GUIA DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA A INDÚSTRIA

CNI
Confederação Nacional da Indústria
PELO FUTURO DA INDÚSTRIA

GUIA DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA A INDÚSTRIA

GUIA DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA A INDÚSTRIA

CNI
Confederação Nacional da Indústria
PELO FUTURO DA INDÚSTRIA

CNI
Diretoria Jurídica - DJ

FICHA CATALOGRÁFICA

C748g

Confederação Nacional da Indústria.
Guia de boas práticas de proteção de dados para a indústria / Confederação Nacional da Indústria. – Brasília : CNI, 2023.

109 p. : il.

1.LGPD. 2. Tratamento de Dados. 3. Segurança da Informação. I. Título.

CDU: 342.721(094.5)

CNI
Confederação Nacional da Indústria
Sede
Setor Bancário Norte
Quadra 1 – Bloco C
Edifício Roberto Simonsen
70040-903 – Brasília – DF
Tel.: (61) 3317-9000
Fax: (61) 3317-9994
http://www.portaldaindustria.com.br/cni/

Serviço de Atendimento ao Cliente - SAC
Tels.: (61) 3317-9989/3317-9992
sac@cni.com.br

SUMÁRIO

APRESENTAÇÃO

A Lei n° 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), estabeleceu uma nova realidade, a que todas as empresas brasileiras devem se submeter para o armazenamento e para a utilização dos dados pessoais dos seus clientes.

Numa época em que a economia e a vida das pessoas estão cadenciadas pela velocidade do mundo digital, o tratamento de dados é crucial para a tomada de decisão das empresas, por ser capaz de aumentar a eficiência desde a concepção dos produtos até a sua venda.

O tratamento dos dados pessoais está na base do desenvolvimento da Indústria 4.0, nome conferido à quarta revolução industrial, que tem como pilar a digitalização de processos, da produção e dos produtos. Com a utilização apropriada das informações, as empresas podem elevar a produtividade, diminuir os custos de produção e aperfeiçoar a segurança.

Assim, a LGPD se revela fundamental para disciplinar o uso dos dados pessoais com transparência e respeito à liberdade e à privacidade dos indivíduos, trazendo segurança jurídica e reduzindo a possibilidade de conflitos.

Certamente, as empresas precisam adaptar os seus modelos de gestão ao imenso volume de informações e à incalculável velocidade com que são geradas em tempo real. Isso demanda investimentos e uma mudança de cultura.

Ciente desse desafio e da importância do tema, que tem inevitável impacto no cotidiano empresarial, a Confederação Nacional da Indústria (CNI) produziu este *Guia de Boas Práticas*, cujo propósito é auxiliar nos processos de adequação à LGPD e no desenvolvimento da governança.

Dessa forma, pretendemos contribuir com a implementação de programas efetivos de governança no que diz respeito à privacidade de dados pessoais pela indústria brasileira, o que é essencial para o crescimento econômico nessa nova era da informação.

Boa leitura.

Robson Braga de Andrade
Presidente da CNI

PARTE 1

1 CONSIDERAÇÕES INICIAIS

A Confederação Nacional da Indústria (CNI) exerce grande papel na economia do Brasil. Dentre seus objetivos, destaca-se a representação, a defesa e a coordenação dos interesses gerais da indústria, contribuindo, direta ou indiretamente, para fomentar a expansão, a competitividade do setor industrial e o desenvolvimento econômico e social do país.

A atuação da CNI tem sido fundamental, também, para estimular a competitividade e a adoção de soluções inovadoras tecnológicas que se inserem no contexto da Quarta Revolução Industrial, além de auxiliar o setor público na formulação de políticas públicas. Em fevereiro de 2022, foi publicada uma edição da **Revista da Confederação Nacional da Indústria** voltada para a discussão das inovações que foram aplicadas aos processos produtivos.

Nesta edição, foram abordados temas, como a mudança estimulada pelo gerenciamento das ondas da pandemia, sendo ressaltado pelo presidente que, "*neste momento, em pequenas startups, empresas e centros de pesquisa brasileiros, surgem inovações que, talvez, alterem profundamente produtos e processos produtivos de importantes setores nos próximos anos*". Ademais, conforme pontuado pelo diretor de Educação e Tecnologia da CNI, Rafael Lucchesi, *"o grande desafio é, de fato, construir políticas integradas que alavanquem o desenvolvimento do país e, é claro, fortalecer a indústria, tornando-a mais produtiva e competitiva"*[1].

Nesse contexto de constante inovação e transformação digital da indústria brasileira, este **Guia de Boas Práticas de Proteção de Dados para a Indústria** insere-se.

Trata-se de iniciativa da CNI que tem como objetivo auxiliar os processos de adequação da indústria à Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/2018) e de desenvolver boas práticas de governança, nos termos art. 50 da LGPD, que possibilitem o setor a manter seu papel de liderança no desenvolvimento da indústria. Assim, este guia irá explorar as especificidades das operações de tratamento de dados realizada pelo setor em três partes.

1 CNI. **Revista Indústria Brasileira**, Brasília, v. 7, n. 63, p. 8, fev. 2022. Disponível em: https://jornalismo.portaldaindustria.com.br/cni/revista_industria/revista-industria-brasileira-02-2022/8/. Acesso em: 30 jun. 2023.

A primeira parte dedica-se à descrição dos principais conceitos e fundamentos da LGPD e a sua aplicação nos processos da indústria. Também são detalhados os processos da indústria submetidos à LGPD, os tipos de dados utilizados pelo setor e o âmbito de aplicação do guia.

A segunda parte destina-se ao desenvolvimento de protocolos gerais para as principais etapas das operações de tratamento, como o tratamento de dados na gestão de pessoas e para a realização de *marketing*. Ademais, também são apresentados os seguintes protocolos: i) implementação de uma cultura de proteção de dados; ii) garantia do direito dos titulares; iii) armazenamento e eliminação de dados; iv) elaboração de relatório de impacto; v) segurança da informação; vi) elaboração de acordos entre agentes de tratamento; e vii) transferência internacional de dados.

Já a terceira parte é dedicada ao desenvolvimento de protocolos específicos do setor, sendo abordadas as especificidades das micro e pequenas empresas (MPEs) e o desenvolvimento de novas tecnologias. Ao final, buscamos esclarecer a função e a importância do **Guia de Boas Práticas de Proteção de Dados para a Indústria**, auxiliando o processo de desenvolvimento tecnológico da indústria e garantindo que os direitos dos titulares e as garantias sejam respeitados e protegidos.

1.1 ASPECTOS POSITIVOS DO CUMPRIMENTO DA LGPD

Na sociedade movida a dados, estes são ativos fundamentais de qualquer negócio e indústria. Nesse contexto, a Lei Geral de Proteção de Dados Pessoais tem como objetivo estabelecer parâmetros mínimos para coleta, uso e compartilhamento de dados, trazendo segurança jurídica para as empresas e proteção da liberdade e da personalidade do titular de dados. A lei pode ser vista não como uma proibição *a priori* para o tratamento de dados, mas como norma que visa viabilizar o fluxo de dados na sociedade à luz de critérios de segurança da informação, transparência e controle.

Além da evidente preocupação dos agentes do mercado com a possibilidade de serem penalizados em caso de descumprimento com a legislação, a criação de uma política de *compliance*[2] de dados tem diversos benefícios para as empresas, como a mitigação de riscos de vazamento de dados e a ocorrência de outros tipos de incidentes de segurança, além da maior exposição a processos judiciais e de riscos reputacionais.

2 Trata-se da "adoção de práticas organizacionais voltadas para a criação de processos e de ambiente corporativo que assegure o cumprimento de normas legais". ABRAPP. **Código de autorregulação em governança corporativa**. 2019. Disponível em: https://www.abrapp.org.br/wp-content/uploads/2021/01/manualautorregulacaocorporativa.pdf. Acesso em: 29 jun. 2023.

De acordo com o *Data Privacy Benchmark Study* 2020 publicado pela Cisco[3], é possível traçar uma correlação entre a implementação da *accountability*[4] na organização e a redução do número de incidentes de segurança e diminuição dos atrasos nas vendas. O mesmo estudo constatou que mais de 40% das organizações internacionais percebem o dobro de retorno do que foi gasto para implementação de programas de privacidade e proteção de dados pessoais.

Como se observa, os benefícios da legislação não se restringem à mitigação de riscos, podendo ser mencionada a possibilidade de obtenção de retornos positivos com a implementação de uma política de proteção de dados. Constata-se que as boas práticas no tratamento de dados podem gerar ganhos de reputação, competitividade e, até mesmo, retornos financeiros[5].

BENEFÍCIOS OBTIDOS POR EMPRESAS QUE IMPLEMENTAM PROGRAMAS DE GOVERNANÇA DE DADOS (CEDIS/IDP E CIPL)[6]

- Auxilia no cumprimento das exigências legais e regulamentares.
- Proporciona melhor organização dos processos de trabalho das empresas envolvendo dados pessoais.
- Auxilia a criação de uma cultura de proteção de dados e privacidade nas corporações.
- Auxilia as empresas a criar uma relação de fidelização e confiança com clientes, que se sentirão mais seguros com seus dados protegidos.
- Amplia as oportunidades de negócios que envolvem dados pessoais e exigem a adoção de medidas de *compliance* de dados.
- Aumenta a confiança com *stakeholders*, ex.: mídia, investidores, reguladores, clientes e funcionários.
- Aumenta a competitividade e criação de diferencial da empresa que investe em proteção de dados.
- Mitiga risco sancionatório e reduz o impacto financeiro das sanções por conta dos esforços de adequação da empresa.

Por fim, a criação de um programa de *compliance* de dados possui evidente benefício na redução do risco de aplicação das penalidades previstas na LGPD, art. 52, sendo mencionadas as possibilidades de advertência, aplicação de multa de até 50 milhões de reais por infração ou mesmo a suspensão parcial ou total das atividades que envolvem o tratamento de dados:

3 CISCO. **2020 Data Privacy Benchmark Study**. Disponível em: https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html. Acesso em: 29 jun. 2023.

4 O termo *accountability* traduz-se em dever fiduciário e, por vezes, em prestação de contas no português. "O dever fiduciário encontra-se no cerne da governança, uma vez que contempla a relação entre o proprietário e o administrador, a quem foi delegado o poder decisório e de gestão de seu patrimônio. A delegação desse poder carrega intrinsecamente a obrigação de sua prestação de contas". Já o conceito de prestação de contas "significa explicar regularmente, qualitativamente e quantitativamente o que foi feito, como e por qual motivo se fez e o que vai ser feito a seguir; bem como justificar aquilo em que se falhou ou deixou de se fazer". ABRAPP. **Código de autorregulação em governança corporativa**. 2019. Disponível em: https://www.abrapp.org.br/wp-content/uploads/2021/01/manualautorregulacaocorporativa.pdf. Acesso em: 29 jun. 2023.

5 IBM. **Why data privacy is much more than compliance**. 2023. Disponível em: https://www.ibm.com/security/digital-assets/data-privacy-matters/. Acesso em: 29 jun. 2023.

6 CIPL; CEDIS/IDP. **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)**. Acesso em: https://www.idp.edu.br/projeto-lgpd. Acesso em: 29 jun. 2023.

PENALIDADES APLICÁVEIS

- **Advertência** com indicação de prazo para adoção de medidas corretivas.
- **Multa simples e multa diária,** observando o limite de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.
- **Publicização da infração** após devidamente apurada e confirmada sua ocorrência.
- **Bloqueio dos dados pessoais** a que se refere a infração até sua regularização.
- **Eliminação dos dados pessoais** a que se refere a infração.
- **Suspensão parcial do funcionamento do banco de dados ou do exercício da atividade de tratamento dos dados pessoais** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período.
- **Proibição parcial ou total do exercício de atividades** relacionadas a tratamento de dados.

2 GLOSSÁRIO

Agentes de tratamento: o controlador e o operador.

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.

Aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

B2B (*business-to-business*): relações entre empresa e empresa.

B2C (*business-to-consumer*): relações entre empresa e consumidor.

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

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

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

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

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

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

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.

Dado pseudonimizado: dado relativo a titular que não possa ser identificado, a não ser pelo uso de informação adicional.

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).

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

Internet: sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.

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

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação mantida separadamente pelo controlador em ambiente controlado e seguro.

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.

Serviço de nuvem (*cloud*): modelo de armazenamento de dados na internet que utiliza um provedor de computação na nuvem para gerenciar as informações.

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

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

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.

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.

3 PRINCIPAIS CONCEITOS E FUNDAMENTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

3.1 O QUE É UM DADO PESSOAL?

Dados pessoais são as informações relacionadas a uma pessoa física que permitem sua identificação (art. 5º, I, da LGPD). Ou seja, ainda que um dado sobre uma pessoa não relacione diretamente o nome dela, ele pode ser considerado um dado pessoal caso ele a torne identificável, uma vez que a legislação traz um conceito amplo para tratar de dados que podem ser relacionados a uma pessoa. Por exemplo, o número do CPF não precisa ser acompanhado do nome do titular para que essa informação seja relacionada a uma pessoa específica ou, então, o *e-mail* de um titular pode ser suficiente para permitir sua identificação.

O mesmo não pode ser dito, por exemplo, sobre a informação acerca da cor de cabelo de um titular. Se, por um lado, em um cadastro, consta apenas pessoa morena brasileira, essa informação isoladamente não permite a identificação do titular de dados, não sendo considerada um dado pessoal. Por outro lado, se a informação for mulher, morena, brasileira, nascida e residente em Brasília, com endereço em SQS 809, Bloco J, apartamento 999, ela pode ser relacionada a uma pessoa específica, podendo ser considerado um dado pessoal, por conta da identificabilidade.

Nesse sentido, o que se conclui a partir do conceito de dados pessoais da legislação é que todas as principais áreas das empresas tratam dados pessoais, seja nos contratos com fornecedores e clientes ou mesmo na gestão de pessoas. Também, no *marketing*, os dados pessoais são extremamente importantes na análise comportamental.

A depender do risco que essas informações podem representar para os direitos do titular, bem como do seu potencial discriminatório, elas podem ser categorizadas como dados pessoais sensíveis.

De acordo com o art. 5º, II, da LGPD, os dados pessoais sensíveis são aqueles "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".

Tendo em vista as especificidades desse tipo de dado pessoal e a necessidade de cuidado adicional para seu tratamento, foram definidas bases legais diferenciadas para o seu tratamento, conforme se verá no próximo item.

3.2 O QUE É UM TRATAMENTO DE DADOS?

O tratamento de dados pessoais envolve todas as operações que dizem respeito a dados pessoais, compreendendo 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*" (art. 5ª, X, da LGPD, grifo nosso). Apesar de as discussões sobre proteção de dados terem sido amplamente difundidas por conta das inovações tecnológicas, o tratamento de dados pode ser feito tanto em meios físicos quanto digitais, não sendo necessária a utilização de tecnologias para esse fim.

Tal fato decorre da amplitude do conceito de tratamento de dados presente na legislação de proteção de dados brasileira. Por exemplo, um dado pessoal – como uma ficha cadastral de um titular – pode ser elaborado por meio do preenchimento de uma folha de papel, sendo utilizada por meio da consulta das informações que nela constam e posteriormente armazenada em um arquivo físico. O fato de não existir qualquer processo digital não impede que esse tipo de processamento do dado se enquadre perfeitamente na definição legislativa.

Não à toa, a própria LGPD reconhece a possibilidade de um banco de dados ser físico, na medida em que a sua definição no art. 5º, IV, trata de "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, *em suporte eletrônico ou físico*" (grifo nosso).

O reconhecimento da existência de operações de tratamento de dados pessoais é importante para que o agente de tratamento possa adotar as medidas necessárias para assegurar o cumprimento da LGPD. Isso porque a lei se aplica "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado" (art. 3º, *caput*, da LGPD).

Assim, o simples armazenamento de um dado pessoal, como um *e-mail*, nome ou CPF, já torna necessário o cumprimento da legislação de proteção de dados brasileira.

Dois conceitos centrais que atraem a aplicação da LGPD são exatamente o conceito de dado pessoal e o conceito de tratamento, isto é, sempre que houver a coleta, o uso, a transferência ou qualquer outro ato envolvendo um dado de uma pessoa natural que possa identificá-la, esse ato está sujeito à lei e precisa seguir seus preceitos.

3.3 CONDIÇÕES DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS

A LGPD estabelece um sistema que ampara os dados pessoais dos titulares em sua completude e regula o fluxo de dados pessoais. A legislação representou verdadeira inovação no ordenamento jurídico brasileiro, ao estabelecer um regime geral de proteção de dados com requisitos específicos de legitimidade para o tratamento de dados, tanto por meio de seus princípios, quanto a partir das bases legais, que não se restringem à simples coleta de consentimento do titular.

Isso significa que qualquer tratamento de dados precisa estar amparado em uma das bases legais dos artigos 7º ou 11 da LGPD, conforme será detalhado adiante, e, ainda, estar de acordo com os princípios previstos no art. 6º da LGPD.

PRINCÍPIOS DA LGPD (art. 6º da LGPD)

BOA-FÉ OBJETIVA (art. 6º, *caput*, da LGPD)
O tratamento de dados deve ser pautado nos ditames éticos e morais.

FINALIDADE (art. 6º, I, da LGPD)
O tratamento deve ter como finalidade propósitos legítimos, específicos e explícitos em toda a sua duração. Caso a finalidade se altere ao longo do processo, esta não pode ser incompatível com essas finalidades.

ADEQUAÇÃO (art. 6º, II, da LGPD)
O tratamento deve ser compatível com as finalidades informadas ao titular.

NECESSIDADE (art. 6º, III, da LGPD)
O tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

LIVRE ACESSO (art. 6º, IV, da LGPD)
Os titulares dos dados devem poder consultar, gratuitamente, a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.

QUALIDADE DOS DADOS (art. 6º, V, da LGPD)
Os dados dos titulares devem ser exatos, claros, relevantes e atualizados.

TRANSPARÊNCIA (art. 6º, VI, da LGPD)
Devem ser disponibilizadas aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

SEGURANÇA (art. 6º, VII, da LGPD)
Os dados pessoais devem ser protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão por meio de medidas técnicas e administrativas.

PREVENÇÃO (art. 6º, VIII, da LGPD)
É necessária adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

NÃO DISCRIMINAÇÃO (art. 6º, IX, da LGPD)
O tratamento de dados não deve ser realizado para fins discriminatórios ilícitos ou abusivos.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS (art. 6º, X, da LGPD)
O agente deve adotar medidas eficazes e deve ser capaz de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os princípios da legislação são fundamentais, uma vez que devem nortear todos os processos de tratamento de dados ao longo de todo o tratamento. Assim, antes mesmo de iniciar uma operação envolvendo dados pessoais, o agente de tratamento de dados deve levar em consideração algumas questões, como, por exemplo:

- Todos os dados pessoais que irei coletar são necessários para a minha operação?
- Eu irei violar algum direito do titular com a minha operação de tratamento de dados?
- O titular foi informado sobre os usos que farei dos dados?
- Eu consigo possibilitar o acesso do titular a informações sobre seus dados pessoais?
- Onde e como irei guardar os dados?
- Os dados que estou tratando estão seguros?
- A finalidade que eu inicialmente estabeleci foi finalizada? Eu, ainda, preciso de todos os dados que coletei inicialmente?
- A finalidade inicial alterou-se ao longo do tratamento?

A partir da reflexão sobre a forma como os dados são tratados, transparência conferida aos processos, expectativa dos titulares e medidas de segurança adotadas, os agentes de tratamento de dados podem garantir a sua conformidade com os princípios da legislação. Mesmo que o tratamento de dados seja necessário para novas finalidades, é necessário que ele seja feito para propósitos legítimos e que os direitos do titular sejam preservados (art. 7º, § 7º, da LGPD).

Além dos princípios, de acordo com a LGPD, todo tratamento de dados pessoais deve estar amparado por uma das bases legais presentes em seus artigos 7º e 11 da LGPD [7]. Em relação ao tratamento de dados pessoais comuns, têm-se como bases legais as seguintes:

BASES LEGAIS (art. 7º da LGPD)

- **Consentimento** (inciso I).
- **Cumprimento de obrigação legal ou regulatória pelo controlador** (inciso II) – essa base legal não se restringe às obrigações que decorrem de leis federais, estaduais e municipais, abarcando obrigações decorrentes de atos infralegais, tais como decretos, portaria, instruções normativas, entre outros.
- **Execução de políticas públicas pela Administração Pública** (inciso III).
- **Realização de estudos por órgão de pesquisa** (inciso IV).
- **Execução de contrato** (inciso V) – o titular deve fazer parte do contrato.
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral** (inciso VI).
- **Proteção da vida ou da incolumidade física do titular ou de terceiros** (inciso VII).
- **Tutela da saúde** (inciso VIII) – deve ser realizada por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- **Legítimo interesse** (inciso IX) – não pode ser aplicada quando prevalecerem direitos e liberdades fundamentais do titular, tais como: o direito à vida, à igualdade, à dignidade – que exijam a proteção dos dados pessoais.
- **Proteção do crédito** (inciso X).

7 SCHERTEL, Laura. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama Setorial da Internet**, v. 11, n. 2, jun. 2019.

É fundamental destacar que não há hierarquia entre as bases legais e que, portanto, o consentimento deve ser utilizado apenas quando as condições específicas do tratamento de dados indicarem que ele é a base mais adequada, conforme será discutido em detalhes no próximo item. O agente de tratamento deve escolher a base legal mais adequada para cada operação de tratamento realizada pela organização, sem esvaziamento de nenhuma das bases legais.

Ademais, conforme mencionado, a LGPD estabelece um nível de proteção maior para os dados sensíveis, tendo em vista a gravidade das consequências negativas do mau uso de tais informações. Assim, no artigo 11 da LGPD, são elencadas as bases legais que podem ser utilizadas para tratamentos envolvendo **dados sensíveis**, que apresentam algumas diferenças das bases previstas no artigo 7º, em especial, a impossibilidade de utilização da base legal do legítimo interesse e da execução contratual, quando esta não estiver vinculada ao exercício de direitos.

BASES LEGAIS DADOS SENSÍVEIS (art. 11 da LGPD)

Diferentemente do tratamento de dados comuns, os dados sensíveis possuem duas hipóteses: **coleta de consentimento específico e destacado** (inciso I) OU quando o **dado for indispensável para** (inciso II):

- **Cumprimento de obrigação legal ou regulatória pelo controlador** (alínea a).
- **Execução de políticas públicas pela Administração Pública** (alínea b).
- **Realização de estudos por órgão de pesquisa** (alínea c).
- **Exercício regular de direitos em contrato, processo judicial, administrativo ou arbitral** (alínea d).
- **Proteção da vida ou da incolumidade física do titular ou de terceiros** (alínea e).
- **Tutela da saúde** (alínea f) – deve ser realizada por profissionais de saúde, serviços de saúde ou autoridade sanitária.
- **Prevenção à fraude e à segurança do titular** (alínea g).

Exemplo 1 – "Execução do contrato" e "Exercício regular de direito"

A base legal da execução do contrato pode ser utilizada para realização de cobrança de faturas vencidas de compradores. Por meio dessa base legal, o agente de tratamento pode utilizar dados pessoais do usuário (como endereço e telefone) para garantir, por exemplo, que os produtos que determinado consumidor comprou *on-line* cheguem até a sua residência[8]. Nessa hipótese, não seria possível garantir a execução do contrato sem que o endereço do titular do próprio contrato fosse utilizado. Caso o titular tenha optado pela retirada do produto diretamente na loja, contudo, a base legal da execução contratual não poderia ser utilizada, tendo em vista que o endereço não é estritamente necessário para a execução do contrato.

A avaliação da necessidade deve ser interpretada à luz das expectativas do titular e não ampara hipóteses nas quais o controlador trata os dados do titular apenas em benefício próprio.

Em outra hipótese, caso haja o inadimplemento das parcelas e seja necessária a judicialização do pagamento, a base legal mais adequada para o tratamento de dados para essa finalidade seria "o exercício regular de direitos" e não "a execução do contrato". Tal fato decorre da existência de base legal específica para que hipóteses nas quais, por exemplo, o contrato foi encerrado ou que o exercício de direitos do controlador dos dados – em um processo judicial, por exemplo – acabe excedendo a expectativa do titular dos dados.

8 EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. p. 10 – 11**. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf. Acesso em: 30 jun. 2023.

Exemplo 2 – "Cumprimento de obrigação legal e regulatória"

A base legal do cumprimento de obrigação legal e regulatória pode amparar o compartilhamento de dados pessoais com autoridades competentes, como a receita federal, desde que exista obrigação legal ou regulatória específica.

No caso da gestão de informações sobre trabalhadores, por exemplo, de acordo com a Consolidação das Leis do Trabalho (CLT), art. 11, o trabalhador tem 2 (dois) anos, após a rescisão do contrato, para ajuizar reclamação trabalhista. Assim, durante esse prazo, o empregador não deve excluir os documentos dos funcionários para possibilitar sua defesa em juízo e eventual pedido de informações no bojo do processo. Mesmo que não seja ajuizada nenhuma ação trabalhista, dados, como contrato de trabalho e fichas de registro que comprovam o vínculo trabalhista, podem ter prazo de tratamento ainda maior, uma vez que também são importantes para cumprimento de obrigações tributárias e previdenciárias.

Exemplo 3 – "Garantia da prevenção à fraude e à segurança do titular"

A base legal da "garantia da prevenção à fraude e à segurança do titular" pode ser empregada em hipóteses, como controle de acesso de terceiros às dependências das empresas ou em setores que possam apresentar alto nível de periculosidade. Ademais, ela também pode subsidiar outras medidas de controle de acesso aos dados pessoais dos titulares por meio da utilização de sistemas de segurança.

Destaca-se que o enquadramento legal de determinado tratamento de dados pessoais a uma das bases do art. 7º da LGPD não isenta o agente do cumprimento das demais normas da lei. Em verdade, esse enquadramento é uma das condições de legitimidade que não exclui a adequação aos princípios da lei e nem o cumprimento dos direitos do titular ou das obrigações dos agentes de tratamento. Deve-se ter especial atenção aos princípios da finalidade, necessidade e adequação, uma vez que independentemente da existência de contrato ou obrigação legal, o tratamento de dados deve ser realizado quando os dados forem pertinentes, adequados e compatíveis aos fins para os quais foram coletados.

Ademais, recursos como pseudonimização e anonimização devem ser utilizados sempre que possível para proteção dos dados, especialmente após transcurso de longo período de armazenamento.

