CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

RESOLUÇÃO Nº 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.

O **CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO**, no exercício das atribuições conferidas pelo art. 130-A, § 2º, I, da Constituição Federal, com fundamento nos arts. 147 e seguintes de seu Regimento Interno, em conformidade com a decisão Plenária proferida na 18ª Sessão Ordinária, realizada em 28 de novembro de 2023, nos autos da Proposição nº 1.00415/2021-60;

Considerando a competência fixada na Constituição Federal e a missão do Conselho Nacional do Ministério Público (CNMP) de desenvolver políticas que promovam efetividade e unidade no âmbito do Ministério Público, orientadas à defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis;

Considerando a autonomia do Ministério Público e a necessidade de uma regulamentação nacional que se proponha à validação das diretrizes do modelo de proteção de dados pessoais que irá nortear a implementação da política de proteção de dados pessoais no âmbito do Ministério Público da União e dos Estados, em consonância com o disposto no art. 55-J, § 3º, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);

Considerando que a autonomia do Ministério Público da União e dos Estados, sob os aspectos administrativo, funcional e financeiro, está consagrada no art. 127, §§ 2º e 3º, da Constituição Federal, e representa o substrato de independência da Instituição, predicado inarredável para o desempenho, com êxito, de suas relevantes atribuições constitucionais;

Considerando que compete ao Conselho Nacional do Ministério Público o controle da atuação administrativa e financeira do Ministério Público e do cumprimento dos deveres funcionais de seus membros, cabendo-lhe zelar pela autonomia funcional e

administrativa do Ministério Público, podendo expedir atos regulamentares, no âmbito de sua competência, ou recomendar providências;

Considerando a relevância da proteção de dados pessoais no Brasil e no mundo, como garantia ao direito fundamental à privacidade, que exsurge do art. 5º, X e LXXIX, da Constituição Federal;

Considerando a necessidade do correto tratamento de dados pessoais no contexto da proteção e, também, dos direitos fundamentais de liberdade e do livre desenvolvimento da personalidade da pessoa natural;

Considerando a necessidade de se desenvolver uma cultura de proteção de dados pessoais, inclusive nos meios digitais, no âmbito do Ministério Público que englobe todas as suas atividades, tanto na atividade administrativa como na atividade-fim e no trato das informações da sociedade em geral e do cidadão em particular;

Considerando a necessidade de instituir um sistema nacional e uma política uniforme de proteção de dados pessoais no âmbito do Ministério Público, com o estabelecimento de diretrizes gerais e mecanismos capazes de garantir, em todo o País, e a despeito das especificidades locais, as condições necessárias para o pleno exercício das atividades da Instituição e de seus integrantes; Considerando as atribuições da Comissão de Preservação da Autonomia do Ministério Público (CPAMP), cuja existência está prevista no art. 31, III, da Resolução CNMP nº 92, de 13 de março de 2013 (Regimento Interno do CNMP);

Considerando a Resolução CNMP nº 156, de 13 de dezembro de 2016, que instituiu a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público (SNS/MP); e

Considerando a criação, por intermédio da Portaria CNMP-PRESI nº 55/2020, do Grupo de Trabalho destinado à elaboração de estudos a respeito da normatização, no âmbito do Ministério Público brasileiro, da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público.

§ 1º A Política Nacional de Proteção de Dados Pessoais estabelece diretrizes para as ações de planejamento e de execução das obrigações funcionais e da gestão administrativa do Ministério Público em alinhamento com as regras e os princípios aplicáveis à proteção de dados pessoais e a autodeterminação informativa da pessoa natural, com os seguintes objetivos:

I - fixar premissas programáticas para que o Ministério Público concretize a tutela do direito fundamental à proteção de dados pessoais por meio de seus órgãos de execução, nas hipóteses de lesão ou ameaça de lesão ocasionadas por pessoa natural ou pessoa jurídica de direito público ou privado, independentemente do meio, de sua sede ou do país onde estejam localizados os dados pessoais, consoante a legislação vigente;

II - fomentar a capacitação contínua de membros e servidores quanto à proteção de dados pessoais em diferentes relações sociais e garantir acesso ao conhecimento necessário ao manejo de medidas administrativas e judiciais adequadas para a tutela integral de direitos violados ou ameaçados;

III - disseminar a cultura de proteção de dados pessoais, com o objetivo de promover a conscientização sobre os riscos derivados do tratamento e formas de minimizá-lo em diferentes ambientes, especialmente tecnológicos;

IV - assegurar que o Ministério Público, no pleno exercício de suas atividades e na defesa do regime democrático e da ordem jurídica, em especial quanto à tutela dos direitos fundamentais, realize o tratamento de dados pessoais de forma a conciliar o dever de transparência e o interesse público com a proteção da intimidade e da vida privada;

V - instituir, no âmbito interno dos ramos e das unidades do Ministério Público, estruturas especializadas, procedimentos e medidas necessárias para a conciliação da imprescindibilidade de tratamento de dados pessoais, a autodeterminação informativa e a proteção à privacidade e à intimidade a eles inerentes; e

VI - estabelecer diretrizes que orientarão o aprimoramento contínuo de mecanismos de proteção de dados pessoais, inclusive nos campos do planejamento, governança, administração de processos e procedimentos, elaboração de normas, rotinas operacionais, práticas organizacionais, desenvolvimento e gestão de sistemas de informação e relação com a imprensa.

§ 2º Esta Resolução não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de atividades de investigação e repressão de infrações penais.

§ 3º O tratamento de dados pessoais previsto no § 2º deste artigo será regido por legislação específica, conforme previsto no § 1º do art. 4º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

CAPÍTULO II
DA POLÍTICA NACIONAL DE PROMOÇÃO DA PROTEÇÃO DE DADOS PESSOAIS PELO MINISTÉRIO PÚBLICO

Seção I
Dos Fundamentos

Art. 2º Constituem fundamentos para a atuação do Ministério Público na proteção de dados pessoais, no âmbito de suas atribuições:

I - o respeito à privacidade, à intimidade, à honra e à imagem;

II - a autodeterminação informativa;

III - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais;

IV - a liberdade de expressão, de informação, de comunicação e de opinião;

V - a proteção aos direitos fundamentais por meio de medidas preventivas e repressivas a lesões e a ameaças de lesões aos direitos do titular e de coletividades;

VI - o desenvolvimento econômico e tecnológico e a inovação;

VII - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VIII - o respeito aos princípios constitucionais da atividade administrativa.

Seção II
Dos Princípios

Art. 3º Esta Resolução adotará os seguintes princípios como vetores para a promoção da proteção de dados pessoais pelo Ministério Público:

I - proporcionalidade e razoabilidade;

II - vedação da proteção insuficiente na tutela dos direitos fundamentais;

III - boa-fé e adequação;

IV - necessidade e finalidade do tratamento;

V - segurança e prevenção;

VI - responsabilização e prestação de contas;

VII - livre acesso aos dados necessários para a tutela de direitos fundamentais, com respeito às hipóteses constitucionais de reserva jurisdicional prévia ao acesso;

VIII - não discriminação;

IX - qualidade e integridade dos dados; e

X - transparência.

Parágrafo único. Em caso de conflito entre os princípios de proteção de dados pessoais e os demais princípios constitucionais, dever-se-á proceder à devida ponderação, observados necessariamente os deveres constitucionais do Ministério Público, buscando alcançar a concordância prática entre os princípios envolvidos.

Seção III
Dos Conceitos

Art. 4º Para os fins desta Resolução, considera-se:

I - agentes de tratamento: o controlador e o operador;

II - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

III - autenticação de dois fatores ou em duas etapas: mecanismo de identificação pessoal que se utiliza de camada adicional de segurança para garantir que o detentor de credencial de acesso seja a única pessoa que consiga utilizá-la, mesmo que alguém saiba sua senha;

IV - autoridade competente: membros do Ministério Público designados para a prevenção, investigação, detecção, persecução ou repressão de violações à ordem jurídica, ao regime democrático e aos interesses sociais e individuais indisponíveis;

V - Autoridade de Proteção de Dados Pessoais no Ministério Público (APDP/MP): é o Conselho Nacional do Ministério Público (CNMP), órgão responsável

por zelar, implementar e fiscalizar a proteção de dados pessoais, no âmbito do Ministério Público brasileiro, por meio da sua Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público (CPAMP);

VI - banco de dados: repositório estruturado ou não estruturado que contenha dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

VII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados pessoais;

VIII - ciclo de vida de dados pessoais: corresponde a tudo o que envolve os dados pessoais obtidos, desde a sua coleta até a sua devida eliminação, sendo o nome que se dá ao período no qual os dados pessoais do titular são armazenados dentro de um órgão de tratamento;

IX - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

X - controle dos dados pessoais: estratégia orientada para o uso de dados pessoais que permite providenciar o maior conhecimento possível do titular (consentimento, alerta, escolha, atualização e retrair);

XI - criptografia: é a prática computacional de segurança que permite codificar e decodificar dados;

XII - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

XIII - dados biométricos: os dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitam ou confirmem a sua identificação única, tais como imagens faciais ou dados dactiloscópicos;

XIV - dados genéticos: os dados pessoais relacionados com as características genéticas, hereditárias ou adquiridas, de uma pessoa natural, e que dão informações únicas sobre a sua fisionomia ou a sua saúde, resultantes, designadamente, da análise de cromossomos, do ácido desoxirribonucleico (DNA), do ácido ribonucleico (RNA) ou de qualquer outro elemento que permita obter informações equivalentes;

XV - dado pessoal: informação relacionada a pessoa natural identificada ou identificável, que é o titular dos dados;

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

XVII - dados relativos à saúde: os dados pessoais relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro;

XVIII - demonstração do tratamento dos dados pessoais: estratégia orientada para o uso de dados pessoais capaz de demonstrar que o processamento respeita a privacidade (registro, auditoria e reporte);

XIX - dicionário de dados: documentação com as descrições (metadados) detalhadas do conteúdo de um conjunto de dados, incluindo títulos de tabelas (principais e auxiliares) e informações sobre o nome, o teor, os tipos de dados e a extensão de cada campo;

XX - eliminação: exclusão, pelos agentes de tratamento, de dado ou de conjunto de dados armazenados em banco de dados pessoais, físico ou digital, independentemente do procedimento empregado;

XXI - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade de Proteção de Dados Pessoais no Ministério Público (APDP/MP), bem como desempenhar outras funções estabelecidas por esta Resolução;

XXII - engenharia social: técnica empregada para o acesso a dados, que podem ser pessoais, a partir da análise de comportamentos humanos e outros elementos sociais, que pode ser conjugada com o emprego de indução psicológica para a coleta de dados de um interlocutor;

XXIII - informação quanto aos dados pessoais: estratégia orientada para o uso de dados pessoais que visa manter o titular devidamente informado da natureza e das condições de processamento (fornecer, explicar e notificar);

XXIV - minimização da coleta de dados pessoais: estratégia orientada para o uso de dados pessoais, com limitação do seu processamento ao mínimo adequado,

relevante e necessário ao propósito do tratamento (selecionar, excluir, segmentar e destruir);

XXV - ocultação de dados pessoais: estratégia orientada para o uso de dados pessoais para evitar fazer com que eles se tornem públicos ou conhecidos (restringir, ofuscar, dissociar e mixar);

XXVI - pseudonimização: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

XXVII - reforço da proteção dos dados pessoais: estratégia orientada para o uso de dados pessoais que visa respeitar e promover o cumprimento das obrigações estabelecidas pelo regulamento atual da proteção de dados em si (criar, manter e sustentar);

XXVIII - Relatório de Impacto à Proteção de Dados Pessoais (RIDP): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XXIX - resumo quanto a dados pessoais (redução de granularidade): estratégia orientada para o uso de dados pessoais a fim de limitar o nível de detalhes usados no processamento ao máximo possível (resumir, agrupar e desorientar);

XXX - separação de dados pessoais: estratégia orientada para o uso de dados pessoais que visa manter conjuntos separados (isolar e distribuir);

XXXI - sistema informatizado: conjunto integrado de componentes que possui o objetivo de coletar, armazenar e processar dados e fornecer informações, conhecimento e produtos digitais;

XXXII - sítio eletrônico: sinônimo de endereço eletrônico (**website** ou **site**), corresponde a um conjunto de páginas da rede de internet acessíveis geralmente pelo protocolo HTTP(S);

XXXIII - tecnologia embarcada ou sistema embarcado: mecanismo que conta com sistema operacional encapsulado (microprocessado) ou dedicado ao dispositivo que ele controla, que realiza um conjunto de tarefas predefinidas, geralmente com requisitos específicos;

XXXIV - titular de dados pessoais: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXXV - tratamento de dados pessoais: toda operação realizada com dados pessoais, como as que se referem à coleta, à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação ou ao controle da informação, modificação, comunicação, transferência, difusão ou extração; e

XXXVI - uso compartilhado de dados pessoais: comunicação, difusão, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos da Instituição, entre o CNMP, os ramos e as unidades do Ministério Público brasileiro.

Parágrafo único. Consideram-se, também, as seguintes siglas:

I - APDP/MP: Autoridade de Proteção de Dados Pessoais do Ministério Público;

II - ANPD: Autoridade Nacional de Proteção de Dados Pessoais;

III - CEPDAP: Comitê Estratégico de Proteção de Dados Pessoais.

IV - CNMP: Conselho Nacional do Ministério Público;

V - CONEDAP: Comitê Nacional de Encarregados de Proteção de Dados Pessoais;

VI - CPAMP: Comissão de Preservação da Autonomia do Ministério Público;

VII - DNA: Ácido Desoxirribonucleico;

VIII - HTTP(S): **Hiper Text Transfer Protocol (Secure)** - Protocolo de Transferência de Hipertexto (Seguro);

IX - LGPD: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);

X - RIDP: Relatório de Impacto à Proteção de Dados Pessoais;

XI - RNA: Ácido Ribonucleico;

XII - SEPRODAP: Secretaria Executiva de Proteção de Dados Pessoais;

XIII - SINPRODAP/MP: Sistema Nacional de Proteção de Dados Pessoais do Ministério Público;

XIV - SNS/MP: Sistema Nacional de Segurança Institucional do Ministério Público;

XV - TCMS: Termo de Compromisso de Manutenção de Sigilo; e

XVI - UEPDAP: Unidade Especial de Proteção de Dados Pessoais.

Seção IV
Dos Direitos do Titular de Dados Pessoais

Art. 5º O Ministério Público, no exercício da atividade de proteção de dados pessoais, deverá se pautar pelo reconhecimento dos direitos dos seus titulares.

Art. 6º Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da legislação aplicável e desta Resolução.

Art. 7º O titular tem direito a obter do controlador, em relação aos seus dados pessoais tratados, mediante requerimento, as seguintes informações:

I - confirmação da existência de tratamento;

II - acesso aos dados pessoais;

III - correção de dados pessoais incompletos, inexatos ou desatualizados;

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

V - portabilidade dos dados pessoais;

VI - eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses necessárias de conservação;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados pessoais;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e

IX - revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

Art. 8º O titular dos dados pessoais receberá um tratamento transparente, conciso, inteligível e de fácil acesso, com o uso de linguagem clara e simples, em especial quando as informações forem dirigidas a crianças e adolescentes.

Parágrafo único. As informações deverão ser prestadas por escrito ou por outros meios, preferencialmente eletrônicos, ou de forma oral, desde que a identidade do titular seja comprovada por meios idôneos.

Art. 9º Deverão ser informados ao titular dos dados pessoais, quando for o caso, a identidade do controlador, a existência da operação de tratamento, as finalidades do tratamento, o direito de apresentar reclamação e a existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais e a sua retificação, o apagamento ou a limitação do tratamento.

