Guia de Boas Práticas no Tratamento de Dados Pessoais: Com base na Lei Geral de Proteção de Dados.

Guia de Boas Práticas no Tratamento de Dados Pessoais na Companhia de Processamento de Dados do Estado da Paraíba.

AGOSTO/2022

CODATA GOVERNO DA PARAÍBA

Companhia de Processamento de Dados do Estado da Paraíba:

Angelo Giuseppe Guido de Araujo Rodrigues (Diretor Presidente)

Equipe Técnica de Elaboração:

Setor de Governança e Privacidade de Dados da CODATA/PB:

Hudyson Santos Barbosa (Encarregado de Proteção de Dados)

Júlia Monteiro Lucena Agra (Advogada)

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
16/08/2022	1.0	Primeira versão do Guia de boas práticas	Setor de Governança e Privacidade de Dados

Sumário

8. BOAS PRÁTICAS PARA TRATAR DADOS PESSOAIS NO PBDOC

9. BOAS PRÁTICAS AO USAR OS EQUIPAMENTOS DA CODATA

    9.1 O bom uso dos computadores da CODATA

    9.2 O bom uso das impressoras da CODATA

    9.3 O uso de ferramentas oficiais da CODATA

    9.4 O uso seguro das senhas

1. INTRODUÇÃO

Esse guia segue as diretrizes do Decreto Estadual n° 41.238, de 07 de maio de 2021, e precisa ser compreendido à luz das disposições de Segurança da Informação e Proteção de Dados Pessoais dispostas na Lei Federal de n° 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados, assim como demais regulamentações relacionadas.

Estamos vivendo uma grande transformação cultural em todas as empresas e instituições, incorporando o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas, alcançando níveis estratégicos, táticos e operacionais de toda empresa. A LGPD veio para proteger a privacidade dos indivíduos em relação aos dados pessoais, tendo a missão de conciliar os valores fundamentais do respeito à vida privada e da livre circulação de informação entre as pessoas, dando aos indivíduos o controle de suas próprias informações pessoais. Para tanto, no dia 14 de agosto de 2018, a Lei Geral de Proteção de Dados foi sancionada, entrando em vigor no dia 18 de setembro de 2020, e suas sanções previstas começaram a valer a partir do dia 01 de agosto de 2021.

Com o advento dessa nova Lei, os negócios foram impactados de forma profunda, tendo em vista que os dados pessoais estão em todas as frentes de operação de uma empresa, abrangendo desde os colaboradores até os clientes, o que provocou a conscientização das empresas para a adequação da LGPD.

Nesse contexto, esse documento tem como finalidade fornecer orientações e boas práticas sobre as operações no tratamento de dados pessoais para os servidores da Companhia de Processamento do Estado da Paraíba - CODATA/PB, de acordo com o art. 50 da Lei Geral de Proteção de Dados.

Assim, esse guia traz informações sobre as noções gerais da Lei Geral de Proteção de Dados, direitos dos titulares de dados, o ciclo de vida do tratamento de dados, como realizar as operações de tratamento de dados e as boas práticas de segurança da informação.

Por isso, é importante entender os fundamentos dessa legislação, como ela se aplica à sua realidade, quais são seus princípios gerais e as bases legais que viabilizam o tratamento de dados.

2. NOÇÕES GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

2.1. Por que sua empresa deve se importar com a proteção dos dados e privacidade?

Nos encontramos em um momento de mudança para uma nova cultura no mercado, em que a conscientização dos usuários sobre seus direitos em relação à proteção de seus dados pessoais está cada vez maior, assim como estar adequado à LGPD tem se tornado um diferencial competitivo para as empresas, tornando os seus processos mais confiáveis e robustos, o que acaba conquistando mais clientes.

De acordo com pesquisa realizada pelo relatório da Consumer Pulse 2019, mais de 75% dos consumidores não estão confortáveis com a coleta de dados via microfone ou assistente de voz e 51% dizem que o número de anúncios invasivos está crescendo. Ou

seja, os consumidores já estão se empoderando da nova Lei e exigindo que seus direitos sejam respeitados e cumpridos.