3.4 DESAFIOS PARA A ESCOLHA DA BASE LEGAL

Para que esta base legal seja considerada válida, o consentimento deve ser a "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*" (art. 5°, XII, da LGPD, grifo nosso).

Para compreendermos o significado dos atributos **livre, informado, inequívoco e para finalidade determinada**, utilizaremos o guia do Comitê Europeu para a Proteção de Dados (EDPB, do inglês *European Data Protection Board*) sobre a utilização dessa base legal[9].

9 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679**. 2020. p. 7-20. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 30 jun. 2023.

De acordo com o órgão europeu, a manifestação **livre** não será aplicável quando existirem condições não negociáveis nos termos e condições, bem como nas hipóteses que o consentimento não puder ser retirado. Entre as condições que devem ser avaliadas em relação à "liberdade" do consentimento estão:

- Desequilíbrio de poder entre as partes – ex.: relação entre regulador e regulado, relações trabalhistas, etc.
- Condicionamento do consentimento a aspectos centrais dos termos do contrato e não execução do contrato em caso de ausência de consentimento – em um contrato de prestação de serviços, por exemplo, é possível solicitar o consentimento para utilização da imagem do titular. Caso ele possa não concordar com a cláusula e o contrato seja executado normalmente, o consentimento pode ser considerado livre.

A **informação** relaciona-se ao princípio da transparência e consiste no fornecimento de informações para o titular antes da coleta do consentimento. Essa medida visa garantir que o titular tenha real escolha e compreenda as consequências dela. Assim, de acordo com o EDPB, algumas informações devem ser apresentadas para possibilitar que a manifestação seja informada[10]:

- Identidade do controlador.
- Finalidade das operações de tratamento para as quais o consentimento é solicitado.
- Tipo de dado que será coletado e tratado.
- Informações sobre a retirada do consentimento.
- Informações sobre a tomada de decisões automatizadas.

Em conjunto com a disponibilização de informações, a garantia de manifestação **inequívoca** pode ser obtida por meio de algumas técnicas que permitem que o usuário participe ativamente do processo de tomada de decisão. Por exemplo, em meios eletrônicos, a utilização de caixas de opção pré-preenchidas pode tornar o consentimento invalidado, uma vez que não fica clara se essa foi efetivamente uma manifestação do usuário ou resultado de sua passividade.

Por fim, com relação à **especificidade da finalidade** para a qual o consentimento foi concedido, os agentes de tratamento devem ter especial atenção quando o dado for tratado para mais de uma finalidade. Isso porque o titular deve poder escolher entre as finalidades e a informação sobre cada uma delas deve ser clara.

Importa ressaltar, ainda, que o consentimento é a base legal mais *célebre* da LGPD, levando à falsa impressão de que ela seria a mais importante. A legislação de proteção de dados

10 EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679**. 2020. p. 15. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 30 jun. 2023.

não criou uma hierarquia entre as bases legais, sendo o consentimento uma base tão importante e legítima quanto as demais.

Além de sua definição legal, o consentimento possui algumas especificidades que devem ser consideradas para que a sua utilização seja adequada:

- Oferecer uma escolha real, devendo constar de cláusula destacada das demais cláusulas contratuais caso seja fornecido por escrito (art. 8º, §1º, da LGPD).
- Possibilitar que o titular possa retirar o consentimento quando bem entender; caso não seja possível, o consentimento não é a base legal adequada (art. 8º, §5º, da LGPD).
- Controlador deve comprovar que o consentimento foi obtido de forma adequada (art. 8º, §2º, da LGPD).
- Ser fornecido para finalidades determinadas, não sendo permitida a utilização de autorizações genéricas (art. 8º, §4º, da LGPD).
- Caso o controlador necessite compartilhar os dados com outros controladores, é necessária a coleta de consentimento específico para este fim (art. 7º, §5º, da LGPD).
- Garantir que o titular possa receber uma cópia integral de seus dados pessoais em formato que permita sua utilização subsequente, nos termos a serem regulamentados pela ANPD e desde que sejam respeitados os segredos comercial e industrial (art. 19, §3º, da LGPD).

Assim, não obstante seu papel de destaque nas discussões sobre proteção de dados pessoais, a utilização do consentimento deve preencher as condições de legitimidade de seu tratamento.

3.5 BASES LEGADAS

As bases legadas referem-se aos dados pessoais que foram coletados antes da entrada em vigor da LGPD e, portanto, não estavam vinculadas às condições de legitimidade para o tratamento de dados à época. Nesse sentido, o art. 63 da LGPD prevê que: "a autoridade nacional *estabelecerá normas sobre a adequação progressiva de bancos de dados* constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados" (grifo nosso).

Não obstante a existência dessa previsão legal, até o momento, a ANPD não disponibilizou as regras sobre a adequação das bases legadas, existindo grande dúvida em relação à forma como devem ser tratadas as bases de dados anteriores à entrada em vigor da LGPD. Assim, ainda que não seja necessário excluir todos os dados coletados antes da nova legislação, recomenda-se que as empresas já iniciem o processo de adequação à LGPD, em especial avaliando quais dados ainda são necessários e quais podem ser descartados.

Essa avaliação deve ser feita levando em consideração o princípio da necessidade, que se refere à realização de tratamento de dados observando somente os dados estritamente necessários àquela operação.

Outro aspecto que as empresas podem considerar é que o diploma europeu (*General Data Protection Regulation* – GDPR) dispensa a nova obtenção de consentimento, quando este já tiver sido coletado considerando os requisitos da legislação, ou seja, quando os dados tiverem sido coletados antes do GDPR e o consentimento estiver de acordo com o conceito do regulamento, como uma "manifestação de vontade, livre, específica, informada e explícita" (art. 4(11) do GDPR).

Assim, tendo em vista a inexistência de manifestação da ANPD, sugerimos que as empresas adequem as bases de dados legadas à nova legislação, considerando, inicialmente, os seguintes aspectos:

- Localizar *backups* e servidores antigos para identificação das bases.
- Avaliar as dificuldades operacionais existentes para o mapeamento dessas bases legadas.
- Verificar se os dados pessoais coletados no passado ainda são necessários e excluir aqueles que não são.
- Avaliar se os dados pessoais armazenados estão atualizados e solicitar novos dados ou excluir aqueles que não estão (princípio da qualidade dos dados).
- Fazer uma análise sobre quais dados compõem as bases antigas e avaliar qual base legal seria necessária para tratá-los à luz da LGPD.
- Caso o consentimento tenha sido coletado, verificar se ele atende às condições de validade da LGPD.

4 LEI GERAL DE PROTEÇÃO DE DADOS APLICADA À INDÚSTRIA

4.1 PROCESSOS DA INDÚSTRIA SUBMETIDOS À LGPD

Conforme demonstrado anteriormente, a LGPD não tem como objetivo impossibilitar o tratamento de dados pelos agentes econômicos, tampouco impede a realização de negócios que envolvam dados pessoais. A legislação cria condições de legitimidade para o tratamento – a exemplo do enquadramento do tratamento nas bases legais e a avaliação de princípios, como a finalidade – e confere maior segurança para o titular, mas não proíbe que, por exemplo, contratos envolvendo dados pessoais sejam firmados.

O tratamento de dados realizado pela indústria possui importante peculiaridade, tendo em vista que grande parte das operações não são realizadas entre empresa e consumidor – *business-to-consumer* (B2C) – e, sim, entre empresas, no chamado *business-to-business* (B2B). Enquanto as atividades B2C envolvem uma quantidade maior de dados de consumidores, especialmente aquelas que utilizam comércio eletrônico e que possuem estratégias de captação de clientes por meio de *marketing* digital, as atividades B2B nem sempre envolvem dados de pessoa natural, pois lidam, na maioria das vezes, com dados de pessoas jurídicas, não abrangidos pela LGPD.

As atividades B2C possuem uma complexidade adicional, tendo em vista que, além da legislação de proteção de dados, é necessário assegurar o cumprimento de normas que dialogam com a LGPD, como o Código de Defesa do Consumidor (CDC). Tais obrigações, por vezes, entrelaçam-se com os direitos do titular, como é a necessidade de implementação de canais de atendimento ao consumidor e a existência de princípios como da transparência e da boa-fé.

Ainda assim, fato é que tanto as operações de tratamento realizadas B2C quanto as realizadas B2B utilizam dados pessoais em suas atividades cotidianas, seja na gestão de pessoas ou no controle de acesso nas dependências físicas das empresas. Também é necessário considerar que, com a rápida evolução digital, mesmo que determinados

processos não utilizem dados pessoais, é possível que eles passem a utilizar, especialmente com a evolução de tecnologias da Indústria 4.0, como a inteligência artificial (IA) e a internet das coisas (IoT).

A Indústria 4.0 representa uma revolução na forma como os produtos são elaborados, fabricados, desenvolvidos e distribuídos. Os processos produtivos passam a contar com tecnologias de ponta que aumentam a automação e otimizam os processos com a utilização de tecnologia, sendo utilizadas, até mesmo, fábricas inteligentes que realizam o desenvolvimento de produtos com tecnologia de ponta.[11]

Nesse contexto, a utilização de dados é essencial para possibilitar a predição de processos, a otimização e a compreensão detalhada da produção de bens mais eficientes. Além disso, os dados também são centrais na criação de novos produtos e expansão para novos mercados.

Ademais, a Indústria 4.0 é uma realidade que envolve tanto processos tecnológicos – que envolvem dados pessoais –, quanto aqueles que não precisam dessas informações para seu desenvolvimento. Assim, compreender quais cuidados devem ser tomados em cada um dos processos de desenvolvimento é essencial para evitar gastos desnecessários ou incidentes indesejáveis.

Nesse sentido, ressalta-se a necessidade de observar os segredos comercial e industrial na LGPD, mencionados em diversos dispositivos da lei, como no princípio da transparência (art. 6º, VI), direito de acesso (art. 9º, II, e art. 19, II, §3º), a apresentação de relatório de impacto à ANPD (art. 10º, §3º e 38), a portabilidade de dados (art. 18, V), tratamento automatizado de dados (art. 20, §§1º e 2º), comunicação sobre incidentes de segurança (48, §1º, III).

Ademais, a legislação também atribui à ANPD a obrigação de zelar pela preservação do segredo comercial e industrial (art. 55-J, II, X, §5º). Nesse contexto, considera-se relevante que a ANPD se manifeste, em momento oportuno, em relação à interpretação dos dispositivos que tratam do segredo comercial e industrial.

4.2 TIPOS DE DADOS TRATADOS PELA INDÚSTRIA

As operações de tratamento de dados pessoais realizadas pela indústria são extremamente diversas e envolvem um conjunto variado de dados pessoais. São tratados tanto dados pessoais comuns quanto sensíveis, a depender da finalidade almejada. Também são tratados

11 IBM. **What is industry 4.0?** 2023. Disponível em: https://www.ibm.com/topics/industry-4-0. Acesso em: 30 jun. 2023.

dados que podem não identificar uma pessoa natural quando avaliado isoladamente, mas, no contexto das bases de dados da empresa, passem a identificar um indivíduo específico.

Além disso, cada organização trata os dados por diferentes setores internos ou empresas subcontratadas, justamente considerando as diferentes finalidades dos tratamentos de dados. Dessa forma, é comum que as seguintes operações de tratamento sejam realizadas por cada setor das entidades da indústria.

RECURSOS HUMANOS

- **Dados utilizados**: nome, RG, CPF, data de nascimento, sexo, estado civil, endereço, título de eleitor, fotos, currículos, telefone, *e-mail*, cópia de documentos, carteira de trabalho, informações sobre cônjuge, informações sobre filhos, dados bancários, folha de ponto, etc.
- **Dados sensíveis**: dados sobre filiação sindical, exames ocupacionais, atestados médicos, informações sobre origem racial, informações sobre Pessoa com Deficiência (PcD); impressão digital, biometria facial, carteira de vacinação, etc.
- **Operações de tratamento de dados**:
  - Análise de currículos para seleção de novos colaboradores.
  - Análise de exame admissional e demissional com dados de saúde.
  - Compartilhamento de dados no eSocial – sistema da Administração Pública que centraliza o envio de informações fiscais, previdenciárias e trabalhistas das empresas.
  - Utilização de dados cadastrais e histórico de funcionários para defesa em processos judiciais e administrativos.
  - Registro de posição na carteira de trabalho do(a) colaborador(a).
  - Levantamento de informações sobre PcD para reforma de estrutura física da empresa.
  - Controle de ponto por meio de impressão digital ou reconhecimento facial.
  - Controle de acesso de áreas autorizadas por meio de impressão digital ou reconhecimento facial.
  - Cadastro de dados de saúde no ambulatório.
  - Inclusão do(a) cônjuge e dos(as) filhos(as) do(a) colaborador(a) no plano de saúde da empresa.
  - Utilização de sistema para gerenciamento de folha de pagamento.
  - Realização de políticas afirmativas, etc.

CONTRATAÇÃO DE FORNECEDORES

- **Dados utilizados**: nome, RG, CPF, data de nascimento, estado civil, endereço, informações de empresário individual (EI) e microempreendedor individual (MEI), certidão Nada Consta de antecedentes criminais, processos judiciais, localização de GPS, etc.
- **Operações de tratamento de dados**:
  - Análise de histórico de EI e MEI em procedimentos pré-contratuais.
  - Seleção de fornecedores.
  - Elaboração de contratos.
  - Realização de auditoria em processos de *compliance*.
  - Acompanhamento da rota do fornecedor por meio de tecnologias de localização, etc.

AÇÕES DE *MARKETING*

- **Dados utilizados**: nome, *e-mail*, telefone, idade, informações comportamentais, hábitos de consumo, histórico de navegação da internet, endereço de IP, etc.
- **Operações de tratamento de dados**:
  - Disparo de *e-mails* com conteúdo de *marketing* para lista de *e-mail*s.
  - Envio de SMS com conteúdo de *marketing*.
  - Realização de ligações telefônicas para oferta de produtos ou serviços.
  - Direcionamento de publicidade com base em hábitos de consumo, localização, idade, etc.
  - Elaboração de estratégias de publicidade com base em comportamentos de consumo.
  - Realização de pesquisas com grupos de controle para testagem de novos produtos, etc.

SEGURANÇA

- **Dados utilizados**: dados cadastrais, *e-mail*, foto, imagens de câmera de segurança, etc.
- **Dados sensíveis**: dados biométricos, etc.
- **Operações de tratamento de dados**:
  - Controle de entrada com a utilização de biometria.
  - Coleta de foto em cadastro de visitantes de prédios comerciais.
  - Controle de acesso para salas com informações sensíveis ou bens valiosos.
  - Videovigilância dos estabelecimentos das empresas, etc.

5 ÂMBITO DE APLICAÇÃO DO GUIA

Este **Guia de Boas Práticas** destina-se à implementação da LGPD pela indústria como um todo, envolvendo todos os setores da indústria contemplados pela atuação da CNI. Por se tratar de grande diversidade de áreas de atuação, com especificidades na forma como os dados pessoais são tratados, foram consideradas as principais demandas e desafios enfrentados pelos mercados com maior desenvolvimento tecnológico e que representam a maior parcela do setor produtivo.

Ainda assim, acreditamos que os protocolos que serão apresentados na Parte 2 poderão contemplar os anseios de grande parte da indústria brasileira e os protocolos da Parte 3 poderão contemplar as pequenas e médias empresas e aquelas que possuem processos tecnológicos que utilizam dados pessoais.

PARTE 2

PROTOCOLOS GERAIS

1 PROTOCOLO PARA IMPLEMENTAÇÃO DE UMA CULTURA DE PROTEÇÃO DE DADOS NAS EMPRESAS

1.1 INTRODUÇÃO

A adequação das empresas à nova legislação de proteção de dados representa enorme desafio para empresas de todos os setores, tendo em vista a verdadeira mudança de paradigma que a LGPD representou.

Conforme abordado na Parte 1, a Indústria 4.0 representa uma revolução na forma como produtos são elaborados, fabricados, desenvolvidos e distribuídos, sendo os dados pessoais apenas uma parte desse novo tipo de produção.

Ainda que a indústria seja extremamente diversa, com diferentes níveis de utilização de recursos tecnológicos que dependem de dados pessoais, é fato que todos os setores utilizam dados pessoais em maior ou menor grau. Isso ocorre porque a crescente utilização de novas tecnologias não se atém ao processo produtivo ou à relação B2C, envolvendo também a gestão de pessoas e a segurança do ambiente de trabalho.

Nesse sentido, é essencial que, além da implementação da chamada *privacy by design* (proteção de dados em todos os passos do desenvolvimento de projetos, desde a sua concepção), seja **criada uma cultura de proteção de dados em toda a organização**.

A criação de uma cultura de proteção de dados vai além do mero cumprimento da legislação, na medida em que requer que o *compliance* de dados considere as especificidades do seu negócio na adoção de medidas de proteção de dados em toda a organização. Tal aspecto é extremamente importante para a efetividade de um programa de *compliance*, tendo em vista que não basta a utilização de *softwares* de ponta, que foram construídos com os mais altos níveis de proteção, mas é necessário que as equipes compreendam os aspectos básicos da proteção de dados e a preocupação em relação à proteção de dados deve ser contínua.

EXEMPLO

Imagine uma situação na qual existe uma política de controle de acesso a um banco de dados sensíveis do RH sobre condições de saúde dos colaboradores, que obriga que apenas colaboradores autorizados possuam senhas de acesso.

Apesar de ser considerada uma boa prática que reduz os riscos para o titular, sugerida pelo escritório especializado, os colaboradores da área não seguem a recomendação, por entenderem que ela não seria necessária, e as senhas dos responsáveis por esse banco de dados são compartilhadas de forma ampla.

O fato de essa senha ser compartilhada torna o mecanismo de controle de acesso ineficaz e possibilita que as informações sobre condições de saúde sensíveis sejam compartilhadas por todos e que colaboradores com determinadas condições de saúde sejam preteridos no ambiente de trabalho.

Por exemplo, o registro sobre saúde mental de um(a) colaborador(a) pode ser utilizado de forma indireta pelo(a) superior(a) na tomada de decisão sobre uma promoção ou a existência de algumas doenças pode ter um efeito social de isolamento caso sejam amplamente divulgadas.

1.2 *ACCOUNTABILITY*

A LGPD estabeleceu expressamente o princípio da *accountability* em seu texto, incluindo-a no rol de princípios previstos no art. 6º da LGPD. O art. 6º, inciso X, traduz o termo como "responsabilização e prestação de contas", compreendidos como a "*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*" (grifo nosso).

Esse princípio foi uma inovação importante trazida pelo Regulamento Europeu de Proteção de Dados, em comparação com a Diretiva nº 46/1995, ao jogar luz sobre a importância de os agentes de tratamento organizarem internamente a governança de dados, bem como por evidenciar tal organização para toda a sociedade. O princípio foi mantido no GDPR, em seu artigo 5(2), estando relacionado aos princípios descritos no artigo 5(1), que incluem a transparência, a minimização, a finalidade, entre outros.

Da mesma forma que no ordenamento europeu, o princípio da *accountability* possui posição central na LGPD e deve ser compreendido como a adoção de medidas para traduzir os requisitos legais, bem como na demonstração da existência e eficácia das medidas (art. 6º, X, da LGPD)[12]. Além disso, em diversas outras passagens da lei, são mencionadas as referidas medidas e mecanismos de demonstração de cumprimento, o que traduz a mudança da "*lógica regulatória do comando e controle, para uma racionalidade mais voltada para a corregulação e accountability*"[13] (grifo nosso).

12 CIPL; CEDIS-IDP. **O Papel do/a Encarregado/a conforme a Lei Geral de Proteção de Dados Pessoais (LGPD)**. set. 2021. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[pt]_cipl-idp_paper_dpo_under_the_lgpd__27_sept_2021_.pdf. Acesso em: 4 mar. 2022.

13 WIMMER, Miriam. Os desafios do *enforcement* na LGPD. *In*: BIONI *et al.* (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 377.

Para auxiliar na implementação desse princípio, o *Centre for Information Policy Leadership* (CIPL), *think thank* global voltado para assuntos de privacidade, reuniu sete elementos centrais na chamada *accountability wheel*[14], quais sejam:

***Accountability wheel* – CIPL**

1) Estabelecer liderança e supervisão para proteção de dados e seu uso responsável.
2) Avaliar e mitigar riscos na proteção de dados.
3) Estabelecer políticas e procedimentos internos.
4) Garantir transparência para todos os *stakeholders*, tanto internamente quanto externamente.
5) Realizar treinamento para colaboradores e adotar medidas de sensibilização.
6) Monitorar e verificar a implementação e efetividade do programa.
7) Implementar procedimentos de resposta e de *enforcement*[15].

A utilização de um programa de *compliance* efetivo requer a fixação de controles internos complementares à regulamentação tradicional, possibilitando a chamada autorregulação regulada[16]. Essa vertente é alinhada com o modelo regulatório que a LGPD busca implementar, cujo foco deve ser uma abordagem baseada no risco, que seja flexível e voltada para a real compreensão acerca dos riscos para o titular que estão envolvidos nas operações de tratamento de dados.

Nesse sentido, o art. 50 da LGPD apresenta a possibilidade de que os agentes de tratamento formulem medidas de governança de dados que possibilitem o efetivo cumprimento da legislação, sendo responsabilidade do controlador a sua implementação. O inciso I do artigo pontua como aspectos essenciais do programa: a) comprometimento do controlador; b) aplicabilidade a todo conjunto de dados pessoais sob seu controle; c) adequação à estrutura da organização; d) existência de políticas e salvaguardas baseadas em risco; e) estabelecimento de confiança do titular; f) integração com a estrutura geral de governança; g) existência de plano de resposta a incidentes e remediação; e h) atualização constante.

1.3 TREINAMENTOS E EVENTOS PARA SENSIBILIZAÇÃO

Como se sabe, a criação de uma cultura interna de proteção de dados não é tarefa fácil e deve considerar as especificidades do mercado no qual a empresa está inserida, bem como as operações de tratamento realizadas por cada um dos setores internamente. Por esse motivo, oferecer treinamentos e eventos de sensibilização para os(as) colaboradores(as)

14 CIPL. **Organisational Accountability**: past, present and future. out. 2019. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organisational_accountability_%E2%80%93_past_present_and_future.pdf. Acesso em: 8 mar. 2022.

15 Esse termo em inglês consiste na aplicação de normas de princípios de determinada legislação.

16 FRAZÃO, Ana; DONATO, Milena; ABILIO, Viviane. Compliance de dados pessoais. *In*: **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019.

é fundamental para envolvê-los(as) nas melhores práticas e garantir a continuidade dos programas de adequação.

Em primeiro lugar, é necessário identificar as áreas estratégicas nos fluxos de informação internos das empresas. Por exemplo, o setor de *marketing*, RH e TI realizam diversas atividades de tratamento de dados diariamente e são estratégicos para a mudança cultural da empresa. Ademais, as áreas de desenvolvimento de produtos, pesquisa e contato com o consumidor também podem precisar de treinamento específico sobre como implementar estratégias de *compliance* de dados em seus projetos e atividades diárias.

Após a identificação dessas áreas, a empresa deve avaliar quais estratégias de conscientização serão aplicadas a depender do nível de envolvimento dos setores com dados pessoais. Isso porque, ainda que todos os(as) colaboradores(as) devam receber treinamentos ou, ao menos, participar de eventos de sensibilização, quando as áreas possuem contato intenso e direto com dados pessoais é recomendável que o treinamento oriente suas necessidades específicas e possibilite maior envolvimento dos participantes. Assim, deve ser realizado um módulo geral para todos os(as) colaboradores(as) – independentemente do cargo, do vínculo com a empresa e da responsabilidades – e também pode ser realizado um treinamento adicional para aqueles que possuem responsabilidades-chave no tratamento de dados[17], se assim a empresa entender viável.

O programa de treinamento deve ser organizado ou aprovado por especialistas ou, de preferência, pelo encarregado ou responsável pelas questões relativas à proteção de dados na empresa[18]. Ademais, após a realização do treinamento, é necessário acompanhar se os(as) colaboradores(as) compreenderam as matérias discutidas, se todos participaram e se é necessário a realização de outros treinamentos sobre outros assuntos.

Ao longo do treinamento, os benefícios da adoção de boas práticas no tratamento de dados deve ser levantado, sendo ressaltado tanto os benefícios individuais quanto os relativos à organização. Esse aspecto depende da realização de diálogos preliminares com as equipes para compreensão das suas atividades diárias e de suas perspectivas individuais[19].

Também recomenda-se a disponibilização permanente dos materiais dos treinamentos, bem como a utilização dos portais eletrônicos da empresa para a publicação de mensagens de conscientização sobre proteção de dados. Além disso, sugere-se que esses treinamentos

17 INFORMATION COMISSIONER'S OFFICE – ICO. **Training and awareness**. Disponível em: https://ico.org.uk/for-organisations/accountability-framework/training-and-awareness/. Acesso em: 30 jun. 2023.

18 INFORMATION COMISSIONER'S OFFICE – ICO. **Training and awareness**. Disponível em: https://ico.org.uk/for-organisations/accountability-framework/training-and-awareness/. Acesso em: 30 jun. 2023.

19 NATIONAL CYBER SECURITY CENTRE – NCSC. **10 Steps to Cyber Security**: engagement and training. Disponível em: https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training. Acesso em: 30 jun. 2023.

sejam realizados de forma frequente, podendo ser complementados com incentivos à participação de eventos sobre proteção de dados.

Por fim, é essencial que as lideranças se engajem nos treinamentos e na implementação das práticas discutidas durante as discussões. A própria adoção de um **Guia de Boas Práticas** pode ser uma forma de engajar as lideranças e os colaboradores na temática da proteção de dados. Os líderes são essenciais para incentivar o cumprimento das diretrizes.

Recursos que podem ser utilizados para conscientização

- Liderança pelo exemplo – envolvimento do alto escalão e dos líderes na propagação das melhores práticas.
- Treinamentos – gerais e específicos para áreas que lidam com um volume maior de dados pessoais ou possuem papel estratégico.
- Disponibilização permanente e de fácil acesso das informações fornecidas nos treinamentos e dos materiais distribuídos.
- Guias internos sobre a LGPD.
- Publicação de *Questions and Answers* (Q&A)/perguntas frequentes sobre a LGPD.
- Utilização de modelos de documentos que devem ser utilizados.
- Publicação periódica de conteúdo sobre LGPD – *newsletters*, *clippings*, chamadas nos portais internos da empresa.
- Incentivo à participação de eventos – dispensa para participação de cursos, pagamento de taxas de inscrição.
- Organização de eventos dentro das empresas.