§ 1º Em casos específicos e no intuito de que seja permitido o exercício dos seus direitos, o titular dos dados pessoais deverá ser informado sobre o fundamento jurídico do tratamento e a duração da conservação dos dados pessoais, na medida em que tais informações adicionais sejam necessárias, tendo em conta as circunstâncias específicas em que os dados pessoais são tratados.

§ 2º Na hipótese de a coleta dos dados pessoais não ter sido feita pelo próprio Ministério Público, deverão estar disponíveis as informações sobre a real origem desses dados, sempre que não interferirem no sigilo de apurações em andamento ou na própria finalidade do tratamento.

§ 3º As obrigações previstas nesta Seção poderão ser afastadas, de forma justificada, se ocasionarem prejuízo às atividades do Ministério Público em prol da defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, difusos, coletivos e individuais homogêneos, bem como às atividades preventivas, persecutórias e de produção de conhecimento imprescindíveis à concretização dessas obrigações constitucionais e à salvaguarda dos ativos da Instituição.

Art. 10. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requerimento do titular, em formato simplificado, de imediato, ou por meio de declaração clara e completa, que indique a origem dos dados pessoais, a existência de registro, os critérios utilizados e a finalidade do tratamento, observados os casos de sigilo ou segredo.

§ 1º O prazo para a emissão da declaração mencionada no **caput** deste artigo é de até 15 (quinze) dias, contado da data do requerimento do titular, podendo ser prorrogado por igual período em casos justificados.

§ 2º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 3º As informações e os dados pessoais poderão ser fornecidos por meio eletrônico ou sob forma impressa, garantindo-se a idoneidade e segurança da comunicação, observado o disposto no art. 6º da Lei nº 13.726/2018.

Art. 11. Caso o responsável pelo tratamento recuse ao titular dos dados pessoais o direito à informação, o acesso a esses dados ou a sua retificação, o apagamento ou a limitação do tratamento, o titular poderá solicitar à UEPDAP que verifique a licitude do tratamento.

Parágrafo único. Ao titular dos dados pessoais poderão ser oferecidas medidas para facilitar a apresentação de reclamações, como, por exemplo, o fornecimento de formulários que possam também ser preenchidos eletronicamente, sem a exclusão de outros meios de comunicação.

Art. 12. O titular tem o direito de ter os seus dados pessoais apagados pelos agentes de tratamento, sem demora injustificada, quando:

I - os dados pessoais não forem mais necessários para a finalidade que motivou a sua coleta ou tratamento;

II - revogar o consentimento, nas hipóteses cabíveis, inexistindo outro fundamento jurídico que autorize a continuidade do tratamento;

III - firmar oposição ao tratamento e não existirem interesses legítimos outros que permitam a sua continuidade;

IV - os dados pessoais foram tratados ilicitamente; e

V - os dados tiverem de ser apagados para o cumprimento de uma obrigação jurídica ou legal, especialmente no caso de crianças e adolescentes, ressalvado, neste caso, o necessário registro de informações referentes à primeira infância (0 a 6 anos), período de acolhimento familiar ou institucional ou que sejam relevantes ao seu desenvolvimento individual.

§ 1º O apagamento dos dados pessoais não será garantido quando o tratamento se revele necessário:

I - ao exercício da liberdade de expressão e de informação;

II - ao cumprimento de uma obrigação legal que exija o tratamento, no exercício das funções de interesse público ou de autoridade pública competente de que esteja investido o responsável pelo tratamento;

III - para fins de arquivo de interesse público, investigação científica, histórica ou estatística; e

IV - para efeitos de declaração, exercício ou defesa de um direito num processo judicial ou na atividade finalística da Instituição.

Art. 13. O titular dos dados pessoais, nos casos de consentimento ou obrigação contratual, tem o direito de receber as informações que lhe digam respeito quanto aos dados pessoais que tenha fornecido, em formato estruturado, inclusive para fins de portabilidade.

Art. 14. A defesa dos interesses e dos direitos dos titulares de dados pessoais poderá ser exercida em juízo, individual ou coletivamente, nos termos legais e com o uso dos instrumentos de tutela individual e coletiva.

Parágrafo único. Ao Ministério Público, por suas autoridades competentes, no exercício de sua atividade finalística, também caberá a defesa desse direito fundamental, de forma coletiva e com os instrumentos pertinentes.

Art. 15. Os direitos dos titulares de dados pessoais elencados neste capítulo deverão ser conjugados com o disposto em legislação específica, em especial as disposições constantes da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), da Lei nº 9.507, de 12 de novembro de 1997 (Lei do **Habeas Data**); da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo); da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação); e da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Parágrafo único. Para o fiel cumprimento dos arts. 127 a 129 da Constituição Federal; da Lei Complementar nº 75, de 20 de maio de 1993 (Lei Orgânica do Ministério Público da União); da Lei nº 8.625, de 12 de fevereiro de 1993 (Lei Orgânica Nacional do Ministério Público); e das leis orgânicas dos Ministérios Públicos dos Estados, aplica-se o **caput** às atividades institucionais, bem como à produção de conhecimento imprescindível à concretização dessas obrigações constitucionais e, ainda, à salvaguarda dos ativos da Instituição.

Seção V

Das Prerrogativas do Ministério Público

Art. 16. O Ministério Público brasileiro, no exercício regular de suas obrigações, de suas prerrogativas e no interesse legítimo da Instituição, independentemente do consentimento dos titulares, realizará o tratamento de dados pessoais sempre que necessário à defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, difusos, coletivos e individuais homogêneos, bem como às atividades preventivas, persecutórias e de produção de conhecimento imprescindíveis à concretização dessas obrigações constitucionais e à salvaguarda dos ativos da Instituição.

Art. 17. O Ministério Público brasileiro, em defesa dos direitos fundamentais individuais indisponíveis, difusos, coletivos, individuais homogêneos e no desenvolvimento de ações preventivas, no contexto do exercício persecutório estatal e no âmbito do devido processo legal, terá acesso incondicional a bancos de dados pessoais de caráter público ou relativos a serviços de relevância pública, bem como a bancos de dados privados, podendo, para tanto, exercitar seu poder de requisição.

§ 1º Com exceção das hipóteses de reserva de jurisdição estabelecidas pela Constituição Federal, o acesso aos bancos de dados indicados no **caput** ocorrerá diretamente pelo Ministério Público, independentemente de prévia autorização do Poder Judiciário.

§ 2º Para o exercício de suas atividades, não poderá ser negado ao Ministério Público acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais, ou, ainda, à proteção de seus ativos.

§ 3º Nenhuma autoridade poderá opor ao Ministério Público, sob qualquer pretexto, a exceção de sigilo, sem prejuízo da subsistência do caráter sigiloso da informação, do registro, do dado ou do documento que lhe seja fornecido, ressalvada a reserva de jurisdição.

Art. 18. Cada ramo e unidade do Ministério Público poderá constituir ou manter estruturas orgânicas seguras especializadas em hospedar, receber, compartilhar ou difundir aos órgãos de execução bases de dados, públicas ou privadas, de relevância pública, para fins de tratamento de dados, inclusive pessoais, ou para assegurar a integração e o intercâmbio das atividades ministeriais.

Art. 19. Para o exercício das funções indicadas nos arts. 16, 17 e 18 desta Resolução, bem como das obrigações constitucionalmente outorgadas, os ramos e as

unidades do Ministério Público poderão compartilhar dados pessoais com estruturas internas de execução e de administração, com órgãos de execução e da estrutura administrativa de outros ramos e unidades com o CNMP.

Parágrafo único. Os ramos e as unidades do Ministério Público poderão também transferir dados para outras instituições públicas, adotando, para tanto, o disposto na presente Resolução e as medidas necessárias ao sigilo e ao resguardo dos direitos dos titulares dos dados pessoais, em especial contra a difusão e a disseminação ilícitas.

CAPÍTULO III
DO SISTEMA NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS (SINPRODAP/MP)

Art. 20. O Sistema Nacional de Proteção de Dados Pessoais no Ministério Público (SINPRODAP/MP) tem por finalidade precípua conferir ao Ministério Público a missão de assegurar a proteção integral dos dados pessoais, incluindo a defesa do direito fundamental à autodeterminação informativa contra lesões de terceiros e a observância, pelas estruturas orgânicas que o compõem, das normas que regem a Política Nacional de Proteção de Dados Pessoais no Ministério Público.

Seção I
Da Estrutura Orgânica Nacional

Art. 21. O SINPRODAP/MP é composto pela seguinte estrutura orgânica:

I - pela Unidade Especial de Proteção de Dados Pessoais (UEPDAP);

II - pela Secretaria Executiva de Proteção de Dados Pessoais (SEPRODAP);

III - pelo Comitê Nacional de Encarregados de Proteção de Dados Pessoais do Ministério Público (CONEDAP);

IV - pelos controladores e pelos encarregados dos ramos do Ministério Público da União e das unidades dos Ministérios Públicos dos Estados e do Conselho Nacional do Ministério Público (CNMP);

V - pelos Comitês Estratégicos de Proteção de Dados Pessoais (CEPDAP); e

VI - pelos órgãos de execução do Ministério Público.

Art. 22. Os órgãos integrantes do SINPRODAP/MP deverão atuar em coordenação com as Ouvidorias, a fim de assegurar que a aplicação dos dispositivos da LGPD esteja em consonância com a Lei de Acesso à Informação, com o Marco Civil da Internet, com a Lei do **Habeas Data**, com a Lei nº 14.129, de 29 de março de 2021 (Governo Digital) e com a Resolução CNMP n º 89, de 28 de agosto de 2012.

Art. 23. A legislação de proteção de dados pessoais deverá ser interpretada pelos órgãos que integram o SINPRODAP/MP harmonicamente com o regime jurídico aplicável ao Ministério Público, em especial com o disposto nos arts. 127 e 129 da Constituição Federal, com as leis orgânicas dos respectivos ramos e unidades e com outras leis especiais.

Art. 24. Na aplicação dos dispositivos previstos na legislação de proteção de dados pessoais, os órgãos do SINPRODAP/MP atenderão à teleologia que lhe é imanente e às exigências do bem comum, ponderando-se os princípios constitucionais subjacentes à defesa dos direitos pelo Ministério Público, para definição do alcance das normas.

Subseção I

Da Unidade Especial de Proteção de Dados Pessoais (UEPDAP)

Art. 25. Fica instituída a Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público (CPAMP), que exercerá a função de Autoridade de Proteção de Dados Pessoais do Ministério Público (APDP/MP), sendo composta:

I - pelo Conselheiro Presidente da CPAMP, que a presidirá;

II - pelo Corregedor Nacional;

III - pelo Ouvidor Nacional;

IV - pelo Coordenador e pelo Vice-Coordenador do Comitê Nacional de Encarregados de Proteção de Dados Pessoais do Ministério Público (CONEDAP), indicados pelo Presidente da CPAMP; e

V - por 2 (dois) membros do Ministério Público, indicados pelo Presidente do CNMP.

Parágrafo único. O Conselheiro Presidente da CPAMP, o Corregedor Nacional e o Ouvidor Nacional poderão indicar membros do Ministério Público que os representarão na UEPDAP.

Art. 26. As reuniões deliberativas da UEPDAP serão instaladas, no mínimo, com a presença da maioria absoluta de seus integrantes.

Art. 27. As deliberações serão tomadas pela maioria simples dos integrantes.

§ 1º Ao Conselheiro Presidente, caberá o voto de desempate, além do voto ordinário.

§ 2º Nenhum integrante poderá escusar-se de votar, salvo nos casos de suspeição ou impedimento.

Art. 28. Compete à UEPDAP:

I - zelar pela proteção de dados pessoais no âmbito do Ministério Público brasileiro e pela efetiva aplicação da presente Resolução;

II - avaliar, direcionar e monitorar a Política Nacional de Proteção de Dados Pessoais, bem como realizar, com apoio da SEPRODAP e do CONEDAP, a gestão e a coordenação do SINPRODAP/MP;

III - receber dos ramos e das unidades do Ministério Público Relatório de Impacto à Proteção de Dados Pessoais, bem como determinar, quando for o caso, a sua elaboração;

IV - expedir recomendações, notas técnicas, protocolos, rotinas, orientações e manuais, objetivando a proteção de dados pessoais pelos ramos e pelas unidades do Ministério Público, inclusive quanto às atividades de comunicação, uso compartilhado e tecnologias que envolvam o tratamento de dados pessoais;

V - definir padrões de interoperabilidade, acesso aos dados pessoais, segurança e manejo de tecnologias, assim como de tempo de guarda dos registros;

VI - requisitar aos ramos e às unidades do Ministério Público informações específicas sobre o âmbito e a natureza do tratamento de dados pessoais;

VII - determinar ao controlador a adoção de providências para regularizar o tratamento de dados pessoais;

VIII - determinar ao controlador medidas para salvaguarda dos direitos dos titulares, em casos de incidentes de segurança, tais como a ampla divulgação do fato em meios de comunicação, além de outras providências para reverter ou mitigar seus efeitos;

IX - fiscalizar e aplicar sanções em caso de tratamento de dados pessoais realizado em descumprimento à legislação ou desta Resolução, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

X - determinar a suspensão ou o término no tratamento de dados pessoais, em casos de grave violação à legislação de regência, quando o controlador não adotar as providências necessárias para regularização no tratamento ou deixar de salvaguardar direitos dos titulares em casos de incidentes de segurança;

XI - apreciar petições formuladas por titulares de dados pessoais em razão de incidentes de segurança ou violações a direitos, no âmbito do Ministério Público, nos casos em que não houver resposta adequada pelo controlador dentro dos prazos fixados por esta Resolução;

XII - determinar a realização de fiscalização sobre o tratamento de dados pessoais efetuado pelos órgãos de controle;

XIII - celebrar compromisso para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, no que concerne ao tratamento de dados pessoais;

XIV - promover ações de cooperação e capacitação com outras autoridades de proteção de dados pessoais dos poderes constituídos, bem como de outros países e de natureza internacional ou transnacional;

XV - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais pelo Ministério Público;

XVI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XVII - comunicar aos órgãos de controle interno e às Corregedorias-Gerais dos ramos e das unidades do Ministério Público o descumprimento do disposto na legislação de proteção de dados pessoais e nesta Resolução;

XVIII - elaborar relatório anual das atividades desenvolvidas;

XIX - fomentar a sensibilização e compreensão dos ramos e das unidades do Ministério Público e da sociedade em geral quanto aos riscos, regras, garantias e direitos associados à proteção dos dados pessoais;

XX - fomentar a integração de bancos de dados objetivando a minimização e a maior eficiência no tratamento de dados pessoais, bem como a redução da replicação desnecessária de repositórios de informações;

XXI - fomentar a padronização e a integração de sistemas de informação de modo que seja gradativamente implementado o princípio da privacidade na concepção e por padrão;

XXII - requisitar, por meio de formulário, dos ramos e das unidades do Ministério Público brasileiro, a prestação de contas relativa à implementação de medidas para a proteção de dados pessoais; e

XXIII - exercer outras funções típicas de autoridade nacional quanto à proteção dados pessoais pelo Ministério Público brasileiro.

§ 1º No exercício do controle administrativo do tratamento dos dados pessoais pelo Ministério Público, a fim de assegurar o cumprimento da legislação de regência e da presente Resolução, a UEPDAP poderá adotar as medidas previstas no art. 52, § 3º, da LGPD, no que couber.

§ 2º No exercício das atribuições previstas neste artigo, a UEPDAP deverá zelar pela preservação do sigilo das informações, para assegurar as funções institucionais do Ministério Público, e nas demais hipóteses legais.

