LEI GERAL DA PROTEÇÃO DE DADOS

INCLUINDO MODELOS, SEGURANÇA
DA INFORMAÇÃO E FASES
DE IMPLEMENTAÇÃO

AUTORIA
SELMA CARLOTO

LEI GERAL DA PROTEÇÃO DE DADOS

INCLUINDO MODELOS, SEGURANÇA DA INFORMAÇÃO E FASES DE IMPLEMENTAÇÃO

4ª EDIÇÃO
2023

LTr Editora Ltda.

Rua Jaguaribe, 571
CEP 01224-003
São Paulo, SP — Brasil
Fone (11) 2167-1101
www.ltr.com.br
Julho, 2023

Produção Gráfica e Editoração Eletrônica: PIETRA DIAGRAMAÇÃO
Projeto de capa: DANILO REBELLO

Versão digital — LTr 9895.6 — ISBN 978-65-5883-256-0
Versão impressa — LTr 6418.5 — ISBN 978-65-5883-255-3

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Carloto, Selma

Lei geral da proteção de dados [livro eletrônico]: incluindo modelos, segurança da informação e fases de implementação/Selma Carloto. – 4. ed. – São Paulo: LTr, 2023.

PDF

Bibliografia.

ISBN 978-65-5883-256-0

1. Direito à privacidade – Brasil 2. Informação -Sistema de armazenagem e recuperação 3. Proteção de dados pessoais 4. Proteção de dados – Direito – Brasil 5. Proteção de dados – Leis e legislação 6. Sistemas de informação I. Título.

23-161785 CDU-342.721(81)

Índice para catálogo sistemático:

1. Brasil: Lei Geral de Proteção de Dados: Direito à privacidade 342.721(81)

Aline Graziele Benitez − Bibliotecária − CRB-1/3129

Dedico esta obra aos meus filhos: Enzo, Marcelo Henrique e Filipe Daniel.

Agradeço a meus pais e esposo, que sempre me apoiam, e, principalmente, a Deus e Nossa Senhora por toda força e mais esta obra.

SUMÁRIO

INTRODUÇÃO

Considerando que nossos dispositivos estão nos ouvindo e rastreando o tempo todo e tudo que estamos fazendo, como podemos manter nossos dados pessoais seguros? Como podemos proteger os dados dos trabalhadores e dos consumidores? A proteção e os cuidados com os dados pessoais, tornou-se uma questão inadiável. A principal preocupação da legislação brasileira de proteção de dados, assim como a do regulamento europeu, é exatamente proteger os dados das pessoas naturais, com a devolução do controle dos dados pessoais para seus titulares. A autodeterminação informativa, conceito que surgiu na Alemanha, é fundamento da Lei Geral de Proteção de Dados e consiste em garantir o controle do cidadão sobre suas próprias informações.

A tecnologia vem avançando em ritmo cada vez mais acelerado, e estamos nos conectando de maneira cada vez mais digital. Algoritmos de inteligência artificial, que dependem de cálculo, estatística, probabilidade e programação, desempenham papéis dominantes e influentes em todos os aspectos de nossas vidas, incluindo relações familiares, de amizade, de consumo, de trabalho e com o Poder Público. Sendo muito mais rápidas e eficazes do que os seres humanos na análise de grandes volumes de dados, essas máquinas são inclusive utilizadas em processos seletivos de algumas empresas. No entanto, ao se beneficiar dessas vantagens, também devemos cuidadosamente avaliar os riscos associados. Especialmente, é necessário garantir que estejam em conformidade com as normas de proteção de dados e a Constituição Federal. Um exemplo de possível risco é a presença de vieses discriminatórios em processos seletivos conduzidos por algoritmos. Tais sistemas, se não

forem devidamente projetados e supervisionados, podem inadvertidamente perpetuar ou exacerbar as desigualdades existentes. Portanto, enquanto a inteligência artificial oferece oportunidades inigualáveis para melhorar a eficiência e eficácia de nossos sistemas, é fundamental que priorizemos a ética, a justiça e a conformidade com a lei em seu uso.

A LGPD tem como objetivo principal a proteção dos direitos fundamentais dos titulares de dados pessoais e sensíveis, garantindo-se o livre desenvolvimento da personalidade e a dignidade da pessoa humana e entrou em vigor em setembro de 2020, tendo sido promulgada em 2018. A vigência ocorreu de forma escalonada e as sanções da Autoridade Nacional de Proteção de Dados (ANPD) entraram em vigor em 1º de agosto de 2021, tendo sido adiadas pelo Projeto de Lei n. 1.179/2020, convertido na Lei n. 14.010/2020.

A Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), e as alterações introduzidas pela Lei n. 13.853/2019, foram inspiradas nas normas de proteção de dados da União Europeia e do Conselho da Europa. Essa inspiração abrange uma série de normas e regulamentações, incluindo a Convenção 108 do Conselho da Europa, um marco pioneiro no que se refere à proteção de dados pessoais, e a Diretiva 95/46/EC da União Europeia, que estabeleceu a proteção de indivíduos com relação ao processamento de dados pessoais e a livre circulação desses dados. Ao mesmo tempo, a LGPD também foi influenciada, no decorrer do seu processo legislativo, pelo Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, que representa uma das legislações mais abrangentes e detalhadas em termos de proteção de dados na atualidade. Assim, a LGPD é fruto de uma evolução legislativa complexa, refletindo diferentes instrumentos normativos europeus que foram se aperfeiçoando ao longo do tempo.

As normas de proteção de dados do Brasil se inspiram nas da União Europeia[1], berço da privacidade e proteção de dados. O RGPD é um regulamento do direito europeu, que entrou em vigor no dia 25 de maio de 2018, sobre privacidade e proteção de dados pessoais e que é aplicável a todos os indivíduos da União Europeia e empresas que operem no Espaço Econômico Europeu, independente do país de origem, o qual revogou a Diretiva 95/46/CE. A Diretiva demandava que cada estado-membro aprovasse uma legislação interna adicional, já o regulamento é vinculativo e aplicável imediatamente a todos países da União Europeia, independentemente de adequação legislativa interna e garantindo o mesmo nível de proteção a todos países da União Europeia. A Diretiva havia sido escrita na fase inicial da internet, quando não eram conhecidos conceitos como internet das coisas, conectando o mundo físico ao digital por meio de objetos, *big data,* nuvem, inteligência artificial, *machine learning* e *deep learning,* não obstante esta já trouxesse conceitos importantes, bases legais de tratamento, diferença de dados pessoais e sensíveis, entre outros institutos e é por essa razão que os estudos do Grupo de Trabalho do Artigo 29, por esta criada, são tão importantes.

Se retrocedermos na história, o direito à privacidade foi consagrado pela primeira vez num instrumento jurídico internacional no artigo 12º da Declaração Universal dos Direitos do Homem, 1948: "Ninguém será sujeito a interferências na sua vida privada, família, lar ou na sua correspondência, nem a ataque à sua honra e reputação. Toda Pessoa tem direito à proteção da lei contra tais interferências ou ataques". A Declaração Universal dos Direitos do Homem

---

(1) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. Abr. 2022. p.13. Acesso em: 26 mar. 2022.

influenciou a formulação de outros instrumentos sobre direitos humanos na Europa.

No final da II Guerra Mundial foi criado o Conselho da Europa, o qual reúne Estados da Europa com o objetivo de promover o Estado de direito, a democracia, os direitos humanos e o desenvolvimento social e que adotou a Convenção Europeia dos Direitos do Homem no ano de 1950 e que entrou em vigor em 1953. Em 1959, foi criado na França o Tribunal Europeu dos Direitos do Homem para garantir que as partes contratantes cumpram as obrigações assumidas ao abrigo da Convenção Europeia de Direitos do Homem e o qual se pronunciou, por meio de sua jurisprudência, em várias situações onde foi suscitada a proteção de dados.

O artigo 8º da Convenção Europeia de Direitos do Homem garante o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência, além de estabelecer as condições em que são permitidas restrições a este direito. O Comité de Ministros do Conselho da Europa logo adotou várias resoluções sobre a proteção de dados pessoais e que faziam referência ao artigo 8º da Convenção Europeia dos Direitos do Homem. Logo, foi aberta para assinatura a Convenção 108 de 1981, a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, no âmbito do Conselho da Europa e primeiro instrumento internacional juridicamente vinculativo, o qual regula expressamente a proteção de dados.

A LGPD tem por objetivo garantir a transparência em todas as operações realizadas com os dados da pessoa natural, como a coleta, processamento, arquivamento, armazenamento, eliminação e compartilhamento dos dados pessoais, além de resguardar os dados pessoais e sensíveis de seus titulares, ou pessoas naturais, tanto nos meios digitais, como

nos físicos,devendo ser observada tanto pelas pessoas jurídicas de direito privado, quanto pelas de direito público.

Os avanços tecnológicos dos últimos anos, com as novas tecnologias da informação, vieram para alterar de forma permanente o mundo que nos rodeia e trouxeram a necessidade de uma legislação sólida de proteção dos dados das pessoas naturais, que buscasse o equilíbrio entre a garantia das liberdades e direitos individuais e que se traduz na reserva da intimidade da vida privada e a liberdade de circulação da informação pessoal:

> "A rapidez dos avanços tecnológicos e da globalização vieram para alterar de forma indelével o mundo que nos rodeia e são assim novos e imensos os desfechos para a proteção de dados. Os regimes de proteção de dados buscam o necessário equilíbrio entre dois princípios: por um lado, a garantia das liberdades e direitos individuais e, por outro lado, a liberdade de utilização e circulação da informação pessoal.
>
> (...)
>
> A verdade é que nos tornamos dependentes das comunicações móveis, do acesso instantâneo à informação e serviços inteligentes. Apesar de todos os benefícios dessas tecnologias, persistem dúvidas e preocupações sobre o quanto de informação pessoal é coligada, armazenada, utilizada e compartilhada para o fornecimento desses serviços persuasivos e convenientes."(2)

(2) De MAGALHÃES, Márcia. *O Regulamento Geral de Proteção de Dados.* Porto: Librum Editora, 2019.

O Regulamento Geral de Proteção de Dados da União Europeia destaca, já no Considerando 1, que a proteção relacionada ao tratamento de dados pessoais das pessoas naturais é um direito fundamental previsto no artigo 8º, número 1, da Carta dos Direitos Fundamentais da União Europeia e no artigo 16º, número 1, do Tratado sobre o Funcionamento da União Europeia:

> "(1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, n. 1, da Carta dos Direitos Fundamentais da União Europeia ("Carta") e o artigo 16º, n. 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
>
> Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares."(3)

---

(3) GDPR EUROPA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

No Brasil, a Proposta de Emenda à Constituição Federal de 1988, número 17/2019, foi recentemente aprovada no Senado e acrescentou o inciso XII-A ao artigo 5º, e o inciso XXX ao artigo 22 da Constituição Federal de 1988, para incluir a proteção de dados pessoais, físicos e digitais, entre os direitos e garantias fundamentais do cidadão no Brasil e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A Lei n. 13.709 de 14 de agosto de 2018 tem como fundamento a tutela aos **direitos fundamentais de liberdade e de privacidade**, **ao livre desenvolvimento da personalidade da pessoa natural e aos direitos humanos**:

> "Art. 1º Esta Lei dispõe sobre o **tratamento de dados pessoais, inclusive nos meios digitais,** por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de **proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei n. 13.853, de 2019)
>
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e

---

(Texto relevante para efeitos do EEE). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679. Acesso em: 13 dez. 2020.

> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."(4)

O escopo da presente legislação brasileira de proteção de dados é a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, a qual é considerada vulnerável em relação aos agentes de tratamento, de forma a buscar-se um equilíbrio nas relações e aplicando-se a máxima da igualdade material, com base na justiça distributiva e compensatória.

Na era do *Big Data* e com um ambiente de globalização, o qual mitiga as fronteiras físicas, trazendo cada vez mais vantagens para o comércio eletrônico e com uma economia totalmente baseada na internet, cada vez mais dependente de dados, o escopo da proteção de dados pessoais é transformar o *Big Data* em *Small Data,* devendo-se limitar o tratamento dos dados ao **mínimo necessário** e com o escopo de ser atingida a **finalidade** pretendida. Esta legislação se aplica no tratamento de **dados das pessoas naturais** e **não se aplica no tratamento de dados das pessoas jurídicas, mas todas as empresas tratam dados de pessoas naturais, ainda que de seus sócios e empregados**.

A LGPD, como já exposto, destina-se às entidades, agentes de tratamento, as quais tratam dados pessoais e dados pessoais sensíveis das pessoas naturais, incluindo as relações de trabalho, as relações de consumo e outras que envolvam o tratamento de dados pessoais.

Esta lei não tratou de forma expressa, em seus dispositivos, as relações de trabalho, como o fez o Regulamento Geral

---

(4) BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 4 jan. 2022.

de Proteção de Dados da União Europeia, mas também se aplica no tratamento de dados pessoais dos empregados e demais trabalhadores pelos empregadores, ou tomadores, os quais são os controladores desses dados e a quem cabe tomar as decisões necessárias sobre o tratamento. Quando falamos de implementação da Lei Geral de Proteção de Dados, esta não poderá ser fatiada, mas deverá abranger todos os departamentos, sem exceção, onde identificados os tratamentos de dados pessoais, desde o departamento de marketing, comercial, financeiro, ao de recursos humanos, ou já teremos um GAP muito grande na implementação.

Sempre que terceirizadas as atividades de tratamento, quando temos um operador, como é comum, por exemplo, com alguns *softwares* de IA e a gestão de folha de pagamento, a empresa responsável deverá incluir, de forma muito clara, as instruções sobre como deverão ser realizadas as atividades de tratamento e fazer uma due diligence naquela, principalmente em medidas de segurança da informação.

É importante elaborar uma política de segurança da informação, cláusulas em contrato, treinamentos e termos de confidencialidade (non-disclosure agreement – NDA) para empregados. Os NDAs também são importantes para terceiros.

A LGPD, assim como o RGPD, destina-se a proteger os dados pessoais e pessoais sensíveis de danos, no tratamento, **não apenas nos meios digitais, mas também em contratos e outros documentos escritos por meios físicos.** O artigo 5º destaca que o banco de dados consiste em um conjunto estruturado de dados em suporte eletrônico ou físico.

A Lei Geral de Proteção de Dados cria um marco legal para a proteção de informações pessoais e tem como escopo

principal dar ao cidadão maior controle sobre o uso das suas informações pessoais, como já exposto anteriormente.

A legislação brasileira de proteção de dados não traz parâmetros mínimos para obrigatoriedade do registro de atividades de tratamento dos dados pessoais, estando todas as empresas que tratam dados pessoais, ou dados pessoais sensíveis, sujeitas aos registros previstos na legislação brasileira de proteção de dados, a Lei n. 13.709/2018. A ANPD poderá trazer parâmetros mínimos objetivos para o registro das atividades de tratamento de dados da pessoa natural.

O Considerando 13, do RGPD, traz uma derrogação para as organizações com menos de 250 trabalhadores, relativamente à conservação do registo de atividades. O regulamento europeu dispõe ainda, de forma expressa, no artigo 30, número 5, que a obrigação de registro não se aplica a empresas com menos de 250 pessoas, a menos que o tratamento seja suscetível de implicar risco para os direitos e liberdades do titular dos dados, não seja ocasional, ou abranja as categorias especiais de dados a que se refere o artigo 9º, número 1, ou dados pessoais relativos a condenações penais e infrações referidos no artigo 10º do regulamento europeu.(5)

É indispensável a existência de medidas técnicas e administrativas aptas a proteger e resguardar os dados pessoais e os dados pessoais sensíveis, para a proteção de direitos fundamentais de liberdade e de privacidade, de cada usuário, para evitar-se acessos não autorizados e situações acidentais ou ilícitas. Os dados pessoais deverão ser apenas

(5) GDPR EUROPA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: <https://eur-lex.europa.eu/ legal-content/PT/ALL/?uri=celex:32016R0679>. Acesso em: 13 dez. 2020.

tratados por pessoas que necessitem dessas informações, na realização de suas tarefas, limitando-se o tratamento ao mínimo necessário para a realização de suas finalidades. A empresa deve utilizar softwares de segurança da informação, monitoramento, criptografia, entre outros. O uso da criptografia é um dos métodos mais eficientes para fornecer a segurança de dados, principalmente para a proteção realizada de ponta a ponta e transmitida entre as redes.

O RGPD trouxe o conceito do *privacy by design* e *privacy by default*, que foi abraçado por nossa legislação. O primeiro, privacidade desde a concepção, tem destaque na proteção do titular dos dados em toda arquitetura do negócio, em todos os projetos desenvolvidos e o segundo, ou privacidade por padrão, traz a ideia de que o direito e a tecnologia devem andar juntos, que um produto ou serviço seja lançado ao público com as mais seguras configurações de privacidade. O responsável pelo tratamento de dados deverá adotar e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a concepção e por padrão.

No Brasil, o Marco Civil da Internet, o qual foi alterado pela Lei Geral de Proteção de Dados, já nos trazia disposições sobre a proteção de dados, assim como o Código de Defesa ao Consumidor (Lei n. 8078/90) e a Lei de Cadastro Positivo (Lei n. 12.414/2011).

Capítulo 1

CONCEITOS BÁSICOS NA LEGISLAÇÃO DE PROTEÇÃO DE DADOS BRASILEIRA

O artigo 5º da nossa legislação de proteção de dados traz alguns conceitos básicos, que é importante conhecer para a continuidade do estudo sobre o tema:

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

I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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

III – 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;

IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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

VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei n. 13.853, de 2019)

IX – agentes de tratamento: o controlador e o operador;

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

XI – 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;

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

XIII – bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI – uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII – relatório de impacto à proteção de dados pessoais: 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;

XVIII – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei n. 13.853, de 2019)

XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei n. 13.853, de 2019)"

1.1. Dado pessoal: informação relacionada à pessoa natural identificada ou identificável

O dado pessoal é aquela informação **relacionada à pessoa natural identificada ou identificável, logo a Lei Geral de Proteção de Dados não se aplica a dados de pessoas jurídicas e nem a dados anonimizados.**

A Lei Geral de Proteção de Dados cria um marco legal para a proteção de informações pessoais coletadas e tratadas, entre as quais nome, RG, CPF, número de passaporte, título de eleitor, endereço, profissão, hábitos de consumo, número de telefone, estado civil, e-mail e patrimônio.

De acordo com a lei brasileira de proteção de dados, tanto os dados da pessoa identificada, como os dados da pessoa natural identificável, são dados pessoais, ou seja, tanto as informações que identificam o titular dos dados pessoais ou a pessoa natural, como aquelas que têm o potencial de identificá-la são dados pessoais. Logo, os dados pessoais podem ser diretos ou indiretos.

Os dados pessoais correspondem, como dispõe o art. 5º da LGPD, à "informação relacionada à pessoa natural identificada ou **identificável**"(6). Portanto, o conceito

(6) BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Dispo-

de dado pessoal da LGPD também deve incluir o de dado identificável, o que significa que, ainda que uma informação sozinha não identifique um titular, muitas vezes, agrupada com outras informações, poderá identificar um titular de dados pessoais, sendo o conceito de dado pessoal aberto, como respondeu a Autoridade Nacional de Proteção de Dados (ANPD), em seu site oficial: "A LGPD adota, no art. 5º, inciso I, um conceito aberto de dado pessoal, definido como a informação relacionada a uma pessoa natural identificada ou identificável".(7)

São dados pessoais diretos os que identificam a pessoa natural de forma inequívoca e sem necessidade de informações adicionais, tais como: RG, CPF, OAB, título de eleitor. Por outro lado, são considerados dados pessoais indiretos aqueles que necessitam de informações adicionais para identificar o titular dos dados, como: profissão, geolocalização, sexo, idade, estado civil, endereço, cargo, função e outras informações relacionadas a uma pessoa natural, tais como seus hábitos de consumo, sua aparência e seus aspectos de personalidade.(8)

No mesmo sentido, o art. 5º do RGPD dispõe que: "os dados pessoais consistem em qualquer informação relativa a uma pessoa singular identificada ou identificável"(9) e preconiza que uma pessoa natural será considerada identificável quando puder ser identificada, de forma direta, ou indireta,

nível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 29 mar. 2023.

(7) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Perguntas e respostas frequentes*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#b1>. Acesso em: 18 dez. 2022.

(8) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Perguntas e respostas frequentes*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#b1>. Acesso em: 18 dez. 2022.

(9) GDPR. *Regulamento Geral sobre a Proteção de Dados*. 2016. Disponível em: <https://gdprinfo.eu/pt-pt>. Acesso em: 26 mar. 2023.

e exemplifica com: "nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular".(10)

A *Information Commissioner's Officers* (ICO), autoridade do Reino Unido, ao interpretar o RGPD, também explica que o titular pode ser identificado, ou identificável, a partir de um ou mais identificadores, ou por meio de determinados fatores específicos desse indivíduo e, explica que, na maioria das circunstâncias, é relativamente simples determinar quando as informações tratadas se relacionam a um titular, mas que, às vezes, existe necessidade de se consideradar outras informações agregadas para um dado ser pessoal.(11)

1.2. Dado pessoal sensível: consiste no dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.(12)

Dados pessoais sensíveis são aqueles de maior potencial discriminatório e que possuem uma tutela maior, sendo

---

(10) GDPR. *Regulamento Geral sobre a Proteção de Dados*. 2016. Disponível em: <https://gdprinfo.eu/pt-pt>. Aces so em: 26 mar. 2023.

(11) INFORMATION COMMISSIONER'S OFFICERS. *What is Personal Data?* [S. d.]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>. Acesso em: 28 mar. 2023.

(12) BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 29 mar. 2023.

o princípio da não discriminação um dos princípios basilares do *compliance* na Lei Geral de Proteção de Dados.

Entre os dados pessoais sensíveis temos os de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde, ou à vida sexual, que podem trazer atos ou atitudes discriminatórias no tratamento e os dados genéticos ou biométricos, que identificam o indivíduo de forma inequívoca e que trazem um risco muito alto ao titular dos dados, caso haja algum incidente durante o tratamento.

O artigo 9º do RGPD também traz o rol de dados sensíveis:

> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.(13)

Esses atributos, quando vinculados a uma pessoa natural, passam a ser dados sensíveis, precisam de um patamar diferenciado de proteção, sendo o tratamento proibido se não for identificada uma base legal de tratamento, nos termos do GDPR, artigo 9º, anteriormente transcrito, e do artigo 11 da LGPD, que dispõe que "o tratamento de dados pessoais sensíveis somente poderá ocorrer nas hipóteses elencadas nesse artigo"(14) e logo traz o rol de bases legais que

---

(13) GDPR. *Regulamento Geral sobre a Proteção de Dados*. 2016. Disponível em: <https://gdprinfo.eu/pt-pt>. Acesso em: 26 mar. 2023.