1.4. MAPEAMENTO DO TRATAMENTO DE DADOS PESSOAIS

O mapeamento de dados pessoais é uma medida imprescindível para a criação de uma cultura de privacidade nas empresas. Afinal, trata-se do primeiro passo para que a empresa conheça as próprias práticas de tratamento de dados, de modo que possa planejar depois a sua adequação e a correção de eventuais falhas encontradas.

Durante o processo de mapeamento de dados, são elaboradas tabelas ou podem ser utilizados *softwares* que permitem que a sua atualização seja constante. Assim, é recomendado que o mapeamento das operações seja acompanhado pelo seu registro (também chamado de *Record of Processing Activities* – RoPA)[20], para que as informações sejam utilizadas de forma contínua e possam subsidiar a avaliação sobre a melhor base legal a ser utilizada.

É a partir do registro de dados pessoais que a ANPD pode avaliar se os agentes de tratamento adotaram medidas preventivas em caso de incidentes, além de outras avaliações que a autoridade possa vir a realizar. Ademais, o registro das operações de tratamento auxilia no cumprimento da base principiológica da legislação, uma vez que ele possibilita que o próprio responsável pela área reflita se, por exemplo, os dados coletados são necessários,

20 Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

qual a finalidade do tratamento daqueles dados, se o consentimento foi coletado de acordo com os seus requisitos legais e, até mesmo, se o titular possui informações sobre os dados que são tratados.

A conscientização acerca dos fluxos de dados é importante, inclusive, para que as empresas que possuem poucas atividades de tratamento possam eventualmente informar se realizam determinado tipo de tratamento de dados ou não, caso sejam questionados pelos titulares. Assim, a elaboração de RoPA representa significativo ganho de tempo na garantia de direitos dos titulares e é medida necessária para que sejam implementadas políticas de proteção de dados nas empresas.

Nesse sentido, com base nas melhores práticas internacionais[21], recomendamos[22], que os seguintes tópicos sejam considerados no mapeamento e no registro de dados realizado pelos agentes de tratamento:

Informações sobre fluxos de dados	Processo de tratamento
	Área de negócio responsável
	Finalidade do tratamento
Informações sobre os dados pessoais tratados	Tipo de dados
	Categoria dos dados (se pessoal ou sensível)
	Categoria do titular dos dados
	Finalidade do tratamento de cada dado coletado
Informações sobre coleta e compartilhamento de dados	Onde o dado foi coletado?
	O dado é compartilhado internamente?
	O dado é compartilhado com terceiros?
	O dado é transferido para outros países?
Armazenamento	Onde os dados são armazenados?
	Existe controle de acesso?
	Por quanto tempo os dados são armazenados?
	Existe uma política de exclusão dos dados?
	Se embasado em norma legal, descrevê-lo
Embasamento	Base legal.
	Se utilizado o consentimento, ele pode ser retirado?
	Se utilizada obrigação legal ou regulatória, descrevê-la.
	Se utilizado legítimo interesse, foi realizada a avaliação de legítimo interesse?

21 Nesse sentido, ver: INFORMATION COMISSIONER'S OFFICE – ICO. **How do we document our processing activities?** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/. Acesso em: 30 jun. 2023

22 A referida tabela também foi apresentada no **Código de Boas Práticas do Setor de Telecomunicações**. Disponível em: https://www.naomeperturbe.com.br/doc/ct_codigo_conduta.pdf.

1.5. ENCARREGADO OU *DATA PROTECTION OFFICER* (DPO)

Outro aspecto que pode contribuir para a demonstração de adequação de uma organização às regras de proteção de dados pessoais é a indicação de um encarregado pelo tratamento de dados pessoais (*Data Protection Officer* – DPO)[23]. A figura do encarregado é estratégica na implementação de uma cultura de dados, uma vez que a função contribui para a conformidade dos programas de governança de dados e pode ser potencializada para aumentar a confiança de titulares, parceiros e consumidores, servindo como controle interno do cumprimento normativo que é responsabilidade dos agentes de tratamento[24].

Suas funções compreendem a intermediação da relação entre ANPD, os titulares e a empresa, além de ser referência do controlador na execução das atribuições relativas à proteção de dados (art. 41 da LGPD). Ademais, sua função na implementação de uma cultura de proteção de dados é reconhecida pela própria LGPD, uma vez que o seu art. 41, §2º, III, da LGPD coloca como atividade do encarregado "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais".

Apesar da sua indicação ser obrigatória apenas para os controladores[25] – não sendo obrigatória para agentes de tratamento de pequeno porte, conforme trataremos em detalhes no protocolo específico –, a indicação de um encarregado pode representar o engajamento da empresa com a proteção de dados pessoais, sendo uma figura estratégica na tradução das obrigações legais na estrutura interna da empresa, bem como para possibilitar a continuidade do processo de implementação do programa de governança em privacidade. Não à toa, diversas organizações reconhecem o encarregado como facilitador da conformidade e elemento estratégico nos programas de governança de dados. Por isso, recomenda-se que os agentes de tratamento indiquem o encarregado de dados, salvo normatização complementar específica sobre a inexigência.

Para que as atividades do DPO sejam plenamente desempenhadas é necessário que exista certa estabilidade no contrato dessa figura para garantir sua independência funcional, mesmo que ele não faça parte do quadro de funcionários da empresa. Além disso, o DPO deve ter espaço para se manifestar perante o alto escalão da empresa, principalmente no desenvolvimento de novos produtos e na tomada de decisões relacionadas à privacidade.

---

23 Existem outras denominações para esse cargo, como a nomenclatura "oficial de proteção de dados" mencionado na Classificação Brasileira de Ocupações (CBO).

24 Nesse sentido ver, SCHERTEL, Laura; FUJIMOTO, Mônica. O papel do "Deputy Protection Officer – DPO" nas instituições de ensino superior privado. *In*: Maria GOLDBERG, Maria (Org.). Ensino Superior Privado: reflexões sobre o passado recente, atualidades e perspectivas futura. [S.l.]: **Revista dos Tribunais**, [2023] (no prelo).

25 Apesar da definição constante no art. 5º, VIII, da LGPD mencionar que o encarregado é pessoa indicada pelo controlador e operador, a legislação indica a obrigatoriedade de indicação do encarregado de forma expressa apenas nas atribuições do controlador (art. 41 da LGPD).

Ainda assim, o encarregado não deve ser responsabilizado pelas ações da entidade, salvo em casos de má-fé.

Ressalte-se que a LGPD e a ANPD[26] optaram por conferir liberdade para o exercício da função, de modo que as competências previstas no art. 41 da LGPD são apenas exemplificativas. Tal liberdade é fundamental para garantir que os encarregados possam desenhar as melhores práticas considerando as singularidades das empresas nas quais atuam.

Em relação à forma de atuação do encarregado, ele pode atuar de forma isolada ou por meio de uma equipe, além de poder atuar para mais de uma empresa, ainda que do mesmo grupo econômico. O importante é que ele cumpra com as funções que constam na LGPD e nas normas complementares expedidas pela ANPD e que não exista conflito de interesses na sua atuação. Ademais, o DPO deve ter conhecimentos técnicos e atualizados sobre os temas relacionados à proteção de dados, devendo sua contratação ser alinhada com um plano de desenvolvimento e capacitação, conforme pontuado no item supra.

Por fim, deve ser disponibilizada publicamente uma forma de contato com o encarregado, de preferência no sítio eletrônico do controlador (art. 41, §1º, da LGPD), podendo ser criado um *e-mail* destinado exclusivamente para essa finalidade.

1.6 PRIORIDADES PARA IMPLEMENTAÇÃO EFETIVA DA LGPD

Para auxiliar nos processos de adequação das empresas à LGPD, o CIPL, em parceria com o Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP), apresentou o seguinte *checklist* com as **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)**[27].

Assim, apresentamos o seguinte *checklist* com as etapas prioritárias para a adequação à LGPD, nos exatos termos do documento elaborado pelas instituições.

26 BRASIL. Autoridade Nacional Proteção de Dados – ANPD. **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/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 4 jul. 2022.

27 CIPL; CEDIS-IDP. **Prioridades Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados (LGPD)**. 2020. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[pt]_cipl-idp_white_paper_on_top_priorities_for_organizations_to__effectively_implement_the_lgpd_7_october_2020_.pdf. Acesso em: 04 jul. 2022.

CHECKLIST: ETAPAS PRIORITÁRIAS PARA A ADEQUAÇÃO À LGPD

Prioridade 1. Entender o impacto da LGPD na organização e obter a adesão da alta administração

- ☑ Compreender o impacto das regras da LGPD na organização e o uso de dados pessoais como controlador e/ou operador.
- ☑ Explicar e demonstrar à alta administração a importância da adequação às regras de privacidade e os benefícios da prestação de contas.
- ☑ Solicitar apoio da alta administração, incluindo para orçamento e recursos.

Prioridade 2. Designar o encarregado pelo tratamento de dados pessoais, e identificar e envolver os principais *stakeholders*

- ☑ Designar o encarregado, documentar e comunicar internamente seu papel e suas responsabilidades.
- ☑ Identificar e envolver os principais *stakeholders* internos e líderes sêniores que patrocinarão o programa de governança de privacidade e proteção de dados pessoais e terão responsabilidade pela implementação do programa.
- ☑ Identificar e envolver os principais *stakeholders* externos.

Prioridade 3. Identificar as atividades de tratamento e os dados utilizados pela organização

- ☑ Definir a metodologia para mapear e registrar as atividades de tratamento de dados pessoais efetuadas pela organização (como controladora e/ou operadora) e revisar periodicamente o ciclo de vida dos dados.
- ☑ Mapear os dados pessoais e as respectivas atividades de tratamento o mais rápido possível.
- ☑ Considerar a anonimização e minimização de dados para reduzir os riscos e o ônus decorrente da obrigação de conformidade da organização.

Prioridade 4. Determinar o papel e as obrigações da organização ao atuar como controladora ou operadora

- ☑ Determinar o papel e as obrigações da organização como controladora ou operadora.
- ☑ Comunicar essas obrigações aos indivíduos e às equipes relevantes dentro da organização.
- ☑ Considerar atualizações necessárias aos contratos dos clientes para refletir o papel da organização.

Prioridade 5. Avaliar os riscos associados ao tratamento de dados pessoais

- ☑ Implementar processo de avaliação de riscos aos indivíduos relacionados ao tratamento de dados pessoais.
- ☑ Priorizar as medidas de conformidade relacionadas ao tratamento de dados pessoais que implicam maiores riscos para os indivíduos e para a organização.

Prioridade 6. Elaborar e implementar um programa de governança de privacidade e proteção de dados pessoais que cubra as exigências da LGPD

- ☑ Elaborar um programa de governança de privacidade e proteção de dados pessoais e um plano de ação para implementá-lo com base nos riscos identificados.
- ☑ Identificar quais são as ações mais simples e implementá-las o mais rápido possível.
- ☑ Manter e revisar o programa de governança de privacidade e proteção de dados pessoais de forma contínua.

Prioridade 7. Definir as bases legais para as atividades de tratamento de dados da organização

- ☑ Identificar os indivíduos ou equipes que serão responsáveis por determinar as bases legais para o tratamento de dados pessoais – esses indivíduos deverão, como prioridade, definir em quais bases legais a organização se baseará.
- ☑ Considerar quais processos devem ser implementados e/ou adaptados para a manutenção contínua das bases legais.

Prioridade 8. Definir medidas técnicas e administrativas para garantir a segurança dos dados pessoais, assim como para elaborar relatórios internos e gerenciamento efetivos de incidentes de segurança

- ☑ Trabalhar com as equipes de segurança da informação e de arquitetura de sistemas/dados para determinar as mudanças necessárias para implementar as medidas apropriadas de segurança.
- ☑ Estabelecer um processo para a elaboração de relatórios internos, gerenciamento de incidentes de segurança, violações de dados pessoais e notificação da ANPD, se necessário.

Prioridade 9. Identificar os terceiros com os quais a organização compartilha dados pessoais e estabelecer um processo de gestão de terceiros

- ☑ Identificar os terceiros que realizam tratamento de dados pessoais em nome da organização e determinar se a organização trata dados pessoais em nome de terceiros.
- ☑ Avaliar e adotar mecanismos de gerenciamento de terceiros, incluindo processos de due diligence e celebração de contratos relacionados ao tratamento de dados.

Prioridade 10. Identificar os fluxos internacionais de dados da organização (entrada e saída) e estabelecer os mecanismos apropriados para permitir tal transferência de dados

- ☑ Identificar se a organização transfere dados pessoais para outros países e, se o faz, para quais finalidades e em qual capacidade (como controlador ou como operador).
- ☑ Avaliar e implementar os mecanismos de transferência de dados mais apropriados.

Prioridade 11. Construir processos eficazes para transparência e gerenciamento dos direitos dos titulares de dados pessoais

- ☑ Preparar avisos de privacidade e outros recursos para fornecer informações facilmente acessíveis aos titulares de dados sobre o tratamento realizado pela organização.
- ☑ Mapear os possíveis casos de exercícios de direitos pelos titulares relacionados aos seus dados pessoais, avaliar o tempo que a organização precisaria para responder e para desenvolver os processos relevantes.
- ☑ Desenvolver processos para responder a tais solicitações.

Prioridade 12. Treinar funcionários sobre as regras da LGPD e criar um programa de conscientização

- ☑ Implementar treinamento contínuo para todos os funcionários, incluindo os terceirizados e os recém-chegados.
- ☑ Planejar atividades de treinamento e comunicação tanto no início do programa de governança de privacidade e proteção de dados pessoais quanto de forma contínua.

2 PROTOCOLO PARA GARANTIA DO DIREITO DOS TITULARES

2.1 INTRODUÇÃO

A garantia dos direitos do titular é aspecto central para o cumprimento da legislação de proteção de dados, tendo em vista que os direitos do titular permitem o controle do fluxo de seus dados. A LGPD prevê uma série de direitos do titular para além desses clássicos que estão estabelecidos em seus artigos 9º, 18 e 20, conforme a seguir.

DIREITO DOS TITULARES

- Acesso facilitado a informações.
- Confirmação da existência de tratamento.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD.
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com regulamentação da ANPD, observados os segredos comercial e industrial.
- Eliminação dos dados pessoais tratados com o consentimento do titular, salvo exceções legais.
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
- Revogação do consentimento.
- Oposição ao tratamento irregular.
- Revisão de decisões automatizadas.
- Petição perante a ANPD ou perante os organismos de defesa do consumidor (art. 18, §1º, da LGPD).

Importa ressaltar que, além da LGPD, outros diplomas, como o **Código de Defesa do Consumidor** (CDC)[28] e o **Código Civil** (CC) possuem dispositivos que amparam os direitos do titular. O CDC, por exemplo, prevê diversas obrigações que têm como objetivo o aumento da transparência na relação do consumidor – que também pode ser o titular do dado pessoal. Já o CC tutela os direitos dos titulares por meio da proteção dos direitos de personalidade e da tutela dos direitos subjetivos[29].

28 Art. 43 da Lei nº 8.078/1990 (CDC): "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".

29 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

Ademais, é necessário observar que, além dos direitos listados nos artigos 9º, 18 e 20, a LGPD prevê que são fundamentos da proteção de dados o respeito à privacidade e a autodeterminação informativa (art. 2º, I e II, da LGPD). Assim, apesar de a legislação reconhecer que os dados pessoais serão utilizados para finalidades econômicas (art. 2º, V e VI, da LGPD), os fundamentos da legislação devem ser levados em consideração na relação com o titular.

É evidente que os direitos dos titulares – assim como outros direitos subjetivos – não podem ser utilizados de forma abusiva, não sendo absolutos. Por esse motivo, diversas autoridades de proteção de dados ao redor do mundo compreendem que o exercício de alguns direitos dos titulares deve ocorrer em situações específicas. Por exemplo, a *Information Commissioner's Office* (ICO), autoridade nacional de proteção de dados do Reino Unido, entende que, quando o tratamento de dados for subsidiado pela base legal "execução contratual", o titular pode exercer o direito de objeção, mas não o direito de eliminação nem a portabilidade[30].

A própria LGPD impõe um limite ao direito à transparência, tendo em vista a necessidade de observância aos segredos comercial e industrial (art. 6º, VI, da LGPD). Assim, na aplicação dos direitos dos titulares, devem ser considerados esses limites, além de outros procedimentos que auxiliam na sua efetivação, conforme será exposto a seguir.

2.2 TRANSPARÊNCIA E POLÍTICAS DE PRIVACIDADE

A transparência é um dos princípios norteadores da LGPD e trata da obrigação de os agentes de tratamento garantirem informações claras, precisas e facilmente acessíveis aos titulares sobre tratamentos, controlador e operador, respeitados os segredos comercial e industrial.

Um dos desafios da implementação desse princípio é encontrar o equilíbrio entre clareza e completude das informações disponibilizadas. A comunicação com o titular dos dados pode ser realizada por meio de políticas de privacidade ou mesmo por meio de *dashboards* (painéis de controle) por meio dos quais o usuário pode, ao mesmo tempo, controlar as suas preferências e acessar as informações sobre o tratamento de seus dados. Entre as informações que devem ser disponibilizadas para o titular estão[31]:

30 INFORMATION COMISSIONER'S OFFICE – ICO. **Guide to the General Data Protection Regulation**. 2021. p. 51. Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. Acesso em: 30 jun. 2023.

31 Essa lista foi elaborada com base nos seguintes *checklists*: INFORMATION COMISSIONER'S OFFICE – ICO. **Right to be informed**. 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Acesso em: 30 jun. 2023; CONFEDERAÇÃO NACIONAL DE SAÚDE – CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 jun. 2023; **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em 2 jul. 2023.

Conteúdo das políticas de privacidade

- Principais formas de coleta dos dados pessoais.
- Operações de tratamento de dados realizadas.
- Finalidades do tratamento de dados do titular.
- Informações sobre compartilhamento de dados (dados compartilhados e com quem).
- Caso os dados sejam coletados de outras fontes e não sejam fornecidos diretamente pelo titular, publicar quais categorias de dados são coletados.
- Principais bases legais utilizadas no tratamento de dados.
- Informações sobre a transferência internacional de dados.
- Informações sobre a existência de obrigações legais que exigem o compartilhamento de dados.
- Informações sobre a utilização de decisões automatizadas, perfilamento e rastreamento.
- Dados para contato com o Encarregado (DPO).
- Caso a política de privacidade seja alterada, disponibilizar avisos e garantir que tal informação seja amplamente difundida, com prazo razoável entre o aviso e a efetiva implementação das mudanças.
- Caso se trate de tratamento de dados de colaboradores, disponibilizar avisos internos sobre a alteração.

Ademais, conforme exposto no "Protocolo para implementação de uma cultura de proteção de dados nas empresas", os agentes de tratamento podem utilizar recursos alternativos para garantir o acesso a informações sobre o tratamento de dados. Além da utilização de textos curtos e linguagem direta, podem ser adotadas como estratégias[32]:

- Utilização de imagens e recursos interativos.
- Promoção de semanas e dias específicos para discussões sobre proteção de dados.
- Utilização de "Perguntas Frequentes" para endereçar questões sobre proteção de dados.
- Criação de marca específica para assuntos relativos à privacidade e proteção de dados.
- Elaboração de infográficos, pôsteres e adesivos sobre o assunto.

2.3 ACESSO

O titular tem direito de acessar e receber uma cópia de seus dados pessoais, bem como outras informações que sejam pertinentes ao tratamento de seus dados. Tal pedido pode ser realizado de forma verbal ou escrita e não é possível cobrança de nenhuma natureza para o exercício desse direito, sob pena de impedimento indireto de acesso.

Como o direito de acesso está relacionado a princípios – como o livre acesso, a transparência e a prestação de contas –, eventual negativa de prestação de informações deve ser excepcional e fundamentada. Dessa forma, recomenda-se que algumas medidas sejam

32 CIPL. **What Good and Effective Data Privacy Accountability Looks Like**: Mapping Organisations' Practices to the CIPL Accountability Framework. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report__27_may_2020__v2.0.pdf. Acesso em: 2 jul. 2023.

tomadas pelas empresas ao preparar o procedimento de atendimento às solicitações de informação, tais como[33]:

Direito de acesso

- Estabelecer fluxos para quando for solicitado o direito de acesso e meios para identificar um pedido de informação.
- Registrar a data do recebimento do pedido.
- Ter uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.
- Estabelecer prazos para atender aos pedidos de informação, respeitando o limite de 15 (quinze) dias estabelecido no art. 19 da LGPD e hipóteses de interrupção do prazo quando são necessárias informações adicionais que impeçam o atendimento do pedido:
  - Caso não seja possível cumprir a diligência no prazo estabelecido, informar tal fato ao titular, explicando as razões para o atraso.
- Estabelecer os limites das informações que não podem ser prestadas, identificando quais informações são relativas a segredos comerciais e industriais.
- Possuir sistemas de gerenciamento de informações eficientes que permitam a identificação e localização das informações.
- Identificar quando um pedido de informação pode envolver informações de outros titulares.
- Identificar se os dados solicitados são pertinentes e informar, ao menos:
  - finalidade específica do tratamento;
  - forma e duração do tratamento, observados os segredos comercial e industrial;
  - identificação do controlador;
  - informações de contato do controlador;
  - informações acerca do uso compartilhado de dados pelo controlador e da finalidade;
  - responsabilidades dos agentes que realizarão o tratamento; e
  - direitos do titular especificados no art. 18 da LGPD.

2.4 RETIFICAÇÃO

De acordo com o art. 18, III, da LGPD ,os titulares têm direito à retificação de dados que sejam incorretos, incompletos ou desatualizados. Tal direito também encontra fundamento no princípio da qualidade dos dados, que garante que os dados dos titulares sejam exatos, claros, relevantes e atualizados. Da mesma forma que o pedido de acesso, o pedido de retificação pode ser recusado tão somente em hipóteses excepcionais.

33 Essa lista foi elaborada com base nos seguintes *checklists*: INFORMATION COMISSIONER'S OFFICE – ICO. **Right to be informed**. 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Acesso em: 30 jun.; CONFEDERAÇÃO NACIONAL DE SAÚDE – CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 jun. 2023; **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações**. Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em: 2 jul. 2023.

Assim, sugerimos os seguintes procedimentos para a garantia desse direito[34]:

Direito de retificação

- Estabelecer quando o direito de retificação se aplica e como identificar um pedido de retificação.
- Registrar a data do recebimento do pedido.
- Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.
- Estabelecer prazos para atender ao pedido de retificação e hipóteses de interrupção do prazo quando são necessárias providências adicionais.
- Ter sistemas de gerenciamento de informações eficientes que permitam a retificação das informações.

2.5 CANCELAMENTO

O direito ao cancelamento refere-se ao pedido de exclusão de dados pessoais, que pode ser utilizado quando o processamento dos dados for realizado de forma ilegal, em descumprimento com a legislação ou mesmo quando o titular tiver retirado seu consentimento. Tal hipótese é restrita e deve observar a necessidade de manutenção de dados pessoais para finalidades, como o cumprimento de obrigações legais ou regulatórias. Nesse sentido, sugerimos os seguintes procedimentos[35]:

Direito de cancelamento

- Estabelecer quando o direito de exclusão se aplica e como identificar esse tipo de pedido.
- Registrar a data do recebimento do pedido.
- Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.
- Estabelecer prazos para atender ao pedido e hipóteses de interrupção do prazo quando são necessárias providências adicionais.
- Identificar se foi dado o consentimento para o tratamento do dado.
- Possuir procedimentos para informar outros agentes de tratamento com quem o dado tenha sido compartilhado sobre eventual cancelamento, que também deverá ser adotado pelos outros agentes.
- Quando o tratamento tiver origem no consentimento do titular ou em contrato, providenciar o acesso do titular à cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
- Fornecer informações claras e adequadas acerca da origem dos dados, da inexistência de registro, dos critérios utilizados para o tratamento de dados e da finalidade do tratamento, observados os segredos comercial e industrial ao atender aos pedidos do titular.
- Possuir sistemas de gerenciamento de informações eficientes que permitam o cancelamento das informações e sua eliminação física.

34 Essa lista foi elaborada com base nos seguintes *checklists*: INFORMATION COMISSIONER'S OFFICE – ICO. **Right to be informed**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Acesso em: 30 jun. 2023; CONFEDERAÇÃO NACIONAL DE SAÚDE – CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 jun. 2023; **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em 2 jul. 2023.

35 Essa lista foi elaborada com base nos seguintes checklists: INFORMATION COMISSIONER'S OFFICE – ICO. **Right to be informed**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Acesso em: 30 jun. 2023; CONFEDERAÇÃO NACIONAL DE SAÚDE - CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 jun. 2023; **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em 02 jul. 2023.

2.6 OPOSIÇÃO

A oposição ao tratamento de dados está prevista no art. 18, §2º, da LGPD. Esse direito define que o titular tem o direito de contestar o tratamento de dados, mesmo que o consentimento não tenha sido coletado, em caso de descumprimento aos dispositivos legais ou para se opor a alguma das finalidades que o seu dado está sendo tratado. Assim, sugerem-se os seguintes procedimentos[36]:

Direito de oposição

- Identificar a oposição ao tratamento de dados e quando esse direito é aplicável.
- Registrar a data do recebimento do pedido.
- Possuir uma política de registro dos pedidos recebidos e criar um canal eficiente para receber tais pedidos.
- Estabelecer prazos para atender à oposição ao tratamento e hipóteses de interrupção do prazo quando são necessárias providências adicionais.
- Possuir sistemas de gerenciamento de informações eficientes que permitam a efetivação do direito de oposição, como cancelamento, retificação e outros tipos de alterações relativas aos dados pessoais.

2.7 MODELO DE FORMULÁRIO

Deve ser fornecido ao titular meio hábil para exercer seus direitos perante os agentes de tratamento. Por meio desse instrumento, também é importante garantir a autenticidade da identidade do titular. Dessa forma, sugere-se a adoção do seguinte modelo de formulário a ser disponibilizado para o titular na sede da empresa, nos *sites* ou aplicativos da entidade:

36 Essa lista foi elaborada com base nos seguintes *checklists*: INFORMATION COMISSIONER'S OFFICE – ICO. **Right to be informed**. 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/. Acesso em: 30 jun. 2023; CONFEDERAÇÃO NACIONAL DE SAÚDE – CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 jun. 2023; **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em 2 jul. 2023.

FORMULÁRIO – SOLICITAÇÃO DO EXERCÍCIO DE DIREITOS DOS TITULARES

De acordo com a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), SOLICITO exercer o seguinte direito:

( ) Confirmação de existência de tratamento.
( ) Receber informações das entidades públicas e privadas com as quais os dados foram compartilhados.
( ) Acesso aos dados.
( ) Correção ou atualização dos dados.
( ) Revogação do consentimento.
( ) Oposição de tratamento de dados.
( ) Esclarecimento sobre decisões automatizadas.
( ) Revisão de decisões automatizadas.