O vazamento de dados ou qualquer violação da Lei podem chegar a gerar prejuízos que chegam a casa dos bilhões. Vê-se, portanto, que os consumidores estão mais atentos e exigindo transparência na forma do tratamento de seus dados pessoais, além das próprias autoridades públicas.

O tema proteção à privacidade não é novo, visto que já é previsto na Constituição Federal desde 1988, reforçado pelo Código Civil de 2002, dialogando fortemente com o CDC e o Marco Civil da Internet. Portanto, com a velocidade da transformação digital e os avanços tecnológicos, fez-se necessário uma regulação para o uso desenfreado dos nossos dados pessoais. Essa tendência não está mais forte apenas no Brasil, mas é uma tendência global, em que a transparência no uso dos dados pessoais e respeito pelos usuários são cada vez mais exigidos e tornando-se indispensável para qualquer empresa, instituição, etc.

Nos últimos anos, o Ministério Público do Distrito Federal e Territórios (MPDFT) aplicou multas milionárias a diversas empresas que não aplicaram medidas de proteção aos dados pessoais.

Ante o exposto, é visível que estar adequado à LGPD não é mais uma opção, mas uma obrigação e dever, e o esforço de todos é muito importante para que a privacidade dos usuários seja respeitada.

2.2. Dados Pessoais e Dados Sensíveis

O dado pessoal está conceituado na própria LGPD em seu art.5°, sendo qualquer informação que permita identificar, direta ou indiretamente, uma pessoa natural, tais como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies.

É importante frisar que CNPJ ou dados bancários de pessoa jurídica não são dados pessoais. Contudo, caso haja informações pessoais do representante legal daquela empresa, por ser uma pessoa natural, também se encaixa em dados pessoais.

Dados pessoais são apenas os relacionados à uma pessoa natural.

Os dados pessoais sensíveis são os que exigem um maior cuidado em seu tratamento, sendo dados que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

2.3. Agentes de Tratamento: Controlador e Operador

A Lei Geral de Proteção de Dados traz duas figuras importantes para esse cenário de tratamento de dados pessoais, os agentes de tratamento conhecidos como o controlador e o operador. Esses agentes são definidos a partir de seu caráter institucional e podem ser pessoais naturais ou jurídicas, de direito público ou privado. A classificação desses agentes é importante para que a responsabilidade seja definida.

Inicialmente, é crucial que se esclareça que os indivíduos subordinados, tais como os funcionários, servidores públicos ou as equipes de trabalho de uma empresa, não são considerados controladores (autônomos ou conjuntos) ou operadores, pois atuam sob o poder diretivo do agente de tratamento. Contudo, esses indivíduos realizam atividades dos agentes de tratamento, tendo obrigações típicas de controladores ou operadores.

O controlador é o agente responsável por definir a finalidade do tratamento de dados e por tomar as principais decisões em relação a ele, incluindo instruções fornecidas aos operadores contratados para aquele determinado tratamento. E suas obrigações serão demonstradas na tabela a seguir:

OBRIGAÇÕES DO CONTROLADOR	LEI GERAL DE PROTEÇÃO DE DADOS
Elaborar Relatório de Impacto à Proteção de Dados Pessoais	Art. 38
Comprovar que o consentimento obtido do titular atende às exigências legais	Art. 8°, § 2°
Comunicar à ANPD a ocorrência de incidentes de segurança	Art. 48
Responsabilidade de reparar danos decorrentes de violação à legislação de proteção de dados pessoais	Art. 42 a 45
Garantir os Direitos dos Titulares, como fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, receber requerimento de oposição a tratamento	Art.18
Indicar o Encarregado de Proteção de Dados	Art. 41

A figura do operador é o responsável por realizar o tratamento dos dados em nome do controlador e seguindo a finalidade delimitada por ele, podendo definir elementos não essenciais do tratamento, como medidas técnicas. Demonstrando a grande diferença entre os dois agentes, o poder de decisão. Assim, as obrigações do operador são:

OBRIGAÇÕES DO OPERADOR	LEI GERAL DE PROTEÇÃO DE DADOS
Seguir as instruções do operador	Art. 39

Manter registro de operações de tratamento	Art. 37
Responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador	Art. 42, § 1º, I

Com isso, resta esclarecer que o agente de tratamento é definido para cada operação de tratamento de dados pessoais, podendo uma mesma empresa ser tanto operador como controlador, de acordo com a sua atuação. Sendo controladores quando atuarem com seus próprios interesses e sendo operadores quando atuarem de acordo com os interesses do controlador.