(14) BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 29 mar. 2023.

permitem o tratamento de dados sensíveis, no mesmo dispositivo e mais restrito que o artigo 7º para dados pessoais.

Não podemos incluir no rol de dados sensíveis informações básicas de identificação, como o nome, número de inscrição no Registro Geral (RG), Cadastro Nacional de Pessoas Físicas (CPF) e endereço residencial[15]. São sensíveis as informações que precisam de proteção qualificada por possuírem potencial discriminatório, ao lado dos dados biométricos e dos genéticos[16], e as que estiverem diretamente relacionadas aos aspectos mais íntimos da personalidade de um indivíduo.[17] Portanto, os dados sensíveis consistem nas informações relacionadas à intimidade do indivíduo, cujo tratamento indevido poderá levar a práticas discriminatórias.[18]

A Lei n. 12.414/2011 disciplina a formação e a consulta a bancos de dados, com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito e inclui no rol dos dados sensíveis a origem social, que não está inserida na LGPD nem no GDPR: "[...] assim consideradas aquelas pertinentes à **origem social** e étnica, à saúde, à informação genética, à orientação sexual

---

(15) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Perguntas e respostas frequentes*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#b1>. Acesso em: 18 dez. 2022.

(16) CARLOTO, Selma. *Lei Geral de Proteção de Dados*. 3. ed. São Paulo: LTr, 2022.

(17) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Perguntas e respostas frequentes*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#b1>. Acesso em: 18 dez. 2022.

(18) ANDRION, Roseli. Saiba a diferença entre dados pessoais, identificáveis, sensíveis e anonimizados. *Canaltech*, 16 ago. 2021. Disponível em: <https://canaltech.com.br/seguranca/saiba-a-diferenca-entre-dados-pessoais-identificaveis-sensiveis-e-anonimizados/>. Acesso em: 18 dez 2022.

e às convicções políticas, religiosas e filosóficas"[19](grifo nosso), o que denota que o rol de dados sensíveis pode incluir outros de potencial discriminatório e não se limita ao rol inserido nos dispositivos da LGPD e do RGPD.

A ICO, autoridade do Reino Unido, assevera que o RGPD diferencia os dados pessoais dos sensíveis, já que estes requerem um nível mais alto de proteção, e indica que as informações relativas a condenações criminais e infrações também requerem um nível mais alto de proteção.[20]

O tratamento de dados pessoais sensíveis é proibido, salvo nas hipóteses autorizadas (quando existir uma base legal de tratamento) e que estão previstas no artigo 11 da LGPD.

Ver capítulo 4.12 desta obra, relacionado ao tratamento de dados pessoais sensíveis.

1.3. 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

A Lei Geral de Proteção de Dados não exige a anonimização, sendo esta apenas uma opção trazida pela própria

---

(19) BRASIL. *Lei n. 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Presidência da República, [2011]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 18 dez. 2022.

(20) INFORMATION COMMISSIONER'S OFFICERS. *What is Personal Data?* [S. d.]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>. Acesso em: 28 mar. 2023.

lei e, ao mesmo tempo, um grande atrativo, já que afasta a incidência da legislação de proteção de dados, mas não é um procedimento obrigatório para quem desejar tratar dados pessoais se existente uma hipótese legal de tratamento e respeitados os princípios da LGPD e os direitos dos titulares de dados pessoais, principalmente do artigo 18 da LGPD. Se a empresa não precisar identificar os titulares dos dados pessoais, ela se resguarda, já que não corre risco de um incidente de vazamento de dados pessoais por falta de adequação à LGPD, sendo a anonimização também uma medida técnica de segurança da informação.

O dado anonimizado consiste naquele em que o titular não pode ser identificado, considerando-se os meios técnicos razoáveis e disponíveis na ocasião do tratamento. O artigo 12 da nossa legislação de proteção de dados preconiza que os dados anonimizados não serão considerados dados pessoais, **salvo quando o processo, ao qual foram submetidos, comportar possibilidade de reversão**, utilizando-se de meios próprios ou quando, com esforços razoáveis, o processo puder ser revertido:

> "Art. 12. **Os dados anonimizados** não serão considerados dados pessoais para os fins desta Lei, **salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido**.
>
> 1º 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.
>
> 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.
>
> 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais."

A anonimização consiste em procedimento por meio do qual os dados pessoais deveriam se tornar anônimos. Resulta do tratamento com a finalidade de evitar-se, de forma irreversível, a identificação dos seus titulares. Por outro lado, a pseudonimização, prevista no artigo 13 da LGPD, relacionado a estudos em saúde pública, consiste em tratamento em que poderemos identificar o titular com informações suplementares e mantidas separadamente, pelo controlador, em ambiente controlado e seguro:

> "Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a **anonimização ou pseudonimização** dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.
>
> 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o *caput* deste artigo em nenhuma hipótese poderá revelar dados pessoais.
>
> 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no *caput* deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.
>
> 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.
>
> 4º Para os efeitos deste artigo, a **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."

Logo, estamos diante da anonimização quando se retira a possibilidade de identificação do titular do dado pessoal, afastando-se a incidência da LGPD. O escopo seria tornar o dado anônimo, sem qualquer possibilidade de reversão, mas isso nem sempre será possível.

1.4. Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

O banco de dados, nos termos do inciso IV, consiste em um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, tanto em suporte eletrônico, como físico.

Com a vigência da nova lei de proteção de dados, os bancos de dados já existentes deverão ser revisados para adequação a esta e a seus princípios, sendo que o tratamento deverá ser realizado atendendo os princípios da nova legislação de proteção de dados, devendo ser eliminados os excessos e atendidos os fins do tratamento, o qual deverá ser compatível com a finalidade informada.

Os empregadores, assim como os fornecedores, costumam coletar mais dados do que precisam, o que não poderá ocorrer com a Lei Geral de Proteção de Dados. O tratamento de dados deverá ter um propósito legítimo e específico.

1.5. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento

O titular é o real proprietário dos dados, é quem deverá ter seus dados pessoais ou dados pessoais sensíveis protegidos e devolvidos, é a própria razão da existência da Lei Geral de Proteção de Dados, a qual tem por escopo proteger os direitos fundamentais da pessoa natural, principalmente os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O Grupo de Trabalho do Artigo 29, no Parecer 4/2007, WP136, escrito na época da Diretiva 95/46/CE orienta, ao definir as pessoas naturais, que a proteção de dados se aplica

apenas aos seres humanos e às pessoas vivas e que o direito proteção dos dados pessoais é no sentido universal, não se restringindo a nacionais ou residentes de um determinado país. Ainda, o conceito de pessoa natural ou singular (pessoa natural em português de Portugal, onde se aplicava a Diretiva 95/46/CE e atualmente o Regulamento Geral de Proteção de Dados da União Europeia e termo utilizado nas traduções para o português dos documentos do Grupo de Trabalho do Artigo 29 e do presente Regulamento Geral de Proteção de Dados da União Europeia, em sites oficiais da União Europeia) é referido no artigo 6º da Declaração Universal dos Direitos do Homem:

> "4. QUARTO ELEMENTO:
>
> "PESSOA SINGULAR" A protecção oferecida pelas regras da Directiva aplica -se a pessoas singulares, isto é, a seres humanos. O direito à protecção dos dados pessoais é, neste sentido, **universal**, **não se restringindo a nacionais ou residentes de um determinado país**. O Considerando 2 da Directiva indica-o expressamente ao referir que "os sistemas de tratamento de dados estão ao serviço do Homem" e que eles "devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência".(21)
>
> O conceito de pessoa singular é referido no artigo 6º da Declaração Universal dos Direitos do Homem, segundo a qual "Todas as pessoas têm o direito a serem reconhecidas como sujeitos perante a Lei". A legislação dos Estados-Membros, normalmente na área do Direito Civil, sublinha de forma mais precisa o conceito de personalidade dos seres humanos, entendida como a capacidade de ser sujeito de relações jurídicas, desde o momento do nascimento da pessoa até à sua morte. Os dados pessoais são assim, em princípio, dados relativos a pessoas vivas identificadas ou identificáveis. Isto suscita uma série de questões no âmbito da presente análise."

---

(21) Parecer 4/2007, WP136: Working Party, WP136. Disponível em: <https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>. Acesso em: 1 dez. 2020.

LGPD e RGPD: em princípio se aplicam apenas aos seres humanos e às pessoas vivas

As informações relacionadas a pessoas mortas, em princípio, não receberão a proteção da legislação de proteção de dados, de acordo com a própria orientação do Grupo de Trabalho, mas em alguns casos, os dados sobre pessoas mortas poderão receber proteção indiretamente por estarem ligados a pessoas vivas. A orientação do Grupo de Trabalho exemplifica:

> "Por outro lado**, a informação sobre pessoas mortas pode também fazer referência a pessoas vivas. Por exemplo, a informação que a falecida Gaia sofria de hemofilia indica que o seu filho Tito também sofre da mesma doença, uma vez que está ligada a um gene contido no cromossoma X**. Assim, quando a informação que constitui dados sobre os mortos puder ser considerada como igualmente relativa aos vivos e constituir dados pessoais sujeitos à Directiva, os dados pessoais dos mortos podem indirectamente usufruir da protecção das regras de protecção de dados."

A ANPD, após questionada pela Polícia Rodoviária Federal – PRF sobre o uso de nome e sobrenome de servidores falecidos com a finalidade de homenageá-los, manifestou-se pela não aplicação da LGPD no tratamento de dados de pessoas falecidas. No documento, a Coordenação-Geral de Fiscalização – CGF da ANPD esclareceu que, conforme o art. 6º do Código Civil, a existência da pessoa natural termina com a morte, sendo assim, pressupõe-se que a incidência da LGPD se dá apenas no âmbito do tratamento de dados pessoais de pessoas naturais vivas.

A CGF citou também que existem outras normas do ordenamento jurídico brasileiro que visam proteger os

direitos de pessoas falecidas, como o direito sucessório e os direitos de personalidade do Código Civil, que incluem o direito ao nome e à imagem. Nesse cenário, quando aplicáveis, os direitos de personalidade podem ser utilizados como ferramentas de proteção dos interesses das pessoas falecidas, não sendo a proteção de dados pessoais seara adequada para defesa desses interesses.[22]

NASCITUROS:

A legislação de proteção de dados não traz disposições, também, quanto à proteção do nascituro, nem a legislação do Brasil e nem o regulamento da União Europeia, e o parecer orienta que cada país deverá adotar um posicionamento, dependendo do seu sistema jurídico.

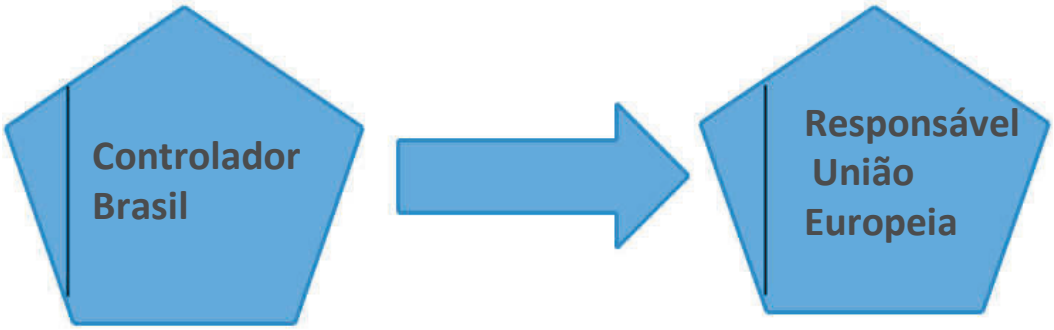
> "A aplicação das regras de proteção de dados antes do nascimento irá depender do posicionamento geral dos sistemas jurídicos nacionais sobre a proteção dos nascituros. Pensando sobretudo nos direitos de sucessão, alguns Estados-Membros reconhecem o princípio de que crianças concebidas, mas ainda não nascidas são consideradas como se tivessem nascido no que respeita aos benefícios (e assim podem receber uma herança ou aceitar uma doação), na condição de que efectivamente possam nascer. Noutros Estados-Membros, é dada protecção especial através de disposições jurídicas específicas, também sujeito à mesma condição. Para determinar se as disposições nacionais de protecção de dados protegem também informação sobre nascituros, deverá ser considerada

(22) ANPD. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-da-anpd-orienta-sobre-tratamento-de-dados-de-pessoas-falecidas>. Acesso em: 3 abr. 2023.

a abordagem geral do sistema jurídico nacional, juntamente com a ideia de que o objectivo das regras de protecção de dados é proteger a pessoa.

