-fim, do que o tratamento de outros dados pessoais que poderão mostrar-se até mais invasivos.

Em síntese, os princípios da razoabilidade e da proporcionalidade devem ser aferidos com base no caso concreto e devem orientar o tratamento dos dados pessoais, inclusive quanto à forma de acesso e de utilização.

Por exemplo, é razoável que, no exercício regular das atribuições do órgão correccional – ainda que não haja prévia instauração de procedimento administrativo disciplinar – seus integrantes (e apenas eles), na instrução de um procedimento ordinário de correção, tenham acesso às manifestações exaradas pelos membros, incluindo informações sobre data de finalização, assinatura e se o acesso ao sistema se deu a partir da rede institucional ou de rede externa, desde que, neste último caso, não seja possível identificar o local de onde ocorreu esse acesso.

Por outro lado, caso a Corregedoria necessite de informações mais específicas sobre o local externo de acesso (como endereço IP, geolocalização, entre outros), por se tratar de medida mais invasiva à privacidade e à proteção de dados pessoais do membro do Ministério Público, não se mostra razoável que esse acesso ocorra de forma ordinária, sem a prévia instauração de procedimento administrativo voltado à apuração de eventual falta funcional e desde que haja indícios razoáveis para tanto.

No tocante à legitimidade, também previsto de forma especial na resolução, tem-se que são desnecessárias maiores considerações, pois não há dúvidas de que a Corregedoria-Geral do Ministério Público a possui para a finalidade de monitoramento e supervisão, pois inerentes às suas funções.

¹⁴ BARROSO, Luís Roberto. Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo. 13. ed. São Paulo: Saraiva, 2025.p.383.

Nesse caminho, mostra-se necessário abordar apenas mais três princípios: o da transparência; o da segurança e o da qualidade dos dados.

No que tange ao princípio da transparência, é necessário admitir que este é um aspecto que, em regra, ainda demanda aprimoramento por parte dos ramos e unidades do Ministério Público. Com efeito, ao que se tem conhecimento, inexistem normas institucionais publicadas disciplinando o uso desses dados pessoais e tampouco os sistemas utilizados pelos membros, no exercício da atividade-fim, apresentam, em sua estrutura, avisos de privacidade com informações claras e precisas sobre o tratamento de dados pessoais realizado, bem como sobre suas finalidades específicas. Assim, imperiosa torna-se essa adequação para que os membros do Ministério Público, assim como servidores, terceirizados e estagiários, tenham ciência de que seus dados pessoais, no caso, consistentes em registros de conexão e de aplicação e de geolocalização, enfim, dados que permitam aferir sua presença física na Promotoria de Justiça, colhidos a partir do uso do sistema para o trabalho na área-fim, possam ser utilizados para fins correccionais.

No que se refere ao princípio da segurança, embora se admitida que suas diretrizes recaiam predominantemente sobre as áreas técnicas – como a Gerência de Segurança da Informação, a Coordenação de Tecnologia, entre outras – e que se aplicam a todos os dados pessoais tratados pela instituição (não apenas de membros), é pertinente destacar, no contexto específico em análise, um aspecto essencial: o controle de acesso.

O controle de acesso deve ser buscado com a adoção de medidas técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados. Assim, por exemplo, devem ser estabelecidos um controle restrito sobre o acesso a esses dados de conexão e de aplicação e de geolocalização, no âmbito da própria Administração, de forma que se conceda acesso apenas a quem efetivamente precise, bem como que se preveja, em conjunto com as áreas técnicas, mecanismos de auditoria de acesso a esses dados, mediante registros robustos de logs, que permitam rastrear, de forma confiável, quem acessou quais dados e em que momento (registros de logs).

Quanto ao acesso aos registros de conexão e de aplicação, é importante destacar ainda que se, em razão do sistema utilizado para o desenvolvimento dos trabalhos na área-fim, o ramo ou a unidade do Ministério Público não detenha esses dados pessoais e seja necessário obtê-los junto a um provedor, imperiosa será a observância do disposto no art. 10 do Marco Civil da Internet.