Descreva o dado objeto da solicitação:

Justifique o pedido que está sendo realizado:

Caso seja necessário, identifique os documentos que subsidiam seu pedido:

Observações ou comentários adicionais:

DADOS DO(A) SOLICITANTE

Nome completo:	
RG:	**CPF:**
Endereço:	
***E-mail*:**	**Celular:**
O solicitante também é o titular dos dados: ( ) Sim ( ) Não – preencher a tabela abaixo	

DADOS DO(A) TITULAR

Nome completo:	
RG:	**CPF:**
Endereço:	
***E-mail*:**	**Celular:**
Relação com o solicitante:	

Observação: é necessário anexar cópia de um documento que comprove a identidade do solicitante (RG, CNH, Passaporte) e comprovante de relação com o titular, em caso de solicitante distinto do titular (procuração, certidão de nascimento). Em caso de dúvidas, encaminhar *e-mail* para o endereço XXXX.

Declaro que as informações apresentadas neste formulário são verdadeiras e que eu sou a pessoa a quem elas se referem, conforme documento de identidade com foto anexado ao pedido.

_____

[assinatura]

[Data da solicitação]

3 PROTOCOLO PARA ARMAZENAMENTO E ELIMINAÇÃO DE DADOS

3.1 INTRODUÇÃO

A avaliação das empresas a respeito do período de armazenamento e do momento que os dados devem ser eliminados precisa ser orientada pelo princípio da necessidade (art. 6º, III, da LGPD). Nos termos do princípio, o tratamento de dados deve ser limitado ao mínimo necessário para realização de suas atividades, de modo que o armazenamento desses dados deve ser realizado pelo menor tempo possível, sendo estabelecidos prazos para sua eliminação, sempre considerando as especificidades do caso concreto[37].

Nos termos do art. 15 da LGPD, o término do tratamento de dados deve ocorrer quando:

- a finalidade for alcançada ou os dados não forem mais necessários;
- o período do tratamento tiver terminado;
- o titular tiver revogado seu consentimento; ou
- a autoridade nacional determinar o término do tratamento por conta de violação à lei.

O protocolo para armazenamento de dados pessoais é importante para as empresas, não só por conta do princípio da necessidade, como também para compreensão de outras obrigações legais que podem exigir que o armazenamento seja realizado por tempo superior ao necessário para a finalidade estrita do tratamento. Ainda assim, as empresas devem garantir que, caso o dado não seja mais necessário, os dados sejam excluídos mesmo que o titular não faça a solicitação de forma ativa.

37 INFORMATION COMISSIONER'S OFFICE – ICO. **Principle**: storage limitation. 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/. Acesso em: 30 jun. 2023; EUROPEAN COMMISSION. **For how long can data be kept and is it necessary to update it?** 2023. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en. Acesso em: 30 jun. 2023.

Dessa maneira, para auxiliar na avaliação quanto ao período de armazenamento dos dados, à criação de tabelas de temporalidade e avaliação de princípios na exclusão ou no armazenamento de dados, sugerimos que alguns aspectos sejam considerados: i) aplicação de princípios; ii) existência de obrigações legais, normas setoriais ou regulatórias; e iii) pedido de exclusão pelo titular do dado.

3.2 APLICAÇÃO DE PRINCÍPIOS

Os princípios da proteção de dados, presentes no art. 6º da LGPD, são parâmetros fundamentais para nortear o tratamento de dados e devem ser observados ao longo de todo tratamento de dados pessoais realizados por organizações. Entre os princípios da LGPD, em relação à avaliação sobre o armazenamento e a eliminação dos dados pessoais, especial atenção deve ser direcionada aos princípios da prestação de contas, finalidade, adequação, necessidade, transparência e qualidade dos dados.

Assim, conforme exposto na Parte 1, a reflexão sobre algumas questões pode auxiliar a aplicação dos princípios da lei:

- Todos os dados pessoais que irei coletar são necessários para atingir a finalidade para a qual eles serão utilizados?
- Existe uma forma menos invasiva de tratar esses dados?
- Eu irei violar algum direito do titular com a minha operação de tratamento de dados?
- Existe o potencial de restrição a direitos ou liberdades com a operação de tratamento que irei realizar?
- O titular foi informado sobre os usos que farei dos dados?
- Eu consigo possibilitar o acesso do titular a informações sobre seus dados pessoais?
- Onde e como irei guardar os dados?
- Os dados que estou tratando estão seguros?
- A finalidade que eu inicialmente estabeleci foi concluída? Eu ainda preciso de todos os dados que coletei inicialmente?
- A finalidade inicial se alterou ao longo do tratamento?

Após reflexão inicial sobre a forma como os dados serão tratados e enquadramento das bases legais para o tratamento deles, devem ser implementados processos internos para manutenção contínua das condições de legitimidade dos dados coletados.

- A empresa deve saber quais dados possui, por quanto tempo eles serão necessários ou para qual(is) finalidade(s), devendo o agente de tratamento ser capaz de apresentar uma justificativa para seu armazenamento (**PRINCÍPIO DA FINALIDADE E PRESTAÇÃO DE CONTAS**).
- É necessário garantir que o tratamento de dados tenha como finalidade propósitos legítimos, específicos e explícitos em todo o ciclo de vida dos dados coletados – ou seja, de forma contínua –, não sendo possível armazenar um dado sem que exista um objetivo claro para tanto **(PRINCÍPIO DA FINALIDADE**).
- Com o acompanhamento permanente das atividades de tratamento de dados, será possível tomar decisões sobre quando determinados dados não precisam mais ser coletados ou devem ser excluídos por não serem mais necessários (**PRINCÍPIO DA NECESSIDADE**).
- Por vezes, nem todos os dados coletados inicialmente são necessários, devendo a sua utilização ser minimizada ao máximo, inclusive, por meio da anonimização ou pseudonimização quando possível (**PRINCÍPIO DA NECESSIDADE**).
- Caso a finalidade se altere ao longo do período de tratamento e não seja possível excluí-lo, devem ser adotadas medidas para que o titular seja informado ou possa acessar informações sobre a mudança de finalidade (**PRINCÍPIO DA ADEQUAÇÃO E DA TRANSPARÊNCIA**).
- É necessário garantir que o dado armazenado está atualizado e é fidedigno após um longo período de armazenamento. Caso não seja possível identificar se ele está correto, pedir a atualização do dado para o titular e reavaliar a necessidade do armazenamento desse dado. Ex. Telefone e endereço são dados que podem ficar desatualizados com rapidez, avaliar se, após longo período, eles ainda são necessários (**PRINCÍPIO DA NECESSIDADE E DA QUALIDADE DOS DADOS**).

3.3 IMPORTÂNCIA DE NORMAS SETORIAIS E REGULATÓRIAS

Ressalta-se que a exclusão dos dados deve ser analisada considerando não apenas a finalidade do tratamento, como também as outras obrigações legais aplicáveis. Por exemplo, no setor de telecomunicações e saúde[38], existem órgãos, como Agência Nacional de Telecomunicações (Anatel), Agência Nacional de Saúde Suplementar (ANS), Agência Nacional de Vigilância Sanitária (Anvisa), conselhos federais e regionais que possuem normas específicas sobre a necessidade de armazenamento de dados pessoais.

Em outros setores, como o de veículos automotivos[39], existem procedimentos como o *recall* (chamamento), que obrigam o fornecedor a comunicar a nocividade ou periculosidade de produtos após sua colocação no mercado de consumo (Portaria nº 618, de 1º de julho de 2019,do Ministério da Justiça). Esse procedimento pode tornar necessário o armazenamento dos dados dos consumidores para apresentar certificados de atendimento aos chamamentos, relatórios e outras informações a órgãos, como a Secretaria Nacional do Consumidor e o Departamento Estadual de Trânsito (Detran), prorrogando o prazo para armazenamento de dados pessoais.

38 Para mais informações sobre as especificidades dos dois setores ver: CONFEDERAÇÃO NACIONAL DE SAÚDE – CNSAÚDE. **Código de boas práticas**: proteção de dados para prestadores privados em saúde. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 30 jun. 2023.

39 O processo no setor de veículos automotivos é regulamentado pela Portaria Conjunta nº 3, de 1º de julho de 2019, do Ministério de Estado da Infraestrutura e do Ministério de Estado da Justiça e Segurança Pública, que dispõe sobre o procedimento de *recall* especificamente para o mercado de veículos.

Não à toa, a LGPD possui bases legais específicas tanto para o tratamento de dados ordinários (art. 7º, II, da LGPD) quanto bases de dados sensíveis (art. 11, II, a, da LGPD), que tem como objetivo endereçar essas demandas regulatórias e legais. A utilização dessas bases deve, contudo, se ater à aplicação dos princípios da necessidade e finalidade, não podendo justificar o armazenamento de todos os dados de um titular de forma irrestrita. Assim, ainda que alguns dados sejam utilizados para o atendimento de obrigações regulatórias, é necessário avaliar se não é possível excluir parte dos dados do titular, pseudonimizar ou mesmo anonimizar as informações.

Além de ser necessário considerar o princípio da minimização em todo o tratamento realizado, outros prazos como prescricionais (ex. arts. 205 e 206 do Código Civil, etc.) também devem ser considerados. Os prazos prescricionais são particularmente importantes para dados que constam em documentos com informações de segurança e acesso, documentos relacionados a relações trabalhistas, obrigações fiscais ou outros documentos relevantes para eventuais defesas em processos judiciais e administrativos. Por esse motivo, a LGPD também prevê base legal específica para endereçar as hipóteses nas quais o tratamento de dados é necessário para o exercício regular de direitos (art. 7º, VI e art. 11, II, d, da LGPD).

A necessidade de armazenar dados para cumprimento de obrigações legais ou regulatórias e para o exercício de direitos por vezes pode demandar um longo período de tempo até a exclusão da informação. Assim, nesses casos, é fundamental que os dados estejam mapeados para quando tiverem que ser excluídos seja possível identificar sua localização.

Assim, recomenda-se que a criação das chamadas tabelas de temporalidade e políticas de retenção possuam informações sobre:

- Dados armazenados.
- Prazo de guarda.
- Finalidade.
- Trata-se de cumprimento de obrigação legal ou regulatória?
  - Qual norma subsidia a obrigação?
- Trata-se de exercício regular de direitos?
  - Quais normas e prazos prescricionais foram considerados?
- Onde o dado está armazenado?

3.4 PEDIDO DE EXCLUSÃO PELO TITULAR DOS DADOS

Na medida em que diplomas normativos como a CLT e o Código Civil possibilitam que os titulares dos dados recorram ao Judiciário mesmo após o término das relações, em algumas situações, as empresas não podem excluir, de forma definitiva, os dados pessoais dos titulares, sob o risco de prejudicarem o seu exercício de defesa em uma *lide* potencial. Ademais, as obrigações regulatórias supramencionadas também impedem que o pedido de exclusão de dados seja atendido de forma irrestrita.

Dessa forma, ainda que os titulares solicitem a exclusão dos dados logo após o término da relação, tais dados podem ser mantidos para garantir o exercício de direitos em processos judiciais e cumprimento de obrigações legais e regulatórias. Tal hipótese foi prevista de forma expressa pelo art. 16 da LGPD, que possibilita a conservação de dados para as seguintes finalidades:

- Cumprimento de obrigação legal ou regulatória pelo controlador (inciso I).
- Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (inciso II).
- Transferência a terceiro (inciso III).
- Uso exclusivo do controlador, desde que anonimizados os dados (inciso IV).

Vale ressaltar que é necessário avaliar quais dados, de fato, são necessários para o atendimento dessas finalidades e quais dados fazem parte do pedido do titular. A utilização das bases legais supramencionadas não pode servir como *guarda-chuva* para todos os dados do titular.

4 PROTOCOLO PARA TRATAMENTO DE DADOS PARA *MARKETING*

4.1 INTRODUÇÃO

A utilização de dados pessoais nas estratégias de *marketing* alterou-se de forma significativa com a utilização de dados pessoais. O tratamento de dados pode ser simples, utilizando-se apenas *e-mail*s e telefones fornecidos para realização de contatos sobre produtos e serviços ou, então, com as novas tecnologias, a publicidade passa a poder ser direcionada com base no comportamento dos consumidores, localização geográfica, IPs, hábitos de navegação, etc. Assim, esta talvez seja uma das maiores preocupações das empresas que buscam a adequação de suas práticas à LGPD.

Ainda que nem todos participantes da indústria realizem operações de tratamento de dados para fins de captação de clientes e *marketing* direto, fato é que a maioria das empresas que se relacionam diretamente com consumidores (B2C) utilizam dados pessoais para essa finalidade ou, então, ainda que a relação de algumas empresas não seja com o consumidor final, por vezes, dados relacionados aos hábitos de consumo podem ser relevantes para o desenvolvimento de novos produtos, de modo que alguns aspectos desse protocolo podem ser úteis.

Independentemente da complexidade do tratamento de dados realizado para estratégias de *marketing*, existem preocupações comuns que devem ser consideradas nas práticas das empresas. Isso porque, com a entrada em vigor da LGPD, as discussões sobre práticas de publicidade passaram a perpassar por temas comuns, como a adequação das bases legais e práticas que garantem a transparência.

Veja-se que a LGPD não proíbe a publicidade direcionada, ela apenas acrescenta as condições de legitimidade para que os dados pessoais sejam utilizados. Essa mudança pode ser vista como positiva, pois as empresas que se adequam à lei podem ter significativa vantagem competitiva em relação às empresas que não estão adequadas.

O direcionamento de publicidade pode ocorrer de três principais formas[40]:

i) **Direcionamento de publicidade com base em dados informados pelo próprio titular** (por ex. lista de *e-mails*).

ii) **Direcionamento com base em dados coletados por conta da utilização de serviços ou aplicativos** (por ex. GPS, histórico de compras, etc.).

iii) **direcionamento com base em dados inferidos** (por ex. formação de perfil por meio do comportamento em redes – histórico de navegação, "curtidas", etc.).

Especialmente nos direcionamentos com base em dados coletados e inferidos, é necessária especial atenção à forma do tratamento de dados. A utilização dos dados do titular deve respeitar o princípio da não discriminação, não podendo ser realizado tratamento para fins discriminatórios, ilícitos ou abusivos[41]. Essa previsão impede, por exemplo, que sejam utilizados critérios manifestamente racistas, que violem o disposto na Lei nº 7.716/1989, para o direcionamento de publicidade.

Insta ressaltar que a utilização de dados pessoais nas estratégias de *marketing* não é novidade. O envio de *e-mails*, inclusive, foi objeto do Código de Autorregulamentação para a Prática de *Email Marketing* (Capem) em 2009[42]. Já nessa época, as preocupações com o disparo de *e-mails* eram similares às que temos hoje com a LGPD, sendo pontuados como aspectos centrais para o envio de *marketing* por *e-mail*:

Elementos centrais da utilização de bases de dados

(art. 3º, Capem)

- Identificação do remetente.
- Vedação da utilização de domínio de terceiro que não faça parte do grupo econômico do remetente ou de parceiros.
- Indicação de assunto que seja relacionado ao conteúdo do *e-mail*.
- Inclusão de opção de descadastramento (*opt-out*), com mais uma opção para contato para essa finalidade, além de inclusão de *link* que possibilite o descadastramento.

40 EUROPEAN DATA PROTECTION BOARD - EDPB. **Guidelines 8/2020 on the targeting of social media users**. set. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 30 jun. 2023.

41 SCHERTEL, Laura; FUJIMOTO, Mônica, MATTIUZZO, Marcela. Discriminação algorítmica à luz da Lei Geral de Proteção de Dados. *In*: Bioni *et al.* (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

42 O código contou com a participação de grandes associações do mercado de anúncio e de comércio, a saber: ABA (Associação Brasileira de Anunciantes), Abemd (Associação Brasileira de *Marketing* Direto), Abradi (Associação Brasileira das Agências Digitais), Abranet (Associação Brasileira dos Provedores de Internet), Abrarec (Associação Brasileira das Relações Empresa Cliente), Agadi (Associação Gaúcha das Agências Digitais), Apadi (Associação Paulista das Agências Digitais), FecomércioRS (Federação do Comércio do Estado do Rio Grande do Sul), FecomércioSP (Federação do Comércio do Estado de São Paulo), Federasul (Federação das Associações Comerciais e de Serviços do Rio Grande do Sul), IAB (Interactive Advertising Bureau do Brasil), Internetsul (Associação dos Provedores de Acesso, Serviços e Informações da Rede Internet), Pro Teste (Associação Brasileira de Defesa do Consumidor), Seprorgs (Sindicato das Empresas de Informática do Rio Grande do Sul), tendo em vista a intenção da própria indústria em melhorar o uso do *email marketing*.

Padrões éticos para o envio de *e-mail*s para fins de publicidade

(art. 4º, Capem)

- Não é permitido o envio de *e-mail* para obtenção de permissão do destinatário para o envio de outros *e-mails*.
- O envio de arquivos em anexo aos *e-mails* deve ser precedido de autorização específica, prévia e comprovável do destinatário.
- Não é permitido enviar *link* que remeta a Códigos Maliciosos[43].
- Não é permitida a utilização de recursos que disfarcem o código original da mensagem, devendo ser utilizado o formato.
- Imagens, áudios e vídeos devem ser hospedados em servidores pertencentes às empresas participantes do processo de envio do *e-mail marketing* ou contratadas pelas empresas.
- O remetente deve disponibilizar a política de *opt-out*, informando o prazo de remoção do seu endereço eletrônico da base de destinatários, não sendo obrigatório o seu uso na existência de contrato entre o remetente e o destinatário (ex.: boleto bancário, avisos e extratos).
- O prazo para remoção de conteúdo não pode ser superior a 2 (dois) dias úteis, quando solicitado diretamente pelo *link* de descadastramento do *e-mail*, e de 5 (cinco) dias úteis quando solicitado por outros meios.

Observe-se que, por se tratar de código de autorregulação com o objetivo de indicar posturas consideradas "éticas", as disposições supracitadas não possuem caráter vinculativo em relação às empresas que pertencem à base industrial. Contudo, tais diretrizes podem auxiliar aqueles que têm como objetivo a realização de estratégias por *e-mail*.

Em relação aos contatos telefônicos, outra iniciativa autorregulada que merece destaque é o **Código de Conduta para oferta de Serviços de Telecomunicações por meio de *Telemarketing*** elaborado pelo Sistema de Autorregulação das Telecomunicações (Sart). Nesse código são apontadas as boas práticas na realização de ligações para consumidores.

43 Art. 2º, IV, da Capem: Código Malicioso – termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de troia, *rootkits*, etc.).

Código de Conduta *Telemarketing* – SART

(art. 4º)

- Não fazer ofertas sob pretexto de pesquisa ou sorteio, quando o verdadeiro objetivo for a comercialização de ofertas para os consumidores.
- Respeitar a vontade do consumidor sempre que ele manifestar a sua contrariedade quanto ao prosseguimento da ligação, encerrando a ligação e liberando a linha imediatamente.
- Não realizar ligações que não permitam a identificação pelos consumidores dos códigos de acesso utilizados pela prestadora na ligação.
- Não realizar ligações apenas para verificar a disponibilidade do consumidor em atender às ligações por meio de discador preditivo.
- Não finalizar as ligações abruptamente sem a identificação da prestadora e apresentação de ofertas.
- Realizar ligações apenas em horários oportunos compreendidos no período das 9 (nove) às 21 (vinte e uma) horas nos dias úteis e das 10 (dez) às 16 (dezesseis) horas nos sábados, salvo aquelas realizadas por solicitação ou com autorização dos consumidores, resguardadas as legislações específicas.
- Não realizar ligações nos domingos e feriados nacionais.
- Não realizar ligações de forma insistente, limitadas a no máximo 2 (duas) chamadas efetuadas pela empresa e recebidas pelo mesmo terminal de acesso do consumidor no mesmo dia, salvo aquelas realizadas por solicitação ou com autorização dos consumidores, resguardadas as legislações específicas.
- Não realizar ligações de forma insistente, limitadas a no máximo 15 (quinze) chamadas efetuadas pela empresa e recebidas pelo mesmo terminal de acesso do consumidor no mesmo mês, salvo aquelas realizadas por solicitação ou com autorização dos consumidores, resguardadas as legislações específicas.
- Não realizar ligações por meio de chamadas a cobrar para os consumidores.
- Não realizar ligações aleatórias ou para números sequenciais de consumidores.
- Assegurar que mensagens gravadas inseridas no início das ligações indiquem claramente a empresa que representa e informe o objetivo da ligação.

Ressalte-se que, ainda que as recomendações supracitadas possuam relação direta com o direito do consumidor[44], sob a perspectiva da proteção de dados, a utilização do *e-mail* ou do telefone para a oferta de produtos ou serviços também é considerada um tratamento de dados. Assim, as práticas mencionadas podem auxiliar as empresas da indústria a criar uma relação de confiança com os titulares e garantir que a utilização dos dados cumpra com os fundamentos principiológicos da legislação.

Em relação às condições de legitimidade para o tratamento de dados, são basicamente duas as principais bases legais utilizadas para essa finalidade: o consentimento e o legítimo interesse[45]. Ademais, os agentes de tratamento devem levar em consideração os direitos dos titulares e, especialmente, os princípios da finalidade, necessidade e transparência.

44 "Art. 6º. São direitos básicos do consumidor: [...] IV – a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços".

45 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 8/2020 on the targeting of social media users**. set. 2020. p. 14. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 30 jun. 2023.

4.2 BASES LEGAIS

A) CONSENTIMENTO

Conforme apontado na Parte 1, o consentimento já foi visto como a principal base legal para o tratamento de dados pessoais, existindo a falsa concepção de que ele seria hierarquicamente superior às outras. Tal noção não é diferente para o tratamento de dados realizado para fins de *marketing*.

Não obstante significativa aclamação de parte do mercado em relação à base legal do consentimento para o tratamento de dados para publicidade, nem sempre esta é a base mais adequada. Em primeiro lugar, o consentimento deve ser "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII, da LGPD).

Assim, a coleta do consentimento como base legal para publicidade (em especial a digital) pode comprometer o alcance da estratégia, bem como se restringir a um público que já teve contato com a marca/empresa. Isso se deve ao fato de que o consentimento exige o *opt-in*, e não apenas o *opt-out*, e garantir que a manifestação é inequívoca pode representar um desafio adicional, especialmente diante de discussões sobre a *fadiga de cliques*.

O EDPB utiliza a expressão *fadiga de cliques* ao tratar das centenas de pedidos de consentimento que o titular encontra diariamente, ressaltando o risco de que se reduzam os efeitos do consentimento como um instrumento de aviso e de reflexão do titular[46].

A própria dificuldade na aplicação do consentimento pode indicar que outra base legal deve ser utilizada no lugar do consentimento.[47] Essa ideia está presente também no relatório do CIPL, segundo o qual se fundamentar excessivamente na base legal do consentimento para além das situações em que o indivíduo tem real alternativa de escolha acerca do tratamento de dados pode levar à *fadiga do consentimento*, além de não atingir o objetivo de colocar as pessoas no controle sobre o fluxo de seus dados.[48]

Assim, a decisão sobre a utilização da base legal do consentimento deve considerar, pelo menos, os requisitos apontados na Parte 1 presentes na LGPD:

---

46 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679**. 2020. p. 19. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 30 jun. 2023.

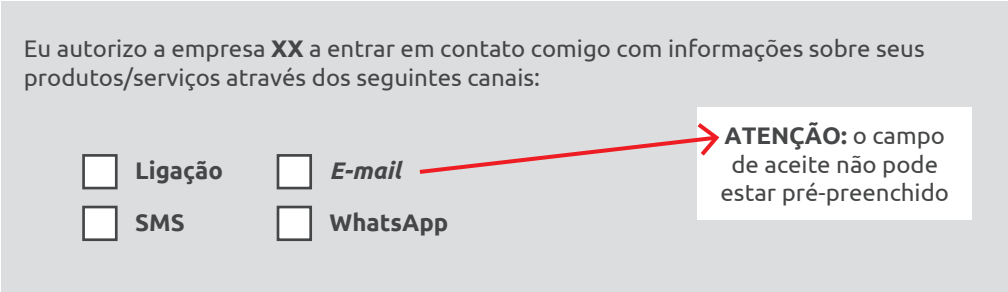
47 RPC. **ICO guidance**: consent is not the 'silver bullet' for GDPR compliance. 2018. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/blog-consent-is-not-the-silver-bullet-for-gdpr-compliance/ Acesso em: 5 jun. 2020.

48 CENTRE FOR INFORMATION POLICY LEADERSHIP - CIPL. **Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR**. 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. Acesso em: 5 jun. 2020.

- Oferecer uma escolha real, devendo constar de cláusula destacada das demais cláusulas contratuais caso seja fornecido por escrito (art. 8º, §1º).
- Possibilitar que o titular possa retirar o consentimento quando bem entender (caso não seja possível, o consentimento não é a base legal adequada (art. 8º, §5º).
- O controlador deve comprovar que o consentimento foi obtido de forma adequada (art. 8º, §2º).
- Ser fornecido para finalidades determinadas, não sendo permitida a utilização de autorizações genéricas (art. 8º, §4º).
- Caso o controlador necessite compartilhar os dados com outros controladores, é necessária a coleta de consentimento específico para este fim.
- Garantir que o titular possa receber cópia integral de seus dados pessoais em formato que permita sua utilização subsequente, nos termos a serem regulamentados pela ANPD e respeitados os segredos comercial e industrial (art. 19, §3º).

Ainda assim, a coleta do consentimento pode ser realizada de diversas formas como instrumentos contratuais, formulários, cadastros realizados para utilização de plataforma digital ou *site*, aviso de *cookies*, sendo mecanismo válido de cumprimento com a LGPD. Contudo, é necessário ressaltar que, apesar da ampla utilização de aviso de *cookies* nos *sites* e confirmação de aceite, no Brasil, diferentemente da Europa, a sua utilização não é obrigatória.

Caso o consentimento seja coletado por meio de caixas de confirmação, é necessário que elas possuam a descrição da finalidade específica e não estejam pré-preenchidas quando o usuário for realizar algum cadastro.



Por fim, a utilização de consentimento pode ser interessante em casos nos quais as tecnologias utilizadas para o direcionamento de publicidade fizerem uso de dados inferidos ou que os dados coletados possam ser considerados excessivos, como a localização. Isso porque, conforme será exposto em detalhes a seguir, a utilização da base legal do legítimo interesse não comporta o tratamento de dados que possa prejudicar os direitos dos titulares ou possa exceder as suas legítimas expectativas[49]. Assim, quando houver dúvidas sobre a aplicação do legítimo interesse, o consentimento também é recomendável.