Art. 29. O CNMP dotará a UEPDAP de estrutura de apoio jurídico e técnico, para o efetivo exercício de suas funções.

Subseção II

Da Secretaria Executiva de Proteção de Dados Pessoais (SEPRODAP)

Art. 30. A Secretaria Executiva de Proteção de Dados Pessoais (SEPRODAP), órgão executivo e regulador do SINPRODAP/MP, será composta pelo Coordenador e pelo Vice-Coordenador do CONEDAP e por membros do Ministério Público designados pelo Presidente da CPAMP, dentre os quais será indicado o secretário executivo.

Parágrafo único. Para assessoramento às atividades da SEPRODAP, poderão ser indicadas pessoas físicas ou jurídicas com notória especialização na área de proteção de dados pessoais e outros temas correlatos.

Art. 31. Compete à SEPRODAP:

I - prestar apoio na gestão do SINPRODAP/MP;

II - assessorar a UEPDAP nas questões afetas à proteção de dados pessoais, especialmente na realização de fiscalizações e na elaboração do relatório anual;

III - prestar auxílio aos ramos e às unidades do Ministério Público quanto ao cumprimento desta Resolução e da legislação de proteção de dados pessoais;

IV - confeccionar, de forma complementar à presente Resolução, recomendações, notas técnicas, protocolos, rotinas, orientações e manuais, a serem aprovados pela UEPDAP, para a proteção dos dados pessoais e para a política de privacidade, no âmbito do Ministério Público, inclusive quanto às atividades de comunicação e de uso compartilhado de dados pessoais, bem como a respeito de:

a) critérios para a aplicação da legislação de proteção de dados pessoais, em harmonia com a Lei de Acesso à Informação, para fins de restringir ou conferir acesso aos dados pessoais mantidos pelo Ministério Público;

b) ciclo de vida do tratamento dos dados pessoais e regras de conservação dos dados em suporte físico ou eletrônico, inclusive em relação aos dados anonimizados;

c) compartilhamento ou transferência de dados pessoais entre o CNMP, os ramos e as unidades do Ministério Público, os órgãos ou entidades públicas e as pessoas jurídicas de direito privado;

d) padrões de interoperabilidade, acesso aos dados pessoais e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência;

e) publicidade quanto às operações de tratamento de dados pessoais, a estrutura mínima dos termos e avisos de privacidade e os padrões de exibição das informações necessárias ao atendimento da legislação;

f) critérios de padronização de resposta ao titular quanto à existência de dados pessoais, em formato que possibilite o exercício do direito ao acesso;

g) procedimento para o exercício dos direitos do titular dos dados pessoais previstos no art. 18 da LGPD, incluindo reclamações e petições formuladas;

h) padrões técnicos e diretrizes para o emprego de tecnologias nas atividades ministeriais que envolvam o tratamento de dados pessoais e para o tratamento automatizado desses dados;

i) regulamentação dos níveis e registros de acesso e os padrões de rastreabilidade quanto ao tratamento de dados pessoais nos sistemas informatizados e nos bancos de dados;

j) regulamentação dos requisitos, distinção e limites entre dados pessoais e metadados (comunicações);

k) regulamentação dos critérios para a terceirização de serviços envolvendo a tecnologia da informação, práticas de estocagem, uso de nuvens de armazenamento de dados pessoais, uso da internet e comunicação, inclusive estabelecer limites para essa contratação;

l) critérios para categorização da relevância dos incidentes de segurança e violações à privacidade e para a aplicação das sanções previstas em lei;

m) critérios para a confecção do Relatório de Impacto à Proteção de Dados Pessoais (RIDP) e para o desenvolvimento de formulários próprios para esse fim; e

n) motores de busca, redes sociais, uso de aparelhos móveis e particulares na Instituição, bem como supervisão de novas tecnologias da informação objetivando a antevisão dos riscos à segurança dos dados pessoais;

V - conferir suporte à UEPDAP para monitoramento da Política Nacional de Proteção de Dados Pessoais e adotar as providências necessárias à sua implementação e cumprimento;

VI - produzir diagnósticos, estudos e avaliações periódicas a respeito da proteção de dados pessoais no Ministério Público brasileiro;

VII - acompanhar e orientar a aplicação da Política Nacional de Proteção de Dados Pessoais e o procedimento de elaboração dos Planos Diretores dos ramos e das unidades do Ministério Público;

VIII - fornecer informações para subsidiar a tomada de decisões pela UEPDAP no que tange à Política de Proteção de Dados Pessoais do Ministério Público brasileiro;

IX - promover a articulação com os ramos e as unidades do Ministério Público brasileiro para a concretização das ações relativas à proteção de dados pessoais; e

X - desenvolver outras atividades inerentes à sua finalidade.

Art. 32. A SEPRODAP poderá, por determinação da UEPDAP, realizar fiscalizações nos ramos e nas unidades do Ministério Público, a fim de assegurar a adequada proteção de dados pessoais.

Subseção III

Do Comitê Nacional de Encarregados de Proteção de Dados Pessoais (CONEDAP)

Art. 33. O Comitê Nacional de Encarregados de Proteção de Dados Pessoais no Ministério Público (CONEDAP), como órgão consultivo, deliberativo e propositivo, tem a função de promover a padronização das ações dos ramos e das unidades do Ministério Público quanto à Política Nacional de Proteção de Dados Pessoais, competindo-lhe:

I - fomentar a integração entre os ramos e as unidades do Ministério Público e entre estes e outros órgãos essenciais à sua atividade;

II - fomentar o desenvolvimento da política de proteção de dados pessoais e da governança de dados pessoais no Ministério Público;

III - difundir as ações dos ramos e das unidades do Ministério Público na prevenção e repressão de violações de dados pessoais;

IV - incentivar adoção de boas práticas na proteção de dados pessoais e na governança de dados pessoais;

V - promover o compartilhamento de experiências, decisões e providências adotadas na proteção dos dados pessoais;

VI - propor padrões, normas e critérios técnicos a serem adotados no âmbito da Política Nacional de Proteção de Dados Pessoais;

VII - propor medidas de padronização de resposta ao titular quanto à existência de dados pessoais, em formato que possibilite o exercício do direito ao acesso;

VIII - propor rotinas em torno da recusa ou limitação do direito de acesso aos titulares de dados pessoais, em razão do exercício das funções institucionais do Ministério Público;

IX - fomentar a difusão de tecnologias que possibilitem o aprimoramento da segurança da informação, da política de governança de dados pessoais e da adequada manutenção de bancos de dados pessoais, no âmbito Ministério Público;

X - favorecer a integração tecnológica do Ministério Público brasileiro, garantindo o contínuo implemento nos padrões de excelência em proteção dos dados pessoais;

XI - propor a adoção de padrões técnicos para o emprego de tecnologias nas atividades ministeriais que envolvam o tratamento de dados pessoais e para o tratamento automatizado desses dados;

XII - propor e organizar, em conjunto com a UEPDAP, treinamentos para membros e servidores na área de proteção de dados pessoais e governança de dados pessoais;

XIII - remeter ao CNMP, por intermédio da UEPDAP, sugestões para a elaboração de atos normativos na área de proteção de dados pessoais; e

XIV - praticar outros atos necessários ao cumprimento do seu objetivo e compatíveis com suas atribuições.

§ 1º O CONEDAP será integrado pelos encarregados do CNMP e de cada ramo e unidade do Ministério Público brasileiro.

§ 2º O CONEDAP será coordenado por um Coordenador e um Vice Coordenador designados pelo Conselheiro Presidente da CPAMP, dentre os integrantes do colegiado.

Seção II
Da Estrutura Orgânica do Sistema de Proteção de Dados Pessoais nos Ramos e nas Unidades do Ministério Público

Art. 34. O CNMP e todos os ramos e as unidades do Ministério Público brasileiro deverão, no prazo de até 90 (noventa) dias, a contar da publicação da presente Resolução, constituir estrutura administrativa interna para o atendimento das diretrizes nela determinadas, no uso e no tratamento de dados pessoais, que será compreendida, no mínimo, pelo encarregado e pelo CEPDAP.

Parágrafo único. As normas que regem o SINPRODAP/MP aplicam-se ao tratamento de dados pessoais realizado pelo CNMP.

Art. 35. O Plano Diretor deverá conter as regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento,

os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, conforme previsto na presente Resolução.

Subseção I

Do Controlador

Art. 36. O CNMP e cada ramo e unidade do Ministério Público brasileiro são considerados controladores na sua esfera de atuação, realizando tratamento de dados pessoais por meio dos seus membros, servidores e demais colaboradores que integrem sua estrutura orgânica.

Art. 37. No âmbito do Ministério Público brasileiro, o controlador é o responsável por determinar o tratamento de dados pessoais, independentemente de serem obtidos de forma espontânea ou por cumprimento de dever legal ou autorização legal.

§ 1º O controlador determina o propósito e os significados do tratamento do dado pessoal, podendo, para tanto, atuar conjuntamente com órgão ou entidade, ou com pessoa natural ou jurídica.

§ 2º O controlador, nos termos das suas competências legal e institucional, é responsável pelas decisões referentes ao tratamento dos dados pessoais.

Art. 38. Caberá aos ramos e às unidades do Ministério Público, na qualidade de controladores e órgãos gestores locais do SINPRODAP/MP, normatizar e deliberar a respeito das regras de tratamento de dados pessoais no âmbito da instituição, bem como:

I - expedir instruções de serviço, para atendimento das boas práticas estabelecidas na LGPD, em especial quanto às normas de segurança, os padrões técnicos e as obrigações específicas para os diversos envolvidos no tratamento dos dados pessoais;

II - orientar as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais;

III - elaborar o RIDP;

IV - decidir sobre o uso compartilhado de dados pessoais;

V - comunicar ao CNMP e ao titular de dados pessoais a ocorrência de incidente de segurança que possa acarretar riscos ou dano relevante aos titulares;

VI - implementar programa de governança em privacidade, enviando ao CNMP as informações pertinentes; e

VII - adotar outras providências necessárias ao cumprimento da legislação de proteção de dados pessoais.

Parágrafo único. As atribuições previstas nos incisos do presente artigo, respeitada a organização interna de cada Instituição, poderão ser delegadas ao encarregado.

Subseção II

Do Co-Controlador

Art. 39. No âmbito do Ministério Público brasileiro, considera-se co-controlador aquele que também é responsável e, em conjunto com o controlador, igualmente determina as finalidades e os meios do tratamento.

§ 1º Os responsáveis conjuntos pelo tratamento devem determinar, por acordo entre si e de modo transparente, as respectivas responsabilidades pelo cumprimento das suas obrigações em matéria de proteção de dados pessoais, notadamente no que diz respeito ao exercício dos direitos do titular e aos seus deveres de prestar informações.

§ 2º Independentemente dos termos do mencionado acordo, o titular dos dados pessoais pode exercer os seus direitos em relação a quaisquer dos responsáveis.

Subseção III

Do Operador

Art. 40. No âmbito do Ministério Público brasileiro, considera-se operador a pessoa natural ou jurídica, de direito público ou privado, que, sem pertencer aos quadros do Ministério Público, com independência jurídica e econômica, realiza, por sua conta e responsabilidade, o tratamento de dados pessoais a mando do controlador.

§ 1º O operador, a mando do controlador, poderá realizar o total ou o parcial tratamento dos dados pessoais dentro ou fora das dependências do controlador.

§ 2º O operador somente poderá tratar os dados pessoais para a finalidade previamente autorizada ou contratada pelo controlador, utilizando-se dos meios de tratamento que, prévia e igualmente, forem autorizados ou contratados pelo controlador.

Art. 41. O operador deve, sempre, apresentar garantias suficientes de execução de medidas técnicas e administrativas adequadas ao tratamento de dados pessoais, que atendam aos requisitos estabelecidos na presente Resolução e, principalmente, assegurem a defesa dos direitos do titular dos dados pessoais.

Art. 42. O operador que, de alguma forma, determine as finalidades e os meios de tratamento de dados pessoais, será considerado, nesse caso, co-controlador para fins legais.

Subseção IV

Co-Operador

Art. 43. No âmbito do Ministério Público brasileiro, considera-se co-operador aquele que, nas hipóteses que lei autoriza, é contratado para realizar o tratamento concomitante de dados pessoais a mando do controlador, incidindo-lhe todas as regras da Seção anterior.

§ 1º O operador somente poderá subcontratar o tratamento de dados pessoais com a autorização prévia e por escrito do controlador.

§ 2º O contrato ou ato normativo que estabelecer o vínculo com o co-operador deverá conter, entre outras, cláusulas que atestem que:

I - realizará o tratamento mediante instruções do controlador e, se for o caso, do operador, de forma segura e com respeito a todos os princípios do tratamento de dados pessoais;

II - prestará as informações cabíveis ao controlador, ao operador e ao titular dos dados pessoais, quando necessário; e

III - apagará todos os dados pessoais ou os devolverá aos agentes de tratamento uma vez concluída a prestação de serviços contratada.

Subseção V

Do Encarregado

Art. 44. O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação e interação entre o controlador, os titulares dos dados pessoais e a APDP/MP, bem como desempenhar outras funções estabelecidas pela legislação pertinente e por esta Resolução.

Art. 45. O encarregado será indicado pelo Chefe de cada ramo ou unidade do Ministério Público, devendo ser membro da Instituição e, para o exercício de suas atribuições, poderá se assessorar de pessoas externas, físicas ou jurídicas.

§ 1º Visando a uma maior autonomia, independência e, principalmente, neutralidade, o exercício das funções de encarregado deve ocorrer, preferencialmente, sem o acúmulo com outras funções ou cargo que envolvam atribuições que ensejem o tratamento ou o armazenamento de dados pessoais.

§ 2º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, em sítio eletrônico específico do portal de cada ramo e unidade do Ministério Público.

§ 3º Ao encarregado deverão ser asseguradas a independência e a autonomia necessárias ao bom desempenho de suas funções, devendo o respectivo ramo ou unidade do Ministério Público ao qual ele se vincula garantir, para tanto, a estrutura mínima de apoio técnico, jurídico e administrativo, com estrutura de apoio à governança e gestão, inclusive.

Art. 46. São atribuições do encarregado:

I - implementar, capacitar, conscientizar, estabelecer responsabilidades e monitorar a conformidade da atuação da Instituição com a Política Nacional de Proteção de Dados Pessoais no Ministério Público e a LGPD;

II - receber e analisar os pedidos encaminhados pelos titulares dos dados pessoais, como reclamações e comunicações, prestar esclarecimentos e adotar providências relacionadas ao tratamento de dados pessoais;

III - delegar, inclusive para servidores, e supervisionar atribuições que não representem risco relevante ao titular de dados pessoais;

IV - elaborar e manter inventário de dados pessoais que documente como e por que o Ministério Público coleta, compartilha e usa esses dados;

V - recomendar e orientar a confecção dos Relatórios de Impacto à Proteção de Dados Pessoais (RIDP) e monitorar a sua correta realização;

VI - informar e emitir recomendação ao controlador e ao operador;

VII - cooperar, interagir e consultar com a APDP/MP; e

VIII - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Art. 47. O CNMP, os ramos e as unidades do Ministério Público indicarão, no prazo de 90 (noventa) dias, a contar da vigência da presente Resolução, o encarregado para implementar a legislação de proteção de dados pessoais.

§ 1º O referido encarregado deverá ter autonomia e conhecimento ou experiência suficientes no tema.

§ 2º Considera-se conhecimento a realização de cursos e capacitação profissional específica a respeito de proteção de dados pessoais, bem como o desenvolvimento de atividade acadêmica na área.