O princípio da qualidade dos dados, previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), determina que os dados pessoais tratados por qualquer instituição –

inclusive pelo Ministério Público no contexto correcional – devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade específica do tratamento.

Isso significa que, ao coletar, armazenar ou utilizar dados pessoais, a instituição deve garantir que essas informações estejam corretas e adequadas ao objetivo pretendido. Por exemplo, se a finalidade é apurar a presença física de um membro, servidor, estagiário ou terceirizado em determinada unidade, devem ser utilizados apenas os dados realmente necessários para essa verificação, assegurando que estejam corretos e não causem interpretações equivocadas.

Além disso, o princípio exige que, sempre que necessário, os dados sejam atualizados e que sejam adotadas medidas para corrigir informações incorretas ou desatualizadas. Isso evita, por exemplo, que decisões sejam tomadas com base em dados errôneos, protegendo tanto o titular dos dados quanto a própria instituição contra eventuais questionamentos ou falhas processuais.

Isso se acentua diante de limitações técnicas conhecidas, como variações na precisão de geolocalização fornecida por provedores ou o acesso intermediado por sistemas de terceiros. Nesses casos, é essencial reconhecer os limites objetivos das inferências possíveis com base em tais dados, evitando conclusões categóricas quando o grau de confiabilidade da informação for restrito.

Em resumo, a qualidade dos dados garante maior segurança, transparência e justiça no tratamento das informações pessoais, reforçando a confiança dos titulares e a responsabilidade dos órgãos públicos no uso desses dados.

6. DO PRAZO DE GUARDA

A LGPD prevê, em seu art. 15, inciso I, que o término do tratamento de dados pessoais ocorrerá, quando for verificado que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

Por sua vez, o artigo 16, inciso I, estabelece que “os dados pessoais serão eliminados após o término de seu tratamento”, mas que é autorizada a conservação para o “cumprimento de obrigação legal ou regulatória pelo controlador”.

Nesses termos, tem-se que, a princípio, devam as Corregedorias fixar um marco temporal que seja razoável para manutenção desses registros, considerando a finalidade correcional almejada, ressaltando-se, contudo, que, caso aplicável, deverão ser observados

os prazos definidos no Marco Civil da Internet, os quais poderão ser utilizados analogicamente¹⁵.

7. CONCLUSÕES E ENCAMINHAMENTOS

Este grupo de trabalho chega ao final deste estudo cômico da complexidade do tema, notadamente quanto às questões técnicas envolvidas que podem impactar até mesmo a categorização ou não dos dados em questão como registros de conexão e de aplicação, nos termos do Marco Civil da Internet, em razão da miríade de sistemas utilizados pelos ramos e Unidades do Ministério Público.

Ocorre que, não obstante essa circunstância, não há dúvidas de que os dados que permitam, tanto apontar a presença numa determinada Promotoria ou um endereço IP, quanto a geolocalização de um determinado membro ou servidor do Ministério Público, extraído a partir do uso de um sistema para trabalho na atividade-fim, são considerados dados pessoais e, portanto, sem prejuízo, nos termos do art. 64 da LGPD¹⁶, de incidência de outras normas protetivas específicas, deve-se observar a LGPD.

Nesse contexto, sugere-se para análise e decisão o seguinte posicionamento: “Reconhece-se a legalidade do tratamento de dados pessoais referentes a membros ou servidores do Ministério Público – incluindo registros de conexão, de aplicação e de geolocalização – realizado pelos órgãos da Administração Superior no exercício de seu poder disciplinar, desde que sejam respeitados os princípios da proteção de dados pessoais e definido um prazo para a guarda dessas informações, nos termos expostos ao longo do estudo”.