No contexto da CODATA/PB, que é uma pessoa jurídica de direito público da administração indireta, podemos citar alguns cenários para melhor visualização do seu papel como controlador ou operador:

Exemplo 1: CODATA/PB como controladora

- Internamente: CODATA/PB toma as decisões de como tratar os dados pessoais e seus setores executam aquele serviço de acordo com o demandado Ou seja, o poder de decisão está na CODATA, tornando-a controladora, e os setores serão operadores.

- Externamente: Quando a CODATA/PB tem poder de decisão sob os dados pessoais e quer terceirizar um serviço de câmera de segurança (CFTV), ela estará será a controladora dos dados por decidir como eles serão tratados e a finalidade daquele tratamento, e a empresa que presta o serviço de câmera de segurança será o operador por seguir as orientações da CODATA/PB.

Exemplo 2: CODATA/PB como operadora

- Uma Secretaria do Estado solicita um determinado serviço da CODATA/PB, ela irá demandar o que deve ser feito com os dados que serão fornecidos à CODATA. Dessa forma, a Secretaria estará tomando as principais decisões diante dos dados, e a CODATA/PB seguindo as instruções. Ou seja, a Secretaria do Estado será a controladora e a CODATA/PB a operadora.

- O DETRAN solicita um serviço de armazenamento de dados pessoais à CODATA/PB. Nesse caso, o DETRAN tem poder de decisão em relação a esses dados e a CODATA apenas prestará o serviço solicitado, assim como seguirá a finalidade. Assim, temos o DETRAN como controlador dos dados pessoais e a CODATA como operadora.

Diante desses cenários, uma coisa é observada, o poder de decisão sobre o tratamento dos dados determina quem é a figura do controlador e quem é o operador, e

poderá sempre mudar dependendo do caso fático. E por isso é tão importante que todos ajam com responsabilidade diante de tratamento de dados pessoais, seguindo a Lei Geral de Proteção de Dados e as boas práticas determinadas pela empresa.

2.4. Encarregado de Proteção de Dados - DPO (Data Protection Officer)

O artigo 41 da LGPD traz a figura do encarregado de proteção de dados, também conhecido como DPO (Data Protection Officer), que deverá ser indicado pelo controlador. O encarregado poderá ser tanto pessoa física como pessoa jurídica, e pode ser um funcionário de uma organização ou um agente externo.

É recomendável que o encarregado seja indicado por um ato formal, como um contrato de prestação de serviço ou um ato administrativo.

Como boa prática, o encarregado deve ter liberdade na realização de suas atribuições e deve ter conhecimento de proteção de dados e segurança da informação em um nível que atenda as necessidades da organização. Ainda, é importante que o encarregado tenha recursos adequados para conseguir realizar as suas atividades, como uma equipe de proteção de dados, prazos apropriados, finanças e infraestrutura.

No caso de um funcionário interno ser indicado para a função de encarregado, a organização também deverá capacitar esse profissional para que consiga exercer suas atividades com excelência.

As funções do encarregado estão definidas na LGPD em seu art. 41, § 2º:

FUNÇÕES DO ENCARREGADO DE PROTEÇÃO DE DADOS
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Além dessas funções, a Classificação Brasileira de Ocupações - CBO, no código 1421-35, reconheceu o encarregado como profissão perante o Ministério do Trabalho em 2022, e estabeleceu que o DPO deve:

1421-35 Oficial de Proteção de Dados Pessoais (DPO)

Planejar processos administrativos, financeiros, de compliance, de riscos e de proteção de dados pessoais e privacidade.
Gerenciar pessoas, rotinas administrativas e financeiras.
Administrar riscos, recursos materiais, serviços terceirizados e canal de denúncia.
Participar da implementação do programa de compliance e/ou governança em privacidade.
Monitorar e avaliar o cumprimento das políticas do programa, normativas, código de ética, procedimentos internos e parceiros de negócios.
Participar da identificação de situações de riscos e propor ações para mitigação dos mesmos.
Prestar atendimento ao cliente e/ou cooperado e/ou titular de dados pessoais.