§ 3º Considera-se experiência o exercício de funções relativas à proteção de dados pessoais por, no mínimo, 6 (seis) meses.

§ 4º As exigências dos parágrafos anteriores poderão ser afastadas, em decisão devidamente fundamentada, desde que o ramo ou a unidade promova a capacitação do encarregado, nos primeiros 6 (seis) meses após a indicação prevista no caput deste artigo.

§ 5º A UEPDAP poderá ser consultada a respeito da credibilidade e do conteúdo da capacitação em proteção de dados pessoais apresentada pelo encarregado.

§ 6º Será obrigatória a participação em cursos periódicos de capacitação durante o exercício da função de encarregado e outras funções relacionadas ao tema, que deverão atender ao seu caráter multidisciplinar, contemplando entre outras matérias:

I - aspectos jurídicos da proteção de dados pessoais;

II - gestão e governança de dados pessoais; e

III - tecnologias da informação e comunicação e segurança da informação.

Art. 48. Os recursos materiais necessários disponibilizados ao encarregado deverão abranger, entre outras atividades:

I - canal eletrônico de recebimento e para resposta com esclarecimento de reclamações e comunicações dos titulares dos dados pessoais e das comunicações da UEPDAP;

II - sistema eletrônico de organização, armazenamento e encaminhamento das providências previstas no inciso I;

III - orientação e capacitação de membros, servidores, terceirizados e qualquer contratado, a respeito das práticas a serem adotadas em relação à proteção de dados pessoais; e

IV - canais e sistemas para o exercício das demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Subseção VI

Do Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP)

Art. 49. Deverá ser instituído, em cada ramo e unidade do Ministério Público brasileiro, no prazo de até 90 (noventa) dias a contar da entrada em vigor da presente Resolução, o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP), órgão colegiado de natureza permanente, subordinado à Chefia da Instituição.

§ 1º O CEPDAP será composto por membros e servidores do respectivo Ministério Público, dentre os quais:

I - o encarregado, que o presidirá;

II - 1 (um) membro indicado pela Corregedoria-Geral;

III - 1 (um) membro ou 1 (um) servidor indicado pela Ouvidoria;

IV - o Secretário-Geral ou equivalente;

V - o Coordenador de Segurança Institucional ou equivalente; e

VI - o Chefe da Secretaria de Tecnologia da Informação ou equivalente.

Art. 50. Compete ao CEPDAP:

I - orientar o controlador e o encarregado nas questões afetas à proteção ou governança de dados pessoais;

II - propor as prioridades dos investimentos em proteção de dados pessoais, para análise e decisão da Chefia da Instituição;

III - coordenar o processo de elaboração e revisão do Plano Diretor de Proteção de Dados Pessoais;

IV - monitorar a execução do Plano Diretor de Proteção de Dados Pessoais e adotar as providências necessárias à sua implementação e ao seu cumprimento;

V - produzir diagnósticos, estudos e avaliações periódicas a respeito do Plano Diretor de Proteção de Dados Pessoais;

VI - opinar sobre a elaboração, revisão, aprovação e publicação de Relatórios de Impacto à Proteção de Dados Pessoais;

VII - propor mecanismos e instrumentos para a investigação e a prevenção de quebra de segurança da informação relativa a dados pessoais, bem como para o tratamento da informação sigilosa comprometida concernente a dados pessoais;

VIII - sugerir critérios acerca da publicidade dos atos quando envolverem a exibição de dados pessoais mantidos pelo Ministério Público; e

IX - opinar sobre outras questões afetas à proteção de dados pessoais.

Parágrafo Único. No exercício de suas competências, o CEPDAP deverá atuar de forma coordenada com as instâncias de gestão e governança da Instituição responsáveis pela implementação de medidas de tecnologia e segurança da informação e com as Ouvidorias.

Art. 51. É facultado ao Presidente do CEPDAP tomar decisões **ad referendum**, nos casos em que houver urgência devidamente fundamentada por um dos seus integrantes.

Art. 52. As reuniões deliberativas do CEPDAP serão instaladas, no mínimo, com a presença da maioria absoluta de seus integrantes.

Art. 53. As deliberações serão tomadas pela maioria simples dos integrantes.

§ 1º Ao Presidente do CEPDAP caberá o voto de desempate, além do voto ordinário.

§ 2º Nenhum integrante poderá escusar-se de votar, salvo nos casos de suspeição ou impedimento.

Art. 54. O Presidente do CEPDAP poderá convocar membros e servidores para assessoramento técnico durante as reuniões do Comitê, cuja participação será restrita ao assessoramento e sem direito a voto.

Art. 55. Os atos cuja publicidade possa comprometer a efetividade das ações deverão ser publicados em extrato.

Seção III
Dos Órgãos do Ministério Público destinados à Proteção de Dados Pessoais contra Lesões de Terceiros

Art. 56. Os ramos e as unidades do Ministério Público deverão promover a estruturação de suas promotorias e procuradorias para atuação na defesa da ordem jurídica e da dimensão coletiva do direito à proteção aos dados pessoais, diante de violações à legislação por pessoas físicas ou jurídicas, de direito público ou privado.

Parágrafo único. Para atendimento do disposto no **caput** deste artigo, o Ministério Público deverá criar promotorias ou procuradorias especializadas, grupos especiais de atuação ou incorporar nas estruturas orgânicas já existentes as atribuições que assegurem a efetiva tutela da privacidade e a proteção dos dados pessoais.

Art. 57. Incumbe ao Ministério Público a proteção dos dados pessoais no âmbito das relações de consumo, das relações de trabalho, nos serviços públicos e de relevância pública ou em relações jurídicas de outra natureza, quando se revelar afetação à coletividade.

Art. 58. Ao Ministério Público caberá a fiscalização do cumprimento da legislação de proteção de dados pessoais pelos órgãos de segurança pública previstos no art. 144 da Constituição Federal, no exercício do controle externo da atividade policial.

Art. 59. O Ministério Público, no âmbito de suas atribuições, deverá atuar para prevenir e coibir a violação das normas de proteção de dados pessoais e da autodeterminação informativa quando constatada lesão ou ameaça de lesão a direitos individuais indisponíveis, difusos, coletivos e individuais homogêneos, em razão de práticas como:

I - transferência de bancos de dados pessoais, inclusive com fins econômicos;

II - disseminação de dados pessoais;

III - tratamentos automatizados de dados pessoais, inclusive sensíveis;

IV - uso de instrumentos de inteligência artificial;

V - análises de perfis de titulares, inclusive por meio de agregações de dados históricos;

VI - prejuízos à igualdade de oportunidades;

VII - abuso de poder econômico;

VIII - abuso do poder de direção em relações de trabalho em geral, inclusive no âmbito de grupos econômicos e em contratos de prestação de serviços;

IX - ausência de interesses legítimos do controlador;

X - ausência de base legal para o tratamento de dados pessoais sem consentimento do titular;

XI - ausência de transparência algorítmica;

XII - prejuízos ao exercício da cidadania em meios digitais;

XIII - manutenção indevida de dados pessoais;

XIV - deficiências em processos de anonimização ou pseudonimização de dados pessoais, sobretudo de dados pessoais sensíveis;

XV - acesso indiscriminado a dados pessoais sensíveis de titulares, em relações como as de consumo e de trabalho;

XVI - incidentes de segurança no tratamento de dados pessoais, notadamente de dados pessoais sensíveis;

XVII - coleta de consentimento de forma genérica, ambígua, induzida, excessiva ou com abuso de poder econômico;

XVIII - perda, modificação ou eliminação indevidas de dados pessoais;

XIX - obtenção indevida de dados pessoais;

XX - coleta de dados pessoais sem necessidade ou finalidade delimitadas;

XXI - informações insuficientes sobre a finalidade do tratamento;

XXII - falha em considerar direitos do titular de dados pessoais;

XXIII - vinculação ou associação indevidas, direta ou indireta, de dados pessoais;

XXIV - falha ou erro de processamento durante a execução de operações de tratamento;

XXV - reidentificação indevida de dados pseudonimizados ou com anonimizações deficientes;

XXVI - técnicas de engenharia social que acarretem o ilícito tratamento de dados pessoais, inclusive a indevida inclusão de dados pessoais inexatos;

XXVII - fundamentação do tratamento em base legal equivocada ou com erro grosseiro; e

XXVIII - quaisquer outras violações aos princípios e às normas protetivas de dados pessoais.

Art. 60. Os membros do Ministério Público poderão requisitar Relatório de Impacto à Proteção de Dados Pessoais (RIDP), com a descrição dos processos de tratamento que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais, de forma a promover medidas, salvaguardas e mecanismos de eliminação e mitigação de danos e riscos.

Art. 61. Para o exercício pleno de suas funções institucionais na proteção dos dados pessoais das pessoas naturais, o Ministério Público poderá realizar o necessário e adequado tratamento dos dados pessoais, no âmbito dos seus procedimentos e processos, bem como na alimentação e manutenção dos bancos de dados pessoais internos.

Art. 62. O CNMP, os ramos e as unidades do Ministério Público deverão desenvolver ações de capacitação de membros e servidores, para qualificar a atuação finalística na tutela do direito fundamental à privacidade, no tocante à proteção dos dados pessoais, inclusive nos cursos de ingresso e vitaliciamente de membros e servidores.

CAPÍTULO IV
DIRETRIZES PARA A PROTEÇÃO DE DADOS PESSOAIS PELO MINISTÉRIO PÚBLICO

Seção I
Do Dado Pessoal

Art. 63. No âmbito do Ministério Público brasileiro, o dado pessoal será protegido e tratado nos termos da presente Resolução, quer na sua atuação administrativa, quer na finalística, com as distinções necessárias e respeitados, sempre, os princípios previstos no art. 3º, com a ressalva do seu parágrafo único.

Seção II
Do Tratamento de Dados Pessoais

Art. 64. Considera-se tratamento toda operação realizada com dados pessoais, nos termos do inciso X do art. 5º da LGPD.

Art. 65. O tratamento de dados pessoais pelo Ministério Público brasileiro será realizado para o atendimento de sua finalidade pública, na persecução do interesse público, em todas as áreas de atuação, com o objetivo de execução e cumprimento das suas atribuições, obrigações e prerrogativas legais e constitucionais.

Parágrafo único. O CNMP e cada ramo e unidade do Ministério Público brasileiro deverão informar, no seu sítio eletrônico, quem é o seu encarregado e as hipóteses em que realizam o tratamento, conforme previsto nesta Resolução.

Art. 66. A atividade administrativa do Ministério Público será regida pelas disposições da LGPD que tratam das entidades públicas, ressalvado o exercício pleno de sua atividade finalística constitucionalmente outorgada à Instituição.

§ 1º Considera-se atividade administrativa, para os fins desta Resolução, aquelas estruturantes como de gestão de pessoas, gestão orçamentária e financeira, comunicação social, gestão administrativa e tecnologia da informação, entre outras.

§ 2º Não se considera atividade administrativa a desempenhada em prol da produção de conhecimento destinado ao desempenho das atividades dos órgãos de execução e à proteção dos ativos da Instituição.

Art. 67. A proteção das pessoas naturais, no que diz respeito ao tratamento dos seus dados pessoais, é um direito fundamental e, por isso, todas elas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Parágrafo único. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados pessoais, bem como os riscos, de probabilidade e relevância variáveis, para os direitos e as liberdades das pessoas naturais, os responsáveis pelo tratamento, no âmbito do Ministério Público brasileiro, devem aplicar as medidas técnicas e administrativas adequadas para assegurar e para poder comprovar que o tratamento é realizado em conformidade com a lei e com a presente Resolução.

Art. 68. Todos os contratos, convênios e atos formais equivalentes a serem celebrados pelo CNMP e pelos ramos e pelas unidades do Ministério Público brasileiro deverão trazer definidas as responsabilidades, de forma transparente e detalhada, dos controladores, dos operadores e, quando possível, de eventuais terceiros envolvidos.

Parágrafo único. Considera-se terceiro uma pessoa natural ou jurídica, uma autoridade pública, um serviço ou outra entidade que não seja o titular dos dados pessoais, o controlador, o operador ou as pessoas que, sob a autoridade direta destes, esteja autorizada a tratar dados pessoais, bem como aquele que não é o destinatário do tratamento, nem parte do contrato ou da Instituição, exsurgindo da lei civil a sua responsabilidade pelo uso indevido de dados pessoais.

Seção III
Dos Princípios do Tratamento de Dados Pessoais

Art. 69. As atividades de tratamento de dados pessoais, no âmbito do Ministério Público brasileiro, deverão observar os princípios previstos no art. 3º da presente Resolução.

Parágrafo único. O responsável pelo tratamento deve adotar as medidas que lhe permitam comprovar que o tratamento de dados pessoais é realizado em conformidade com esses princípios.

Art. 70. Os princípios da proteção de dados pessoais não se aplicam às informações que não se refiram à pessoa natural identificada ou identificável e a dados pessoais anonimizados, que não permitam a identificação do seu titular.

Art. 71. Os dados anonimizados não serão considerados dados pessoais para os fins desta Resolução, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Parágrafo único. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

Seção IV
Das Exceções que autorizam o Tratamento

Art. 72. É legítimo o tratamento de dados pessoais nas atividades imprescindíveis à segurança da sociedade ou institucional do Ministério Público, principalmente visando ao não comprometimento das atividades de produção de conhecimento, bem como de investigação ou fiscalização, relacionadas com a prevenção ou repressão de infrações.

Art. 73. Para o exercício de suas atribuições, não se aplica ao Ministério Público a restrição de acesso a dados pessoais, quando as informações colhidas se destinarem a atividades de segurança pública, de produção de conhecimento ou de atividades de investigação e repressão de infrações penais, quando no exercício da segurança institucional, bem como quando forem destinadas à sua atividade finalística, compreendida nela todas as atribuições legais contidas na Constituição Federal, notadamente as ações e atribuições inseridas no seu art. 129 e nas leis esparsas que lhe dão suporte.

Parágrafo único. As operações de tratamento posteriores à finalidade inicial, para fins de arquivo de interesse público, de investigação científica ou histórica, ou, ainda, para fins estatísticos, serão consideradas igualmente lícitas e compatíveis.

Art. 74. O Ministério Público, quando utilizar técnicas de vigilância, monitoramento e controle no desenvolvimento das suas atividades preventivas e persecutórias em prol da defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, bem como da produção de conhecimento imprescindível à concretização dessas obrigações constitucionais e, ainda, da salvaguarda dos ativos da Instituição, deverá adotar medidas de cautela para o reforço da proteção dos dados pessoais.

§ 1º Incluem-se nas hipóteses do **caput** deste artigo os dados pessoais referentes a DNA, voz, imagem facial, reconhecimento automatizado, inclusive facial, expressão corporal, inclusive trejeitos e modo de andar, impressões digitais e outros dados biométricos ou de comportamento.

§ 2º É possível ao Ministério Público brasileiro realizar o tratamento de dados pessoais coletados com o emprego de tecnologias embarcadas em mecanismos de vigilância, controle e monitoramento.

Art. 75. A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, garantido o devido processo legal com contraditório e ampla defesa, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

Seção V

Do acesso aos dados pessoais para o tratamento realizado pelo Ministério Público

Art. 76. Nos termos do art. 10 da presente Resolução, o pedido de acesso do titular dos dados pessoais relativo ao tratamento realizado pelo Ministério Público será protocolizado e recepcionado pelo controlador ou operador que, de imediato, o encaminhará ao encarregado para análise e providências cabíveis.