49 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 8/2020 on the targeting of social media users**. set. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 30 jun. 2023.

B) LEGÍTIMO INTERESSE

Diante dos desafios que o consentimento representa, a base legal do legítimo interesse vem sendo amplamente utilizada. Inclusive, autoridades, como a Information Commissioner's Office (ICO), aconselham a utilização dessa base para "evitar o bombardeio de pessoas com solicitações de consentimento desnecessárias e a '*consent fatigue*'". Quando realizado de forma cuidadosa, acompanhado de informações claras sobre o tratamento de dados e *opt-out*, essa pode ser uma ótima maneira de proteger os interesses do titular, de acordo com a autoridade[50].

No bojo do tratamento de dados para fins publicitários, a utilização do legítimo interesse pode ser uma alternativa mais simples que a coleta do consentimento. Assim, de acordo com o Código de Conduta do setor publicitário espanhol, quando da escolha acerca da base legal aplicável, contudo, é necessário levar em consideração[51]: i) as expectativas dos titulares; ii) se os titulares são grupos minoritários ou que necessitam de proteção adicional por conta de alguma vulnerabilidade; iii) se o titular pode se opor ao tratamento com facilidade; iv) se a publicidade se baseia na formação de perfis; e v) frequência dos envios.

Nesse sentido, por se tratar de hipótese autorizativa considerada "ampla", a Avaliação de Legítimo Interesse (LIA) é um passo que pode ser adotado no processo de tomada de decisão das empresas a respeito da aplicação da base legal prevista no art. 7°, IX. Importa ressaltar que o legítimo interesse pode ser utilizado para "apoio e promoção de atividades do controlador" (art. 10, I, da LGPD); e "proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem" (art. 10, II, da LGPD), devendo o controlador:

- Respeitar as expectativas dos titulares (art. 10, II, da LGPD).
- Respeitar os direitos e liberdades fundamentais dos titulares (art. 10, II, LGPD).
- Utilizar apenas dados estritamente necessários para a finalidade pretendida (art. 10, §1°, da LGPD).
- Adotar medidas que garantam a transparência no tratamento de dados (art. 10, §2°, da LGPD).
- Apresentar relatório de impacto à ANPD quando ela solicitar (art. 10, §3°, da LGPD).

50 INFORMATION COMMISSIONER'S OFFICE – ICO. When can we rely on legitimate interests? 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/. Acesso em: 30 jun. 2023.

51 ASSOCIATION FOR THE SELF-REGULATION OF COMMERCIAL COMMUNICATION - AUTOCONTROL. **Code of Conduct**: data processing in advertising activities. 2021. Disponível em: https://edpb.europa.eu/system/files/2021-04/code_of_conduct_data_processing_in_advertising_activities_en.pdf. Acesso em: 30 jun. 2023. Esse código foi aprovado pela: AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS – AEPD. **Resolution approving the code of conduct and accreditation of the monitoring body**. 2018. Disponível em: https://edpb.europa.eu/sites/default/files/conduct/resolucion-aprobacion-cc.0004.2018-autocontrol_en.pdf. Acesso em: 30 jun. 2023.

Especialmente quando comparada à base legal *consentimento*, o legítimo interesse pode trazer vantagens para o tratamento, tendo em vista que o consentimento pode não ser facilmente coletado ou pode não ser passível de revogação. Assim, o legítimo interesse não deve ser considerado o *último recurso* quando os dados não sensíveis forem tratados.

Nesse sentido, uma vez que a utilização dessa base legal pode gerar uma grande insegurança, recomenda-se a utilização do LIA antes que o tratamento seja iniciado ou quando a finalidade do tratamento foi modificada. Esse procedimento baseia-se nas melhores práticas do setor, bem como nas melhores práticas internacionais[52], sendo o modelo Europeu a base para o protocolo proposto. Assim, recomenda-se que os seguintes elementos sejam observados:

- Contexto, propósito e benefício das atividades de processamento de dados, além dos riscos de não realizar o processamento.
- O interesse legítimo do controlador, terceiros ou grupos de indivíduos ou da sociedade, assim como seus direitos e liberdades e outros direitos relativos à proteção de dados.
- Interesses, liberdades e direitos dos titulares, bem como suas expectativas legítimas nas quais estão fundadas a sua relação com o controlador.
- Riscos e danos que podem resultar do tratamento ou da ausência de tratamento, bem como a gravidade que tais danos podem causar aos titulares.

Para análise desses elementos, recomenda-se a utilização do teste de três etapas, para que sejam verificadas: i) finalidade; ii) necessidade; e iii) proporcionalidade.

PARTE 1 – Identificando o legítimo interesse

Qual o propósito do processamento de dados?
Qual o benefício que se espera do processamento?
O tratamento de dados pessoais é realizado pelo controlador ou por terceiro para atender a um legítimo interesse da companhia?
Por que esse processamento é importante para o controlador?
Algum interesse público pode ser atingido com o processamento?
Existe algum problema ético ou discriminatório no processamento?

52 INFORMATION COMMISIONER'S OFFICE – ICO. **How do we apply legitimate interests in practice?** 2023. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/. Acesso em: 30 jun. 2023; CENTRE FOR INFORMATION POLICY LEADERSHIP – CIPL. **How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation**. 2021. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf. Acesso em: 30 jun. 2023; INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS – IAPP. **Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation**. 2018. Disponível em: https://iapp.org/resources/article/guidance-on-the-use-of-legitimate-interests-under-the-eu-general-data-protection-regulation/. Acesso em: 30 jun. 2023.

PARTE 2 – Teste da necessidade

Este processamento irá auxiliar no propósito buscado?
Este propósito pode ser atingido de outras formas?
É possível atingir o mesmo objetivo utilizando menos dados ou processando esses dados de forma menos invasiva?

PARTE 3 – Teste da proporcionalidade

Há expectativa do titular de que esses dados sejam tratados?
Qual a natureza da relação entre o titular dos dados e o controlador?
Quais os possíveis impactos do tratamento de dados nos titulares e o quão graves eles podem ser?
Algum dos titulares são vulneráveis de alguma forma?
Os dados foram obtidos diretamente dos titulares?
É possível oferecer o *opt-out* ao titular sem que o tratamento seja comprometido?
Informações sobre o tratamento de dados são fornecidas ao titular? Há comunicação clara e anterior aos propósitos do tratamento de dados?
É possível adotar salvaguardas?

Ressalte-se que o teste não tem como objetivo apresentar resposta exata sobre a possibilidade de utilização dessa base legal, sendo necessária a avaliação do controlador se os benefícios gerados pelo processamento não serão superados pelos riscos. Adicionalmente, caso não tenham sido adotadas, sugerimos a adoção de salvaguardas e controles, tais como a anonimização, o controle de acesso aos dados, os mecanismos de autenticação, o inventário com acessos aos registros de conexão e o acesso a aplicações sejam adotadas sempre que possível.

4.3 TRANSPARÊNCIA E CONTROLE PELO USUÁRIO

Para assegurar a adequação das medidas supracitadas elas devem ser acompanhadas pelo princípio da transparência. Em especial quando se trata de disponibilização de informações para os usuários, recentemente a transparência centrada no usuário (*user-centric transparency*)[53] vem sendo pontuada como aspecto importante a ser considerado. Este é um conceito voltado para a compreensão do usuário e não somente destinado ao cumprimento de requisitos impostos pelos reguladores, que acabou resultando em uma relação paradoxal entre a garantia do acesso à informação e o seu excesso.

53 CENTRE FOR INFORMATION POLICY LEADERSHIP - CIPL. **Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR**. 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. Acesso em: 5 jun. 2020.

O conceito está presente em relatório do CIPL que defende que o princípio da transparência deve ser centrado no usuário, sendo específico ao contexto, flexível, dinâmico e passível de adaptações, possibilitando que o usuário obtenha informação de forma clara e compreensível, mesmo nas situações em que o consentimento não seja a base legal aplicável.

Ou seja, a transparência deve ir além das políticas de privacidade disponibilizadas nos *sites*, devendo ser adaptadas aos contextos específicos do tratamento de dados e por meio da utilização de outros mecanismos que não apenas a linguagem escrita descritiva. Esse conceito mais atual de transparência, voltado para a efetiva compreensão do titular de dados, acaba por contrastar com interpretações que visam a um detalhamento exaustivo das atividades de tratamento de dados, sem qualquer preocupação com a acessibilidade e compreensão pelo titular de dados pessoais.

Nesse sentido, o documento formulado pelo CIPL ressalta melhores práticas para garantir que a transparência seja efetiva, tendo em vista "o equilíbrio entre a clareza e a completude e buscando formas inovadoras para garantir que o equilíbrio em favor da clareza conste no conteúdo dos informativos"[54].

Transparência centrada no usuário tem como fundamento repensar a relação entre o usuário e a confiança no meio digital, construindo a compreensão sobre os benefícios do tratamento de dados e o valor do produto/serviço, bem como as opções disponíveis, de maneira apartada da informação voltada para cumprir com exigências legais[55]. Nesse sentido, reunimos, a seguir, algumas das práticas recomendadas divididas em cinco eixos: i) clareza; ii) seletividade; iii) razoabilidade; iv) contexto; e v) *design* personalizado[56]:

CLAREZA

- Dispor de forma clara informações-chave sobre:
  - objetivos do tratamento;
  - base legal de processamento;
  - lógica envolvida na decisão automatizada;
  - envolvimento de outros agentes de tratamento e eventuais compartilhamentos;
  - transferência de dados internacionais; e
  - direitos do usuário (acesso, retificação, objeção, etc.).

54 CENTRE FOR INFORMATION POLICY LEADERSHIP – CIPL. **Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR**. 2017. p. 6. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. Acesso em: 5 jun. 2020.

55 CENTRE FOR INFORMATION POLICY LEADERSHIP – CIPL. **Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR**. 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. Acesso em: 5 jun. 2020.

56 CENTRE FOR INFORMATION POLICY LEADERSHIP – CIPL. **Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR**. 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. Acesso em: 5 jun. 2020; SCHAUB, HOLZ, UTZ, Op. Cit, PP. 13; MCDONALD, Aleecia; LOWENTHAL, Op. Cit. pp. 331-354; GLUCK, et al., Op. Cit.

SELETIVIDADE

- Nem todas as informações sobre o tratamento de dados precisam ser apresentadas ao mesmo tempo, sendo possível que informações gerais sejam disponibilizadas nas políticas de privacidade e as informações que apresentam risco maior ou que o tratamento fuja das expectativas do usuário sejam apresentadas no momento da coleta.

RAZOABILIDADE

- A medida da transparência e o formato deve ser razoável, considerando especificidades do tipo de tratamento realizado.

CONTEXTO

- Para garantir que o usuário compreenda as informações e exerça seus direitos de forma apropriada, as organizações devem considerar a compreensão dos usuários em relação a produtos e serviços em contextos determinados e no momento adequado.
- Recomenda-se a utilização de diversas ferramentas, como políticas de privacidade, *pop-ups*, painéis de controle, *dashboards*, guias do usuário, tutoriais, etc.

***DESIGN* PERSONALIZADO**

- Estratégias, como posicionamento das informações e utilização de ícones, podem facilitar a compreensão do usuário.

5 PROTOCOLO PARA ELABORAÇÃO DE RELATÓRIO DE IMPACTO

5.1 INSTRUMENTOS DE AVALIAÇÃO DE RISCO

O Relatório de Impacto à Proteção de Dados (RIPD) possibilita o registro e a avaliação de 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 (art. 5º, XVII, da LGPD). Como o documento, ainda, não foi objeto de regulamentação pela ANPD, utilizaremos as melhores práticas setoriais[57] e internacionais para propor este protocolo, em especial o Relatório do *Article 29 Data Protection Working Party.*

O RIPD é mencionado nos arts. 10, §3º e 38[58] da LGPD, mas as hipóteses nas quais a ANPD pode solicitar o relatório de impacto, ainda, são amplas. Nesse ponto, importa ressaltar que a legislação brasileira difere da europeia, que prevê, em seu art. 35 (GDPR)[59], um rol exemplificativo com atividades que deveriam ser precedidas da realização de relatório de impacto, tendo em vista que esse pode ser um instrumento de mitigação de riscos.

Nos termos do parágrafo único do art. 38 da LGPD, o relatório de impacto deve conter, no mínimo, "*descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados*" (grifo nosso). Apesar

57 CONEXIS. **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em: 2 jul. 2023.

58 Art. 10. [...] § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

59 Art. 32. (1) Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. (2) Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado. (3) A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.o 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou c) Controle sistemático de zonas acessíveis ao público em grande escala.

de a ANPD, ainda, não ter endereçado especificamente a metodologia de elaboração e as hipóteses de elaboração obrigatória, sugere-se que a metodologia de elaboração do relatório seja associada à perspectiva de risco.

Nesse sentido, extrai-se da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, os seguintes critérios para definição de operações de tratamento de alto risco:

DADOS PESSOAIS DE ALTO RISCO

- **Critério geral:** tratamento de dados pessoais em larga escala ou que possa afetar significativamente interesses e direitos fundamentais dos titulares
- **Critérios específicos:**
  - Uso de tecnologias emergentes ou inovadoras.
  - Vigilância ou controle de zonas acessíveis ao público.
  - Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular.
  - Utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

Assim, sugerimos um modelo de relatório de impacto que pode ser aplicado em algumas hipóteses nas quais identificamos risco elevado, sem prejuízo de elaboração em outras que a empresa entenda necessário[60]:

- Controle sistemático dos titulares de dados ou sistema de pontuação (*scoring*).
- Realização de decisão automatizada com efeitos jurídicos.
- Perfilamento (*profiling*).
- Processamento de dados pessoais em larga escala tendo em vista, número de titulares envolvidos, volume de dados, duração da atividade e dimensão geográfica da atividade de tratamento.
- Realização de correspondências ou combinação de dados diferentes – enriquecimento de bases de dados.
- Tratamento envolvendo dados de pessoas vulneráveis (crianças, idosos ou pessoas com necessidades especiais).
- Uso ou aplicação inovadora de soluções técnicas ou organizacionais.
- Tratamentos de dados que possam impedir ou dificultar que titulares de dados exercitem seus direitos ou usem um serviço/contrato.

60 Modelo elaborado com base nas melhores práticas indicados pelos documentos: **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em: 2 jul. 2023; **WP29. Guidelines on Data Protection Impact Assessment (DPIA)**. Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. Acesso em: 2 jul. 2023

5.2 MODELO DE RELATÓRIO DE IMPACTO

A elaboração de um Relatório de Impacto deve passar pelas seguintes etapas[61]:

ETAPAS – RELATÓRIO DE IMPACTO

1) Descrição do tratamento.
2) Avaliação da necessidade e proporcionalidade.
3) Medidas prevista para demonstrar conformidade.
4) Avaliação dos riscos para direitos e liberdades.
5) Medidas previstas para mitigar riscos.
6) Documentação.
7) Controle e reexame.

Ademais, entre as informações que devem constar no relatório de impacto, estas devem ser definidas por meio da análise específica das operações de tratamento realizadas pelas empresas. Contudo, alguns aspectos são fundamentais para a avaliação de risco do tratamento de dados: i) compreensão sobre as atividades desempenhadas e tipos de dados pessoais tratados; ii) identificação dos direitos dos titulares; iii) riscos envolvidos nas operações e medidas adotadas para mitigá-los; e iv) avaliação do DPO acerca dos riscos e das estratégias adotadas.

INFORMAÇÕES DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS[62]

Descrição das atividades e dos dados pessoais	Finalidade do tratamento de dados
	Quem são os titulares dos dados?
	Qual a relação do controlador com o titular?
	Quais dados são utilizados no tratamento?
	São tratados dados sensíveis?
	O titular possui informações sobre o tratamento de dados?
	Os dados pessoais são compartilhados com terceiros?
	Os dados foram coletados diretamente dos titulares?
	O tratamento de dados é realizado em bases enriquecidas?
Direito dos titulares	O titular possui informações sobre o tratamento de dados?
	Os titulares possuem acesso ao relatório de dados tratados?
	Os dados são tratados por meio de decisões automatizadas?
	O tratamento de dados pode levar a tratamento discriminatório?

61 Adaptação do esquema apresentado pelo Relatório do *Article 29 Data Protection Working Party*. WP29. Guidelines on Data Protection Impact Assessment (DPIA). Disponível em: https://ec.europa.eu/newsroom/article29/items/611236. fl 19. Acesso em: 2 jul. 2023.

62 A referida tabela também foi apresentada no Código de Boas Práticas do Setor de Telecomunicações: **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em: 2 jul. 2023.

Riscos e mitigação	Existem riscos que podem afetar a qualidade ou confidencialidade dos dados? Se sim, quais?
	Identificar a fonte do risco.
	Quais são os eventos potencialmente lesivos?
	Existem controles, salvaguardas ou planos de ação capazes de mitigar os riscos?
	Qual a avaliação da gravidade do risco?
Avaliação DPO	Avaliação de proporcionalidade e necessidade.
	Avaliação sobre existência de atendimento aos direitos do titular.
	Avaliação sobre a estratégia de mitigação de riscos proposta.

6 PROTOCOLO PARA SEGURANÇA DA INFORMAÇÃO

6.1 INTRODUÇÃO

A Segurança da Informação consubstancia-se na LGPD por meio dos princípios da segurança (art. 6º, VII, da LGPD), da prevenção (art. 6º, VIII, da LGPD) e das obrigações específicas previstas no art. 46 da LGPD, por meio do qual:

> os agentes de tratamento devem **adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

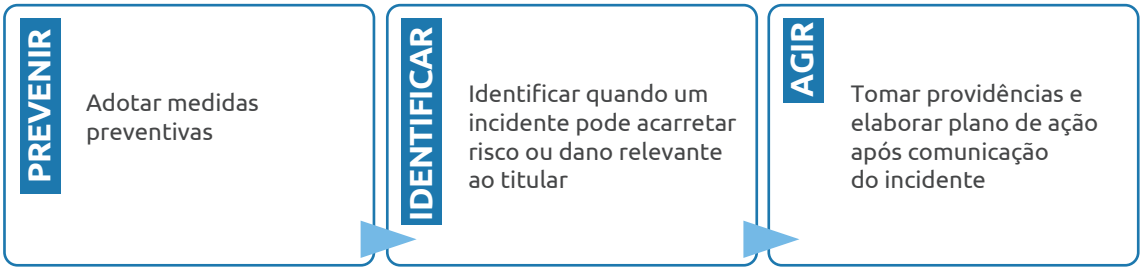
Na hipótese de as medidas adotadas não serem suficientes e um incidente de segurança ocorra, o controlador deve notificar o incidente à autoridade e aos titulares dos dados, caso o incidente possa acarretar **risco ou dano relevante aos titulares dos dados pessoais** (art. 48 da LGPD[63]). Esse quesito vem sendo discutido pela ANPD em suas consultas públicas e já foram divulgadas as primeiras linhas sobre os critérios que devem ser utilizados para a constatação desses riscos e danos[64].

Para a ANPD, importam apenas aqueles incidentes de segurança que efetivamente envolvam dados pessoais, e não todo tipo de violação à segurança informacional das empresas. Por exemplo, se um sistema que possui apenas listagem de produtos e estoque é violado, sem qualquer dado pessoal ou informação que possa identificar uma pessoa natural, tal incidente não precisa ser comunicado para a autoridade.

63 Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I – a descrição da natureza dos dados pessoais afetados; II – as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV – os riscos relacionados ao incidente; V – os motivos da demora, no caso de a comunicação não ter sido imediata; e VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I – ampla divulgação do fato em meios de comunicação; e II – medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

64 ANPD. **Comunicação de incidente de segurança**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 2 jul. 2023.

Nesse sentido, esse protocolo baseia-se em três fases relacionadas à segurança da informação[65]:



6.2 ASPECTOS PREVENTIVOS

Para que sejam adotados os aspectos preventivos do protocolo de segurança, três níveis de requisitos podem ser adotados. Assim, foram estabelecidos três níveis de prioridade para implementação dos requisitos de segurança: i) **requisitos mínimos**; ii) **requisitos prioritários** – que, caso não tenham sido implementados, podem ser iniciados imediatamente ou podem estar em fase de implementação; iii) **requisitos avançados** – podem ser implementados assim que os requisitos prioritários estiverem cumpridos.[66]

REQUISITOS DE SEGURANÇA MÍNIMOS	
Políticas e Conscientização	Criar, revisar e comunicar diretrizes considerando melhores práticas para assegurar a proteção e privacidade dos dados pessoais.
Gestão de Identidades e Acessos	Fornecer acessos somente às pessoas autorizadas e revogá-los quando não forem mais necessários ou a pessoa não trabalhar mais na empresa.
Gestão de *Backups*	Garantir que os dados relevantes para o negócio tenham uma cópia de segurança, devidamente protegida contra acessos não autorizados.
Gestão de Ativos	Inventariar os ativos que tratam dados pessoais e garantir os requisitos mínimos de segurança.
Gestão de Segurança *Endpoint*	Garantir que todos os ativos que tratam dados pessoais tenham uma solução de *antimalware* e *personal firewall* instalada e atualizada periodicamente.

65 Divisão semelhante foi adotada no Código de Boas Práticas do setor de Telecomunicações. **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações.** Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em: 2 jul. 2023.

66 Divisão semelhante foi adotada no Código de Boas Práticas editado pela CNSAÚDE. Disponível em: http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/. Acesso em: 30 jul. 2021.

REQUISITOS DE SEGURANÇA PRIORITÁRIOS	
Monitoramento e Gestão de Incidentes	Monitorar o comportamento dos acessos e da segurança dos ativos envolvidos no tratamento dos dados. Estar preparado para identificar comportamentos e/ou acessos não autorizados.
Gestão de Fornecedores	Avaliar se o fornecedor contratado possui cláusulas contratuais de segurança e privacidade quanto ao tratamento de dados pessoais.
***Log* de Sistemas Críticos**	Avaliar e garantir que sejam registradas as atividades de tratamentos dos dados: data, horário, duração, identidade do funcionário/responsável pelo acesso e a ação executada/processada.
Controle para Vazamento de Informações	Prevenir o vazamento dos dados pessoais em todo o seu ciclo de tratamento.
Segurança Física	Garantir a segurança do acesso físico às informações tratadas em mídias eletrônicas, papel e sistemas.
Gestão de Vulnerabilidade / *Pentest*	Avaliar a execução de testes de segurança nos sistemas que tratam dados pessoais, priorizando os sistemas expostos na internet.
Transferência de Dados	Garantir a segurança na comunicação durante os processos de transferências de dados.

REQUISITOS DE SEGURANÇA AVANÇADOS	
Arquitetura de Segurança	Analisar e identificar melhorias para a proteção dos dados pessoais envolvendo a arquitetura de tecnologias que suportam os produtos/sistemas, incluindo Cloud.
Exclusão de Dados Tratados	Mapear a localização dos dados pessoais para que possam ser excluídos quando solicitado.
Mascaramento de Dados	Avaliar o uso de mascaramento de dados quando aplicável.
Pseudoanonimização	Avaliar o uso de pseudonimização quando aplicável.
Desenvolvimento Seguro	Avaliar se o produto ou sistema estão integrados na esteira atual que contempla análise e implementação de requisitos de segurança para o desenvolvimento seguro.
Criptografia	Avaliar a utilização de recursos de criptografia de dados pessoais quando necessária.

6.3 IDENTIFICAÇÃO DE INCIDENTE DE SEGURANÇA E ANÁLISE DE RISCO

O estudo sobre as melhores práticas para identificação de incidente de segurança e análise de risco foi uma das primeiras iniciativas tomadas pela ANPD quando de sua criação, tendo sido realizada por meio da tomada de subsídios sobre incidentes de segurança nos termos do art. 48 da LGPD, proposta pela Nota Técnica nº 3/2021/CGN/ANPD. Esse passo é de suma importância, tendo em vista que nem todo incidente de segurança poderá afetar dados pessoais. Por esse motivo, a identificação do risco ou danos que o incidente pode ter causado para os titulares é etapa necessária antes da notificação do incidente à ANPD.

Para **avaliação de risco ou de dano relevante**, sugere-se adotar métricas e parâmetros para a realidade brasileira. Com o objetivo de verificar a criticidade de um incidente, o controlador deverá considerar uma combinação da gravidade do impacto potencial sobre os direitos e as liberdades dos indivíduos e a probabilidade da sua ocorrência. Nessa avaliação, os seguintes passos devem ser realizados:

Realizar investigação diretamente com a fonte denunciante, a fim de verificar a veracidade do incidente, obtendo informações comprobatórias da ocorrência deste.

↓

Avaliar se os dados são efetivamente passíveis de danos aos titulares, com base nos critérios apontados no primeiro item desta tomada de subsídios.

↓

Avaliar se o volume de informações relevantes comprovadamente comprometidas é expressivo em relação ao volume (%) de informações de posse da organização que sofreu o dano.

↓

Considerar a classificação do risco.

↓

Avaliar os controles e as medidas mitigatórias existentes e associadas aos riscos na organização.

CHECKLIST – AVALIAÇÃO DO INCIDENTE DE SEGURANÇA

- ☑ **Natureza, sensibilidade e volume de dados pessoais:**
  – Perda de integralidade de dados.
  – Indisponibilidade de dados.
- ☑ **Veracidade do incidente.**
- ☑ **Facilidade da identificação dos titulares:**
  – Dados anonimizados e/ou criptografados.
  – Titulares relacionados às chaves de criptografia dos dados violados.
  – Dados relacionados às credenciais de autenticação (matrícula, por exemplo) das partes interessadas.
- ☑ **Nível de atualização e validade dos dados.**
- ☑ **Severidade das consequências aos titulares.**
- ☑ **Características especiais dos titulares.**
- ☑ **Número de titulares afetados.**
- ☑ **Grau de exposição de dados vulnerados** (ambiente interno, externo e público).
- ☑ **Medidas técnicas, organizacionais e administrativas adotadas para mitigar o impacto sobre os titulares.**
- ☑ **Aspectos relacionados à violação de segurança para acesso aos dados** (intencional, não intencional, ataque cibernético).
- ☑ **Se o responsável pelo dado objeto do incidente auferiu, direta ou indiretamente, vantagem com o ocorrido.**
- ☑ **Se o ambiente afetado pelos incidentes está relacionado ao país de operação de negócio do controlador/operador.**

6.4 COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

Até o momento, a ANPD prescreveu o prazo de 2 (dois)[67] dias úteis para comunicação de um incidente de segurança. Nos termos das instruções dadas pela autoridade[68], esta recomenda a comunicação das seguintes informações em caso de incidente de segurança:

Identificação e dados de contato de:

- Entidade ou pessoa responsável pelo tratamento.
- Encarregado de dados ou outra pessoa de contato.
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

Informações sobre o incidente de segurança com dados pessoais:

- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, entre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados.
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.
- Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Possíveis problemas de natureza transfronteiriça.
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Já o titular de dados deve ser comunicado quando o incidente possa acarretar risco ou dano relevante. De acordo com a ANPD, a probabilidade de um incidente acarretar risco ou dano é maior quando podem "causar aos titulares danos materiais ou morais, expô-los a situações de discriminação ou de roubo de identidade, especialmente se envolverem dados em larga escala, sensíveis e de grupos vulneráveis como crianças e adolescentes ou idosos"[69].