Os detalhes de contato do encarregado de dados devem estar facilmente acessíveis, nos termos no § 1º do art. 41 da LGPD, para que os titulares possam entrar em contato, assim como a Autoridade Nacional de Proteção de Dados.

2.5. Autoridade Nacional de Proteção de Dados - ANPD

A Autoridade Nacional de Proteção de Dados é um órgão federal responsável por fiscalizar e aplicar a Lei Geral de Proteção de Dados, tendo suas principais competências estabelecidas no art. 55-J da LGPD, inclusive a de aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

O art. 52 da LGPD define que a ANPD, após procedimento administrativo que possibilite a ampla defesa, pode aplicar as seguintes sanções administrativas:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, 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;
- Multa diária, observado o limite total a que se refere o inciso II;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;

- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

- Suspensão 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.

A aplicação dessas advertências são analisadas mediante algumas circunstâncias, como a gravidade daquela ação, como afetou os titulares de dados, a cooperação do infrator, a adoção de políticas de boas práticas e governança e a pronta ação para adoção das medidas corretivas.

3. O CICLO DE VIDA DO TRATAMENTO DE DADOS PESSOAIS

3.1. O tratamento dos dados pessoais

A definição de tratamento de dados pessoais está no art. 5°, X, da LGPD, no qual diz que é “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.”

É importante deixar claro que até se você tem acesso àquele dado pessoal e não realiza nenhuma atividade com ele, ainda assim você estará fazendo um tratamento de dados pessoais e necessita seguir a Lei Geral de Proteção de Dados.

O art. 4° da LGPD determina as hipóteses em que a Lei não será aplicada:

- Dados Pessoais tratados por pessoas naturais para fins não econômicos: podemos citar o exemplo de uma pessoa que posta uma foto de uma terceira pessoa na sua conta do instagram.

- Dados Pessoais tratados para fins Jornalísticos ou Artísticos: essa hipótese garante a liberdade de imprensa, um exemplo é um caso de um jornalista que publica em um site o nome e foto de um suspeito de cometer um crime.

- Dados Pessoais tratados para fins Acadêmicos: se os dados forem utilizados para pesquisas sem fins diretamente comerciais, valendo ressaltar que, sempre que possível, esses dados devem ser anonimizados. Um exemplo é o de um pesquisador de universidade federal que utiliza dados pessoais anonimizados para fundamentar sua pesquisa em relação ao COVID.

- Dados Pessoais tratados para fins de Segurança Pública, Defesa Nacional, Segurança do Estado e Atividades de Investigação e Repressão de Infrações Penais: essa hipótese é um tratamento feito pelo Poder Público.

- Dados Pessoais Provenientes de Fora do Território Nacional Sem Comunicação ou Compartilhamento com Empresas Brasileiras, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei: como exemplo podemos citar uma empresa brasileira que é contratada por uma empresa europeia para tratamento de dados pessoais dos cidadãos europeus, e os dados são devolvidos para a empresa após o término do tratamento, dessa forma, se aplica a legislação europeia (GDPR).

Para que o tratamento de dados pessoais seja realizado em conformidade com a Lei Geral de Proteção de Dados, é necessário que seja feita uma análise dos processos para verificar se eles atendem às diretrizes estabelecidas na LGPD, se as bases legais da LGPD estejam sendo cumpridas, garantir que a finalidade do tratamento esteja de acordo com a lei e confirmar se as normas em relação aos compartilhamentos de dados estejam sendo seguidas.