§ 1º O tratamento do pedido será realizado de forma específica, em canal único, independentemente do canal de recebimento ou de entrada do pedido, o qual centralizará o trâmite de todos os procedimentos afetos ao tema, notadamente visando ao controle e à reunião das informações pertinentes à proteção de dados pessoais.

§ 2º Nas hipóteses de pedido de confirmação de existência ou de acesso a dados pessoais, observados os casos de sigilo ou segredo (art. 77), a resposta, clara e o mais completa possível, será dada em até 15 (quinze) dias, contados da data do requerimento, prorrogáveis por igual período em casos justificados.

§ 3º Nas demais hipóteses de pedido, o prazo da resposta será de até 30 (trinta) dias, contados da data do requerimento, prorrogáveis por igual período em casos justificados.

§ 4º Tratando-se de pedido que exija uma resposta com informações mais complexas, o prazo da resposta poderá ser excedido mediante a devida justificativa, informando-se o requerente.

§ 5º A resposta poderá ser fornecida por meio eletrônico, seguro e idôneo, ou sob forma impressa.

§ 6º Sempre que possível, a resposta será fornecida da mesma forma que o pedido foi feito.

Seção VI
Das Exceções de Prover Informação ao Titular do Dado Pessoal Tratado

Art. 77. A prestação de informações e a concessão de acesso a dados pessoais podem ser adiadas, limitadas ou recusadas se e enquanto tais restrições forem necessárias e proporcionais para:

I - evitar prejuízo para procedimentos, investigações, inquéritos ou processos administrativos e judiciais;

II - evitar prejuízo para a prevenção, a detecção, a investigação ou a repressão de infrações penais ou para a execução de sanções penais, igualmente, para evitar prejuízo às atividades finalísticas que tenham como objeto a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis;

III - proteger a segurança institucional ou a atividade de produção de conhecimento; ou

IV - proteger os direitos e as garantias de terceiros.

§ 1º Também haverá restrição de informações e acesso a dados pessoais quando o pedido exigir uma complexidade de medidas que inviabilizem o seu atendimento.

§ 2º Nos casos previstos e sem prejuízo às atividades, o responsável pelo tratamento deve informar o titular, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso.

§ 3º A comunicação pode ser omitida apenas à medida que a sua prestação possa prejudicar uma das finalidades previstas neste artigo, hipótese na qual a UEPDAP poderá ser instada pelo titular dos dados pessoais para analisar os motivos pelos quais o pedido foi negado.

Art. 78. Nos termos do art. 7º da Resolução CNMP nº 23, de 17 de setembro de 2007, e do art. 15 da Resolução CNMP nº 181, de 7 de agosto de 2017, e visando ao respeito ao princípio da publicidade previsto no art. 37 da Constituição Federal, os atos e as peças que compõem os processos e procedimentos no âmbito do Ministério Público

são públicos, com exceção dos casos motivados em que haja sigilo legal ou em que a publicidade possa acarretar fundado prejuízo.

Art. 79. A fim de assegurar a proteção aos dados pessoais das pessoas naturais no âmbito de procedimentos ou processos que tramitam no Ministério Público, poderá ser promovido o controle de acesso, a pseudonimização ou a decretação de sigilo dos autos ou de documentos específicos neles contidos, inclusive em relação às petições e aos documentos juntados pelas partes envolvidas.

Parágrafo único. Sempre que possível, as petições e os documentos juntados pelas partes envolvidas deverão ser apresentados ao Ministério Público com respeito às diretrizes de proteção de dados pessoais previstas na presente Resolução.

Seção VII
Do Mapeamento e da Custódia de Dados Pessoais

Art. 80. Os ramos e as unidades do Ministério Público deverão realizar o mapeamento ou o inventário das bases de dados, abrangendo todos os dados pessoais que estejam sob seu controle, incluindo aqueles que tenham sido compartilhados, independentemente do modo como se realizou a sua coleta.

§ 1º As coleções de dados pessoais inventariadas deverão ser catalogadas conforme os processos de trabalho desenvolvidos institucionalmente, de maneira a permitir a identificação precisa da natureza e da finalidade de todo tratamento, das estruturas orgânicas que o realizam e da forma de coleta dos dados pessoais.

§ 2º Na realização do inventário de dados pessoais, deverão ser identificados os processos e mecanismos técnicos pelos quais serão colhidas as informações necessárias para o atendimento dos direitos dos titulares de dados pessoais.

§ 3º A finalidade atribuída ao tratamento para os objetivos do **caput** não obsta que os dados pessoais sejam utilizados na execução de outras missões institucionais do Ministério Público, inclusive para efeitos de prevenção, investigação, detecção ou repressão de ilícitos ou execução de sanções, bem como para a produção de conhecimento necessária ao Ministério Público, para a salvaguarda e para a prevenção de ameaças à segurança pública e à segurança institucional.

§ 4º O inventário de dados pessoais deverá ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas dos processos de trabalho.

Art. 81. Cada ramo e unidade do Ministério Público deverá manter controle sobre as origens dos dados pessoais coletados e sobre os canais de sua captura, como sítio eletrônico na internet, parceiros, empresas, órgãos públicos, servidores e público externo.

Art. 82. O inventário de bases de dados pessoais não importa nem autoriza o acesso ao seu conteúdo, cabendo aos ramos e às unidades do Ministério Público estabelecerem procedimentos específicos para a identificação e classificação de suas bases sigilosas e confidenciais.

Parágrafo único. Na hipótese prevista no **caput** deste artigo, o inventário terá natureza estratégica, podendo ter a sua publicidade restringida, total ou parcialmente.

Seção VIII
Do Tratamento do Dado Pessoal Sensível

Art. 83. No tratamento de dados pessoais sensíveis, para instruir investigação de natureza cível ou criminal, para as ações de segurança institucional, de produção de conhecimento, no âmbito de seus procedimentos extrajudiciais ou na atuação em processos judiciais, bem como nos bancos de dados pessoais mantidos para conferir suporte a tais atividades, os ramos e as unidades do Ministério Público brasileiro agirão com reforço de proteção e cuidados específicos nas suas etapas.

Art. 84. O tratamento de dados pessoais sensíveis, nas atividades administrativas do Ministério Público, deverá ser realizado mediante consentimento expresso e específico do titular ou de seu representante legal.

§ 1º O consentimento previsto no **caput** deste artigo será dispensado, todavia, nos seguintes casos, entre outros:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - tratamento compartilhado de dados necessários à execução, pelo Ministério Público, de políticas públicas previstas em leis ou regulamentos;

III - tratamento necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular;

IV - 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);

V - tratamento necessário à declaração, ao exercício ou à defesa de um direito num procedimento extrajudicial ou processo administrativo;

VI - tratamento necessário por motivos de interesse público, que deve ser proporcional em relação ao objetivo visado, deve respeitar a essência do direito à proteção dos dados pessoais e deve prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular;

VII - proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - proteção de interesses vitais do titular dos dados pessoais ou de terceiro, se o titular estiver física ou legalmente impossibilitado de dar o seu consentimento;

IX - 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 da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

X - tratamento relacionado com dados pessoais manifestamente tornados públicos pelo seu titular;

XI tratamento efetuado por fundações, associações ou outros organismos sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais;

XII - tratamento necessário por motivos de interesse público no domínio da segurança pública e institucional;

XIII - tratamento necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, que deve ser proporcional em relação ao objetivo visado, deve respeitar a essência do direito à proteção dos dados pessoais e deve prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular; e

XIV - tratamento necessário às atividades de segurança institucional e de produção de conhecimento para o exercício das funções finalísticas do Ministério Público.

§ 2° Nos casos de aplicação do disposto nos incisos I e II do **caput** deste artigo pelos órgãos competentes do respectivo Ministério Público, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do **caput** do art. 23 da LGPD.

Seção IX
Do Tratamento de Dados Pessoais de Crianças e Adolescentes

Art. 85. Para fins desta Resolução, nos termos legais, considera-se criança o titular de dados pessoais que possua até 12 anos de idade incompletos e adolescente o titular de dados pessoais que possua entre 12 e 18 anos de idade, e ambos devem ter proteção especial no tratamento de seus dados pessoais.

Parágrafo único. O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado no seu melhor interesse, nos termos desta Resolução e da legislação pertinente.

Art. 86. O tratamento de dados pessoais de crianças e adolescentes, no âmbito das atividades administrativas do Ministério Público, além de observar os princípios do art. 3º da presente Resolução, deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 1° É dispensado o consentimento dos pais ou responsáveis legais quando o tratamento de dados pessoais de crianças e adolescentes for necessário ao desenvolvimento da atividade finalística do Ministério Público.

§ 2° A dispensa do consentimento também dar-se-á nas hipóteses de necessidade de contato ou de conflito de interesses, quando os pais ou responsáveis legais derem causa à situação que desafia a atuação protetiva do órgão competente do Ministério Público respectivo.

Art. 87. O controlador e o responsável pelo tratamento devem realizar todos os esforços razoáveis para verificar se o consentimento, quando necessário, foi dado pelo responsável pela criança ou pelo adolescente.

Art. 88. No tratamento de dados pessoais de crianças e adolescentes desempenhado no âmbito da atividade administrativa do Ministério Público, o controlador, ressalvadas as hipóteses previstas no § 2º do art. 66 desta Resolução, deverá

manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 da LGPD.

Art. 89. Para o exercício da atividade de proteção de dados pessoais de crianças e adolescentes, as informações do respectivo tratamento deverão ser de fácil acesso e compreensão e formuladas em termos claros e simples, 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 ou adolescente, na forma da lei e respeitadas as regras nos casos de sigilo ou de segredo de justiça.

Art. 90. O tratamento de dados pessoais de crianças e adolescentes, iniciado em data anterior à vigência da LGPD e ainda não finalizado, deverá, quando necessário e possível, ser informado a pelo menos um dos pais ou responsável legal e colhido o consentimento para a continuidade da operação.

Art. 91. Na coleta de dados pessoais de crianças e adolescentes, todos os registros deverão, quando possível, estar acompanhados de documento válido que comprove essa peculiar condição pessoal.

Seção X
Do Tratamento Automatizado

Art. 92. As decisões que possam produzir efeitos adversos na esfera jurídica do titular de dados pessoais, baseadas em mecanismos automatizados de tratamento, poderão ser objeto de revisão mediante intervenção humana e levarão em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados pessoais.

§ 1º Os ramos e as unidades do Ministério Público avaliarão, periodicamente, o tratamento automatizado de dados pessoais para evitar, entre outras hipóteses:

I - práticas abusivas;

II - erros e desvios decorrentes das limitações das amostras, intervalos de confiança, incorreções de dados, viés da base de dados e estágio do desenvolvimento tecnológico;

III - tratamento discriminatório;

IV - adoção de premissas falsas, incompletas ou inexatas; e

V - manipulação dos algoritmos por terceiros ou interessados.

§ 2º Ainda que haja o tratamento automatizado de dados pessoais, há de se garantir ao titular o direito de obter a intervenção humana do responsável pelo tratamento, especialmente na hipótese prevista no **caput**.

§ 3º Não é considerado tratamento de dado pessoal aquele realizado em dados que não requerem identificação.

Seção XI
Do Limite Territorial e Material – Do território brasileiro

Art. 93. A presente Resolução aplica-se em todo território nacional, nas hipóteses de tratamento de dados pessoais pelo Ministério Público brasileiro, principalmente no compartilhamento e na transferência – exportação e importação – com outras instituições internacionais e, ainda, na hipótese de incidentes de tratamento de dados pessoais que extrapolem o território nacional.

Parágrafo único. Nas hipóteses em que o armazenamento, o tratamento e o compartilhamento ou a transferência de dados pessoais ocorrer fora do território nacional, também deve ser aplicada a presente Resolução.

Seção XII
Das Medidas de Compartilhamento e de Transferência de Dados Pessoais

Art. 94. Para os fins desta Resolução considera-se compartilhamento a troca de informações e dados, inclusive pessoais, entre os órgãos do CNMP e os órgãos dos ramos e das unidades do Ministério Público, enquanto a transferência significa a troca havida com órgãos e entidades distintas.

§ 1º O compartilhamento seguro de bases de dados pessoais entre o CNMP, os ramos e as unidades do Ministério Público, bem como a transferência segura de dados pessoais, deverão ser formalizados, cabendo aos órgãos envolvidos informarem a origem da base de dados e atestarem o seu recebimento e a sua integridade.

§ 2º Finalizada a transferência e o compartilhamento seguros, o órgão ministerial que os concretizou não será responsabilizado pelos incidentes de segurança ocasionados pelo tratamento realizado pelo órgão ou pela instituição que os recebeu.

Art. 95. O compartilhamento interno e externo de dados pessoais entre órgãos do Ministério Público brasileiro, consideradas a sua unidade, independência e autonomia, é permitido e necessário para o exercício de suas atribuições legais e constitucionais.

Parágrafo único. Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados pessoais previstos no **caput**.

Art. 96. Para as finalidades previstas no art. 95 não se pode impor limitações à amplitude do compartilhamento de dados pessoais, devendo ser observadas as restrições legais, os requisitos de segurança da informação e comunicações e os preceitos de proteção dos dados pessoais.

Art. 97. O fornecimento dos dados pessoais a terceiros e a sua utilização para finalidades diversas daquelas para as quais foram coletados poderão ocorrer mediante consentimento fornecido pelo seu titular ou, ainda, nas hipóteses de tratamento para a execução das atribuições constitucionais e regimentais de cada ramo ou unidade do Ministério Público, além da transferência para órgãos ou entidades visando à execução de atividades de interesse público.

Art. 98. A transferência ou o compartilhamento de dados pessoais inexatos, incompletos ou desatualizados serão realizados conforme definido pelas instituições envolvidas, observada a efetividade, a finalidade e o protocolo comum de tratamento.

Parágrafo único. O protocolo comum, sempre que possível, documentará a fonte, a natureza, as características, o tempo, o histórico, e os dicionários dos dados transferidos ou compartilhados, bem como os objetivos e resultados esperados após o tratamento.

Subseção I
Da Transferência entre Instituições Públicas Parceiras e de Controle

Art. 99. A transferência de dados pessoais para instituições públicas parceiras e de controle deverá ocorrer sempre de forma segura para atender a finalidades específicas

de segurança pública, segurança de estado, de produção de conhecimento e, também, para a execução de políticas públicas e atribuição legal pelos demais órgãos e por entidades públicas.

Subseção II

Da Transferência e do Compartilhamento nos Casos de Atuação Conjunta

Art. 100. São autorizados o compartilhamento e a transferência de dados pessoais, sempre de forma segura, respectivamente, entre os diferentes ramos e unidades do Ministério Público e entre esses e outras instituições públicas, nos casos de atuação conjunta no exercício de suas atribuições, inclusive na hipótese de transferência internacional de dados e informações.

Parágrafo único. Cada instituição envolvida é considerada controladora dos dados pessoais transferidos ou compartilhados.

Subseção III

Da Transferência Público-Privada

Art. 101. É vedado ao ramo ou à unidade do Ministério Público respectivo transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade institucional 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 - nos casos em que os dados pessoais forem acessíveis publicamente;

III - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

IV - na hipótese de a transferência objetivar exclusivamente a prevenção de fraudes e irregularidades ou proteger e resguardar a segurança e a integridade do titular dos dados pessoais, desde que vedado o tratamento para outras finalidades.

§ 1º Nas hipóteses previstas neste artigo, os contratos e convênios respectivos deverão ser comunicados à UEPDAP, na forma por esta definida.

§ 2º Em quaisquer das hipóteses previstas neste artigo, a transferência deverá respeitar os requisitos de segurança da informação e a compatibilidade de sistemas que impeçam o vazamento das bases de dados pessoais transferidas.