Uma segunda questão é suscitada pelo facto de a resposta geral do sistema jurídico se basear na expectativa de que a situação dos nascituros é limitada no tempo ao período da gravidez. Não tem em consideração o facto de esta situação poder na verdade durar consideravelmente mais tempo, tal como no caso de embriões congelados. Por último, poderão encontrar-se respostas jurídicas específicas em disposições especiais sobre técnicas de reprodução, que tratem do uso de informação médica ou genética sobre embriões."(23)

1.6. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais



O controlador, ou responsável, é um agente de tratamento a quem compete as decisões referentes ao tratamento de dados pessoais. Na legislação da União Europeia, o

(23) Parecer 4/2007, WP136: Working Party, WP136. Disponível em: <https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf>. Acesso em: 1 dez. 2020.

controlador se denomina contratante ou responsável pelo tratamento. É tarefa imprescindível definir quem é o controlador e quem é operador.

Os controladores, exercendo seus poderes decisórios, atuarão conforme seus interesses particulares, determinando as finalidades e os elementos essenciais do tratamento de dados. Como agentes de tratamento, os controladores definem os propósitos e estratégias do processamento, bem como os meios e os objetivos a serem alcançados.

Os controladores atuarão de acordo com os próprios interesses e terão poder de decisão sobre as finalidades e os elementos essenciais de tratamento.

O controlador, como agente de tratamento responsável,

quem determina os objetivos e meios do processamento, assim como os seus meios e objetivos.

Na legislação da União Europeia, o controlador se denomina contratante, ou responsável pelo tratamento, e passou a ser tarefa imprescindível, na jornada de implementação e conformidade, definir quem é o controlador e quem é o operador. Em regra, o controlador é uma entidade que decide sobre os elementos-chave de um processamento.

Já o operador trata dados de acordo com as instruções do controlador. Podemos dizer que consiste em uma verdadeira "terceirização de atividades de tratamento" para outras entidades, seja pessoas jurídicas ou naturais. Não existe impedimento para uma pessoa natural ser contratada como operadora em atividades específicas de tratamento de dados, sendo considerada operadora de dados, mas os empregados, os servidores públicos, os sócios, assim como outras pessoas naturais, que integram e estão vinculados a uma pessoa jurídica, expressando sua vontade, não poderão ser considerados

agentes de tratamento, operadores ou controladores neste cenário. Na verdade, a entidade responderá pelos atos destes prepostos que agem e tratam dados e seu nome.

O Parecer 1/2010 do Grupo de Trabalho do Artigo 29, na União Europeia, ainda elaborado durante a vigência da Diretiva 95/46/CE, sobre os conceitos de responsável pelo tratamento, ou controlador e operador ou subcontratante, WP 169, já nos brindava com o conceito de responsável pelo tratamento dos dados e trazia a sua relação com o conceito de subcontratante, que corresponde ao operador no Brasil.

O controlador era inicialmente denominado, na Convenção n. 108 do Conselho da Europa, de 'responsável pelo ficheiro', e o termo foi substituído por "responsável pelo tratamento" de dados pessoais. A Diretiva introduziu também o conceito de "subcontratante", que não era mencionado na Convenção n. 108.

Os conceitos iniciais foram formulados durante as negociações relativas ao projeto de proposta da Diretiva 95/46/CE, no início da década de 90, e o conceito inicial de responsável pelo tratamento foi basicamente retirado da Convenção n. 108 do Conselho da Europa, adotada em 1981.

BRASIL	EQUIVALENTE NA UNIÃO EUROPEIA
CONTROLADOR	RESPONSÁVEL
OPERADOR	SUBCONTRATANTE

O que é e como devemos avaliar se existe uma controladoria conjunta?

A controladoria conjunta existe quando estivermos diante de mais de um responsável pelo tratamento de dados pessoais e a mesma existirá quando alguns critérios trazidos pela

guideline 07/2020[24] do CEPD e o Guia orientativo da ANPD para definições de agentes de tratamento forem observados:

> Deverá existir o poder de decisão no tratamento de dados pessoais conjunto, ou de mais de um agente de tratamento.
>
> Deverá existir interesse mútuo de pelo menos dois controladores e que tenham finalidades próprias no mesmo tratamento.
>
> Estes controladores conjuntos deverão tomar decisões conjuntas, comuns ou convergentes, tanto sobre os elementos essenciais como sobre as finalidades do tratamento.

TODOS OS CRITÉRIOS DEVERÃO SER SEGUIDOS CONCOMITANTEMENTE PARA TERMOS CONTROLADORES OU RESPONSÁVEIS CONJUNTOS.

Seguem alguns exemplos do guia orientativo para definições dos agentes de tratamento:

No primeiro exemplo não há controladoria conjunta, mas todas as organizações são responsáveis:

"Exemplo 1 – Uso de dados abertos disponibilizados por Agência Reguladora:

A Agência Reguladora disponibiliza acesso público aos dados relativos às outorgas dos serviços regulados, incluindo informações de pessoas naturais sócias de prestadoras. A base de dados é armazenada pela própria

---

(24) EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, set. 2020. Disponível em: <https://edpb.europa.eu/sites/edpb/files/consulta-tion/edpb_guidelines_202007_controllerprocessor_en.pdf> Acesso em: 25 jun. 2021.

Agência e utilizada para subsidiar decisões administrativas. A Organização da Sociedade Civil tem acesso aos dados disponibilizados pela Agência e efetua, com base em solução de inteligência artificial, cruzamento com outras bases de dados visando à realização de ações de controle social de entidades e agentes públicos. A Sociedade Empresária também trata os dados em questão, visando, porém, fornecer serviços de consultoria aos agentes do setor regulado. Embora a mesma base de dados seja utilizada pelas três entidades (Agência Reguladora, Organização da Sociedade Civil e Sociedade Empresária), cada uma dessas organizações é responsável e responde pelos respectivos tratamentos realizados, sendo controladores singulares ou independentes. Neste contexto, não há controladoria conjunta pois o tratamento de dados ocorre no âmbito das atividades e das finalidades definidas por cada organização."[25](destaques nossos)

"Exemplo 2 – Campanha de marketing de empresas I: **decisões comuns.**

As empresas ARGENTINA e BRASIL lançaram um produto de marca conjunta COSMÉTICO e desejam organizar um evento para promover este produto. Para esse fim, decidem compartilhar dados de seus respectivos clientes e banco de dados de clientes potenciais e decidir sobre a lista de convidados para o evento com base nesses dados. Eles também concordam sobre as modalidades de envio dos convites para o evento, como coletar feedback durante os eventos e sobre as ações de marketing de acompanhamento. Por fim, contratam a agência de marketing DINAMARCA para executar a campanha. A agência traz sugestões de como os clientes poderiam

(25) ANPD. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>.

ser mais bem alcançados e define os canais, ferramentas e produtos da campanha. As empresas ARGENTINA e BRASIL podem ser consideradas controladores conjuntos para o tratamento de dados pessoais relacionados com a organização do evento e promoção do produto da marca COSMÉTICO, por terem definido, em conjunto, a finalidade e os elementos essenciais dos dados tratados nesse contexto. Já a agência de marketing DINAMARCA atuará como operadora de dados para as empresas ARGENTINA e BRASIL. Ainda que opine sobre os meios de tratamento, ela não é a responsável pela tomada de decisão final, limitando-se a definir elementos não essenciais como os canais, ferramentas e produtos da campanha. Caso a agência de marketing DINAMARCA contrate serviços de terceiros de armazenamento de dados em nuvem, por exemplo, essa empresa prestadora de serviços será caracterizada como suboperadora."[26]

O Parecer 1/2010, sobre os conceitos de responsável pelo tratamento, ou controlador e operador ou subcontratante, WP 169, traz o conceito de responsável pelo tratamento dos dados e a sua relação com o conceito de subcontratante ou operador, ainda elaborada na vigência da Directiva 95/46/CE. Os conceitos iniciais foram formulados durante as negociações relativas ao projeto de proposta da diretiva, no início da década de 90 e o conceito de responsável pelo tratamento foi basicamente retirado da Convenção n. 108 do Conselho da Europa, adotada em 1981.[27]

"Em primeiro lugar, o termo 'responsável pelo ficheiro' constante da Convenção n. 108 foi substituído pelo termo 'responsável pelo tratamento' de dados pessoais. O

(26) ANPD. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Disponível em: <https://www.gov.br › pt-br › assuntos› noticias>.

(27) Opinion 1/2010 on the concepts of "controller" and "processor. Disponível em: <http://ec.europa.eu › article-29 › files › wp169_en>. Acesso em: 25 jun. 2021.

termo 'tratamento de dados pessoais' é um conceito muito vasto, sendo definido no artigo 2º, alínea b), da Directiva como 'qualquer operação ou conjunto de operações efectuadas sobre tratamento de dados pessoais, com ou sem meios automatizados, tais como a coleta, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, o apagamento ou a destruição'. Assim, o conceito de 'responsável' deixou de ser utilizado por referência a um objecto estático ('o ficheiro'), sendo antes associado a actividades que reflectem o ciclo de vida da informação, desde a sua recolha sua destruição, o que exigia uma análise pormenorizada e global ('operação ou conjunto de operações'). Embora o resultado possa ter sido o mesmo em muitos casos, foi atribuído ao conceito um significado e um âmbito muito mais vastos e dinâmicos.

Outras alterações envolviam a previsão da possibilidade de 'controlo colectivo' ('individualmente ou em conjunto com outrem'), o requisito de que o responsável pelo tratamento 'determine as finalidades e os meios de tratamento dos dados pessoais' e a ideia de que esta determinação pode ser efectuada pela legislação nacional ou comunitária ou de outra forma. A Directiva introduziu também o conceito de 'subcontratante', que não é mencionado na Convenção n. 108. Estas e outras alterações serão analisadas mais pormenorizadamente ao longo do presente parecer[28]."

(28) Opinion 1/2010 on the concepts of "controller" and "processor. Disponível em: <http://ec.europa.eu › article-29 › files › wp169_en>. Acesso em: 25 jun. 2021.

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

O operador, assim como o controlador, poderá ser uma pessoa natural ou jurídica, de direito público ou privado, mas com uma diferença essencial, que o operador realiza o tratamento de dados pessoais em nome do controlador.

O empregado é subordinado à empresa responsável pelo tratamento, podendo ser um preposto desta, não havendo razão para se lhe atribuir responsabilidade, como agente de tratamento, ou operador. Neste mesmo sentido, a Autoridade Nacional de Proteção de Dados editou guia orientativo, onde preconiza que empregados, administradores, sócios, servidores, ademais de outras pessoas naturais que integrem a pessoa jurídica, não deverão ser considerados como operadores[29].