Após discussão, o posicionamento supra foi aprovado por unanimidade na reunião do Colégio dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público – CEDAMP, realizada no dia 22 de agosto de 2025, na sede do Ministério Público do Mato Grosso do Sul, no 6º Encontro Nacional de Encarregados e da Rede Nacional de Inovação Digital, com a sugestão de destaque dos seguintes pontos para que não houvesse dúvidas acerca das balizas a serem observadas quanto ao tratamento de dados pessoais em

¹⁵ Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

¹⁶ Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

questão: "Reconhece-se a legalidade do tratamento de dados pessoais referentes a membros ou servidores do Ministério Público - incluindo registros de conexão, de aplicação e de geolocalização - realizado pelos órgãos da Administração Superior no exercício de seu poder disciplinar, desde que a sua coleta tenha sido decorrente do uso voluntário, pelo integrante da Instituição, de sistemas eletrônicos internos ou redes de internet geridas pelo próprio órgão, e que sejam respeitados os princípios da proteção de dados pessoais, com a definição de prazo para a guarda dessas informações, nos termos expostos ao longo do estudo".

Campo Grande/MS, 22 de agosto de 2025.

ANDERSON BATISTA DE
SOUZA
Encarregado MPAP

CARLOS RENATO SILVY
TEIVE
Encarregado MPSC

GUILHERME
MAGALHÃES MARTINS
Encarregado MPRJ

REFERÊNCIAS BIBLIOGRÁFICAS

BARROSO, Luis Roberto. *Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 13. Ed. São Paulo: Saraiva, 2025.

BASAN, Arthur Pinheiro. Art. 5º. In *Comentários à lei geral de proteção de dados pessoais / Alexandre Pereira Bonna ... [et al.]; coordenado por Guilherme Magalhães Martins, João Victor Rozatti Longhi, José Luiz de Moura Faleiros Júnior*. Indaiatuba, SP: Editora Foco, 2022. p. 41.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília: Congresso Nacional, 1988.

_____. *Decreto n. 8.771, de 11 de maio de 2016 (Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.)*. Brasília: Presidência da República, 2016.

_____. *Guia orientativo: tratamento de dados pessoais pelo Poder Público*. Versão 2.0. Brasília: ANPD, 2023. Disponível em < <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf/view> >. Acesso em 05 ago. 2025.

_____. *Lei n. 8.078, de 11 de setembro de 1990 (Dispõe sobre a proteção do consumidor e dá outras providências)*. Brasília: Congresso Nacional, 1990.

_____. *Lei n. 8.625, de 12 de fevereiro de 1993 (Lei Orgânica Nacional do Ministério Público)*. Brasília: Congresso Nacional, 1993.

_____. *Lei n. 12.257, de 18 de novembro de 2011 (Lei de Acesso à Informação)*. Brasília: Congresso Nacional, 2011.

_____. *Lei n. 12.965, de 23 de abril de 2014 (Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil)*. Brasília: Congresso Nacional, 2014.

_____. *Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)*. Brasília: Congresso Nacional, 2018.

_____. *Recomendação de caráter geral n. 1, de 16 de julho de 2024 (Recomenda às Corregedorias-Gerais dos Ministérios Públicos da União e dos Estados a fiscalização regular da presença física dos(as) membros(as) do Ministério Público em audiências e atos judiciais presenciais, bem como em sessões de tribunais)*. Brasília: Conselho Nacional do Ministério Público e Corregedoria-Geral do Ministério Público, 2024.

_____. *Resolução n. 281, de 12 de dezembro de 2023 (Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no*

Ministério Público e dá outras providências). Brasília: Conselho Nacional do Ministério Público, 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2.ed. São Paulo: Revista dos Tribunais, 2020.

PEREIRA, Jane Reis. Os imperativos de razoabilidade e proporcionalidade. In: BARROSO, Luis Roberto(org.). *A reconstrução democrática do Direito Público no Brasil*. Rio de Janeiro: Renovar, 2007.

VAINZOF, Rony. *Capítulo I - Disposições Preliminares*. In MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice (Coord.). *LGPD: lei geral de proteção de dados comentada*. 2ª ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2022. p. 21-22.