3.2.Fases do ciclo de vida do tratamento dos dados pessoais

Para que a implementação da Lei Geral de Proteção de Dados na empresa seja feita, é preciso que se tenha conhecimento dos dados pessoais gerenciados, dos fluxos dos processos e dos ativos que estão presentes no ciclo de vida do tratamento dos dados pessoais. Assim, o ciclo de vida do tratamento de dados pessoais é como cada operação de dado pessoal se inicia e como é finalizada e a forma como seus ativos organizacionais estão em cada fase. Começando com a coleta do dado pessoal e se encerrando com a eliminação ou descarte. Suas fases são:

- ➔ Coleta: essa fase inclui coleta, produção e recepção de dados pessoais, podendo ser através de documento em papel, formulário eletrônico, sistema de informação, banco de dados, etc.

- ➔ Retenção: trata do armazenamento dos dados ou arquivamento, independente de ser por meio eletrônico (banco de dados), documento salvo no computador, documento em papel, guardado em uma pasta ou em armário, etc.

- ➔ Processamento: são as operações relacionadas a classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador. Em suma, é o que você faz com aquele dado pessoal, se acessa ele para autorização de pagamento, se utiliza para preenchimento de cadastro, para realização de treinamentos, etc.

- ➔ Compartilhamento: envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais. Por exemplo, quando compartilha dados pessoais para o banco para determinada finalidade.

- ➔ Eliminação: é a operação que exclui/elimina dados pessoais.

Em cada fase do ciclo, existem tipos de ativos organizacionais, principalmente: base de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais:

- ➔ Base de dados: uma coleção de dados logicamente relacionados.
- ➔ Documento: unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005).
- ➔ Equipamento: objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.
- ➔ Local físico: determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal.
- ➔ Pessoa: qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais.
- ➔ Sistema: qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais.
- ➔ Unidade organizacional: órgãos e entidades da Administração Pública.

Na realização do mapeamento do tratamento dos dados pessoais, em casa fase os ativos organizacionais envolvidos precisam ser identificados. Geralmente, na fase da coleta, os dados podem entrar na empresa através de algum documento e algum sistema. Na fase da retenção, os ativos são os que armazenam os dados, como base de dados, documentos, equipamentos, sistemas, locais físicos onde são armazenados, serviço de nuvem contratado. No processamento, pode ser realizado em documento, sistema interno ou até um serviço contratado, também sendo necessário identificar as pessoas envolvidas, os equipamentos. E dessa forma, os ativos estão presentes em cada fase do ciclo de tratamento de dados pessoais.

Após o mapeamento de todas essas informações em relação ao tratamento de dados pessoais, pode-se identificar quais medidas de segurança a empresa deverá implementar em cada etapa do fluxo dos processos, e garantir que o adequado grau de proteção de dados exigido pela LGPD seja alcançado.

4. COMO REALIZAR O TRATAMENTO DE DADOS PESSOAIS

4.1. Hipóteses de Tratamento de Dados Pessoais - Bases Legais

Para que o tratamento de dados pessoais possa ser realizado, ele precisa se enquadrar nas hipóteses elencadas no art. 7° e 11° da Lei. As finalidades e contextos de cada situação de tratamento de dados deve ser analisada para que sejam documentadas, pois o titular de dados deve conhecer a hipótese legal que autoriza o processamento de seus dados.

Dessa forma, com o intuito de ajudar na identificação dessas hipóteses, o Guia de Boas Práticas elaborado pelo Governo Federal, criou uma série de perguntas como checklists e destacando obrigações para os controladores e operadores que procedem da escolha da hipótese legais:

HIPÓTESE 1: CONSENTIMENTO DO TITULAR

Essa hipótese deve ser escolhida em último caso, quando as demais foram descartadas e avaliando os seguintes questionamentos, que devem ser respondidos positivamente para que essa hipótese possa ser aplicada:

1. Serão viáveis a coleta e o armazenamento da opção de consentimento do titular de modo a poder comprovar posteriormente a sua expressa manifestação de vontade?

2. Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado?

3. O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento?

   Para responder a pergunta 3, é preciso analisar essas questões:

   a) É vedado o tratamento de dados pessoais mediante vício de consentimento.

   b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

   c) Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.

   d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

4. Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado?

5. No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal?

6. No caso do tratamento de dados pessoais sensíveis, será registrada a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento?