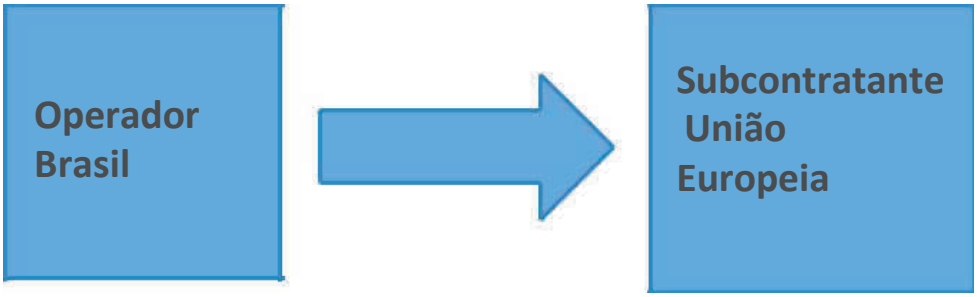
Quando falamos de pessoa jurídica, a organização é que sempre será o agente de tratamento para os fins da LGPD e não o empregado. Os representantes ou prepostos seguirão as ordens a serem executadas por estas.

A legislação brasileira traz a responsabilidade solidária do operador e do controlador. Exemplo de operador, que é aquele que trata os dados por ordem do controlador, seria um serviço de nuvem. Outros exemplos de operadores: uma empresa de *call center* em um banco, uma empresa de gestão de folha de pagamento, ou mesmo um contador em relação à empresa contratante.

---

(29) Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. ANPD (Autoridade Nacional de Proteção de Dados). Governo Federal.

Os operadores deverão manter registros de suas atividades executadas no tratamento de dados pessoais por ordem do controlador. A denominação dada ao operador no regulamento de proteção de dados europeu é subcontratante ou processador.



O operador responderá solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados, ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, nos termos da LGPD. Verificamos a importância desta diferenciação.

A *guideline* da União Europeia 07/2020 do CEPD (Comitê Europeu de Proteção de Dados), assim como anterior parecer Opinion 1/2010 do Grupo de Trabalho do Artigo 29 definem trazem as diretrizes sobre a diferença entre controlador e operador, além do guia orientativo para definições.

OPERADOR: é agente de tratamento e poderá ser uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O principal elemento distintivo entre estes atores é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro ("operador") realize o tratamento em seu nome. Um controlador pode compartilhar

dados, por exemplo, para um contador, empresa de folha de pagamento, transportadora, *courier*, entre outros, os quais apenas poderão tratar dados de acordo com as instruções claras do controlador, não podendo ser utilizados para finalidade distinta, ou além daquela determinada pelo controlador.

O operador, subcontratante, na União Europeia, poderá apenas decidir sobre certos assuntos, como, por exemplo, qual software usar, segregação de acesso e outras medidas técnicas e administrativas de segurança da informação, o que não altera seu papel como operador.

Talvez ficasse mais claro se no Brasil tivéssemos repetido as nomenclaturas eleitas e utilizadas pela legislação da União Europeia, não dando uma falsa ideia de que o empregado, um servidor, ou departamento poderia ser agente de tratamento e assim polo passivo em uma ação judicial dos entes legitimados para ações civis públicas, ou mesmo em uma ação individual, ou uma sanção da Autoridade Nacional de Proteção de Dados.

Esta diferenciação é fulcral não apenas para os profissionais especializados na área, mas também para o cidadão comum e em uma implementação por uma empresa ou entidade, principalmente pelo papel assumido pelo controlador, como responsável pelas atividades de tratamento, que detém poder de decisão.

Tínhamos já anteriormente importantes documentos que nos ajudavam na interpretação da Lei Geral de Proteção de Dados e nas diferenças entre os agentes de tratamento e mesmo o DPO, ou encarregado (o qual não é agente de tratamento), como a *guideline* da União Europeia n. 07/2020 do CEPD (Comitê Europeu de Proteção de Dados) e o anterior parecer do Grupo de Trabalho do Artigo 29 de número 1/2010.

A Autoridade Nacional de Proteção de Dados, no Brasil, preocupada com a identificação dos agentes de tratamento e as dúvidas recorrentes sobre esta temática, constatada não apenas em empresas privadas, mas principalmente em órgãos públicos, publicou o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado", em 2021, o qual pode ser encontrado no site do Governo Federal. Este guia foi atualizado e hoje já está disponível a versão 2.0 de 2022.

De acordo com o guia da Autoridade Nacional de Proteção de Dados do Brasil, os agentes de tratamento (controlador e operador) poderão ser pessoas naturais ou jurídicas, de direito público ou privado, **devendo estes ser definidos a partir de seu caráter institucional**. **Importante destacar que os empregados, como subordinados, os servidores públicos, ou as equipes de trabalho de uma organização, não serão considerados controladores (autônomos ou conjuntos), nem operadores,** já que atuam sob o poder diretivo do agente de tratamento.[30]

Desta forma, um contador que trabalhe internamente como empregado, ou um departamento de contabilidade composto por empregados da própria entidade controladora, não são considerados agentes de tratamento pelo vínculo existente. Eles estão integrados à pessoa jurídica, e sua função é interna, não estabelecendo, portanto, uma relação de operador ou controlador sobre os dados tratados.

Por outro lado, se a empresa controladora decidir contratar um contador externo, que pode ser um profissional liberal, ou um escritório de contabilidade terceirizado, estes

(30) ANPD. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>. Acesso em: 25 jun. 2021.

serão classificados como agentes de tratamento. Dependendo da atividade de tratamento executada, eles podem ser considerados operadores ou controladores. Por exemplo, quando o contador gerencia a folha de pagamento, seguindo as instruções do empregador sobre quem pagar, quando e onde, ele atua como operador. A sua função contratada e externa para o tratamento de dados distingue-os da estrutura interna da entidade controladora, consolidando a sua posição como agente de tratamento.

De acordo com a atividade de tratamento, o contador pode atuar ainda como controlador. Isso é evidenciado na diretriz 7 de 2020 do Comitê Europeu de Proteção de Dados. No cenário proposto, o empregador A contrata a empresa de contabilidade C para realizar auditorias em sua contabilidade e, consequentemente, transfere dados sobre transações financeiras, que incluem dados pessoais, para C. Nesse contexto, a empresa de contabilidade C processa esses dados sem instruções detalhadas de A e decide, conforme as disposições legais que regulam as atividades de auditoria realizadas por C, que os dados coletados serão processados apenas para fins de auditoria de A. A empresa C também determina quais dados precisa ter, quais categorias de pessoas precisam ser registradas, por quanto tempo os dados devem ser mantidos e que meios técnicos utilizar. Nessas circunstâncias, a empresa de contabilidade C é considerada controladora independente ao realizar seus serviços de auditoria para A. No entanto, esta avaliação pode variar dependendo do nível de instruções de A. Se a lei não estabelecer obrigações específicas para a empresa de contabilidade e a empresa cliente fornecer instruções muito detalhadas sobre o processamento, a empresa de contabilidade estaria atuando como operadora. Uma distinção pode ser feita entre uma situação em que o processamento é feito - de acordo com as leis que regulam essa profissão - como

parte da atividade principal da empresa de contabilidade e onde o processamento é uma tarefa acessória mais limitada, realizada no âmbito da atividade da empresa cliente (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2020).(31)

Destaquemos que o guia da Autoridade Nacional de Proteção de Dados ainda preconiza que: "**sempre que falamos de pessoa jurídica, a organização é que será o agente de tratamento para os fins da Lei Geral de Proteção de Dados**, sendo que esta que estabelecerá as regras para o tratamento de dados pessoais, as quais serão executadas por seus representantes ou prepostos".

A pessoa jurídica, sempre que esta existir, será o agente de tratamento, controlador ou operador. Será controlador se tomar decisões e der instruções sobre as atividades de tratamento. Será operador dos agentes de tratamento de dados pessoais e do encarregado da Autoridade Nacional de Proteção de Dados.

Outro ponto importante é que o agente de tratamento será definido para cada operação de tratamento de dados pessoais e, por conclusão, a mesma empresa ou organização poderá ser controladora e operadora em tratamentos distintos e de acordo com sua atuação em diferentes operações de tratamento. Outro detalhe que uma pessoa natural poderá ser controladora, como, por exemplo, um advogado ou um médico tratando os prontuários de seus pacientes.

---

(31) COMITÊ EUROPEU DE PROTEÇÃO DE DADOS. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en>. Acesso em: 11 jun. 2023.

OPERADORAS – quando atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento.

O operador deve ser uma entidade distinta do controlador.

Uma empresa poderá assumir os dois papéis em atividades de tratamento distintas. Por exemplo, uma transportadora ou uma empresa de gestão de folha de pagamento, geralmente são operadoras, ao tratarem dados para outras empresas, mas são controladoras em relação aos próprios empregados.

FUNCIONÁRIOS – atuarão em subordinação às decisões do controlador, não se confundindo, portanto, com os operadores de dados pessoais.

Exemplos práticos do Guia Orientativo para Definições dos Agentes de Tratamento da Autoridade Nacional de Proteção de Dados:

"Exemplo 1 – Médica profissional liberal:

Uma médica, profissional liberal, armazena os prontuários e os demais dados pessoais de seus pacientes no computador de seu consultório. **A médica, pessoa natural, é a controladora dos dados pessoais."**[32] **(destaques nossos)**

"Exemplo 2 – Médica empregada de um hospital:

Uma médica é empregada de um hospital, constituído sob a forma de associação civil sem fins lucrativos. Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes

(32) ANPD. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>.

em nuvem, inclusive assinando os contratos correspondentes. **O hospital, isto é, a associação civil, pessoa jurídica de direito privado, é o controlador na hipótese.** A médica, por atuar sob o poder diretivo da organização, não se caracteriza como agente de tratamento."[33] (**destaques nossos)**

"Exemplo 3 – Órgão público contratante de um serviço de inteligência artificial:

Um órgão público, vinculado à União, contrata uma solução de inteligência artificial fornecida por uma sociedade empresária com a finalidade específica de realizar o tratamento automatizado de decisões com base em um banco de dados gerido pelo órgão. **Seguindo as instruções fornecidas** pelo gestor público responsável e estabelecidas em contrato, a sociedade empresária realiza as operações necessárias para viabilizar o tratamento dos dados em questão. **A União, pessoa jurídica de direito público, é a controladora na hipótese.** Não obstante, o órgão público responsável detém obrigações legais específicas em face dos titulares e da ANPD, conforme previsto na LGPD. A sociedade empresária é a operadora, uma vez que realiza o tratamento dos dados conforme as instruções fornecidas pelo controlador. Por fim, o gestor público responsável, por atuar como servidor público subordinado à União, não se caracteriza como agente de tratamento."[34] (**destaques nossos)**

A Lei Geral de Proteção de Dados dispõe no artigo 39 que "o operador deverá realizar o tratamento segundo

---

(33) ANPD. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>.

(34) ANPD. G*uia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>.

as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria".(35)

Não obstante a lei determine que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, atuando em nome deste, este poderá e deverá adotar medidas de segurança, técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, como agente de tratamento, nos termos do artigo 46 da Lei Geral de Proteção de Dados. A Autoridade Nacional de Proteção de Dados poderá dispor sobre os padrões técnicos mínimos. Se o operador agir de forma dolosa é possível sustentar a ausência da responsabilidade do controlador.