§ 3º Antes de concretizar a transferência, o órgão ministerial deve se certificar do cumprimento, pelo receptor dos dados pessoais, das medidas assecuratórias previstas nesta Resolução.

Subseção IV

Da Transferência Internacional

Art. 102. A transferência internacional de dados pessoais no âmbito do Ministério Público brasileiro é permitida desde que:

I - o controlador ofereça e comprove garantias de cumprimento dos princípios, dos direitos do titular e do regime adequado de proteção de dados pessoais, previstos na legislação pertinente e nesta Resolução;

II - os países ou os organismos internacionais proporcionem grau de proteção de dados pessoais adequado; e

III - sejam adotados instrumentos de direito internacional.

Parágrafo único. Para os fins deste artigo, os ramos e as unidades do Ministério Público brasileiro, no âmbito de suas atribuições legais, poderão requerer à UEPDAP a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional, aplicando-se, então, o disposto no art. 34 da LGPD.

Art. 103. Respeitadas as obrigações estabelecidas no artigo anterior é permitida a transferência internacional de dados pessoais, no âmbito do Ministério Público brasileiro, nas seguintes hipóteses:

I - para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução;

II - para a proteção da vida, da incolumidade física, da liberdade e da dignidade sexual;

III - quando resultar em compromisso assumido em acordo de cooperação internacional;

IV - para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do **caput** do art. 23 da LGPD;

V - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente essa de outras finalidades;

VI - para atender às hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD; e

VII - para outras hipóteses institucionais não previstas nos incisos anteriores, desde que mediante prévia autorização da UEPDAP.

Seção XIII
Das Relações de Trabalho Dos Dados Pessoais dos Membros, Servidores, Estagiários e Prestadores de Serviços

Subseção I
Das Bases Legais para o Tratamento de Dados Pessoais

Art. 104. Para os fins do tratamento de dados pessoais dos seus membros, servidores, estagiários e prestadores de serviços, o CNMP, os ramos e as unidades do Ministério Público deverão adotar como bases legais, principalmente:

I - as leis orgânicas e as demais leis aplicáveis;

II - o consentimento;

III - o contrato; e

IV - o legítimo interesse.

Subseção II
Do Tratamento de Dados Pessoais Sensíveis dos Membros, Servidores, Estagiários e Prestadores de Serviços

Art. 105. Os dados pessoais sensíveis dos membros, servidores, estagiários e prestadores de serviços, no âmbito do Ministério Público, deverão ser tratados de acordo com as exceções previstas no inciso II do art. 11 da LGPD, para a finalidade específica,

pelo controlador, do cumprimento de obrigação legal, estatutária, contratual ou regulatória, e, também, a partir do consentimento dos seus titulares.

Parágrafo único. Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do **caput** do art. 11 da LGPD, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do **caput** do art. 23 da mesma Lei.

Subseção III

Dos Comunicados

Art. 106. O CNMP, os ramos e as unidades do Ministério Público brasileiro deverão estabelecer uma política transparente de tratamento de dados pessoais, na qual deverá haver a clara informação e a comunicação acerca dos propósitos e de como se realiza o tratamento em razão do vínculo estatutário ou contratual existente.

Parágrafo único. Aplica-se ao tratamento de dados pessoais dos membros, servidores, estagiários e prestadores de serviços, de forma complementar, os princípios e as regras do tratamento em geral, nos termos da presente Resolução.

Subseção IV

Do Armazenamento dos Registros Pessoais

Art. 107. O CNMP e cada ramo e unidade do Ministério Público deverão assegurar, quando possível, que o armazenamento dos dados pessoais referentes aos seus membros, servidores, estagiários e prestadores de serviços será feito em bases específicas, que deverão receber reforço de proteção por registro e nível de acesso e, o quanto antes, pseudonimização e criptografia, sem prejuízo das demais técnicas de proteção.

§ 1º Os padrões definidos no **caput** deste artigo serão adotados na evolução e no desenvolvimento de aplicações e respectivos bancos de dados pessoais, inclusive por terceiros contratados.

§ 2º As técnicas de armazenamento a serem empregadas devem servir, na mesma medida, para proteção e para buscar impedir a violação ou o vazamento dos dados pessoais, notadamente em decorrência de acesso indevido por pessoa física ou jurídica após o encerramento do vínculo estatutário, empregatício ou contratual.

Subseção V

Do Monitoramento e da Prevenção da Perda de Dados Pessoais

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.

§ 2º O acesso e o necessário tratamento de dados pessoais com a finalidade de investigação social de pessoa física ou jurídica que tenha interesse em estabelecer vínculo, de qualquer natureza, com a Instituição, pode ser realizado para fins de segurança institucional.

§ 3º Para a proteção dos dados pessoais e de acordo com o interesse público inerente às suas atribuições, o CNMP e cada ramo e unidade do Ministério Público, em relação aos seus membros, servidores, estagiários e prestadores de serviços, poderão editar regras claras e transparentes que:

I - restrinjam o acesso, total ou parcial, à rede mundial de computadores e à Internet;

II - definam o uso do e-mail e as demais formas de comunicação oficial ou funcional;

III - controlem e disciplinem o uso no ambiente interno da Instituição, de dispositivos móveis, como aparelhos celulares e **notebooks**, notadamente se forem particulares, hipótese em que poderá ser exigida, pelo controlador, a instalação de antivírus e quaisquer outros aplicativos ou sistemas de proteção, inclusive de monitoramento; e

IV - estabeleçam outros mecanismos de proteção e segurança da informação, tal como a autenticação de dois fatores ou em duas etapas.

§ 4º Aplicam-se aos terceirizados e prestadores de serviços as mesmas regras referentes ao tratamento de dados pessoais dos servidores e membros do Ministério Público.

§ 5º Na elaboração das regras necessárias à proteção da privacidade e aos dados pessoais previstas neste artigo, deverá ser ouvido, sempre, o órgão ou a coordenadoria responsável pela área de segurança institucional do respectivo ramo ou unidade do Ministério Público.

Subseção VI

Do Modelo para Reclamações

Art. 109. O CNMP, os ramos e as unidades do Ministério Público deverão disponibilizar aos seus membros, servidores, estagiários e prestadores de serviços, nos termos da presente Resolução, fácil e simples acesso aos formulários preexistentes, para o protocolo de reclamações ou pedido de informações relativas a ofensas à proteção de seus dados pessoais, que serão direcionadas ao correspondente órgão do SINPRODAP/MP.

Subseção VII

Dos Contratos Administrativos e da Terceirização de Serviços

Art. 110. Os contratos administrativos e aqueles decorrentes de licitações devem atender aos ditames estabelecidos na presente Resolução.

§ 1º O CNMP, os ramos e as unidades do Ministério Público deverão se certificar e assegurar, quando da contratação de entidades públicas e privadas cujo objeto seja a prestação de serviços, inclusive terceirizados, que elas cumprem com as exigências técnicas e legais de proteção de dados pessoais, incluindo a capacitação regular dos seus colaboradores.

§ 2º Em se tratando de contratação cujo objeto seja quaisquer das formas de tratamento de dados pessoais, deverão igualmente se certificar e assegurar que o operador contratado cumpre com as exigências da LGPD, especialmente a proteção de dados

pessoais por concepção e por padrão, incluindo a capacitação regular dos seus colaboradores.

Seção XIV
Das Técnicas de Boas Práticas e Governança de Dados Pessoais

Art. 111. No que se refere à segurança e à prevenção no tratamento de dados pessoais, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a relevância dos danos para os titulares dos dados pessoais, o controlador poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou a coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados pessoais tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado à sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado, em especial, a pedido da UEPDAP.

Art. 112. Nas hipóteses em que o titular dos dados pessoais interagir com a Instituição a respeito dos seus direitos disciplinados por esta Resolução, deverá ser

verificada a sua identidade pelos meios razoáveis, atentando-se à idoneidade da solicitação e exigindo-se, sempre que possível, a comprovação dela.

Seção XV
Do Ciclo de Vida do Tratamento de Dados Pessoais

Art. 113. O responsável ou o operador que trate dados pessoais em sistemas de tratamento, automatizados ou não, deverá dispor de métodos eficazes, tais como registros cronológicos ou outros, para demonstrar a licitude do tratamento, permitir o autocontrole e garantir a integridade e a segurança dos dados pessoais.

§ 1º Deverão ser conservados, no mínimo, os registros cronológicos das seguintes operações de tratamento: coleta, alteração, consulta, visualização, divulgação, transferência, interconexão e eliminação.

§ 2º A conservação dos registros cronológicos das operações de consulta e divulgação deve determinar o motivo, a data e o horário de tais operações e, na medida do possível, a identificação da pessoa que consultou ou divulgou os dados pessoais, além da identidade dos destinatários deles.

§ 3º Os registros cronológicos serão utilizados apenas para efeitos de verificação da licitude do tratamento; auditoria; atividade correcional; e garantia da integridade e segurança dos dados pessoais envolvidos, além de prova em processos judiciais.

§ 4º Os registros cronológicos serão disponibilizados pelos agentes de tratamento à UEPDAP quando devidamente requisitados, bem como quando determinado por lei ou por esta Resolução.

Art. 114. A acessibilidade aos dados pessoais coletados poderá ter efetivo controle e gradação, nos termos desta Resolução, com limitação do acesso aos dados ao mínimo efetivamente necessário ao desenvolvimento das atividades.

Subseção I
Do Término do Tratamento de Dados Pessoais

Art. 115. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados pessoais deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da LGPD, resguardado o interesse público; ou

IV - determinação da UEPDAP, quando houver violação ao disposto nesta Resolução.

Art. 116. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados pessoais dispostos nesta Resolução e na LGPD;

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados pessoais; e

V - utilização em outra finalidade pública, incluindo-se a necessidade de produção de conhecimento interno.

Parágrafo único. Considera-se também a ocorrência do término do tratamento quando ocorre a anonimização dos dados pessoais.

Art. 117. Não se considerará finalizado o tratamento de dados pessoais quando subsistir o interesse público para o atendimento de outras finalidades, inclusive para produção de conhecimento interno em prol do cumprimento das obrigações constitucionais do Ministério Público e para as questões atinentes à segurança institucional.

Art. 118. O término do tratamento e, principalmente, a eliminação de dados pessoais deverão se vincular, quando existentes, às tabelas de temporalidade e classificação de documentos, inclusive os eletrônicos.

Art. 119. Quanto aos sistemas de informação, a exclusão dos dados pessoais dependerá da possibilidade técnica e, principalmente, da inexistência de interesse público ou institucional, incluindo-se a segurança institucional.

Seção XVI
Das Técnicas de Sistemas de Informação

Subseção I
Da Segurança do Dado Pessoal

Art. 120. No âmbito do Ministério Público brasileiro, aplicam-se à segurança do dado pessoal, em geral, as regras previstas na Subseção IV da Resolução CNMP nº 156, de 13 de dezembro de 2016, que trata da segurança da informação.

Parágrafo único. A segurança da informação visa garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade do dado, da informação ou do conhecimento.

Art. 121. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e relevância variável, para os direitos e liberdades das pessoas naturais, os agentes de tratamento, no âmbito do Ministério Público brasileiro, poderão aplicar as medidas técnicas e administrativas aptas para assegurar um nível de segurança adequado ao risco e para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, subtração, cópia, transferência, comunicação ou difusão, incluindo, no que for possível:

I - a anonimização, a pseudonimização e a criptografia dos dados pessoais;

II - a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

III - a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais, a tempo e modo, no caso de um incidente físico ou técnico; e

IV - um procedimento para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e administrativas que garantam a segurança do tratamento.

Art. 122. O CNMP e cada ramo ou unidade do Ministério Público, no que diz respeito ao tratamento de dados pessoais, inclusive o automatizado, deverá determinar que os agentes de tratamento, após a devida avaliação dos riscos, priorizem e apliquem medidas que signifiquem e possam gerar:

I - controle de acesso ao equipamento: impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento;

II - controle dos bancos de dados: impedir que os bancos de dados pessoais sejam lidos, copiados, alterados ou retirados sem autorização;

III - controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados;

IV - controle dos utilizadores: impedir que os sistemas de tratamento sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados;

V - controle do acesso aos dados: assegurar que as pessoas autorizadas a utilizar um sistema de tratamento só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso;

VI - controle da comunicação: assegurar a possibilidade de verificação do controle de transmissão dos dados pessoais;

VII - controle da introdução: assegurar que possam ser verificados e determinados **a posteriori** quais dados pessoais foram introduzidos, visualizados, alterados ou eliminados nos sistemas de tratamento automatizado, quando e por quem;

VIII - controle do transporte: impedir que, durante os compartilhamentos e as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização;

IX - recuperação: assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção; e

X - integridade: assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados e que os dados pessoais conservados não possam ser falseados por uma falha do sistema.

Parágrafo único. Estas medidas aplicam-se, no que couber, ao tratamento de dados pessoais que seja realizado em procedimentos e processos físicos, incluindo instalações prediais e respectivos recintos.

Art. 123. O CNMP, os ramos e as unidades do Ministério Público brasileiro devem desenvolver mecanismos de proteção e níveis de segurança e de acesso diferenciados com relação às redes e ao Wi-Fi em prol do resguardo dos dados pessoais.

Art. 124. Considerando que, em todas as atividades, funções e atribuições desenvolvidas pelo Ministério Público brasileiro, há o tratamento de dados pessoais, o CNMP, os ramos e as unidades do Ministério Público brasileiro deverão, com relação a seus integrantes e em prol da efetiva proteção ao direito fundamental a elas correspondente, determinar a assinatura do Termo de Compromisso de Manutenção de Sigilo (TCMS).

§ 1º A assinatura do TCMS deverá ser regularizada e concretizada a partir da vigência desta Resolução e, principalmente, adotada no momento do ingresso do integrante na Instituição.

§ 2º O compromisso de manutenção do sigilo dos dados pessoais igualmente deverá ser inserido em todos os atuais e futuros contratos celebrados com prestadores de serviços, de qualquer natureza.

§ 3º A assinatura do TCMS deve ser realizada também pelos estagiários.

Art. 125. Para o cumprimento do objetivo indicado no **caput** do art. 124, o CNMP, os ramos e as unidades do Ministério Público brasileiro, antes do desligamento de quaisquer de seus integrantes, deverão adotar medidas para a continuidade do resguardo do sigilo dos dados pessoais tratados enquanto estavam no exercício das atividades, funções e atribuições por eles desenvolvidas.

Subseção II

Da Proteção de Dados Pessoais por Concepção e por Padrão (*design* e *default*)

Art. 126. Desde a concepção e durante todo o ciclo de vida dos projetos, processos, sistemas, bancos de dados, serviços e produtos, atuais e futuros, no âmbito do Ministério Público brasileiro, os responsáveis deverão, quanto à privacidade e à proteção dos dados pessoais, respeitar os seguintes princípios:

I - proatividade e prevenção, não reativo nem corretivo;

II - privacidade como padrão dos sistemas de tecnologia da informação, dos bancos de dados pessoais ou outras práticas de negócio;

III - privacidade incorporada;

IV - funcionalidade total;

V - segurança e proteção, de ponta a ponta, durante o ciclo de vida de tratamento de dados pessoais;

VI - visibilidade e transparência; e

VII - respeito pela privacidade do usuário.

§ 1º Na mesma medida, em relação aos softwares e às bases de dados pessoais a serem desenvolvidos ou adquiridos, devem assegurar que eles contenham a proteção como requisito desde a sua concepção e por padrão, prevendo, entre outras, as atividades de treinamento dos usuários, design, codificação, testes e manutenção adequados.