HIPÓTESE 2: CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

Nessa hipótese, o tratamento de dados pessoais será feito para garantir o cumprimento de outras leis ou normas, não se enquadrando as obrigações oriundas de contratos. Assim, devendo ser respondidas positivamente, as perguntas para determinação dessa hipótese são:

1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?
2. É possível identificar a competência legal do órgão que dará cumprimento à obrigação legal ou regulatória?
3. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?
4. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei?

HIPÓTESE 3: EXECUÇÃO DE POLÍTICAS PÚBLICAS

Essa base legal só se aplica à administração pública e não às empresas, garantindo que o poder público possa tratar e fazer uso compartilhado de dados pessoais se eles forem necessários para colocar em prática políticas públicas previstas em leis e regulamentos ou respaldadas em contratos e convênios. Os casos de tratamento de dados para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, segundo o art. 4° da LGPD, não se aplicam nessa hipótese e nem na LGPD. Devendo-se avaliar:

1. O controlador é pessoa jurídica de direito público?
2. Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência?
3. O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?
4. É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais?
5. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?
6. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?

7. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei, inclusive quando da necessidade de compartilhamento de dados?

8. Será indicado um encarregado (Art. 5º, inciso VIII) para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a Autoridade Nacional de Proteção de Dados, que verificará a observância das instruções e normas sobre a política pública em questão?

As questões citadas devem ser respondidas positivamente para enquadramento nessa hipótese. O art. 23 da LGPD aduz que "o tratamento de dados pessoais pelas pessoas jurídicas de direito público, deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", cabendo a análise do caso concreto para estar de acordo com a norma e seus requisitos.

HIPÓTESE 4: REALIZAÇÃO DE ESTUDOS E PESQUISAS

Os órgãos de pesquisa que realizam estudos com base em tratamento de dados pessoais se enquadram nessa hipótese, a Lei ainda aduz que, sempre que for possível, os dados utilizados devem ser anonimizados. Devendo-se avaliar as questões e necessitando de respostas positivas:

1. O controlador ou operador é órgão de pesquisa?

2. Os dados pessoais serão utilizados dentro do órgão estritamente para a finalidade estabelecida para o estudo ou pesquisa?

3. Em se tratando de estudos em saúde pública, os dados serão mantidos em ambiente seguro e controlado, e será garantida, sempre que viável, a anonimização ou pseudonimização dos dados?

4. O órgão de pesquisa garante que não serão revelados dados pessoais em caso de divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa realizada?

5. O órgão de pesquisa que tiver acesso aos dados pessoais assume a responsabilidade pela segurança da informação e se compromete a não transferir os dados a terceiros em circunstância alguma?

HIPÓTESE 5: EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS AO CONTRATO

Essa hipótese é para os dados pessoais utilizados para executar ou preparar um contrato do qual o titular seja parte, a pedido do próprio titular. Por exemplo, dados fornecidos para formalizar a contratação de um funcionário. A forma como esses dados serão tratados e as obrigações das partes perante a LGPD, estarão previstos no contrato. Analisando tal questão:

1. O tratamento de dados pessoais se faz necessário para a consecução dos termos do contrato ou para a realização de procedimentos preliminares relacionados ao contrato?

HIPÓTESE 6: EXERCÍCIO DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL

Nessa hipótese, os dados tratados serão os necessários para o exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas. Devendo-se avaliar:

1. O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?
2. O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?

HIPÓTESE 7: PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO

Por exemplo, uma pessoa sofre um acidente e é preciso acessar seus documentos para que comunique à família. Para que se enquadre nessa hipótese:

1. O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros?
2. O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?

HIPÓTESE 8: TUTELA DA SAÚDE DO TITULAR

Essa hipótese é utilizada por profissionais de saúde, serviços de saúde ou autoridades sanitárias ao tratar dados pessoais que sejam necessários para suas atividades. Para enquadramento, deve-se analisar:

1. O tratamento de dados pessoais será realizado por profissional de saúde, serviço de saúde ou autoridade sanitária?
2. O tratamento de dados pessoais se faz necessário para a tutela da saúde do titular?