67 Durante a revisão deste guia, a ANPD publicou, em 2 de maio de 2023, consulta pública para receber contribuições sobre a minuta de resolução referente ao Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. Com o objetivo de regular a comunicação com a ANPD e com os titulares afetados no caso da ocorrência de incidente de segurança envolvendo dados pessoais que possa causar risco ou dano relevante aos titulares, conforme artigo 48 da LGPD, entre suas disposições, a minuta regula prazo para a comunicação, que deverá ser realizada pelo controlador à ANPD e ao titular dos dados em 3 (três) dias úteis a contar do conhecimento do incidente.

68 Para mais informações acessar: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 31 jul. 2021.

69 ANPD. **Comunicação de incidente de segurança**. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis>. Acesso em: 7 jul. 2023.

Assim, caso ocorra um incidente de segurança envolvendo dados pessoais, a ANPD solicita que o seguinte formulário seja preenchido[70]:

Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD)

Dados do Controlador	
Razão Social / Nome:	
CNPJ/CPF:	
Endereço:	
Cidade:	Estado:
CEP:	
Telefone:	E-mail:
Declara ser Microempresa ou Empresa de Pequeno Porte:	( ) Sim ( ) Não
Declara ser Agente de Tratamento de Pequeno Porte[71]:	( ) Sim ( ) Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:	
Dados do Encarregado	
Possui um encarregado pela proteção de dados pessoais?	( ) Sim ( ) Não
Nome:	
CNPJ/CPF:	
Telefone:	E-mail:
Dados do Notificante / Representante Legal	
( ) O próprio encarregado pela proteção de dados.	
( ) Outros (especifique):	
Nome:	
CNPJ/CPF:	
Telefone:	
E-mail:	
A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente. • *Encarregado*: ato de designação/nomeação/procuração. • *Representante*: contrato social e procuração, se cabível.	

70 Reproduzimos o mais recente formulário disponibilizado pela ANPD. Versão acessada em 23/12/2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/coordenacao-geral-de-fiscalizacao-da-anpd-divulga-novo-formulario-para-envio-de-comunicados-de-incidentes-de-seguranca>. Atualmente, a ANPD indica que o formulário deve ser protocolado eletronicamente por meio do Peticionamento Eletrônico do SUPER.BR (Sistema Único de Processo Eletrônico em Rede). Diante da possibilidade de atualizações, é recomendável o acompanhamento rotineiro sobre as atividades da ANPD.

71 Nos termos do REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, aprovado pela RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019)

Tipo de Comunicação	
( ) Completa	*Todas as informações a respeito do incidente estão disponíveis e **a comunicação aos titulares já foi realizada**.*
( ) Preliminar	*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a **comunicação aos titulares ainda não foi realizada**.* *A complementação deverá ser encaminhada em até **30 dias corridos** da comunicação preliminar.*
( ) Complementar	*Complementação de informações prestadas em comunicação preliminar.*

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

- A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

Avaliação do Risco do Incidente
( ) O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
( ) O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**
( ) O risco do incidente aos titulares ainda está sendo apurado. **(Comunicação Preliminar)**
Justifique, se cabível, a avaliação do risco do incidente:

Da Ciência da Ocorrência do Incidente		
Por qual meio se tomou conhecimento do incidente?		
( ) Identificado pelo próprio controlador.	( ) Notificação do operador de dados.	( ) Denúncia de titulares/ terceiros.
( ) Notícias ou redes sociais.	( ) Notificação da ANPD.	( ) Outros. (especifique)
Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:		
Caso o incidente tenha sido comunicado ao controlador por um operador, informe: **Dados do Operador** Razão Social / Nome: CNPJ/CPF: E-mail:		
Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.		

Da Tempestividade da Comunicação do Incidente
Informe as seguintes datas, sobre o incidente: Quando ocorreu Quando tomou ciência Quando comunicou à ANPD Quando comunicou aos titulares
Justifique, se cabível, a não realização da comunicação completa à ANPD e aos titulares de dados afetados no prazo sugerido de 2 (dois) dias úteis após a ciência do incidente:
Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:

Da Comunicação do Incidente aos Titulares dos Dados	
Os titulares dos dados afetados foram comunicados sobre o incidente?	
( ) Sim.	( ) Não, mas o processo de comunicação está em andamento.
( ) Não, por não haver risco ou dano relevante a eles.	( ) Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)
Se cabível, quando os titulares serão comunicados sobre o incidente?	
De que forma a ocorrência do incidente foi comunicada aos titulares?	
( ) Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)*	( ) Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
( ) Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)*	( ) Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*especifique abaixo*)
( ) Outros. (*especifique abaixo*)	( ) Não se aplica.
Descreva como ocorreu a comunicação:	
Quantos titulares foram comunicados individualmente sobre o incidente?	
Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:	
O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações: 1. resumo e data de ocorrência do incidente; 2. descrição dos dados pessoais afetados; 3. riscos e consequências aos titulares de dados; 4. medidas tomadas e recomendadas par mitigar seus efeitos, se cabíveis; 5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.	

O comunicado aos titulares atendeu os requisitos acima?

( ) Sim ( ) Não

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

Da Comunicação do Incidente aos Titulares dos Dados

Qual o tipo de incidente? (Informe o tipo mais específico)

( ) Sequestro de Dados (*ransomware*) sem transferência de informações.	( ) Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações.
( ) Exploração de vulnerabilidade em sistemas de informação.	( ) Vírus de Computador / *Malware*.
( ) Roubo de credenciais / Engenharia Social.	( ) Violação de credencial por força bruta.
( ) Publicação não intencional de dados pessoais.	( ) Divulgação indevida de dados pessoais.
( ) Envio de dados a destinatário incorreto.	( ) Acesso não autorizado a sistemas de informação.
( ) Negação de Serviço (DoS).	( ) Alteração/exclusão não autorizada de dados.
( ) Perda/roubo de documentos ou dispositivos eletrônicos.	( ) Descarte incorreto de documentos ou dispositivos eletrônicos.
( ) Falha em equipamento (hardware).	( ) Falha em sistema de informação (*software*).
( ) Outro tipo de incidente cibernético. (especifique abaixo)	( ) Outro tipo de incidente não cibernético. (especifique abaixo)

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Que medidas foram adotadas para corrigir as causas do incidente?

Impactos do Incidente Sobre os Dados Pessoais

De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):

( ) Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
( ) Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
( ) Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)

( ) Origem racial ou étnica. ( ) Convicção regiliosa. ( ) Opinião política.

( ) Referente à saúde. ( ) Biométrico. ( ) Genético.

( ) Referente à vida sexual. ( ) Filiação a organização sindical, religiosa, filosófica ou política.

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação)

( ) Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)*

( ) Número de documentos de identificação oficial. *(ex: RG, CPF, CNH, passaporte)*

( ) Dados de contato. (*ex: telefone, endereço, e-mail*)

( ) Dados de meios de pagamento. *(ex: cartão de crédito/débito)*

( ) Cópias de documentos de identificação oficial.

( ) Dados protegidos por sigilo profissional/legal.

( ) Dado financeiro ou econômico.

( ) Nomes de usuário de sistemas de informação.

( ) Dado de autenticação de sistema. (*ex: senhas, PIN ou tokens)*

( ) Imagens / Áudio / Vídeo

( ) Dado de geolocalização. *(ex: coordenadas geográficas)*

( ) Outros (especifique abaixo)

Descreva os tipos de dados pessoais não sensíveis violados:

Riscos e Consequências aos Titulares dos Dados

Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?

( ) Sim ( ) Não

Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?

Qual a quantidade aproximada de titulares afetados[72] pelo incidente?

Total de titulares afetados

Crianças e/ou adolescentes

Outros titulares vulneráveis

Se aplicável, descreva as categorias de titulares vulneráveis afetados:

72 Titular afetado é aquele cujos dados podem ter tido a confidencialidade, integridade ou disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.

Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)

( ) Funcionários. ( ) Prestadores de serviços. ( ) Estudantes/Alunos.

( ) Clientes/Cidadãos. ( ) Usuários. ( ) Inscritos/Filiados.

( ) Pacientes de serviço de saúde. ( ) Ainda não identificadas. ( ) Outros. (especifique abaixo)

Informe o quantitativo de titulares afetados, por categoria:

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)

( ) Danos morais. ( ) Danos materiais. ( ) Violação à integridade física.

( ) Discriminação social. ( ) Danos reputacionais. ( ) Roubo de identidade.

( ) Engenharia social / Fraudes. ( ) Limitação de acesso a um serviço. ( ) Exposição de dados protegidos por sigilo profissional/legal.

( ) Restrições de direitos. ( ) Perda de acesso a dados pessoais. ( ) Outros (especifique abaixo).

Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:

Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)

( ) Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.

( ) Podem sofrer danos, superáveis com certa dificuldade.

( ) Podem sofrer danos importantes, superáveis com muita dificuldade.

( ) Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.

Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?

Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?

( ) Sim, integralmente protegidos por criptografia / pseudonimização. ( ) Sim, parcialmente protegidos por criptografia / pseudonimização. ( ) Não.

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)

( ) Políticas de segurança da informação e privacidade.	( ) Processo de Gestão de Riscos.	( ) Registro de incidentes.
( ) Controle de acesso físico.	( ) Controle de acesso lógico.	( ) Segregação de rede.
( ) Criptografia/Anonimização.	( ) Cópias de segurança. (*backups*)	( ) Gestão de ativos.
( ) Antivírus.	( ) Firewall.	( ) Atualização de Sistemas.
( ) Registros de acesso (logs).	( ) Monitoramento de uso de rede e sistemas.	( ) Múltiplos fatores de autenticação.
( ) Testes de invasão.	( ) Plano de resposta a incidentes.	( ) Outras (especifique).

Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:

Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)

( ) Políticas de segurança da informação e privacidade.	( ) Processo de Gestão de Riscos.	( ) Registro de incidentes.
( ) Controle de acesso físico.	( ) Controle de acesso lógico.	( ) Segregação de rede.
( ) Criptografia/Anonimização.	( ) Cópias de segurança. (*backups*)	( ) Gestão de ativos.
( ) Antivírus.	( ) Firewall.	( ) Atualização de Sistemas.
( ) Registros de acesso (logs).	( ) Monitoramento de uso de rede e sistemas.	( ) Múltiplos fatores de autenticação.
( ) Testes de invasão.	( ) Plano de resposta a incidentes.	( ) Outras (especifique).

Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:

As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?

( ) Sim ( ) Não

Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>

6.5 PLANO DE AÇÃO APÓS A COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

O momento posterior à comunicação do incidente de segurança também é estratégico para redução dos danos potenciais, por esse motivo pode ser elaborado um plano de ação para corrigir possíveis falhas e evitar que novos incidentes venham a ocorrer. Para auxiliar as empresas, sugere-se que as seguintes medidas administrativas e técnicas sejam adotadas:

Medidas administrativas no âmbito da governança

- Políticas corporativas.
- Treinamentos, capacitação de colaboradores, comunicação e aculturamento.
- Contratos: inclusão de anexos de SI e LGPD; revisão; cláusulas; DPA.
- Comitês de crise e executivo.
- Políticas de privacidade, de *cookies*, termos de uso para *sites* e aplicativos.
- Controles, entre outros.

Medidas técnicas adotadas no âmbito da Tecnologia da Informação

- Análise e seleção de fornecedores por meio de processo de *Vendor Assessment*.
- Utilização de ferramenta de *Data Loss Prevention* (DLP).
- Simulados de incidentes de segurança, a fim de verificar a aderência ao Plano de Gerenciamento de Incidentes.
- Realização de testes de invasão dentro do processo de desenvolvimento com o objetivo de que as aplicações sejam publicadas com a menor quantidade possível de vulnerabilidades.
- Mapeamento das superfícies de ataque interna e externa, visando identificar ativos não documentados e vetores de ataques ao ambiente.
- Testes de invasão nos ativos críticos legados e/ou que não estejam integrados à esteira *DevSecOps*.
- Monitoramento contínuo dos sistemas por meio de testes recorrentes nesses sistemas/aplicações em ambiente produtivo.
- Realização de testes visando a fortalecer os mecanismos de monitoramento, detecção e resposta frente a ameaças cibernéticas.
- Processo de identificação de vulnerabilidades por meio de ferramentas automatizadas.
- Governar o processo de aplicação de *patches* por meio do monitoramento de *patches* de segurança lançados e avaliação do ambiente para aplicação desses *patches* de acordo com suas criticidades e impactos para o negócio.

7 PROTOCOLO PARA O TRATAMENTO DE DADOS NA GESTÃO DE PESSOAS

7.1 INTRODUÇÃO

O tratamento de dados para gestão de pessoas requer cautela e é a modalidade de tratamento que é realizada tanto pelos setores da indústria com atuação B2B quanto B2C. Assim, ainda que se trate de processamento de dados realizado internamente, os direitos dos titulares devem ser igualmente assegurados e o tratamento de seus dados deve ser realizado em conformidade tanto com a legislação de proteção de dados, quanto com a trabalhista.

Conforme apontado na tabela apresentada na Parte 1, os tipos de dados e as operações de tratamento de dados são diversas e compreendem diversas etapas da relação trabalhista. Portanto, apresentamos o esquema para sintetizar as principais fases do ciclo de vida dos dados na gestão de pessoas:

CICLO DE VIDA DOS DADOS NA GESTÃO DE PESSOAS

- **Fase pré-contratual**: a realização de processos seletivos requer a análise de currículos, cartas de motivação e são apresentadas informações na fase de entrevistas.
  - **Dados utilizados**: nome, endereço, *e-mail*, telefone, experiência profissional, formação acadêmica, informações sobre disponibilidade para trabalho no sábado (pode incluir dados sensíveis sobre religião), certidão de antecedentes criminais, etc.
- **Processo de contratação**: a contratação do(a) colaborador(a) requer a coleta de informações necessárias para elaboração do contrato de trabalho.
  - **Dados utilizados**: nome, data de nascimento, RG, CPF, CNH, CTPS, foto 3x4, endereço, telefone, *e-mail*, grau de escolaridade, número de registro no conselho profissional, naturalidade, nacionalidade, etnia, comprovante de residência, certificado militar, biometria, PIS/Pasep, passaporte, dados de saúde (p.ex. carteira de vacinação, laudo com comprovação de deficiência), exames admissionais, exames complementares (p.ex. teste de audição), etc.
- **Execução do contrato de trabalho**: a execução do contrato de trabalho é processo contínuo que pode demandar uma multiplicidade de dados pessoais para diferentes formas de tratamento. De forma geral, o empregador irá acompanhar o desempenho do(a) colaborador(a), devendo cumprir com suas obrigações trabalhistas, assim como garantir a segurança do ambiente de trabalho. Esses processos podem utilizar tecnologias de administração de folha de pagamento, de ponto, etc.
  - **Dados controle de ponto**: nome completo, RG, CPF, PIS, endereço, data de nascimento, sexo (M/F), impressão digital (biometria), atestados médicos, etc.

  - **Dados para procedimentos financeiros**: nome completo, CPF, conta, agência, banco, conta do FGTS, tipo de conta, relatório de horas trabalhadas, informações sobre horário de entrada e saída, crédito consignado, informações sobre filiação, etc.
  - **Dados para concessão de benefícios**: nome completo, CPF dos filhos e cônjuge, PcD, saúde ocupacional, atestados, licenças, pensionista, gravidez, certidão de nascimento dos filhos, certidão de casamento ou comprovação de união estável e carteira de vacinação dos filhos, etc.
  - **Dados de utilização de equipamentos**: cookies, IP, localização, *wi-fi*, *bluetooth*, registros de *downloads*, assinaturas de *e-mail*, telefone, *e-mail*, etc.
  - **Dados para segurança no ambiente de trabalho**: câmeras de segurança, cadastro biométrico, dados cadastrais de visitantes (nome, CPF, RG, foto), carteira de vacinação, etc.
- **Encerramento da relação trabalhista**: após o encerramento da relação trabalhista, diversos documentos e informações que contêm dados pessoais devem ser armazenadas por períodos determinados tanto pela existência de obrigações legais, quanto pela existência de processos trabalhistas em curso ou cujo prazo prescricional ainda não findou.
  - **Dados armazenados:** informações relativas ao FGTS (GFIP – guia recolhimento do FGTS e informações à previdência social; GRFC – guia de recolhimento rescisório do FGTS e da contribuição social), à contribuição previdenciária, à folha de pagamento, etc.

7.2. BASES LEGAIS

No quadro acima, as operações de tratamento de dados variam a depender da etapa da relação e do regime de contratação do(a) colaborador(a). De modo geral, as principais bases legais que devem ser utilizadas no tratamento de dados não sensíveis são: i) legítimo interesse; ii) cumprimento de obrigação legal ou regulatória; iii) execução de contrato; iv) exercício regular de direitos; e v) proteção da vida ou da incolumidade física do titular ou de terceiros.

Por conta da existência de desigualdade fática na relação entre empregador e empregado, a utilização do consentimento como base legal é discutível, especialmente no bojo da execução do contrato de trabalho, tendo em vista que manifestação "livre" pode ser questionada diante da existência de hierarquia na relação e possibilidade de que o(a) colaborador(a) possa ser prejudicado caso não forneça seu consentimento.

Esse é o entendimento do *Article 29 Working Party* (WP29)[73], que compreende que dificilmente o consentimento poderia ser dado por um empregado de forma "livre", tendo em vista a natureza da relação[74]. Essa base legal pode ser utilizada em situações excepcionais na relação trabalhista, quando o desequilíbrio de poder não gera qualquer consequência caso o consentimento não seja concedido (ex.: autorização para equipe de filmagem).

73 Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cujas atribuições estão previstas no artigo 30º da Diretiva 95/46/CE e no artigo 15º da Diretiva 2002/58/CE.

74 WORKING PARTY 29. **Guidelines on Consent under Regulation 2016/679**. Disponível em: https://ec.europa.eu/newsroom/article29/items/623051/en. Acesso: 7 jun. 2023.

Assim, passa-se à análise da aplicação de cada uma dessas bases legais nas principais fases do ciclo de vida dos dados não sensíveis utilizados na gestão de pessoas.

Fase pré-contratual:

- **Execução de contrato**: apesar de se tratar de momento pré-contratual, a base legal da execução do contrato pode se aplicar à coleta de currículo e entrevista, uma vez que o titular é parte da relação e o objetivo é celebrar um contrato caso a fase preliminar seja bem-sucedida.

Processo de contratação:

- **Execução de contrato**: nesse momento, o titular é parte efetiva do contrato e as informações coletadas devem ter como objetivo celebrar a relação entre empresa e colaborador(a) – ainda que não seja de natureza trabalhista.
- **Legítimo interesse**: atividades de tratamento de dados – como a exigência de antecedentes criminais, etc. – não estão diretamente vinculadas à hipótese de execução do contrato por não serem realizadas a pedido do titular, mas podem ser enquadradas na base legal do legítimo interesse.

Execução do contrato

- **Execução de contrato**: a execução contratual pode ser utilizada como base legal apenas em relação à finalidade específica do contrato de trabalho, cuja impossibilidade de tratar o dado impediria a execução do contrato. Essa base pode ser utilizada para atividades, como o pagamento do salário.
- **Legítimo interesse**: atividades de tratamento de dados – como o acompanhamento de desempenho do(a) colaborador(a), etc. – não estão diretamente vinculadas à hipótese de execução do contrato, por não serem realizadas a pedido do titular, mas podem ser enquadradas na base legal do legítimo interesse.
- **Cumprimento de obrigação legal ou regulatória**: as atividades de gestão de pessoas, por vezes, envolve o tratamento de dados que devem ser armazenados para cumprimento de obrigações fiscais e trabalhistas, por forma de leis, como a Lei nº 8.036/1990 (FGTS), CLT, CTN, etc.

Encerramento da relação

- **Cumprimento de obrigação legal ou regulatória**: mesmo após o encerramento da relação trabalhista, os empregadores devem armazenar dados, como GFIP – guia recolhimento do FGTS e informações à previdência social; GRFC – guia de recolhimento rescisório do FGTS e da contribuição social por conta de obrigações expressas em CTN, CLT, etc.
- **Exercício regular de direitos**: as relações trabalhistas recorrentemente são objeto de disputas judiciais. Assim, até que os prazos prescricionais finalizem e os processos sejam arquivados de forma definitiva, dados essenciais para subsidiar essa disputa podem ser armazenados. É possível, ainda, e até comum na prática, a empresa precisar comprovar o tempo de serviço do colaborador em processo judicial para fins de aposentadoria, fato que pode se dar muitos anos após o prazo prescricional de uma reclamação trabalhista.

Cumpre ressaltar que a utilização de cada uma das bases legais depende do contexto específico no qual ela seja aplicada, e o enquadramento da operação de tratamento deve sempre ser acompanhada dos outros princípios norteadores da legislação. Deve-se ter especial atenção ao princípio da finalidade, necessidade e adequação, uma vez que, independentemente da existência de contrato ou obrigação legal, o tratamento de dados deve ser realizado quando os dados forem pertinentes, adequados e limitados aos fins para os quais são processados.

Ademais, recursos como pseudonimização e anonimização devem ser utilizados sempre que possível para proteção dos dados, especialmente após transcurso de longo período.

7.3 TRATAMENTO DE DADOS SENSÍVEIS

7.3.1 DADOS DE SAÚDE

Os dados de saúde são incluídos na categoria de dados sensíveis por conta de seu potencial discriminatório e de restrição de direitos. Interessante notar que a LGPD não traz o conceito de saúde trazido pelo GDPR, fazendo menção tão somente aos conceitos de "Dado Pessoal" e "Dado Pessoal Sensível".

Ainda assim, podemos extrair a definição do conceito de "Dados de Saúde" a partir da legislação europeia, qual seja:

> todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação (Considerando 35, GDPR).

Por serem dados sensíveis, as hipóteses de tratamento desses dados são mais restritas, não compreendendo bases legais mais amplas, como a execução contratual e o legítimo interesse. Assim, inicialmente, cabe avaliar as finalidades da utilização desse dado na gestão de pessoas.

De forma geral, esses dados são utilizados para finalidades, como admissão de funcionários, contratação de planos de saúde ou políticas afirmativas para PcD. Nesses casos, em geral, não é possível utilizar a base legal da tutela da saúde, uma vez que a LGPD faz essa ressalva ao pontuar "procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária".

De acordo com o GDPR, trata-se da base legal aplicável se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social. Assim, em geral, essa base legal não pode ser utilizada no bojo da gestão de pessoas, em especial pelo departamento de Recursos Humanos (RH). Contudo, caso a indústria possua ambulatório médico no local de trabalho, o tratamento de dados de saúde pode ser enquadrado na base legal da tutela da saúde.

De qualquer forma, os dados de saúde podem ser tratados sob a base do exercício regular de direitos em contrato (art. 11, II, d, da LGPD). Tal base é mais restrita que a execução

contratual, mas pode ser aplicável quando o tratamento pelo controlador é indispensável para a execução do contrato, como é o caso de uma seguradora de saúde que precisa de informações sensíveis para adimplir o contrato ou, então, o dado também pode ser tratado sob a base "prevenção de fraudes" e garantir a segurança do titular (art. 11, II, d, da LGPD), caso o dado de saúde seja utilizado para autenticação do titular e para impedir que seu seguro de saúde seja fraudado, por exemplo.

COMPROVANTE DE VACINA

A discussão sobre a possibilidade de exigência de comprovante de vacinação contra a covid-19 suscitou diversas discussões sobre a possibilidade de exigência do comprovante de vacinação pelo empregador. Buscando endereçar a controvérsia, o Ministério Público do Trabalho (MPT) editou a Portaria nº 620/2021, que proíbe a exigência de comprovante de vacina na contratação ou durante a relação de trabalho.

Contudo, em decisão liminar, o Supremo Tribunal Federal (STF) suspendeu a portaria, permitindo a exigência do comprovante tendo em vista que a medida tem como objetivo a proteção da saúde e da vida dos empregados e do público em geral (ADPF 898).

Assim, até o momento, é permitida a exigência de comprovante de vacinação e, sob o prisma da proteção de dados, o tratamento de dados de saúde pode ser realizado quando necessário para proteção da vida ou da incolumidade física do titular, desde que seja utilizada de forma excepcional e específica.

Novamente, a utilização de cada uma das bases legais depende do contexto específico no qual ela seja aplicada; e o enquadramento da operação de tratamento deve sempre ser acompanhada dos outros princípios norteadores da legislação.

7.3.2 TRATAMENTO DE DADOS BIOMÉTRICOS

O tratamento de dados biométricos é realizado com frequência pelos empregadores para controle de ponto, entrada e para segurança do ambiente de trabalho. Por se tratar de dado sensível, essa modalidade de tratamento de dados não pode ser feita sob bases genéricas, assim como os dados de saúde.

De forma geral, os dados biométricos podem ser tratados sem consentimento quando forem utilizados para prevenção de fraudes, tendo em vista que eles possibilitam a identificação dos colaboradores, evitando a ampla circulação de estranhos no ambiente de trabalho. Inclusive, a própria CLT, em seu art. 157, obriga os empregadores a tomarem precauções para proteção do trabalhador, sendo obrigação das empresas "cumprir e fazer cumprir as normas de segurança e medicina do trabalho" (inciso I).

Em relação ao acompanhamento do ponto do empregador, também a CLT determina que o ponto do empregado seja registrado, podendo o registro ocorrer no formato eletrônico (art. 74). Assim, respeitado o princípio da minimização, a biometria pode ser utilizada também sob a base legal do cumprimento de obrigação legal pelo controlador.

8 PROTOCOLO PARA A ELABORAÇÃO DE ACORDOS ENTRE AGENTES DE TRATAMENTO

8.1 INTRODUÇÃO

Os agentes de tratamento, o controlador e o operador podem ser pessoas natural ou jurídica, de direito público ou privado, sendo figuras essenciais ao ecossistema de proteção de dados pessoais. O controlador é o responsável pelas decisões referentes ao tratamento de dados pessoais, já ao operador compete a realização de tratamentos de dados pessoais em nome do controlador.