§ 2º Quanto ao treinamento dos usuários, deverão ser considerados os seguintes itens básicos, no mínimo:

I - internos:

a) proteção de dados pessoais;

b) segurança da informação;

c) controle interno;

d) gestão de recursos;

e) análise de riscos; e

f) requisitos referentes à documentação.

II - externos:

a) leis e regulamentações de proteção de dados pessoais;

b) regulamentações específicas das atividades ministeriais;

c) importância dos princípios da proteção de dados pessoais; e

d) direitos dos indivíduos detentores dos dados pessoais.

Art. 127. O responsável pelo tratamento deve aplicar, tanto no momento da definição dos meios como durante o próprio tratamento, as medidas técnicas e administrativas adequadas, como a minimização, a pseudonimização e a autenticação de dois fatores ou em duas etapas, destinadas a colocar efetivamente em prática os princípios da proteção de dados pessoais e a integrar as garantias necessárias no tratamento.

Art. 128. O responsável pelo tratamento deve implementar e aplicar medidas técnicas e administrativas adequadas para assegurar que, por padrão, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento.

Parágrafo único. As disposições do **caput** deste artigo se aplicam à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade, inclusive para prevenir a disponibilização, sem intervenção humana, a um número indeterminado de pessoas.

Art. 129. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD, na presente Resolução e nas demais normas regulamentares, devendo tais medidas serem observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 130. Quando possível e necessário, em quaisquer de suas atividades, ao uso de dados pessoais pelo Ministério Público brasileiro serão aplicadas, isoladamente ou em conjunto, as seguintes estratégias orientadas: minimização, ocultação, separação, resumo, informação, controle, reforço e demonstração, além da criptografia.

Art. 131. Para a proteção de dados pessoais por concepção e por padrão (**design** e **default**), aplica-se o disposto no art. 71 da presente Resolução.

Seção XVII
Dos sítios eletrônicos e sistemas informatizados

Art. 132. Os sítios eletrônicos e sistemas informatizados deverão descrever as hipóteses em que se realiza o tratamento de dados pessoais, fornecendo informações atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.

Parágrafo único. Serão disponibilizadas, ainda, informações sobre:

I - as obrigações dos controladores e os direitos dos titulares dos dados pessoais;

II - o encarregado, nos termos do §1º do art. 41 da LGPD;

III - a política de privacidade para navegação no sítio eletrônico;

IV - a política geral de privacidade e de proteção de dados pessoais do Ministério Público; e

V - o uso de cookies ou tecnologia similar pelos sítios e sistemas.

Art. 133. A UEPDAP definirá a política de coleta de informações de usuários dos sítios eletrônicos ou sistemas informatizados, de forma a garantir, mediante anonimização e pseudonimização, o uso adequado de:

I - dados pessoais sobre preferências de usuário, a incluir seleções de linguagem e ferramentas de acessibilidade, mediante consentimento;

II - dados pessoais sobre visitas e formas de utilização, para aprimoramento da qualidade da prestação de serviços; e

III - dados pessoais essenciais para gerenciamento de funcionalidades, tráfego de rede e requisitos de segurança, incluindo o monitoramento de endereços de IP e ações maliciosas, inclusive o uso de rastreadores.

Parágrafo único. As informações a respeito da política de coleta e gestão do consentimento dos usuários, quanto ao uso de cookies ou tecnologias similares, serão disponibilizadas nos sítios eletrônicos e nos sistemas informatizados.

Art. 134. Deverão ser implementados mecanismos de controle, identificação e registro de acesso do usuário a dados pessoais que sejam disponibilizados por meio de sítios eletrônicos ou sistemas informatizados com acesso remoto, a fim de assegurar a proteção de dados pessoais e a segurança da informação.

Seção XVIII
Da Aferição dos Riscos ao Tratamento Indevido dos Dados Pessoais

Art. 135. A violação ou o vazamento de dados pessoais, voluntária ou acidentalmente, é considerado um incidente de segurança no tratamento, notadamente se ocasionar destruição, perda, alteração, subtração, cópia, transferência, comunicação ou difusão de dado pessoal.

§ 1º Ocorre o incidente de segurança no tratamento de dados pessoais quando se verifica, sem autorização ou de maneira acidental, uma ou mais das seguintes violações ou perdas:

I - da confidencialidade: quando há uso, divulgação ou acesso indevido do dado pessoal;

II - da integridade: quando há alteração do dado pessoal; e

III - da disponibilidade: quando há perda de acesso ou destruição do dado pessoal.

§ 2º Também pode caracterizar risco de violação de dados pessoais, de probabilidade e relevância variáveis, quando o tratamento causar danos físicos, materiais ou morais e imateriais, em especial:

I - quando possa dar origem à discriminação, à usurpação ou subtração da identidade, a perdas financeiras, a prejuízos para a reputação, a perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização ou a quaisquer outros prejuízos importantes de natureza econômica ou social;

II - quando os titulares possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controle sobre os respetivos dados pessoais;

III - quando forem revelados, sem autorização, dados pessoais sensíveis;

IV - quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou aos interesses pessoais, à fiabilidade ou comportamento e à localização ou aos deslocamentos das pessoas, a fim de definir ou fazer uso de perfis;

V - quando forem tratados indevidamente dados relativos a pessoas naturais vulneráveis, em particular crianças e adolescentes; ou

VI - quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares.

§ 3º O controlador e o operador deverão assegurar que o tratamento de dados pessoais não seja efetuado por pessoas não autorizadas, obrigando-se a garantir a segurança da informação em relação a tais dados, mesmo após o término do tratamento.

Art. 136. A probabilidade e a relevância dos riscos deverão ser determinadas por referência à natureza, ao âmbito, ao contexto e às finalidades do tratamento de dados pessoais, devendo a aferição dos riscos ser feita com base numa avaliação objetiva, de

modo a determinar se é provável que as operações de tratamento impliquem um relevante risco ao direito do titular.

§ 1º Para a aferição e gestão dos riscos, o responsável deverá priorizar os métodos e o uso das melhores práticas, a serem estabelecidos pela SEPRODAP.

§ 2º No juízo de relevância do incidente, será avaliada eventual comprovação de que foram adotadas prévias medidas técnicas adequadas para tornar os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

§ 3º Na avaliação do nível de risco no tratamento de dados pessoais, deverão ser consideradas, no mínimo, a probabilidade de ocorrência de danos à sua esfera de proteção e a potencial relevância de suas consequências, devendo-se observar, ainda, eventual incidência das hipóteses previstas no art. 60 da presente Resolução.

Seção XIX
Do Relatório de Impacto à Proteção de Dados Pessoais (RIDP)

Art. 137. O controlador elaborará Relatório de Impacto à Proteção de Dados Pessoais (RIDP), nos processos de tratamento de dados pessoais, na sua atividade administrativa, que possam gerar riscos às liberdades civis e aos direitos fundamentais, em particular:

I - quando houver risco relevante de infração à legislação de proteção de dados pessoais;

II - quando ocorrer a adoção de novas tecnologias, serviços ou iniciativas que envolvam o tratamento de dados pessoais;

III - quando o tratamento implique a formação de perfil comportamental e de atributos personalíssimos da pessoa natural;

IV - nas hipóteses de tratamento envolvendo dados sensíveis da pessoa natural;

V - no tratamento de dados pessoais realizado mediante decisões automatizadas;

VI - no tratamento de dados pessoais referentes a crianças e adolescentes;

VII - no advento de legislação que implique alteração nas regras de tratamento de dados pessoais; ou

VIII - por determinação da UEPDAP.

§ 1º Nas hipóteses dos incisos I, II, III, V e VIII a elaboração do RIDP será obrigatória.

§ 2º Também poderá ser determinada a elaboração de RIDP em outros casos de tratamento de dados pessoais que, após a devida análise de risco, constate-se tratar de grau relevante, hipóteses em que o encarregado sempre deverá ser ouvido.

§ 3º A aferição dos riscos de qualquer tratamento decorre do resultado da realização do inventário de dados pessoais, conforme previsto na Seção VII do Capítulo IV da presente Resolução.

§ 4º Tratando-se de aferição de risco não relevante, o RIDP não precisará ser elaborado.

Art. 138. A UEPDAP determinará aos ramos e às unidades do Ministério Público brasileiro a elaboração de RIDP padronizado, a fim de garantir a observância das disposições da legislação de regência e da presente Resolução, bem como para ensejar a adoção de boas práticas no tratamento de dados pessoais.

Parágrafo único. A UEPDAP também poderá exigir, excepcionalmente, a elaboração de RIDP detalhado, nos casos em que se verifique risco relevante de incidente no tratamento de dados pessoais e nas hipóteses de infração grave à legislação de proteção de dados pessoais.

Art. 139. O RIDP deverá conter, no mínimo, a descrição dos tipos de dados pessoais coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Parágrafo único. A UEPDAP confeccionará os manuais e formulários eletrônicos necessários à elaboração do RIDP, a fim de assegurar sua padronização e auditabilidade, observados os critérios previstos na presente Resolução.

Art. 140. A elaboração do RIDP deverá contemplar as seguintes etapas, sem prejuízo de outras consideradas necessárias:

I - identificação dos agentes de tratamento e do encarregado;

II - identificação da necessidade da elaboração do relatório;

III - descrição do tratamento;

IV - identificação das partes interessadas consultadas;

V - descrição da necessidade e da proporcionalidade;

VI - identificação e avaliação dos riscos;

VII - identificação das medidas para tratamento dos riscos;

VIII - aprovação do relatório; e

IX - manutenção de revisão periódica.

Art. 141. A elaboração do RIDP poderá ser feita por qualquer pessoa, física ou jurídica, com conhecimento sobre o tema e desde que autorizada pelo controlador.

Parágrafo único. O RIDP será subscrito pelo responsável pela sua elaboração, pelo encarregado, pelos representantes do controlador e, se for o caso, do operador.

Art. 142. O CNMP e os respectivos ramos e unidades do Ministério Público brasileiro analisarão periodicamente as suas próprias operações de tratamento de dados pessoais para avaliar a possibilidade de realização de um único RIDP para todas as operações ou para cada projeto, sistema ou serviço, em decisão fundamentada.

Art. 143. A revisão e atualização do RIDP será feita com a periodicidade definida pelo controlador e deverá ocorrer nas seguintes hipóteses, sem prejuízo de outras:

I - significativa alteração da finalidade do tratamento de dados pessoais;

II - alteração no processo de tratamento de dados pessoais;

III - aumento na quantidade e diversidade do tratamento dos dados pessoais;

IV - alteração na percepção de risco ou vulnerabilidade dos dados pessoais ou seus titulares; ou

V - ocorrência de falha de segurança, emprego de nova tecnologia ou alteração normativa.

Art. 144. O RIDP poderá ter a sua publicidade restringida, total ou parcialmente, por motivos de segurança institucional ou outras razões de interesse público.

Seção XX

Das Comunicações e da Resposta a Incidentes de Segurança com Dados Pessoais

Art. 145. Todo responsável pelo tratamento de dados pessoais deverá reportar ao encarregado e ao órgão de tecnologia da informação competente, imediatamente, a ocorrência de incidente de segurança com dados pessoais, com finalidade de permitir a imediata tomada de medidas de contenção e outras necessárias ao controle e à mitigação do dano, devendo ser informados no comunicado:

I - a descrição e a natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os casos de sigilo legal e institucional;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Parágrafo único. Em caso de incidente de segurança com vazamento de dados pessoais criptografados, também será obrigatória a comunicação prevista no **caput** quando a confidencialidade dos dados pessoais, de alguma forma, tiver sido violada.

Art. 146. Em qualquer hipótese de incidente de vazamento de dados pessoais, independentemente da sua relevância, o operador deverá comunicar imediatamente ao controlador a sua ocorrência, devendo a comunicação conter, minimamente, as informações indicadas no art. 145.

Parágrafo único. Os contratos de prestação de serviços de tratamento de dados pessoais, atuais e futuros, deverão conter cláusula determinando a obrigação prevista no **caput** deste artigo.

Art. 147. O controlador deverá documentar quaisquer vazamentos de dados pessoais, registrando os fatos relacionados, os respectivos efeitos e a medida de reparação adotada, visando a permitir, principalmente, a verificação do cumprimento das medidas protetivas desta Resolução.

Parágrafo único. Aos documentos mencionados no **caput** deste artigo aplicam-se as hipóteses de sigilo legal e institucional, podendo o acesso a eles ser restringido.

Art. 148. O controlador, ao tomar conhecimento do incidente de segurança relativo ao tratamento de dados pessoais com possibilidade de causar dano relevante aos

titulares, comunicará à UEPDAP, sem demora injustificada, sempre que possível no prazo de até 72 (setenta e duas) horas.

§ 1º A comunicação deverá conter, no mínimo:

I - a descrição da natureza do incidente incluindo, se possível, as informações sobre o número aproximado de titulares de dados afetados, bem como a natureza e o número aproximado de registros de dados pessoais em causa;

II - o nome e o contato do encarregado da proteção de dados pessoais;

III - a descrição das consequências prováveis do vazamento; e

IV - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observadas as hipóteses de sigilo legal, além das medidas que foram ou que serão adotadas para reverter ou mitigar os prejuízos.

§ 2º A comunicação das informações acerca do incidente de vazamento não importará na remessa dos dados pessoais vazados e das bases nas quais esses se encontram.

§ 3º A comunicação prevista no **caput** deste artigo, em hipóteses de tratamento de dados pessoais para fins de segurança pública, de segurança institucional, de assuntos institucionais e jurídicos ou, ainda, por questão de natureza estratégica, deve ser destinada à UEPDAP com a informação classificada como de sigilo absoluto.

Art. 149. A UEPDAP, no procedimento próprio instaurado para a apuração do incidente de segurança comunicado, poderá, diante da aferição da sua relevância, determinar ao controlador a adoção de providências, como a ampla divulgação do fato em meios de comunicação e medidas outras específicas para reverter ou mitigar os efeitos do incidente.

Parágrafo único. Constatada a necessidade da apuração da conduta responsável pelo incidente, inclusive se dolosa ou culposa, a UEPDAP deverá formular representação à autoridade correcional ou disciplinar local que detenha atribuição para a apuração da possível falta funcional, encaminhando todas as informações possíveis e necessárias que permitam a instauração do devido processo legal, garantidos o contraditório e a ampla defesa.

Art. 150. Quando o incidente de segurança relativo ao tratamento for suscetível de criar um relevante risco para os direitos e as liberdades das pessoas naturais e, também, quando o controlador ou o encarregado entenderem oportuno, os titulares de

dados pessoais e a ANPD deverão ser informados sem demora injustificada, a fim de permitir que tomem as precauções necessárias, devendo constar da comunicação a natureza da violação de dados pessoais e as recomendações destinadas a atenuar potenciais efeitos adversos.

§ 1º A comunicação poderá ser atrasada, restrita ou omitida, se se tratar de atividade institucional sigilosa ou protegida por lei, e nas hipóteses tratadas no art. 77 desta Resolução.

§ 2º A UEPDAP poderá dispor a respeito de outras hipóteses complementares de restrição à comunicação dos incidentes de segurança aos titulares dos dados pessoais.

§ 3º A comunicação não será exigida se:

I - o responsável pelo tratamento de dados pessoais tiver aplicado medidas de proteção adequadas, tanto tecnológicas como administrativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação, especialmente medidas que os tornem incompreensíveis para qualquer pessoa não autorizada a acessá-los, como, por exemplo, a criptografia; ou

II - o responsável pelo tratamento de dados pessoais tiver tomado medidas subsequentes capazes de assegurar que a ocorrência de relevante risco para os direitos e as liberdades dos titulares referida no caput deixou de ser provável.