HIPÓTESE 9: LEGÍTIMO INTERESSE

Essa hipótese é utilizada para tratamento de dados pessoais quando necessários para atender os interesses legítimos do controlador ou de terceiro, exceto quando prevalecem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Entidades públicas e órgãos não podem utilizar essa hipótese se tratamento de dados ocorre para a consecução de políticas públicas ou de suas próprias competências legais. No entanto, em caso de finalidade diversa, essa opção poderá ser aplicável. Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificado interesse legítimo do controlador, considerado a partir de situações concretas, que respeite as legítimas expectativas do titular em relação ao tratamento de seus dados?

2. O controlador se responsabiliza por garantir a proteção do exercício regular dos direitos do titular ou a prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?

3. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

4. Serão adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador?

HIPÓTESE 10: PROTEÇÃO AO CRÉDITO

O tratamento de dados pessoais para proteção ao crédito é uma hipótese para garantir aos órgãos de proteção ao crédito que eles podem continuar incluindo dados de consumidores em cadastros positivos, e também a possibilidade das empresas com as quais o titular tenha pendências financeiras comunicarem aos órgãos competentes que existe essa dívida. Para enquadramento, deve-se avaliar:

1. Foi identificada necessidade de tratamento de dados pessoais para a proteção do crédito do titular?

2. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

HIPÓTESE 11: GARANTIA DA PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR

Essa hipótese está associada ao tratamento de dados sensíveis, sendo aplicável para assegurar a identificação e autenticação do titular para a autenticação de cadastro em sistemas eletrônicos. Essa hipótese será utilizada em último caso, quando não houver outro meio para identificar o titular. Ainda, essa hipótese não pode ser utilizada se prevalecem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

4.2. Verificação de conformidade do tratamento de dados quanto aos princípios da LGPD

Após a identificação das hipóteses legais para o tratamento de dados pessoais, se faz necessário que a conformidade com os princípios elencados na LGPD sejam verificados na operação. Dessa forma, a compreensão dos mesmos se faz de grande importância, os quais estão dispostos no art. 6° da Lei, tais sejam:

- ➔ Finalidade: “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;”, esse princípio aduz que nenhuma operação pode ser feita sem uma finalidade específica e clara.

- ➔ Adequação: “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;”, a justificação e garantia de que os dados que são coletados sejam condizentes com o modelo de negócio da organização e tenham valor.

- ➔ Necessidade: “ limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;”, é um princípio que exige que apenas os dados pessoais essenciais para o desenvolvimento do negócio sejam tratados.

- ➔ Livre acesso: “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;”

- ➔ Qualidade dos dados: “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;”

- ➔ Transparência: “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;”

- ➔ Segurança: “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;”

- ➔ Prevenção: “adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;”

- ➔ Não discriminação: “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;”

- ➔ Responsabilização e Prestação de contas: “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.”

Em suma, antes de começar uma operação com tratamento de dados pessoais, deve-se observar e estar de acordo com os princípios e enquadrado em uma hipótese da Lei Geral de Proteção de Dados.

5. DIREITOS DOS TITULARES DE DADOS PESSOAIS

Inicialmente, vale destacar que o titular de dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Assim, a Lei Geral de Proteção de Dados traz em seu art. 18° os direitos desses titulares, garantindo maior visibilidade, transparência e controle ao titular em relação aos seus próprios dados e como são tratados.

- ➔ Confirmação da existência de tratamento: o titular tem o direito de confirmar se uma empresa trata ou não seus dados pessoais;

- ➔ Acesso aos dados: o titular também pode pedir a empresa uma cópia dos seus dados pessoais que elas possuem;

- ➔ Correção de dados incompletos, inexatos ou desatualizados: é o caso de atualização de informações;

- ➔ Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- ➔ Portabilidade dos dados a outro fornecedor de serviço ou produto: O titular tem direito de solicitar que a empresa transfira suas informações pessoais a outro fornecedor.
- ➔ Eliminação dos dados pessoais tratados com o consentimento do titular: Da mesma forma que o titular pode dar seu consentimento para o tratamento de seus dados pessoais, também pode retirá-lo e pedir a eliminação dos dados;
- ➔ Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados: O titular tem o direito de saber exatamente com quem seus dados pessoais estão sendo compartilhados;
- ➔ Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- ➔ Revogação do consentimento.