As situações nas quais uma pessoa física assume o papel de agente de tratamento são específicas e terão um tratamento diferenciado definido pela ANPD. Já nos cenários mais corriqueiros, uma pessoa jurídica irá ocupar as funções dos agentes de tratamento; nesses casos, a organização assumirá o papel, não sendo necessária a representação por qualquer funcionário ou sócio da empresa.[75]

Além disso, a definição do papel ocupado por cada pessoa envolvida naquele determinado processo é feita a partir da avaliação de cada atividade. Ou seja, uma organização pode desenvolver o papel de operador em determinado tratamento que envolve outra organização e, em outro processo, esses papéis podem ser invertidos. Esse é mais um dos motivos que justificam a necessidade de manutenção de registro das operações de tratamento de dados realizadas (art. 37 da LGPD), obrigação compartilhada por ambos os agentes de tratamento.

A relação entre os agentes de tratamento de cada tratamento, muitas vezes, é definida contratualmente, mas a efetiva identificação de cada agente será determinada pelas funções desempenhadas por cada um. Assim, independentemente de acordos estabelecidos entre os agentes de tratamento, o que é essencial para determinar se uma organização está atuando como controladora dos dados é justamente o **poder de decisão** sobre os

75 ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021.

tratamentos realizados. Para a caracterização do mencionado poder decisório, é necessário o controle sobre os elementos essenciais do tratamento, como a definição da finalidade do tratamento, da natureza dos dados pessoais tratados e a duração do processo. [76]

Ainda existe a controladoria conjunta, caracterizada por situações em que existem dois ou mais responsáveis pelo tratamento, ou seja, mais de um agente participa da determinação dos elementos essenciais daquele tratamento. As decisões conjuntas podem ser tomadas a partir de uma atuação comum, em que há verdadeira atuação conjunta, ou por meio de decisões convergentes que, apesar de distintas, são complementares. Nos casos em que restar comprovada a controladoria conjunta, haverá responsabilidade solidária dos controladores, conforme disposição do art. 42, §1º, II, da LGPD. [77]

Dessa forma, em caso de atuação do operador fora do escopo das determinações do controlador em relação aos elementos essenciais do tratamento, o operador atua como verdadeiro controlador. Isso afasta as responsabilidades do suposto controlador sobre aquele tratamento e as traz para o operador atuando como controlador, de tal forma que esse deverá cumprir com todas as obrigações do controlador (art. 42, §1º, I, da LGPD).

Elementos essenciais do tratamento de dados[78]

- **Objetivos** que justificam o tratamento de dados realizado e a base legal utilizada.
- **Meios de tratamento dos dados pessoais.**
- **Tipos de dados pessoais tratados**, incluindo a natureza desses dados.
- **Período** de duração da operação de tratamento e definição do prazo para eliminação dos dados.

Além disso, existe a figura do suboperador, agente contratado pelo operador para participar do tratamento de dados definido pelo controlador. Portanto, não há relação direta entre o controlador e o suboperador, apesar de estarem envolvidos no mesmo tratamento. Para fins de responsabilidade, o suboperador é equiparado ao operador e, por isso, segue a mesma lógica do art. 42, §1º, I, da LGPD. Caso descumpra as determinações do operador ou do controlador, o suboperador passará a atuar como controlador e responderá como controlador. Em princípio, a mera existência desse agente não é suficiente para caracterizar a controladoria conjunta, pois ele não atua na determinação dos elementos essenciais para o tratamento de dados, como será abordado adiante.

76 *Idem ibidem.*

77 ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021.

78 ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.** Atualização em: maio 2022. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 4 maio 2022.

A definição dos papéis dos agentes de tratamento e o estabelecimento de condições por meio de contratos pode ser importante aspecto para a redução da exposição do controlador. Tal fato decorre da maior carga de responsabilidade que o controlador possui em relação à comprovação do cumprimento com os termos da legislação, assim como na garantia dos direitos dos titulares.

Por esse motivo, o controlador tem papel estratégico na definição do operador, sendo o contrato instrumento importante para a definição das obrigações dos operadores e os limites da atuação dos subcontroladores[79].

8.2 DEFINIÇÃO DE PAPÉIS

O papel desempenhado por cada agente em determinado tratamento de dados é essencial para fins de responsabilidade e para compreender quais são as obrigações de cada entidade envolvida naquela cadeia de tratamento. Essa definição pode ser formalizada por meio de um contrato, contudo, o efetivo desempenho das funções é essencial para identificação do papel de cada agente de tratamento. Isso porque a LGPD define diferentes encargos aos diferentes agentes de tratamento. Algumas dessas atribuições são comuns a todos os agentes, mas outras são específicas para cada papel, devido às peculiaridades de sua atuação[80].

A relação entre os agentes de tratamento de cada tratamento muitas vezes é definida contratualmente, mas também é possível que a definição seja feita por meio de outras formas de interação empresarial. Contudo, independentemente de acordos estabelecidos entre os agentes de tratamento, o que é essencial para determinar se uma organização está atuando como controladora dos dados é justamente o **poder de decisão** sobre os tratamentos realizados.

Para a caracterização do mencionado poder decisório, é necessário o controle sobre os elementos essenciais do tratamento, como a definição da finalidade do tratamento, da natureza dos dados pessoais tratados e a duração do processo.[81] Portanto, situações, como a definição de papéis em contrato que seja incompatível com as responsabilidades reais do agente de tratamento ou a excessiva atribuição de responsabilidades ao operador quando não é ele o tomador de decisão, não são resguardadas à luz da legislação.

---

79 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. Jul/2021. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: 6 ago. 2021.

80 LAPIN. **Cartilha 'controlador ou operador: quem sou eu?** Disponível em: https://lapin.org.br/2021/04/09/cartilha-controlador-ou-operador-quem-sou-eu/

81 ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021.

Ainda existe a controladoria conjunta, caracterizada por situações em que existem dois ou mais responsáveis pelo tratamento, ou seja, mais de um agente participa da determinação dos elementos essenciais daquele tratamento. As decisões conjuntas podem ser tomadas a partir de uma atuação comum, em que há verdadeira atuação conjunta, ou por meio de decisões convergentes que, apesar de distintas, são complementares. Nos casos em que restar comprovada a controladoria conjunta, haverá responsabilidade solidária dos controladores, conforme disposição do art. 42, §1º, II, da LGPD.[82]

Dessa forma, em caso de atuação do operador fora do escopo das determinações do controlador em relação aos elementos essenciais do tratamento, o operador atua como verdadeiro controlador. Isso afasta as responsabilidades do suposto controlador sobre aquele tratamento e as traz para o operador atuando como controlador, de tal forma que esse deverá cumprir com todas as obrigações do controlador (art. 42, §1º, I, da LGPD).

Nesse sentido, destacamos os deveres de cada um dos agentes de tratamento, assim como aqueles que são comuns aos dois:

Deveres comuns aos agentes de tratamento

- Conformidade com os **princípios** da LGPD.
- Implementação de **medidas de segurança técnicas e organizacionais.**
- **Registro** de operações de tratamento de dados pessoais.
- Observância das regras de **transferências internacionais.**

Obrigações dos operadores

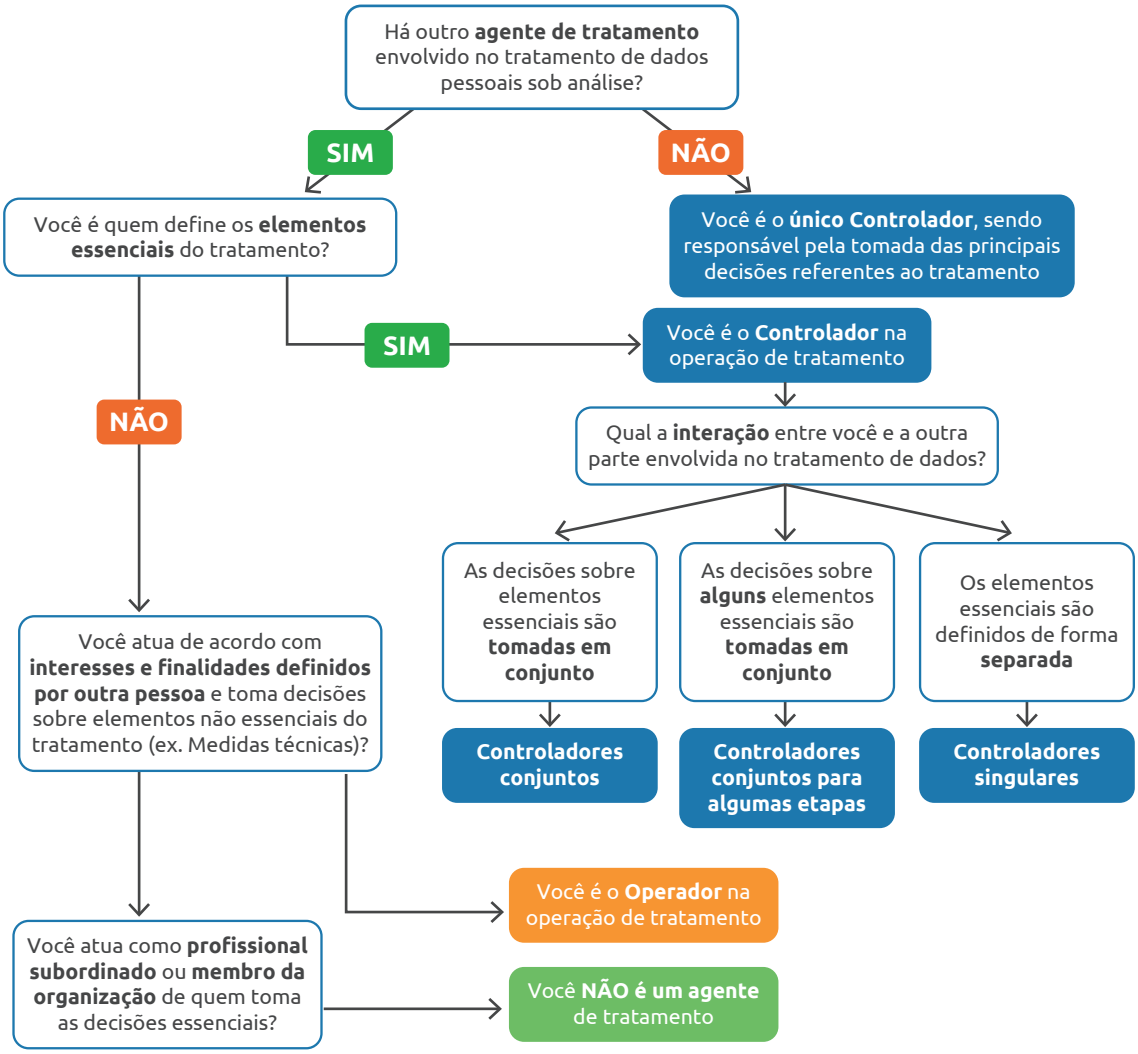
- Cumprir com as **instruções do controlador** sobre o tratamento de dados.
- **Notificar** incidentes de segurança ou possível violação de proteção de dados ao controlador.
- **Reparar os danos causados** em razão do exercício de atividade de tratamento de dados pessoais, **quando este descumprir com suas obrigações ou não seguir as orientações do controlador.**

Obrigações dos controladores

- Manutenção do **ônus da prova** de que o consentimento do titular foi obtido em conformidade com a LGPD.
- Observância dos **direitos dos titulares.**
- **Comunicação de incidentes de segurança que possam acarretar risco ou dano relevante** à ANPD e aos titulares afetados.
- Elaboração de **Relatório de Impacto de Proteção de Dados.**
- Nomeação de **encarregado** de dados.
- Implementação de **programa de governança em privacidade** com os requisitos previstos no art. 50, §2º**.**

82 ANPD. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acesso em: 6 ago. 2021

Para auxiliar a aplicação dos conceitos de controlador e operador, a ANPD divulgou o seguinte fluxograma[83] na versão mais recente (maio/2022) do **Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**:



8.3 ELABORAÇÃO DE CLÁUSULAS CONTRATUAIS

Conforme mencionado, ainda que haja a identificação do papel de cada um dos agentes pelo contexto fático da relação, a definição de papéis pode ser formalizada por meio de contratos. A inclusão de cláusulas contratuais pode ser importante para o estabelecimento das obrigações de cada parte e definição das instruções sobre procedimentos a serem adotados, por exemplo, em incidentes de segurança.

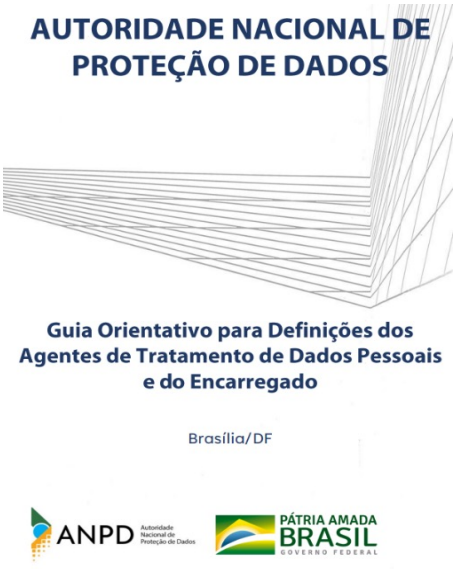
83 Fluxograma do **Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado** da ANPD reproduzido de forma resumida.

Contudo, conforme exposto anteriormente, é necessário ressaltar que a efetiva identificação dos papéis dos agentes de tratamento decorre do contexto fático. Assim, ainda que um contrato estabeleça quem é o controlador e quem é o operador, a avaliação dos papéis efetivamente assumidos será determinante para avaliação das responsabilidades de cada um dos agentes.

De acordo com o Guia do EDPB[84], os contratos podem contribuir para o balanceamento das posições negociais e podem ser importante mecanismo de garantia de cumprimento com a legislação de proteção de dados. O órgão recomenda, portanto, que o contrato não se restrinja aos termos da legislação, levando em consideração as responsabilidades das partes, o nível de segurança que é exigido no tratamento de dados realizado, a confidencialidade da matéria tratada, assim como deve prever informações sobre o risco envolvido no tratamento de dados realizado sob o contrato em questão[85].

Também é possível definir os limites das funções de cocontroladores, podendo ser definidas as decisões comuns (duas empresas decidem em conjunto as finalidades e meios de tratamento) ou decisões convergentes (decisões distintas, mas complementares) por meio do instrumento contratual.

Dessa forma, mesmo que a responsabilização dos agentes de tratamento seja avaliada contextualmente pela ANPD, a elaboração de cláusulas contratuais pode auxiliar no estabelecimento do regime de atividades e as responsabilidades de cada parte. Nos termos do Guia de Agentes de Tratamento da ANPD:



> Ainda que a LGPD não determine expressamente que o controlador e o operador devam firmar um contrato sobre o tratamento de dados, tal ajuste se mostra como uma boa prática de tratamento de dados, uma vez que as cláusulas contratuais impõem limites à atuação do operador, fixam parâmetros objetivos para a alocação de responsabilidades e reduzem os riscos e as incertezas decorrentes da operação.
> **Os pontos que podem ser definidos contratualmente são o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD** (p. 16, grifo nosso).

84 EUROPEAN DATA PROTECTION BOARD – EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: jul. 2021. p. 34

85 *Idem ibidem.*

Assim, sugerimos que a elaboração de cláusulas contratuais considere os seguintes tópicos:

- Glossário com terminologia da LGPD.
- Duração das atividades de tratamento.
- Indicação de agentes de tratamento.
- Finalidades específicas do tratamento de dados.
- Vedação à utilização de dados pessoais sem ciência ou autorização da controladora.
- Exigência de adequação das partes do contrato à LGPD.
- Vedação ao compartilhamento de dados pessoais e obrigatoriedade de notificação à parte caso o compartilhamento seja necessário.
- Obrigação de registro de informações.
- Obrigação de implementação de medidas técnicas e administrativas que garantam a segurança dos dados tratados.
- Possibilidade de realização de auditorias para demonstração de cumprimento da legislação.
- Deveres de confidencialidade.
- Periodicidade de atualização de informações do contrato.
- Hipóteses de transferência de dados.
- Obrigatoriedade de elaboração de plano de incidentes envolvendo dados pessoais.
- Procedimentos de destruição e devolução de dados pessoais.
- Obrigatoriedade de notificação em caso de determinações oficiais que obriguem o fornecimento de dados pessoais.
- Obrigatoriedade de contratação de DPO por operador.

8.4 CONTRATAÇÃO DE EMPRESAS TERCEIRIZADAS

Por vezes, a complexidade das relações empresariais exige a contratação de empresas terceirizadas para o auxílio no desempenho de determinadas atividades. Quando essas atividades envolverem o tratamento de dados pelo operador, as empresas terceirizadas serão caracterizadas como suboperadores.

O suboperador é o agente contratado pelo operador para participar do tratamento de dados definido pelo controlador, então não há relação direta entre o controlador e o suboperador, apesar de estarem envolvidos no mesmo tratamento. Insta ressaltar que, para fins de responsabilidade, o suboperador é equiparado ao operador, então segue a mesma lógica do art. 42, §1º, I, da LGPD – se descumprir as determinações do operador/controlador, o suboperador passará a atuar como controlador e responderá como controlador.

Assim, recomenda-se que os contratos estabeleçam cláusulas que impeçam que a contratação de suboperadores ocorra sem anuência prévia do controlador e que vedem o compartilhamento de dados pessoais com outros parceiros comerciais que não estão envolvidos na relação. Ademais, no caso de contratação de outro operador de dados, é necessário garantir que esse agente esteja submetido às mesmas condições que o operador, incluindo a possibilidade de se realizar auditorias para garantir o cumprimento dos termos do contrato[86].

86 EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. Disponível em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf. Acesso em: jul. 2021. p. 37.

9 PROTOCOLO PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS

9.1 INTRODUÇÃO

A transferência internacional de dados é um processo importante para a indústria, especialmente por conta da utilização de serviços de *cloud* internacionais para armazenamento de informações. Nos termos do art. 5º, inciso XV, da LGPD, a transferência internacional é aquela realizada "para país estrangeiro ou organismo internacional do qual o país seja membro".

Assim, mesmo que se trate apenas de armazenamento de dados, as empresas devem cumprir com as condições de legitimidade da LGPD quando forem armazenados dados pessoais ou forem realizadas outras operações de tratamento que envolvam a transferência internacional. Tendo em vista a ampla realização de transferências de dados pessoais para outros países, diversas jurisdições somente autorizam transferências internacionais de dados se um grau de proteção semelhante ao nacional for comprovado.

Buscando conferir um grau de proteção similar ao que é exigido no tratamento de dados que ocorre em território nacional e, ao mesmo tempo, possibilitando que nem todas as hipóteses precisem passar pelo crivo da ANPD, o art. 33 da LGPD estrutura três regimes de tutela dos dados quando da transferência internacional de dados[87]: i) declaração de existência de grau de proteção adequado; ii) existência de garantias de cumprimento com os preceitos da lei; e iii) derrogações específicas que tem como objetivo a promoção de interesse público.

Em especial a declaração de existência de grau de proteção adequada e a garantia de cumprimento dos preceitos da legislação dependem de manifestação da ANPD. Esses aspectos, contudo, ainda carecem de regulamentação pela ANPD, gerando dúvidas a respeito das bases legais aplicáveis para a sua realização.

87 PRATA DE CARVALHO, Angelo. Transferência internacional de dados na lei geral de proteção de dados - força normativa e efetividade diante do cenário transnacional. , TEPEDINO Gustavo *et al.* (Coords.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 624.

Nesse sentido, apresentaremos breve descrição de cada um dos requisitos para a transferência internacional para esclarecer o seu âmbito de aplicação e os aspectos pendentes de regulamentação pela autoridade[88].

9.2 BASES LEGAIS PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS

A LGPD prevê em seu art. 33 algumas hipóteses nas quais a transferência internacional de dados seria permitida. Contudo, conforme mencionado, a ANPD ainda deve se manifestar sobre algumas questões.

Por exemplo, o art. 35 da LGPD prevê que "a *definição do conteúdo* de cláusulas-padrão contratuais, bem como a *verificação* de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, *será realizada pela autoridade nacional*" (grifo nosso).

Ademais, os parágrafos do art. 35 também preveem que, para definição do conteúdo de **cláusulas-padrão** e **cláusulas contratuais específicas, normas corporativas globais, selos, códigos de conduta etc**.:

- deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta lei (§ 1º);
- na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário (§ 2º);
- a autoridade nacional poderá designar organismos de certificação para a realização do previsto no art. 33 (§ 3º);
- os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, podem ser submetidos à revisão ou anulados (§ 4º); e
- as garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no *caput* serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46[89] da LGPD (§ 5º).

88 CONEXIS. **Código de Boas Práticas de Proteção de Dados para o Setor de Telecomunicações**. Disponível em: https://conexis.org.br/wp-content/uploads/2022/08/LGPDBoasPraticasDesktop.pdf. Acesso em: 2 jul. 2023.

89 Art. 46 – § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Cumpre notar que as cláusulas-padrão remetem ao sistema das *Standard Contractual Clauses* (SCC) da União Europeia, nas quais o conteúdo pré-aprovado das cláusulas deve ser utilizado nos exatos termos propostos pela autoridade. Contudo, como a experiência da própria União Europeia apresenta, caso esse modelo seja excessivamente rígido, os negócios globais podem ser prejudicados. Assim, espera-se que a autoridade inspire-se em modelos flexíveis que não impeçam a realização de negócios internacionais.

Destaca-se que a rígida interpretação do modelo europeu das SCC, adotada na decisão *Schrems* II do Tribunal de Justiça da União Europeia (TJUE)[90], não precisa ser necessariamente seguida pelo Brasil, o que pode ser demonstrado pelo sistema da Nova Zelândia que, mesmo desenvolvendo um sistema de transferência internacional mais flexível do que o europeu, obteve decisão favorável de adequação da UE.

Ademais, passa-se às outras hipóteses que autorizam a transferência internacional que estão previstas no art. 33 da LGPD.

Países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado (inciso I)	• O nível de proteção do país necessita de análise pela ANPD. • A decisão de adequação será pautada nos seguintes critérios: i) as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; ii) a natureza dos dados; iii) a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; iv) a adoção de medidas de segurança previstas em regulamento; v) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e vi) outras circunstâncias específicas relativas à transferência.
Garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD (inciso II)	• A transferência internacional pode ocorrer quando o controlador garantir o cumprimento do regime de proteção de dados da LGPD, por meio de: i) cláusulas contratuais específicas; ii) cláusulas contratuais padrão; iii) normas corporativas globais; e iv) selos, certificados e códigos de conduta.
Cooperação jurídica internacional entre órgãos públicos de inteligência (inciso III)	• Não se aplica a agentes privados. • A transferência pode ocorrer caso existam acordos bilaterais entre órgãos públicos.
Proteção da vida ou da incolumidade física do titular ou de terceiros (inciso IV)	• Hipótese excepcional – deve ser utilizada apenas quando a vida do titular ou do terceiro dependa do tratamento de dados possibilitado pela transferência internacional. • Não é possível realizar interpretação ampla sobre proteção da vida, assim como na aplicação do art. 7º, VII e 11, II, e, da LGPD.
Autorização pela ANPD (inciso V)	• Hipótese ampla que possibilita que transferências internacionais sejam realizadas quando a ANPD autorizar, possibilitando que a autoridade avalie as especificidades de cada caso.
Compromisso assumido em acordo de cooperação internacional (inciso VI)	• Hipótese garante que os instrumentos de cooperação não sejam submetidos a procedimentos excessivamente burocráticos que podem comprometer relações diplomáticas.

90 Note-se que, depois da decisão proferida no caso *Schrems* II invalidando o *Privacy Shield* (acordo que permitia a transferência de dados entre EUA e UE), uma nova política de transferência internacional vem sendo negociada entre os EUA e a UE. Para mais informações, ver: EDPB. **Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework**. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-012022-announcement-agreement-principle-new_en. Acesso em: abr. 2022.

Execução de política pública (inciso V)	• Não se aplica a agentes privados. • Hipótese deve ser utilizada pelos agentes que possuem prerrogativas para tanto, não sendo necessária a sua submissão à ANPD.
Consentimento (inciso VIII)	• Para ser válido, deve ser livre, informado e inequívoco; além de cumprir com os requisitos de transparência e acesso à informação. • O titular deve ser informado de forma específica sobre essa modalidade de tratamento. • Importa notar que nem sempre o consentimento será a base mais adequada, tendo em vista as restrições mencionadas na Parte 1.
Hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD (inciso IX)	• Possibilita a utilização de bases legais que já permitem a realização de tratamento de dados em território nacional, quais sejam: i) cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD); ii) execução de contrato do qual o titular seja parte (art. 7º, V, da LGPD); e iii) exercício regular de direitos (art. 7º, VI, da LGPD).

9.3 BOAS PRÁTICAS PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Independentemente da base legal adotada, é necessário que as partes envolvidas na transferência busquem meios de assegurar que os princípios da legislação serão cumpridos, em especial o da minimização. Além disso, sempre que possível, recomenda-se que a transferência internacional seja realizada com a menor quantidade de dados e da forma menos invasiva para o titular.

Caso as cláusulas contratuais sejam adotadas, é importante que o instrumento contratual preveja expressamente a realização da transferência internacional para o cumprimento ou a execução do contrato. Nesse sentido, a principal obrigação do controlador em relação a esse ponto é garantir que o titular tenha acesso a informações sobre a transferência internacional, garantindo o cumprimento do princípio da transparência.

No caso dos contratos firmados entre os agentes de tratamento, recomenda-se que sejam inseridas cláusulas contratuais prevendo salvaguardas para a segurança dos dados para assegurar o nível adequado de proteção. Ademais, as informações sobre as transferências internacionais realizadas pela organização devem constar das políticas de privacidade disponibilizadas pela empresa.

Na União Europeia[91] e na Nova Zelândia[92] são utilizados os contratos denominados *Data Transfer Agreement* (DTA) ou *International Data Transfer Agreement* (IDTA) como forma de garantir o cumprimento da legislação do país de origem quando da transferência internacional, bem como das salvaguardas previstas nas legislações. Assim, espera-se que, em breve, a ANPD divulgue instrumento similar que possa subsidiar as operações de tratamento de dados realizadas com outros países.