O regulamento europeu traz as regras relacionadas ao operador ou subcontratante no artigo 28:

> "Artigo 28º
>
> Subcontratante
>
> 1. Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.
>
> 2. O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao

(35) BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>.

aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.

3. O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o subcontratante:

a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adota todas as medidas exigidas nos termos do artigo 32º;

d) Respeita as condições a que se referem os ns. 2 e 4 para contratar outro subcontratante;

e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III;

f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32º a 36º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;

g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros; e

h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

No que diz respeito ao primeiro parágrafo, alínea h), o subcontratante informa imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar o presente regulamento ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

4. Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o subcontratante, referidas no n. 3, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do presente regulamento. Se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante.

5. O facto de o subcontratante cumprir um código de conduta aprovado conforme referido no artigo 40º ou um procedimento de certificação aprovado conforme referido no artigo 42º pode ser utilizado como elemento para demonstrar as garantias suficientes a que se referem os ns. 1 e 4 do presente artigo.

6. Sem prejuízo de um eventual contrato individual entre o responsável pelo tratamento e o subcontratante, o contrato ou outro ato normativo referido nos ns. 3 e 4 do presente artigo podem ser baseados, totalmente ou em parte, nas cláusulas contratuais-tipo referidas nos ns. 7 e 8 do presente artigo, inclusivamente quando fazem parte de uma certificação concedida ao responsável pelo tratamento ou ao subcontratante por força dos artigos 42º e 43º.

7. A Comissão pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos ns. 3 e 4 do presente artigo pelo procedimento de exame a que se refere o artigo 93º, n. 2.

8. A autoridade de controlo pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos ns. 3 e 4 do presente artigo e de acordo com o procedimento de controlo da coerência referido no artigo 63º.

9. O contrato ou outro ato normativo a que se referem os ns. 3 e

4 devem ser feitos por escrito, incluindo em formato eletrónico.

10. Sem prejuízo do disposto nos artigos 82º, 83º e 84º, o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão."

1.8. Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

O encarregado deve possuir domínio da legislação de proteção de dados e das práticas de tratamento de dados pessoais. Este poderá ser um empregado da empresa ou mesmo um terceiro contratado, um DPO *as a service*. Com a alteração promovida pela Lei n. 13.853/2019 à legislação de proteção de dados, este pode ser inclusive uma pessoa jurídica.

A Lei Geral de Proteção de Dados preconiza no artigo 41 que o controlador deverá indicar um encarregado pelo tratamento dos dados:

"Art. 41. O controlador **deverá indicar encarregado pelo tratamento de dados pessoais.**

1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

2º As atividades do encarregado consistem em:

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

> II – receber comunicações da autoridade nacional e adotar providências;
>
> III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
>
> 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados."

As funções do encarregado de proteção de dados, também e mais conhecido como *Data Protection Officer* (DPO) estão descritas no parágrafo 2º do artigo 41, da LGPD, conforme demonstrado anteriormente. No entanto, essas responsabilidades não são limitativas, pois a Lei Geral de Proteção de Dados (LGPD), em seu parágrafo 3º do artigo 41[36], permite que a Autoridade Nacional de Proteção de Dados (ANPD) estabeleça normas complementares sobre as funções e as definições do encarregado. Essas normas também podem abranger as circunstâncias em que a indicação de um encarregado pode ser dispensada, levando em conta a natureza e o porte da entidade ou o volume de operações de tratamento de dados. De acordo com o artigo 11 da Resolução CD/ANPD n. 2/2022, os agentes de tratamento de pequeno porte não são obrigados a indicar um encarregado, no entanto, devem disponibilizar um canal de comunicação com o titular de dados para atender o disposto no artigo 41, § 2º, I da LGPD. Mesmo na ausência de obrigatoriedade definida por orientações futuras expedidas pela ANPD, a nomeação do encarregado pode ser realizada de

(36) BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 12 jun. 2023.

várias formas. Essa indicação será considerada política de boas práticas e governança para os agentes de tratamento de pequeno porte, de acordo com o artigo 52, §1º, IX da LGPD. [37]

Em resumo:

1. Indicação de um Encarregado de Proteção de Dados/ DPO conforme o artigo 41 da LGPD[38] e Resolução CD/ ANPD n. 2/2022[39] :

- A nomeação de um encarregado de dados é um dever de todo controlador de dados.

- A lei brasileira LGPD não detalha as circunstâncias que exigem a designação de um encarregado, portanto, por padrão, espera-se que todas as organizações indiquem uma pessoa para esta função.

- No entanto, a Resolução CD/ANPD n. 2/2022 apresenta diretrizes específicas e algumas circunstâncias de isenção deste requisito, especialmente para agentes de tratamento de dados de pequeno porte.

---

(37) ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD Nº 2, de 27 de janeiro de 2022. Diário Oficial da União, Brasília, DF, 28 jan. 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper>. Acesso em: 12 jun. 2023.

(38) ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Brasília, DF, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf>. Acesso em: 12 jun. 2023.

(39) ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD Nº 2, de 27 de janeiro de 2022. Diário Oficial da União, Brasília, DF, 28 jan. 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd>.

- Esta obrigação aplica-se a ambas as esferas, instituições privadas e públicas.

2. Características e Papel do Encarregado de Proteção de Dados/DPO:

- A natureza do encarregado pode ser tanto física quanto jurídica, podendo ser um funcionário interno ou um agente externo contratado.

- Este não é agente de tratamento

- A designação do encarregado deve ser formalizada.

- O encarregado deve gozar de autonomia para desempenhar suas tarefas, e suas qualificações profissionais devem ser determinadas pelo controlador de acordo com as necessidades.

- O apoio de uma equipe de proteção de dados ao encarregado é permissível e aconselhável.

3. Obrigações do Encarregado de Proteção de Dados/DPO:

- Este deve receber e tratar reclamações e comunicações dos titulares de dados e da ANPD.

- Este deve instruir empregados e contratados sobre boas práticas de proteção de dados.

- É responsável por desempenhar outras tarefas determinadas pelo controlador ou definidas por normas complementares.

O regulamento europeu de proteção de dados também traz, no artigo 39, as funções do encarregado de proteção de dados:

"Artigo 39º

Funções do encarregado da proteção de dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Esta--dos-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º;

d) Coopera com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento."

O regulamento europeu, artigo 37, a seguir, diferente da Lei Geral de Proteção de Dados, que deixa o encargo para a Autoridade Nacional de Proteção de Dados, como já foi ressaltado, já traz as hipóteses em que o encarregado é necessário:

"Encarregado da proteção de dados Artigo 37º Designação do encarregado da proteção de dados

1 – O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento

que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º.

2. Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

3. Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

4. Em casos diferentes dos visados no n. 1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um encarregado da proteção de dados. O encarregado da proteção de dados pode agir em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes.

5. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39º.

6. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços.

7. O responsável pelo tratamento ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo."

Diferentemente dos agentes de tratamento, que são o controlador e o operador, o encarregado não será responsável

pessoalmente por eventual falta de conformidade com a legislação de proteção de dados, salvo se agir com dolo ou culpa com previsão contratual.

1.9. Agentes de tratamento: o controlador e o operador

Este dispositivo demonstra que o controlador e operador são agentes de tratamento. Ambos poderão ser responsabilizados civilmente por violação à Lei Geral de Proteção de Dados, no tratamento dos dados da pessoa natural.

Os agentes de tratamento, controlador e operador, deverão realizar registros das operações de tratamento de dados pessoais, além de demonstrarem as medidas eficazes e capazes de comprovarem a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas (*accountability*).

Uma das inovações do Regulamento Geral de Proteção de Dados da União Europeia, em relação à antiga e revogada Diretiva 95/46/CE, é o princípio da *accountability*, o qual também foi incorporado em nossa legislação de Proteção de Dados de forma expressa, artigo 6º, inciso X, como princípio da responsabilização e da prestação de contas:

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

Os agentes de tratamento poderão ser pessoas naturais ou jurídicas e de direito público ou privado, devendo estes ser definidos a partir de seu caráter institucional.

1.9.1. Pessoa natural como agente de tratamento

Quando a Lei Geral de Proteção de Dados conceitua controlador e operador e traz que podem ser pessoas naturais não

está se referindo a empregados, equipes, departamentos, gestores, sócios e nem servidores. Se estes fossem agentes de tratamento, os empregados e servidores passariam a estar no polo passivo de ações individuais e coletivas, nos termos do artigo 42 da LGPD, e poderiam sofrer sanções da Autoridade Nacional, a qual, na sua função educativa, entre outras, como de conscientizar, regulamentar, fiscalizar o cumprimento da LGPD e aplicar sanções, em seu primeiro guia do Brasil, já demonstrou a preocupação com a possibilidade deste cenário com interpretações equivocadas, no Brasil, ao eleger este tema como o primeiro para a elaboração de um guia orientativo, entre tantos temas a tratar e regulamentar.

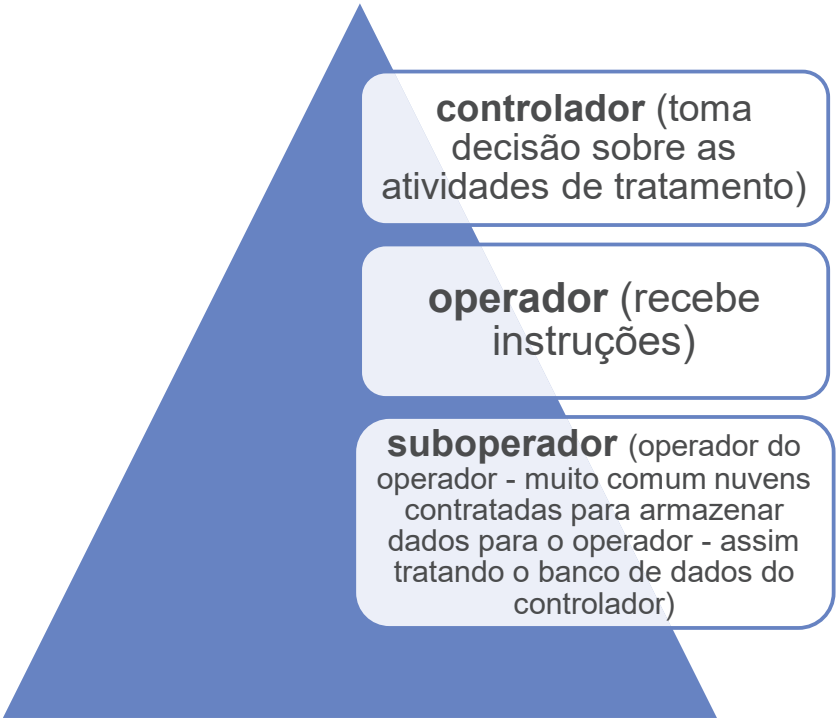
Empregados, equipes, departamentos, gestores, sócios e servidores NÃO PODERÃO SER CONSIDERADOS AGENTES DE TRATAMENTO.

Uma pessoa natural poderá ser controladora, como, por exemplo, um advogado ou um médico tratando os prontuários de seus pacientes, já que estes tomam decisões nas atividades de tratamento. Da mesma forma, um vendedor que tem sua tenda de pipoca ou cachorro-quente, ou uma pequena loja, mas nunca os empregados vinculados a estes.

Estas entidades serão controladoras sempre que atuarem de acordo com os próprios interesses e tiverem poder de decisão sobre as finalidades e os elementos essenciais de tratamento, e serão operadoras quando atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento.