Art. 151. Na hipótese de a comunicação individual implicar um esforço desproporcional para o controlador, será feita uma comunicação coletiva ou adotada medida semelhante por meio da qual os titulares dos dados pessoais serão informados de forma igualmente eficaz.

§ 1º Para efetivar a comunicação coletiva devem ser adotadas cautelas necessárias que não acarretem exposição indevida dos dados pessoais a ela correspondentes.

§ 2º O controlador deve manter página específica no seu sítio eletrônico, na qual deverão estar disponibilizadas as comunicações coletivas previstas no **caput** deste artigo.

Art. 152. Para fins de quantificação e qualificação dos danos decorrentes do incidente de segurança no tratamento de dados pessoais, devem ser levados em conta, primordialmente, os seguintes critérios:

I - o tipo de dado pessoal afetado;

II - a confidencialidade do dado e da informação afetados;

II - a natureza do dado pessoal vazado;

IV - a sensibilidade do dado pessoal afetado;

V - o volume de dados pessoais vazados;

VI - a facilidade da identificação do titular de dados pessoais;

VII - o impacto das consequências para o titular de dados pessoais;

VIII - as características pessoais do titular;

IX - as características especiais do tipo de tratamento que estava sendo utilizado no dado pessoal vazado;

X - o número de titulares afetados; e

XI - se a análise conjugada dos dados pessoais vazados implicar uma maior probabilidade de ofensa às liberdades e garantias fundamentais dos titulares.

§ 1º Para fins de aferição da relevância dos danos decorrentes do incidente de vazamento, tanto a UEPDAP quanto o responsável pela verificação e comunicação deverão levar em conta os critérios indicados no **caput** deste artigo.

§ 2º Para fins de quantificação e qualificação do dano coletivo decorrente de um incidente de vazamento de dados pessoais, os órgãos de execução do Ministério Público deverão se pautar pelos critérios indicados no **caput** deste artigo.

§ 3º Sem prejuízo da imediata atuação dos órgãos de execução do Ministério Público em prol da efetiva proteção ao direito fundamental tratado nesta Resolução, a UEPDAP poderá fixar orientações, de caráter geral e abstrato, concernentes à quantificação e qualificação dos danos causados e dos prejuízos sofridos em âmbito coletivo, inclusive financeiro, observados os critérios definidos no **caput** deste artigo.

CAPÍTULO V
DAS DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 153. Nos termos do inciso IV do art. 28 desta Resolução, a UEPDAP estabelecerá diretrizes complementares acerca da adequação progressiva de bancos de dados pessoais constituídos até a data de sua entrada em vigor, consideradas a complexidade das operações de tratamento e a natureza dos dados pessoais.

Art. 154. O Presidente do CNMP indicará, ouvida a UEPDAP, membros do Ministério Público para integrarem, como representante e suplente, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, conforme previsto no inciso V do art. 58-A da LGPD.

Art. 155. As Ouvidorias de cada ramo e unidade do Ministério Público e do CNMP poderão funcionar como órgãos de apoio e canal de trâmite dos procedimentos relacionados à presente Resolução, na hipótese da inexistência ou impossibilidade da criação imediata da estrutura administrativa própria, respeitados os prazos estabelecidos para a necessária adequação.

Parágrafo único: A estrutura administrativa prevista nesta Resolução deverá ser implementada, em cada ramo e unidade do Ministério Público brasileiro, no prazo de até 1 (um) ano.

Art. 156. No prazo de até 1 (um) ano a contar da publicação desta Resolução, o CNMP, os ramos e as unidades do Ministério Público brasileiro deverão a ela adequar todos os seus atos internos.

Art. 157. Durante os dois primeiros anos de vigência da presente Resolução, não se aplicam as restrições previstas no § 1º do seu art. 45.

Art. 158. Os ramos e as unidades do Ministério Público brasileiro deverão, no prazo de até 90 (noventa) dias contados da entrada em vigor da presente Resolução, elaborar cronograma para confeccionar ou adaptar seus Planos Diretores, suas normas, seus procedimentos, seus protocolos, suas rotinas, sua estrutura administrativa e suas ações de proteção de dados pessoais.

Art. 159. A tutela coletiva do direito fundamental à proteção de dados pessoais, pelos órgãos de execução do Ministério Público, deverá ser implementada imediatamente.

Parágrafo único. No prazo de 90 (noventa) dias a partir da entrada em vigor da presente Resolução, os ramos e as unidades do Ministério Público deverão informar à UEPDAP quais os órgãos de execução que possuem atribuição para a tutela coletiva do direito fundamental à proteção de dados pessoais.

Art. 160. A UEPDAP poderá implementar modelos de formulários e relatórios para inventário de dados pessoais e para aferição de riscos (RIDP), devendo ser reavaliados e atualizados de forma constante.

Art. 161. No prazo de 120 (cento e vinte) dias a contar da publicação da presente Resolução, os ramos e as unidades do Ministério Público deverão realizar um relatório de conformidade em relação a esta Resolução, o qual deverá ser enviado à UEPDAP e renovado anualmente.

Parágrafo único. O relatório de conformidade deverá ser confeccionado nos moldes do modelo anexo, o qual será reavaliado e atualizado pela UEPDAP.

Art. 162. A UEPDAP deverá ser instalada no prazo de até 90 (noventa) dias a contar da entrada em vigor da presente Resolução, inclusive com a designação de seus integrantes e suplentes.

Art. 163. A UEPDAP deverá promover ações de cooperação com autoridades, organismos, entidades públicas e privadas de estudo e proteção de dados pessoais de outros países.

Art. 164. A UEPDAP priorizará a orientação e a capacitação de membros e servidores a respeito da tutela do direito fundamental à proteção de dados pessoais realizada pelos órgãos de execução do Ministério Público.

Art. 165. Ato do Presidente do CNMP, delegável ao Secretário-Geral, poderá dispor sobre o compartilhamento recíproco de estrutura física e de pessoal entre o seu encarregado de dados pessoais e a UEPDAP, para o desenvolvimento de suas correspondentes atividades.

Art. 166. Os ramos e as unidades do Ministério Público, por meio dos órgãos de comunicação social, a partir da publicação da presente Resolução, desenvolverão plano de comunicação da Política Nacional de Proteção de Dados Pessoais do Ministério Público.

Art. 167. Aplicam-se ao CNMP, quando cabível e possível, todas as regras previstas nesta Resolução que sejam dirigidas aos ramos e às unidades do Ministério Público brasileiro.

Art. 168. A presente Resolução aplica-se às Escolas de Governo, aos Centros de Estudos, Aperfeiçoamento e Capacitação, ou equivalentes, dos ramos e das unidades do Ministério Público, observado o disposto na alínea “b” do inciso II do art. 4º da LGPD, sendo facultado à administração superior de cada ramo e unidade o emprego da estrutura administrativa disposta no art. 45 ou o estabelecimento de estrutura paralela dedicada exclusivamente à tutela dos dados pessoais.

Art. 169. Aplicam-se os arts. 7º a 11 da LGPD ao tratamento de dados pessoais custodiados pelo Ministério Público sempre que utilizados para fins exclusivamente acadêmicos.

Art. 170. Para complementar a regulamentação de proteção de dados pessoais no âmbito do Ministério Público brasileiro, o CNMP, pela sua UEPDAP, deverá, no prazo de 2 (dois) anos, estabelecer as medidas necessárias para a criação de recomendações, notas técnicas, protocolos, rotinas, orientações e manuais relativos às transferências de dados nacionais e internacionais e, também, referentes ao uso das tecnologias e tratativas com as Autoridade Nacional de Proteção de Dados Pessoais (ANPD) brasileira e internacionais.

Art. 171. Os convênios e contratos em vigor de tratamento de dados pessoais entre o Ministério Público e instituições públicas e privadas deverão se adequar aos termos da presente Resolução, no prazo de 1 (um) ano da sua publicação.

Art. 172. O art. 7º da Resolução CNMP nº 89, de 28 de agosto de 2012, passa a vigorar acrescido de § 4º, com a seguinte redação:

"Art. 7º .....

.....

§ 4º As informações individuais e nominais da remuneração de membro ou servidor mencionadas no inciso VII serão automaticamente disponibilizadas mediante prévia identificação do interessado, a fim de se garantir a segurança e a vedação ao anonimato, nos termos do art. 5º, caput e inciso IV, da Constituição Federal, salvaguardado o sigilo dos dados pessoais do solicitante, que ficarão sob a custódia e responsabilidade da unidade competente, vedado o seu compartilhamento ou divulgação, sob as penas da lei." (NR)

Art. 173. O Ministério Público atuará, interna e externamente, sempre que possível, de modo a colaborar com a Autoridade Nacional de Proteção de Dados, especialmente quando o objetivo de sua atuação disser respeito à interpretação da LGPD.

Art. 174. Esta Resolução entre em vigor na data de sua publicação.

Brasília-DF, 12 de dezembro de 2023.

ELIZETA MARIA DE PAIVA RAMOS

Presidente do Conselho Nacional do Ministério Público em exercício

ANEXO

Governança

1 - As partes envolvidas com a implementação da LGPD realizaram a leitura da Resolução de regência?

2 - O órgão já publicou seu Plano Diretor de Privacidade (PDP), nos termos do previsto no art. 35 da Resolução, ou outro ato normativo a reger o programa de privacidade do órgão ministerial?

3 - O órgão desenvolveu um plano de comunicação interno acerca da LGPD e da Resolução de regência?

4 - O órgão já realizou a indicação de um encarregado com conhecimento, experiência e autonomia para implementar a LGPD e a Resolução de regência?

5 - O encarregado exerce o cargo com exclusividade?

6 - O órgão disponibilizou para o encarregado os recursos necessários para implementação da LGPD e Resolução de regência, bem franqueou acesso direto à alta administração?

7 - Já houve atribuição de responsabilidade para atuação na proteção de tratamento dos dados pessoais às áreas jurídica, técnica e de gestão da Instituição?

8 - O órgão elaborou Relatório de Impacto à Privacidade de Dados Pessoais - RIDP?

9 - O RIDP foi elaborado com base nas orientações da Seção XX, Capítulo IV, da Resolução de regência?

10 - O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) já foi constituído?

Conformidade legal e respeito aos princípios

11 - O órgão, dentro dos limites de suas competências legais, implementou ações para não tratar e coletar de forma inadequada ou excessiva os dados pessoais dos cidadãos e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada?

12 - O órgão realizou um mapeamento entre os dados processados e a competência legal/finalidade para a qual eles são necessários?

13 - O órgão estabeleceu procedimento ou metodologia para verificar se os princípios da LGPD estão sendo respeitados durante o desenvolvimento dos sistemas informatizados e dos sítios eletrônicos que tratarão dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução (Privacy by Design)?

14 - Os princípios da LGPD são aplicados a todo tratamento de dados pessoais realizados pelo órgão, tanto para usuários dos sistemas informatizados e dos sítios eletrônicos, prestados pelo órgão ministerial, quanto servidores, funcionários e/ou colaboradores da instituição?

15 - O órgão conscientizou a(s) área(s) envolvida(s) com tratamento de dados pessoais que os ramos e unidades do Ministério Público (e o CNMP) podem efetuar o tratamento de dados pessoais no exercício de suas atribuições constitucionais e legais ou na execução de políticas públicas e que nesses casos não precisará colher o consentimento do titular dos dados pessoais?

16 - O órgão, em suas atividades administrativas, confere publicidade sobre a finalidade e a forma de efetuar o tratamento de dados pessoais nas hipóteses em que não é colhido consentimento do titular dos dados pessoais?

17 - O órgão adota sistemas e procedimentos para cumprir o direito de retificação de informações do titular do dado pessoal?

Transparência e direitos do titular

18 - A identidade e as informações de contato do encarregado foram divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?

19 - O órgão comunica internamente os objetivos do Plano Diretor de Privacidade (PDP) e da Política Nacional de Proteção de Dados Pessoais do Ministério Público?

20 - O órgão elaborou uma política de privacidade para cada sistema informatizado ou sítio eletrônico de modo a informar os direitos dos titulares de dados e revisou as políticas de privacidade já existentes?

21 - As Políticas de Privacidade dos sistemas informatizados e dos sítios eletrônicos são elaboradas em linguagem simples e acessível?

Rastreabilidade

22 - O órgão já realizou um inventário dos sistemas informatizados e dos sítios eletrônicos que tratam dados pessoais?

23 - O órgão já realizou uma classificação dos dados tratados entre dados pessoais e dados pessoais sensíveis?

24 - O órgão mantém rastreabilidade dos dados pessoais do titular para assegurar o exercício dos seus direitos?

Adequação de contratos e de relações com parceiros

25 - O órgão já realizou uma adequação dos instrumentos convocatórios que estão sendo elaborados?

26 - O órgão já realizou uma revisão dos contratos em vigência para adequá-los à Lei Geral de Proteção de Dados e à Resolução de regência?

Segurança da Informação

27 - O órgão implementou efetivamente os controles de segurança para os riscos identificados no Relatório de Impacto à Proteção dos Dados Pessoais?

28 - O órgão instituiu uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais?

29 - O órgão gera evidências para comprovar que tomou medidas de segurança para proteger os dados pessoais contra ameaças externas e internas?

30 - Medidas de segurança são planejadas desde a fase de concepção do produto ou do serviço até a sua execução (Security by Design)?

Violações de dados

31 - O órgão estabeleceu o processo de comunicação interno dos possíveis incidentes de segurança no tratamento de dados pessoais?

32 - O órgão estabeleceu o processo de comunicação externa dos possíveis incidentes de segurança no tratamento de dados pessoais?

33 - O órgão estabeleceu o processo de comunicação ao titular dos possíveis incidentes de segurança no tratamento de dados pessoais, nas hipóteses indicadas na Resolução?

34 - O órgão estabeleceu o processo de comunicação ao CNMP dos possíveis incidentes de segurança no tratamento de dados pessoais?

35 - O órgão realiza uma gestão de incidentes para tratar possíveis violações dos dados de forma efetiva?

36 - O órgão fornece um canal para recebimento de comunicações de ocorrências de irregularidades, como possíveis vazamento de dados e falhas de segurança?

Capacitação

37 - O órgão mapeou as competências profissionais que os membros e servidores precisarão desenvolver na jornada de proteção de dados pessoais?

38 - O órgão desenvolveu ações de capacitação para os membros e servidores sobre a temática de proteção de dados pessoais para adequação do órgão às normas de regência?

39 - O órgão desenvolveu ações de capacitação para os membros e servidores sobre a temática de proteção de dados pessoais para atuação dos órgãos de execução na proteção do direito subjacente?

Atuação finalística

40 - O órgão promoveu a estruturação de suas promotorias/procuradorias para a atuação dos seus órgãos de execução na proteção dos dados pessoais?

41 - Foram criadas promotorias/procuradorias especializadas ou grupos especiais de atuação para a execução de sua atividade finalística de proteção dos dados pessoais?

42 - O órgão incorporou às atribuições das promotorias/procuradorias, mediante modificação de seus atos normativos, o dever de realizar a efetiva tutela da privacidade e a proteção dos dados pessoais?

43 - Houve registro de atuação finalística dos órgãos de execução relativo ao tratamento de dados realizado por pessoas físicas ou jurídicas privadas, desde a entrada em vigor da LGPD?

44 - Houve registro de atuação finalística dos órgãos de execução relativo ao tratamento de dados realizado por órgãos ou entidades públicos, desde a entrada em vigor da LGPD?