91 ICO. **International data transfer agreement and guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

92 PRIVACY COMMISSIONER. **Principle 12 - Disclosure outside New Zealand**. Disponível em:https://privacy.org.nz/privacy-act-2020/privacy-principles/12/

PARTE 3

PROTOCOLOS ESPECÍFICOS

1 PROTOCOLO PARA IMPLEMENTAÇÃO DA LGPD POR MICRO E PEQUENAS EMPRESAS

1.1. INTRODUÇÃO

Por conta das especificidades das micro e pequenas empresas, a LGPD possui previsão expressa em seu art. 55-J, XVIII, que é competência da ANPD editar normas que orientem o tratamento diferenciado para esses agentes. Tal previsão justifica-se por conta dos altos custos de adequação que a lei pode impor e do impacto que esses custos podem causar em agentes de pequeno porte[93].

Por esse motivo, a ANPD vem realizando diversas iniciativas para orientar os processos de adequação de tais agentes, como, por exemplo: a publicação do Relatório de Análise de Impacto Regulatório voltado para a construção do modelo regulatório previsto para aplicação da LGPD a microempresas e empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais[94]; guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte[95]; *checklist* de medidas de segurança para agentes de tratamento de pequeno porte[96] e, a Resolução CD/ANPD nº 2/2022, publicada em 28 de janeiro de 2022.

Dentre as iniciativas da ANPD, merece destaque a Resolução CD/ANPD nº 2/2022, que apresenta o regime especial de proteção de dados para agentes de tratamento de pequeno porte, que incluem microempresas, empresas de pequeno porte, *startups* e pessoas jurídicas de direito privado. E é justamente sobre essas iniciativas que trataremos neste protocolo.

Isso porque sabemos que a indústria conta com expressiva parcela de micro e pequenas empresas que podem estar com dificuldades em implementar seus programas de adequação à legislação de proteção de dados. Assim, apresentaremos os principais aspectos já regulamentados pela ANPD, além de medidas que podem auxiliar as micro e pequenas empresas em seu processo de adequação.

---

93 A discussão sobre esse assunto foi apresentada anteriormente no artigo: SCHERTEL, Laura; FUJIMOTO, Mônica. O papel do "Deputy Protection Officer – DPO" nas instituições de ensino superior privado. *In:* GOLDBERG, Maria (Org.). Ensino Superior Privado: reflexões sobre o passado recente, atualidades e perspectivas futura". **Revista dos Tribunais** (no prelo).

94 ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/2021.08.17___AIR_Reg_MPE___versao_final.pdf.

95 ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf .

96 ANPD. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf

1.2 DEFINIÇÕES

Em primeiro lugar, é necessário compreender quais empresas podem ser compreendidas como "agentes de tratamento de pequeno porte".

De acordo com o inciso II do art. 2º da Resolução CD/ANPD nº 2/2022, essa categoria inclui microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, que assumam obrigações típicas de agentes de tratamento (operador e controlador). Assim, cabe compreender como definir cada grupo de empresas.

	Requisitos[97]
Microempresas Lei Complementar nº 123/2006	Ser sociedade empresária, sociedade simples, sociedade limitada unipessoal devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas.
	Auferir, em cada ano-calendário, receita bruta igual ou inferior a R$ 360.000,00.
Empresas de pequeno porte Lei Complementar nº 123/2006	Ser sociedade empresária, sociedade simples, sociedade limitada unipessoal devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas.
	Auferir, em cada ano-calendário, receita bruta superior a R$ 360.000,00 e igual ou inferior a R$ 4.800.000,00.
Microempreendedor Individual (MEI) Lei Complementar nº 123/2006	Ser sociedade empresária, sociedade simples, sociedade limitada unipessoal devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas.
	Auferir, no ano-calendário anterior, de até R$ 81.000,00.
	Não ter filiais.
	Não ser sócio ou administrador de outra empresa.
	Atuar nas ocupações permitidas pelo Anexo XI da Resolução CGSN nº 140, de 2018[98].
Startups Lei Complementar nº 182/2021	Empresário individual, empresa individual de responsabilidade limitada, sociedades empresárias, sociedades cooperativas e sociedades simples
	Receita bruta de até R$ 16.000.000,00 no ano-calendário anterior ou de R$ 1.333.334,00 multiplicado pelo número de meses de atividade no ano-calendário anterior, quando inferior a 12 meses
	Recém-inauguradas em operação recente (até 10 anos de inscrição no CNPJ.
	Atuação caracterizada pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados ou enquadramento no regime especial Inova Simples.

97 Resolução CD/ANPD nº 2/2022 "Art. 2º [...] I – agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador; II – microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006; III – *startups*: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no Capítulo II da Lei Complementar nº 182, de 1º de junho de 2021".

98 Disponível em: http://www8.receita.fazenda.gov.br/SimplesNacional/Arquivos/manual/Anexo_XI.pdf

1.3 OBRIGAÇÕES DOS AGENTES DE TRATAMENTO

Após breve descrição sobre a categoria dos agentes de pequeno porte, cumpre destacar que a Resolução CD/ANPD nº 2/2022 prevê a flexibilização de obrigações em relação aos seguintes aspectos:

a) Dispensa de indicação do encarregado (art. 11).
b) Endereçamento coletivo de reclamações de titulares por entidades que representem os setores (art. 8º).
c) Registro simplificado de operações de tratamento (art. 9º).
d) Política simplificada de segurança da informação (art. 13).
e) Política simplificada de comunicação de incidente de segurança (art. 10).

Apesar de a Resolução CD/ANPD nº 2/2022 flexibilizar e dispensar diversas obrigações dos agentes de tratamento de pequeno porte, é necessário atenção especial dos agentes que tratam os "dados pessoais de alto risco", apontando um critério geral e um específico. O critério geral (art. 4º, I) exige que o tratamento de dados pessoais seja realizado em larga escala ou que possa afetar significativamente interesses e direitos fundamentais dos titulares. Já o critério específico previsto no art. 4º, II, aponta algumas situações nas quais o tratamento pode ser de alto risco, conforme se vê a seguir:

DADOS PESSOAIS DE ALTO RISCO

- **Critério geral:** tratamento de dados pessoais em larga escala ou que possa afetar significativamente interesses e direitos fundamentais dos titulares
- **Critérios específicos:**
  - Uso de tecnologias emergentes ou inovadoras.
  - Vigilância ou controle de zonas acessíveis ao público.[99]
  - Decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular.
  - Utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

Importa notar que a ANPD se reserva o direito de rever a flexibilização das obrigações a depender da natureza ou do volume das operações, bem como dos riscos envolvidos no tratamento de dados.

99 Nos termos do art. 2º, IV, são entendidas como zonas acessíveis ao público os "espaços abertos ao público, como praças, centros comerciais, vias públicas, estações de ônibus, de metrô e de trem, aeroportos, portos, bibliotecas públicas, dentre outros".

Ademais, ainda que a indicação de encarregado não seja obrigatória para agentes de tratamento de pequeno porte, a indicação de um DPO pode ser importante passo para o fortalecimento da política de governança em privacidade e dados da empresa. De modo que sugerimos que essa hipótese seja sempre avaliada, especialmente se os dados pessoais forem elementos centrais do modelo de negócio da IES.

1.4 PRAZOS DIFERENCIADOS

A Resolução CD/ANPD nº 2/2022 apresenta um regime especial de proteção de dados para agentes de prazos em dobro para as seguintes hipóteses:

Atendimento das solicitações dos titulares.
Comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional.
Fornecimento de declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, quando requisitados pelo titular.
Outros prazos para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento.

1.5 MEDIDAS DE SEGURANÇA PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE

Em linha com o previsto na Resolução CD/ANPD nº 2/2022, a ANPD também prevê medidas de segurança específicas para agentes de tratamento de pequeno porte. Antes mesmo da publicação desta resolução, a autoridade editou o guia orientativo de segurança da informação para agentes de tratamento de pequeno porte, orientando a adoção de medidas técnicas e administrativas de segurança da informação para auxiliar as empresas que não possuem corpo técnico especializado na matéria.

Além disso, a autoridade disponibilizou *checklist* com medidas de segurança que podem ser adotadas pelos agentes, conforme a seguir colacionado [100]:

100 O *checklist* da autoridade foi apenas reproduzido em novo formato. O original está disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf.

CHECKLIST ANPD – Medidas de segurança para agentes de tratamento de pequeno porte

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- ☑ Estabelecer uma política de segurança da informação simplificada, que estabeleça controles relacionados ao tratamento de dados pessoais, como cópias de segurança, uso de senhas, acesso à informação, compartilhamento de dados, atualização de *softwares*, uso de correio eletrônico e uso de antivírus.
- ☑ Realizar revisões periódicas da política de segurança da informação.
- ☑ Gerenciar contratos e aquisições com observância ao tratamento adequado dos dados pessoais.

CONSCIENTIZAÇÃO E TREINAMENTO

- ☑ Realizar a conscientização dos funcionários, via treinamentos e campanhas sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD e nas normas da ANPD.
- ☑ Informar e sensibilizar todos os funcionários da organização, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD.
- ☑ Criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas.

Informar funcionários sobre:

- Como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário.
- Como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de *phishing*, que podem ocorrer, por exemplo, ao clicar em *links* recebidos na forma de *pop-up* de ofertas promocionais ou em *links* desconhecidos que chegam por *e-mail*.
- Manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas.
- Não compartilhar *logins* e senhas de acesso das estações de trabalho.
- Bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros.
- Seguir as orientações da política de segurança da informação.

GERENCIAMENTO DE CONTRATOS

Estabelecer contratos com cláusulas de segurança da informação que assegurem a proteção de dados pessoais, tais como:

- Regras para fornecedores e parceiros.
- Regras sobre compartilhamentos.
- Relações entre controlador-operador.
- Orientações sobre o tratamento a ser realizado com vedação a tratamentos incompatíveis com as orientações do controlador.

☑ Assinar termos de confidencialidade (*Non-Disclosure Agreement* – NDA) com os funcionários da empresa.

CONTROLE DE ACESSO

- ☑ Implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais.
- ☑ Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem certo nível de complexidade.

Implementar um adequado gerenciamento de senhas, estabelecendo controles tais como:

- Evitar o uso de senhas-padrão disponibilizadas pelos fornecedores de *software* ou *hardware* adquiridos.
- Utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos.
- Não reutilizar senhas.

☑ Proibir o compartilhamento de contas ou de senhas entre funcionários.

☑ Aplicar o princípio do menor privilégio (*need to know*).

☑ Utilizar a autenticação multifator para acessar sistemas ou base de dados que contenham dados pessoais.

☑ Implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI (caso o agente de tratamento possua rede interna de computadores).

SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

☑ Coletar e processar apenas os dados pessoais que são, realmente, necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados.

☑ Implementar soluções de pseudonimização, como a criptografia, para cifrar dados pessoais.

☑ Orientar os funcionários para não desativar ou ignorar as configurações de segurança de estações de trabalho.

☑ Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como *pendrives* e discos rígidos externos.

☑ Inventariar e cifrar dados de dispositivos externos e armazená-los em locais seguros.

☑ Realizar *backups offline*, periódicos e armazená-los de forma segura.

☑ Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las ou, quando não for possível a sobrescrita, destruir as mídias físicas.

☑ Estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte).

SEGURANÇA DAS COMUNICAÇÕES

☑ Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim a fim para serviços de comunicação.

☑ Instalar e manter um sistema de *firewall* e/ou utilizar um *Web Application Firewall* (WAF), filtro de aplicação.

☑ Proteger *e-mail*s via adoção de ferramentas AntiSpam, filtros de *e-mail* e integrar o antivírus ao sistema de *e-mail*.

☑ Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.

GERENCIAMENTO DE VULNERABILIDADES

☑ Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar *patches* de segurança disponibilizados pelos fornecedores).

☑ Adotar e atualizar periodicamente *softwares* antivírus e *antimalwares*.

☑ Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

DISPOSITIVOS MÓVEIS

☑ Utilizar técnicas de autenticação multifator para controle de acesso de dispositivos móveis – como *smartphones* e *laptops*.

☑ Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível.

☑ Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

SERVIÇOS EM NUVEM

☑ Realizar um contrato de acordo de nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados.

☑ Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende aos demais requisitos de segurança da informação estabelecidos.

☑ Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado.

☑ Utilizar técnicas de autenticação multifator para acesso aos serviços em nuvem relacionados a dados pessoais.

2 PROTOCOLO PARA INOVAÇÃO E DESENVOLVIMENTO DE NOVAS TECNOLOGIAS

2.1 PESQUISA E DESENVOLVIMENTO (P&D)

O processo de pesquisa e desenvolvimento (P&D) é central para possibilitar o crescimento da indústria e a inovação nos mais diversos setores. De acordo com pesquisa realizada pela CNI em parceria com o Instituto FSB Pesquisa[101], foi relatado pelas empresas que importante forma de passar pela pandemia da covid-19 foi o investimento em inovação. Entre as empresas ouvidas pela pesquisa, 80% relataram que a inovação gerou importantes ganhos de produtividade, competitividade e aumentou os lucros.

Ademais, a mesma pesquisa identificou que as prioridades para inovação pós-pandemia envolvia, em sua maioria, a relação com o cliente e consumidor[102]. Esse fato é crucial para a discussão deste guia, pois a proteção de dados pessoais deve ser uma aliada dos processos de desenvolvimento de novas tecnologias.

Até mesmo processos que não se relacionam diretamente com o consumidor final – e, portanto, titular dos dados pessoais – podem necessitar de dados pessoais para que sejam desenvolvidos. Em primeiro lugar, dados também levantados pela CNI de 2020[103] demonstram que o maior investimento realizado com P&D internamente nas empresas consiste em "despesas correntes com pessoal", correspondendo a cerca de 56,9% dos dispêndios internos, sendo o investimento com pesquisadores importante fator dos setores.

Veja-se que logo no início da construção de um departamento de pesquisa e desenvolvimento já é necessário o tratamento de dados pessoais dos colaboradores envolvidos.

101 CNI. Disponível em: https://noticias.portaldaindustria.com.br/noticias/inovacao-e-tecnologia/80-das-industrias-inovaram-na-pandemia-e-tiveram-aumento-de-lucro-e-produtividade/

102 CNI. Disponível em: https://static.portaldaindustria.com.br/portaldaindustria/noticias/media/filer_public/5a/1f/5a1f2e83-64e1-4e2e-ad27-7cb03220db5b/fsb_pesquisa_cni_inovacao_-_imprensa_embargo.pdf. p. 72.

103 CNI. Disponível em: https://static.portaldaindustria.com.br/portaldaindustria/noticias/media/filer_public/c0/ae/c0aeaca0-975d-4826-a709-c27daa70b039/resultados_sondagem_sobre_pd_e_inovacao_empresarial.pdf. p. 14.

Outro exemplo da relevância do tratamento de dados pessoais nos projetos de P&D é o desenvolvimento de tecnologias da chamada internet das coisas (IoT). Trata-se de tecnologia que tem como objetivo a conexão entre objetos por meio de internet, possibilitando um nível cada vez maior de automação desses dispositivos. Os dados pessoais acabam sendo centrais para o desenvolvimento dessas tecnologias, pois elas utilizam *softwares* de inteligência artificial e, muitas vezes, utilizam o padrão comportamental do usuário para automatizar determinadas funções.

Essas tecnologias fazem parte da Indústria 4.0[104] mencionada anteriormente e envolvem um grande investimento em P&D em outras tecnologias, como: computação em nuvem, cibersegurança, robótica avançada, manufatura digital e aditiva, digitalização, integração de sistemas e utilização de sistemas de simulação. É claro que nem todos esses recursos necessariamente requerem o tratamento de dados pessoais, contudo, a utilização de *big data* e dados de consumidores é uma tendência cada vez mais comum na área.

O desenvolvimento de projetos de P&D, envolvendo a relação com o consumidor, em geral, acaba abrangendo novas estratégias de *marketing*. Essa relação não é novidade entre os estudiosos da matéria, sendo identificada a sinergia entre as áreas há anos[105].

Enquanto os processos de P&D estão voltados ao desenvolvimento de novas soluções, produtos e tecnologias, as estratégias de *marketing* estão voltadas para a venda dos produtos. Contudo, entre as duas áreas, existe um grande campo de cooperação, especialmente no que diz respeito às soluções inovadoras e à busca por novos mercados consumidores. Em especial, a prospecção de novos mercados deve passar pela avaliação das necessidades dos consumidores e desenvolvimento de produtos que atendam a essas necessidades ou, então, a melhoria de um produto existente deve passar pela análise do mercado consumidor e pela coleta e análise de seus dados pessoais.

Todos esses processos acabam passando pelo tratamento de dados pessoais e, não raras vezes, pelo tratamento de dados que pode ser considerado de alto risco. Seja pelo tipo de informações coletadas (se dados sensíveis, de saúde, etc.), seja pela realização de perfilamento com base em dados pessoais.

Outro aspecto que deve ser considerado nos processos de P&D relaciona-se com a necessidade de envolvimento de pessoas no processo de desenvolvimento de um novo

104 CNI. **Indústria 4.0**: Entenda seus conceitos e fundamentos. Para mais informações, ver: https://www.portaldaindustria.com.br/industria-de-a-z/industria-4-0/

105 GRIFFIN, Abbie. HAUSER. John. **Integrating R&D and *Marketing***: a Review and Analysis of the Literature. The International Center for Research on the Management of Technology. WP 112-94, out. 1994. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/2533/SWP-3735-33836420.pdf?sequence=1&isAllowed=y; MYERS, John G.; GREYSER, Stephen A.; MASSY, William F. The Effectiveness of *Marketing*'s "R&D" for *Marketing* Management: An Assessment/ The Effectiveness of *Marketing*'s "R&D" for *Marketing* Management: An Assessment. **Journal of Marketing**, 43(1), p. 17-29, 1979. Disponível em https://www.jstor.org/stable/1250754

produto, como é o caso do setor de medicamentos. O processo é complexo e envolve procedimento regulamentado pelo Sistema CEP/Conep, tendo em vista a sensibilidade do tratamento de dados dos participantes e dos princípios éticos envolvidos.[106]

Assim, tendo em vista a importância dos dados pessoais nesses processos, passa-se à recomendação de implementação de novas tecnologias por meio da chamada privacidade na concepção ou *privacy by design*.

2.2 *PRIVACY BY DESIGN*

A importância da adoção da *privacy by design* pode ser observada nos arts. 46 e 50 da LGPD, que estimulam a adoção de medidas de segurança e de mitigação de riscos pelos agentes de tratamento. Essa recomendação de ação da privacidade na concepção alinha-se com a concepção de que a preocupação com o desenho de sistemas informacionais é elemento de grande importância para garantir a efetividade de um programa de privacidade.

Tal fato decorre da complexidade em se garantir a proteção dos dados pessoais dos titulares por meio de medidas rígidas e padronizadas, quando as atividades de tratamento variam de forma substancial a depender do ramo. Mesmo considerando apenas o escopo de atuação da CNI, o que se verifica é que dentro de sua base, a indústria possui atividades muito distintas, sendo extremamente desafiador estabelecer um único padrão de adequação à LGPD para todos eles.

Por esse motivo, o desenvolvimento e a implementação de novas tecnologias e metodologias considerando os efeitos para a privacidade e proteção de dados em todas as fases do processo de elaboração e implementação de uma tecnologia ou metodologia é altamente recomendável. Dessa forma, confere-se maior garantia de proteção aos titulares de dados, ao mesmo tempo em que se torna viável a introdução de inovações decorrentes do tratamento de dados.

São princípios da concepção de sistemas por meio da privacidade na concepção, ou *privacy by design*: i) proatividade e não reatividade; prevenção e não reparação; ii) privacidade como padrão; iii) privacidade incorporada ao *design*; iv) total funcionalidade – resultado positivo, e não soma zero; v) segurança do começo ao final – proteção do ciclo de vida; vi) visibilidade e transparência; e vii) respeito pela privacidade do usuário[107].

106 Código de Boas Práticas editado pela CNSAÚDE. Disponível em: http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/ Acesso em: 30 jul. 2021.

107 Tradução livre de: CAVOUKIAN, Ann. **Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices**. Disponível em: http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

A partir desses princípios, o desenvolvimento de sistemas deve perpassar pela avaliação de questões como[108]:

- Prevenir riscos de incidentes de segurança como regra para que eles não ocorram ou, caso ocorram, para que medidas sejam adotadas o mais rápido possível.
- Processar dados de acordo com a estrita necessidade e finalidade informada ao titular.
- Garantir que os titulares não devam ter que tomar nenhuma ação específica para proteger seus dados pessoais quando da utilização dos seus sistemas.
- Apresentar informações sobre os encarregados pelo tratamento de dados.
- Utilizar linguagem acessível em documentos públicos para facilitar a compreensão dos usuários e possibilitar que os usuários possam gerenciar a forma como seus dados são tratados.
- Ao processar um dado pessoal, ter certeza de que os todos os agentes, fornecedores, sistemas e serviços utilizados no tratamento de dados – em todas as etapas do tratamento – adotem medidas técnicas e operacionais para proteção dos dados.
- Utilizar tecnologias de aprimoramento de privacidade (PETs) para auxiliar no cumprimento de suas obrigações.

108 Recomendações inspiradas no *checklist* da ICO sobre o tema. **Data protection by design and default**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

3 CONCLUSÃO

Este **Guia de Boas Práticas de Proteção de Dados para a indústria** busca apresentar aos integrantes da base industrial a importância da adoção de medidas que visem à proteção dos dados pessoais tratados no bojo de sua atuação.

Não se trata apenas de prevenir a aplicação de multas pela recém-constituída autoridade de proteção de dados brasileira, a ANPD, e, sim, de possibilitar que os participantes da indústria possam aproveitar as oportunidades apresentadas pela nova legislação. Conforme já apontado, os benefícios da adoção de políticas sólidas de proteção de dados envolvem desde a criação de relação de fidelização e confiança com clientes, até o aumento das oportunidades de negócios que envolvem dados pessoais[109].

É justamente nesse sentido que o art. 50 da LGPD, *caput*, da LGPD busca possibilitar que os setores formulem normas próprias de governança de dados. No caso da indústria, a utilização de dados pessoais nas organizações passa pelos departamentos internos – como a gestão de recursos humanos – e alcança processos mais avançados que envolvem a Indústria 4.0 e a constante inovação de processos que os setores vivenciam. Ademais, também ocupa importante papel no desenvolvimento da indústria a utilização de dados pessoais para ações de publicidade e desenvolvimento de novos produtos.

Por conta da importância das operações de tratamento de dados para a indústria e da diversidade de atores que fazem parte desse ecossistema, a CNI lidera mais uma importante iniciativa que tem como objetivo promover a inovação e o desenvolvimento dos participantes do setor.

As diretrizes apresentadas neste trabalho, portanto, têm como objetivo possibilitar que os agentes da indústria possam extrair o máximo possível desses benefícios, inclusive com o aumento de produtividade proporcionado pela Indústria 4.0,[110] permitindo que seus integrantes se sintam seguros no processo de adequação de suas operações à LGPD por meio das diretrizes gerais apresentadas neste documento.

---

109 Para mais informações ver Parte 1, item 1.1 *Aspectos positivos do cumprimento da LGPD*, deste guia e CIPL e CEDIS/IDP. **Prioridades das Organizações Públicas e Privadas Implementarem de Forma Eficaz a Nova Lei Geral Brasileira de Proteção de Dados** (LGPD). Disponível em: https://www.idp.edu.br/projeto-lgpd.

110 CNI. **Empresas ganham em produtividade com a indústria 4.0**. Disponível em: https://noticias.portaldaindustria.com.br/noticias/inovacao-e-tecnologia/empresas-ganham-em-produtividade-com-a-industria-40/

CNI
Robson Braga de Andrade
Presidente

DIRETORIA JURÍDICA – DJ
Cassio Augusto Muniz Borges
Diretor Jurídico

Gerência Executiva de Estratégia Jurídica
Alexandre Vitorino Silva
Gerente Executivo de Estratégia Jurídica

Gerência de Consultoria
Fabiola Pasini Ribeiro de Oliveira
Gerente de Consultoria

Cassio Augusto Muniz Borges
Fabiola Pasini Ribeiro de Oliveira
Coordenação Técnica

Christina Aires Correa Lima
Fabiola Pasini Ribeiro de Oliveira
Julio Cesar Moreira Barbosa
Luisa Campos Faria
Equipe Técnica

Laura Schertel Mendes
Mônica Tiemy Fujimoto
Coordenação Científica

DIRETORIA DE COMUNICAÇÃO – DIRCOM
Ana Maria Curado Matta
Diretora de Comunicação

Superintendência de Publicidade e Mídias Sociais
Mariana Caetano Flores Pinto
Superintendente de Publicidade e Mídias Sociais

Marcela Louise Moura Santana
Sarah de Oliveira Santana
Produção Editorial

DIRETORIA DE SERVIÇOS CORPORATIVOS – DSC
Fernando Augusto Trivellato
Diretor de Serviços Corporativos

Superintendência de Administração – SUPAD
Maurício Vasconcelos de Carvalho
Superintendente Administrativo

Alberto Nemoto Yamaguti
Normalização

Candeia Revisões / Danúzia Queiroz / Fabiano Gama
Revisão Gramatical

Editorar Multimídia
Projeto Gráfico e Diagramação

Associação Brasileira da Indústria de Máquinas e Equipamentos (ABIMAQ)
Anne Joyce Angher
Associação Colaboradora

Grupo FarmaBrasil
Amanda Do Couto Ferrari
Associação Colaboradora

Associação Brasileira da Indústria Têxtil e de Confecção (Abit)
Fernanda Garcia Tamburus
Associação Colaboradora

Associação Brasileira da Indústria do Plástico (ABIPLAST)
Paulo Henrique Rangel Teixeira
Associação Colaboradora

Associação Brasileira da Industria de Alimentos (ABIA)
Vanessa Amaral
Associação Colaboradora

Associação Brasileira da Indústria Elétrica e Eletrônica (ABINEE)
Ana Paula Bialer
Kelly Caporalli
Associação Colaboradora

Associação Brasileira da Indústria Química (ABIQUIM)
Yhebert Gouveia Afonso
Associação Colaboradora

Câmara Brasileira da Indústria da Construção (CBIC)
Erika Albuquerque Calheiros
Associação Colaboradora

Associação Brasileira dos Fabricantes de Brinquedos (ABRINQ)
Synésio Batista da Costa
Associação Colaboradora

Instituto Aço Brasil
Mônica Aguiar
Associação Colaboradora

www.cni.com.br

/cnibrasil

@CNI_br

@cnibr

/cniweb

/company/cni-brasil

CNI

Confederação Nacional da Indústria

PELO FUTURO DA INDÚSTRIA