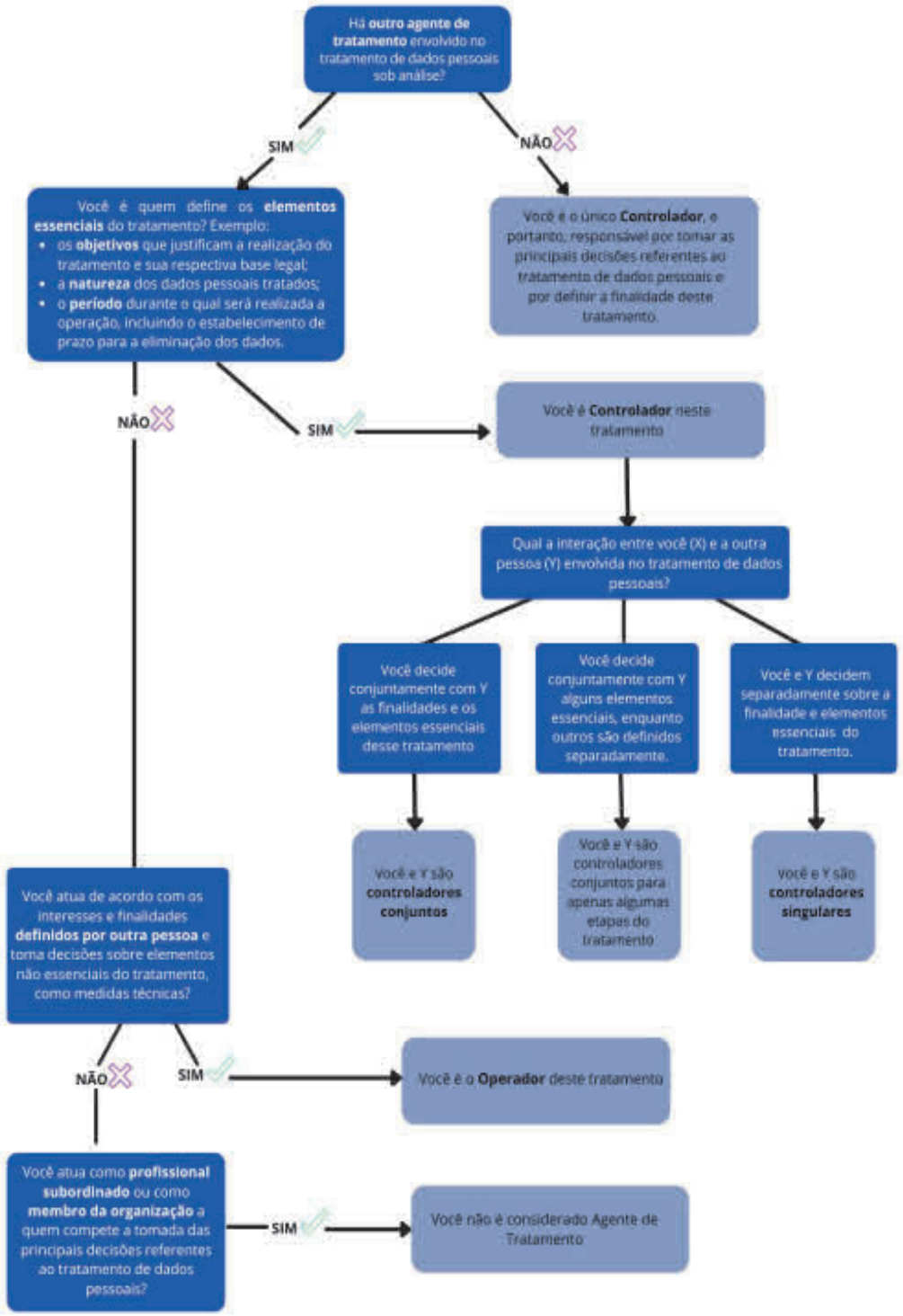
O guia da Autoridade Nacional de Proteção de Dados, da mesma forma que a *guideline 07/2020*, da União Europeia, reza que os funcionários atuarão em subordinação às decisões do controlador, não se confundindo, portanto, com os operadores de dados pessoais:

"Daí decorre que não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos. É o caso de empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta. Nesse sentido, a definição legal de controlador não deve ser entendida como uma norma de distribuição interna de competências e responsabilidades. De forma diversa, trata-se de comando legal que atribui obrigações específicas à pessoa jurídica, de modo que esta assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD."(40)



Fonte: Guia da Autoridade Nacional de Proteção de Dados: Versão 2.0

(40) ANPD. *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>.



[41]Fonte: Guia da Autoridade Nacional de Proteção de Dados: Versão 2.0

(41) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/

1.9.2. Agentes de tratamento e Poder Público

Os agentes de tratamento são o controlador e o operador. O controlador, ou responsável[42], é quem toma as decisões sobre as atividades de tratamento, e o operador trata dados, em nome de um controlador, como se fosse uma terceirização de atividades de tratamento,[43] não podendo este (operador) deixar de seguir as instruções passadas por aquele (controlador) sobre as atividades de tratamento contratadas, as quais deverão estar claramente definidas. Os servidores públicos, assim como empregados, sócios e administradores, não podem ser considerados agentes de tratamento.[44]

O controlador é o agente de tratamento responsável e poderá responder solidariamente com o operador, nos termos do art. 42 da LGPD, que dispõe: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".[45]

Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 12 nov. 2022.

(42) Como denominado o controlador na União Europeia.

(43) CARLOTO, Selma. Lei Geral de Proteção de Dados. 3. ed. São Paulo: LTr, 2020.

(44) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 12 nov. 2022.

(45) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 12 nov. 2022.

Quando falamos de pessoas jurídicas de direito público, cujas competências decisórias são distribuídas internamente entre diferentes órgãos públicos, como ocorre, por exemplo, com a União (pessoa jurídica de direito público) e os Ministérios, órgãos públicos despersonalizados e os quais integram a União e realizam tratamento de dados pessoais conforme o previsto na legislação, **o controlador será a União, responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrativa, serão exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte**, fenômeno que caracteriza a distribuição interna das competências. No entanto, **destaque-se que essa conclusão apenas se refere à Administração Pública direta e não à indireta, a qual poderá ser controladora, seguindo o regramento estabelecido pela LGPD**.(46)

1.10. Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

O Tratamento dos dados pessoais e dos dados pessoais sensíveis fica sujeito às regras da Lei Geral de Proteção de Dados e este tratamento inclui toda operação ou atividade realizada com os dados pessoais das pessoas naturais. A Lei Geral de Proteção de dados tem por objetivo garantir a transparência nas operações realizadas com os dados da

(46) *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: <https://www.gov.br › pt-br › assuntos › noticias>.

pessoa natural, desde o início do tratamento, com a coleta, durante o processamento, arquivamento, armazenamento, compartilhamento e até a eliminação dos dados pessoais.

Os agentes de tratamento deverão, nas atividades de tratamento, observar sempre a boa-fé e os princípios da necessidade, finalidade e adequação, tratando a menor quantidade possível de dados pessoais e devendo o tratamento estar sempre adstrito à finalidade informada desde a coleta dos dados pessoais.

Estudaremos no capítulo 3 os princípios basilares da Lei Geral de Proteção de Dados, que estão previstos no artigo 6º da presente lei: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

1.11. 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

Lembre-se que o dado anonimizado, já tratado no item 3.3, neste capítulo, consiste naquele em que o titular não poderá ser identificado, considerando-se os meios técnicos razoáveis e disponíveis na ocasião do tratamento.

1.12. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

Esta é a primeira hipótese de tratamento de dados pessoais e de dados pessoais sensíveis trazida pela Lei Geral

de Proteção de Dados, a qual será demonstrada em capítulo próprio. Esta, aparentemente, seria a hipótese que melhor resguarda o controlador, mas desde que o consentimento seja **livre, inequívoco e informado,** não podendo ser base legal de atividades de tratamento obrigatórias, quando deveremos buscar uma das demais bases legais de tratamento do artigo 7º para dados pessoais e artigo 11 para dados sensíveis**.**

O Grupo de Trabalho da União Europeia, em seus estudos, destacou a necessidade de restrição no uso do consentimento como base legal para o tratamento de dados em casos relacionados às relações de trabalho e com o Poder Público. Isso se deve ao desequilíbrio ou assimetria de poder existente nas relações laborais, em que os empregados estão subordinados aos empregadores, que possuem o poder empregatício. Este desequilíbrio também está presente em relações com o Poder Público. A diretriz anteriormente estabelecida pela WP259 rev01, que tratava das orientações relativas ao consentimento de acordo com o Regulamento (UE) 2016/679, foi substituída pela diretriz do Comitê Europeu de Proteção de Dados (CEPD), publicada no guia 05 de 2020, reforçando a necessidade de restrição no uso do consentimento em relações assimétricas.

O Regulamento Geral de Proteção de Dados da União Europeia também preconiza, no Considerando 43, que em casos específicos, em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública, quando é improvável que o consentimento tenha sido dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais.

A autorização do titular (consentimento) deverá ser intencional, e este deverá ser informado, previamente, para atender o princípio da transparência, sobre a finalidade para a qual este poderá ou não autorizar o tratamento de seus dados pessoais, que não será obrigatório. É vedada a autorização tácita e para finalidades genéricas.

O art. 4º, número 11, do RGPD dispõe que o consentimento do titular de dados pessoais consiste na manifestação de vontade **livre, específica, informada e explícita**, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.(47)

Quando forem tratados dados sensíveis, assim como dados de crianças, o consentimento deve ser fornecido "de forma específica e destacada, para finalidades específicas" (arts. 11, I, e 14, § 1º, ambos da LGPD, respectivamente).

A Autoridade Nacional de Proteção de Dados (ANPD) divulgou um enunciado com o objetivo de estabelecer uma interpretação padronizada sobre a aplicação das hipóteses legais no tratamento de dados pessoais de crianças e adolescentes. Segundo o enunciado, o tratamento desses dados pode ser realizado com base nas hipóteses legais previstas na Lei Geral de Proteção de Dados Pessoais (LGPD), como o consentimento fornecido pelo titular, o cumprimento de obrigações legais, a proteção à vida e o atendimento a interesses legítimos do controlador. No entanto, em todas as

---

(47) COMISSÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados Pessoais). Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection_pt. Acesso em: 30 mar. 2023.

situações, o melhor interesse da criança e do adolescente deve prevalecer, exigindo uma avaliação cuidadosa por parte do controlador. O enunciado visa orientar e ressaltar a importância do melhor interesse dos menores como critério fundamental na avaliação das operações de tratamento de dados envolvendo esses titulares. Essa iniciativa da ANPD está em conformidade com o artigo 14 da LGPD e representa um avanço na proteção dos dados pessoais de crianças e adolescentes.[48]

Além disso, o consentimento pressupõe uma escolha efetiva entre autorizar e recusar o tratamento dos dados pessoais, incluindo a possibilidade de revogar-se o consentimento a qualquer momento. Por essa razão, o consentimento, em muitas ocasiões, não poderá ser a base legal de tratamento escolhida, notadamente no que se refere às atividades de tratamento do Poder Público.

1.13. Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados

O titular dos dados pessoais tem direito de solicitar ao controlador, em relação aos seus dados, a qualquer momento e mediante requisição, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade, nos termos do artigo 18, inciso IV, da Lei Geral de Proteção de Dados:

---

(48) AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ANPD divulga enunciado sobre o tratamento de dados pessoais de crianças e adolescentes. Publicado em 24/05/2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o-tratamento-de-dados-pessoais-de-criancas-e-adolescentes>. Acesso em: 12 jun. 2023.

"Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, **bloqueio** ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;"

E o bloqueio dos dados, a que se refere a infração, e até a sua regularização, está previsto dentro das sanções administrativas, no artigo 52 da Lei Geral de Proteção de Dados:

"Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

(...)

V – **bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;"

1.14. Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado

Se o controlador não conseguir justificar o tratamento, dentro das hipóteses legais, sendo que o artigo 7º traz as hipóteses autorizadoras de tratamento dos dados pessoais e artigo 11º dos dados pessoais sensíveis, terá obrigação de eliminar de imediato estes dados pessoais. Logo, o controlador deverá bloquear o tratamento de dados, já que este apenas poderá tratar os dados necessários para a realização de suas finalidades, minimizando o tratamento, com abrangência dos dados pertinentes, proporcionais e não excessivos, em relação às finalidades do tratamento de dados, o que se

traduz no princípio da necessidade, artigo 6º, inciso III, da Lei Geral de Proteção de Dados.

O controlador deverá ainda analisar se a finalidade do tratamento dos dados pessoais foi alcançada para eliminar os dados ou banco de dados que deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.

A legislação de proteção de dados brasileira traz as hipóteses de término de tratamento dos dados pessoais, incluindo a verificação da finalidade alcançada, o fim do tratamento para o fim informado e do período de tratamento autorizado pelo titular, a comunicação do titular, inclusive no seu direito de revogação e a determinação da Autoridade Nacional de Proteção de Dados, quando houver violação do disposto na Lei Geral de Proteção de Dados:

> "O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I – verificação de que a finalidade foi alcançada ou de que os dados 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 artigo 8º desta Lei, resguardado o interesse público; ou
>
> IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei."

A nossa legislação preconiza que os dados deverão ser eliminados após o término do tratamento, mas traz as hipóteses e as finalidades em que é autorizada a conservação:

> "Art. 16. 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 dispostos nesta Lei; ou
>
> IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

O artigo 52 da Lei Geral de Proteção de Dados, ao elencar as sanções administrativas, traz, no inciso VI a eliminação dos dados pessoais a que se refere a infração:

> "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> (...)
>
> VI – eliminação dos dados pessoais a que se refere a infração."

1.15. Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro

Foram eliminadas as fronteiras físicas na era digital e esta transferência ocorre diariamente quando as empresas utilizam e-mail, ou serviços de aplicação de internet. A transferência internacional de dados pessoais é uma questão crítica para muitas empresas que operam globalmente. No caso de empresas que possuem matriz no exterior e filiais no Brasil, ou mesmo as que utilizam soluções de armazenamento em nuvem fora do país, a transferência de dados envolve a movimentação de informações pessoais através das fronteiras internacionais.(49)

---

(49) BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm>. Acesso em: 9 jun. 2022.

O artigo 33 da Lei Geral de Proteção de Dados traz as hipóteses em que é possível a transferência internacional de dados pessoais:

"Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I – para países ou organismos internacionais que **proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei**;

II – **quando o controlador oferecer e comprovar garantias de cumprimento dos princípios**, **dos direitos do titular e do regime de proteção de dados** previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas-padrão contratuais;

c) normas corporativas globais;

d) selos, certificados e códigos de conduta regularmente emitidos;

III – **quando a transferência for necessária para a cooperação jurídica internacional** entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV – quando a transferência for necessária **para a proteção da vida ou da incolumidade física do titular ou de terceiro**;

V – **quando a autoridade nacional autorizar a transferência**;

VI – quando a transferência resultar em **compromisso assumido em acordo de cooperação internacional**;

VII – quando a **transferência for necessária para a execução de política pública ou atribuição legal do serviço público,** sendo dada publicidade nos termos do inciso I do *caput* do artigo 23 desta Lei;

VIII – **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 esta de outras finalidades; ou

IX – **quando necessário para atender as hipóteses previstas nos incisos II, V e VI** do artigo 7º desta Lei.

> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do artigo 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional."

A Lei Geral de Proteção de Dados (LGPD) do Brasil, que entrou em vigor em setembro de 2020, é a legislação que regula essas transferências. Segundo a LGPD, a transferência internacional de dados pessoais só é permitida em algumas situações acima mencionadas, nos termos do artigo 33 da LGPD.

Além disso, as empresas devem implementar medidas de segurança, práticas e políticas institucionais adequadas para proteger os dados pessoais, e os titulares têm o direito de livre acesso e outros previstos no capítulo 3 da LGPD, principalmente os do artigo 18.

A transferência de dados pessoais é um elemento essencial na era digital atual, permitindo que as empresas operem efetivamente em uma escala global. No entanto, é fundamental garantir que essas transferências estejam em conformidade com a legislação local e internacional para proteger os direitos dos indivíduos e evitar sanções ou condenações.

O artigo 34 da Lei Geral de Proteção de Dados (LGPD) estabelece que a autoridade nacional de proteção de dados avaliará o nível de proteção de dados do país estrangeiro ou organismo internacional de destino levando em consideração diversos critérios, incluindo as normas gerais e setoriais da legislação em vigor no país de destino, a natureza dos dados, a observância dos princípios de proteção de dados previstos na lei, a adoção de medidas de segurança, a existência de garantias judiciais e institucionais para o respeito

aos direitos de proteção de dados, e outras circunstâncias específicas relacionada à transferência.(50)

O artigo 35 determina que a definição do conteúdo de cláusulas-padrão contratuais e a verificação de cláusulas contratuais específicas, normas corporativas globais ou selos, certificados e códigos de conduta para uma transferência específica serão realizadas pela autoridade nacional. São estabelecidos requisitos, condições e garantias mínimas que devem ser observados nesse processo de verificação. A autoridade nacional pode solicitar informações adicionais ou realizar diligências de verificação quando necessário. A autoridade nacional também pode designar organismos de certificação para realizar essas avaliações, que ficarão sob sua fiscalização e por fim, o artigo 36 dispõe que qualquer alteração nas garantias apresentadas para a observância dos princípios de proteção de dados e dos direitos do titular deve ser comunicada à autoridade nacional.(51)

1.16. Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados

(50) BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm>. Acesso em: 9 nov. 2022.
(51) *Idem.*

Independentemente da forma de compartilhamento de dados, os agentes de tratamento deverão observar os princípios da legislação de proteção de dados.

Importante ressaltar que quando os dados pessoais forem tratados com base no consentimento, ao haver necessidade de compartilhamento pelo controlador com outros controladores, este deverá obter novo consentimento e específico para esta nova finalidade, salvo se a nova hipótese ensejadora de tratamento tiver outro fundamento legal, com base no artigo 7º (hipóteses autorizadoras de tratamento de dados pessoais) ou 11º (hipóteses autorizadoras de tratamento de dados pessoais sensíveis) da Lei Geral de Proteção de Dados.

Apenas poderão ser compartilhados dados mediante consentimento ou se presente e indicada previamente outra base legal de tratamento, além de respeitados os princípios de proteção de dados e os direitos do titular.

1.17. Relatório de impacto à proteção de dados pessoais: 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

O relatório de impacto à proteção de dados é um documento do controlador e poderá ser solicitado a qualquer tempo pela ANPD. O artigo 38 da Lei Geral de Proteção de Dados dispõe que a ANPD poderá determinar, que o controlador elabore o presente documento, inclusive de dados sensíveis, relacionado a suas operações de tratamento de dados, observados os segredos comercial e industrial.

O artigo 5º da LGPD conceitua o RIPD, no inciso XVII: "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".

O relatório de impacto à proteção de dados tem como escopo minimizar os riscos na proteção de dados, avaliando e mapeando o risco no tratamento dos dados pessoais objeto do relatório. Este se destina a atividades de tratamento de alto risco.

O artigo 55-J, da LGPD, incluído pela Lei n. 13.853, de 2019, preconiza que compete à ANPD:

> "XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei".

O relatório de impacto à proteção de dados pessoais será melhor detalhado em capítulo específico (5), com este título.

1.18. Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; (Redação dada pela Lei n. 13.853, de 2019)

Aqui inclui tanto os órgãos da administração pública direta ou indireta, como as pessoas jurídicas de direito privado, legalmente constituídas e sem fins lucrativos, como

associações e fundações, sendo este conceito relevante porque dispensa o consentimento para tratamento dos dados pessoais. Destaca-se ainda que os órgãos de pesquisa aqui definidos deverão possuir sede ou foro no Brasil.

1.19. Autoridade nacional de Proteção de Dados:

A Lei n. 13.853 foi promulgada e criou a Autoridade Nacional de Proteção de Dados, como elo entre sociedade e governo, em uma fase que cada vez há mais necessidade de proteção dos dados pessoais e com o objetivo principal de proteger a privacidade dos titulares destes dados.

A Autoridade Nacional de Proteção de Dados foi inicialmente criada como um órgão transitório da administração pública, vinculado à Presidência da República, com a possibilidade de ser transformada, em até dois anos, pelo Executivo, em uma entidade da administração pública federal indireta, submetida a um regime autárquico especial e vinculada à Presidência da República. Conforme estabelecido pelo artigo 55-B da Lei nº 13.709/2018, a Autoridade possui autonomia técnica e decisória. Ela é composta pelo Conselho Diretor, que é o órgão máximo de direção, pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, pela Corregedoria, pela Ouvidoria, por um órgão de assessoramento jurídico próprio e pelas unidades administrativas e especializadas necessárias para a aplicação da referida lei, conforme descrito no artigo 55-C.

A Lei 14.460/22, resultante da conversão da Medida Provisória 1124/22, transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia especial, conferindo-lhe autonomia técnica e decisória, patrimônio próprio e sede no Distrito Federal. A nova lei, que altera as Leis 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e

13.844/2019, estabelece a estrutura e competências da ANPD como autarquia especial. Além disso, define a criação de um cargo comissionado para o diretor-presidente da ANPD e prevê a alocação dos servidores atuais na autarquia. A regulamentação da transição do órgão vinculado à Presidência para autarquia independente será feita em ato conjunto do secretário-geral da Presidência e do diretor-presidente da ANPD[52].

A proposta inicial da presente autoridade é orientar preventivamente, dando preferência ao diálogo e posteriormente fiscalizar, advertir e, apenas penalizar, caso a legislação continue sendo descumprida, incentivando e reconhecendo as boas práticas dos agentes de tratamento como parâmetro de dosimetria da sanção, nos termos do artigo 52, parágrafo primeiro e da resolução cd/anpd n. 4/2023 , regulamento de aplicação de sanções administrativas e mais conhecido como Regulamento de Dosimetria da Sanção.

Com a recente derrubada dos vetos à Lei n. 13.853/2019, oriunda da MP n. 869/2018, artigo 52, incisos X, XI e XII, a Autoridade Nacional de Proteção de Dados poderá penalizar os agentes de tratamento, com as penalidades restabelecidas nestes incisos de suspensão parcial do funcionamento de banco de dados por até seis meses e prorrogável por igual período até a regularização da atividade pelo controlador, suspensão do exercício da atividade de tratamento dos dados pessoais pelo período máximo de seis meses, prorrogável por igual período e a proibição parcial ou total

---

(52) Brasil. (2022). *Lei 14.460, de 25 de outubro de 2022*. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis ns. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. Disponível em:L14460 (planalto.gov.br). Acesso em 10 de jun. 2023.

do exercício de atividades relacionadas a tratamento de dados. Estas três novas penalidades se somam às iniciais e já estavam previstas na Lei Geral de Proteção de Dados inicialmente: advertência, multa simples, multa diária, publicização da infração após devidamente apurada e confirmada a sua ocorrência, bloqueio dos dados pessoais a que se refere a infração até a sua regularização e eliminação dos dados pessoais a que se refere a infração.