Os direitos citados acima podem ser exercidos a qualquer tempo e mediante requisição expressa ao controlador. Além desses direitos, a LGPD também traz em seus outros artigos mais direitos relacionados ao titular de dados, que devem ser observados nos princípios e demais artigos.

A importância de protegermos a forma como os dados pessoais são tratados vai muito além de evitar receber multas e advertências, mas de garantir que esses dados sejam verídicos, que não sejam utilizados para decisões automatizadas sem o devido acompanhamento, e para que os titulares possam ter escolha de como suas informações pessoais podem ou não ser utilizadas. É proteger a privacidade das pessoas e a forma como serão julgadas pelo tratamento dos dados pessoais. A LGPD empodera os titulares de dados para que eles possam realmente ser donos das suas informações.

6. LAI E LGPD

A Lei de Acesso à Informação e a Lei Geral de Proteção de Dados têm gerado muita confusão entre os servidores públicos em relação a qual lei utilizar. A diferença entre a finalidade das duas leis é que a LAI regula o acesso da sociedade à informação pública, e a LGPD regula o tratamento de dados pessoais pela esfera pública e privada. Ambas estão pautadas no tripé confidencialidade, integridade e disponibilidade, alinhadas aos princípios da prevenção e da segurança.

Contudo, as duas leis protegem os dados pessoais e estão em harmonia, o que deve ser analisado para a aplicação correta, é o caso em si. Por exemplo, quando uma pessoa solicita informações à Administração Pública, deve ser analisado se o teor do acesso é pessoal ou coletivo, e a partir disso ora se aplicará a LAI ora a LGPD.

Na realidade, a LAI e a LGPD são leis sistematicamente compatíveis entre si e são duas normas que harmonizam os direitos fundamentais de acesso à informação e da

proteção de dados pessoais, não havendo oposição entre seus dispositivos, em que se pode observar a proteção da informação pessoal.

7. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

7.1. Privacidade desde a concepção e por padrão (Privacy by Design e by Default)

Os agentes de tratamento e todos que atuam no ciclo de vida do tratamento dos dados pessoais devem estar atentos para antecipar as situações que podem ferir a privacidade das pessoas e evitar que elas aconteçam. Assim, ao tratar dados pessoais, você é obrigado a assegurar a segurança da informação, como demonstrado no art. 46 da LGPD:

> *"Art. 46. 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.*
>
> *§ 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."***

O *captu* do artigo aduz que a proteção dos dados pessoais deve ser alcançada por meio de medidas de segurança, técnicas e administrativas, e seu § 2º menciona que essas medidas devem estar sendo observadas desde a fase de concepção do produto ou do serviço até a sua execução, ou seja, o *Privacy by Design.*

O *Privacy by Design* ou Privacidade desde a Concepção é composto por 7 princípios fundamentais mais específicos, sendo possível garantir o desenvolvimento tecnológico e a inovação com respeito aos direitos humanos e liberdades fundamentais. Sendo assim, os princípios são:

1. Proativo e não reativo; preventivo e não corretivo: a empresa não deve esperar que os riscos à privacidade se materializem, ao contrário: deve impedir que eles ocorram. Para isso, podemos adotar medidas organizacionais (comprometimento dos diretores, gerentes e servidores em adotar os mais altos padrões de privacidade) e medidas técnicas (incluir na fase do planejamento os melhores esforços preventivos).

2. Privacidade como padrão (by default): os dados pessoais devem ser automaticamente protegidos em qualquer sistema de tecnologia da

informação (TI) ou prática de negócio de modo que as pessoas não precisem fazer esforços para ter sua privacidade garantida. Para isso, podemos adotar medidas organizacionais (especificar a finalidade da coleta) e medidas técnicas (limitar a coleta às informações necessárias, limitar o uso apenas para o estritamente necessário).

3. Privacidade incorporada ao Design: A privacidade deve ser incorporada nas tecnologias de maneira holística, segura e criativa.

4. Funcionalidade Total: busca acomodar todos os objetivos e interesses legítimos de uma maneira positiva, com "ganhos em dobro" para os indivíduos e sociedade.

5. Segurança de ponta-a-ponta e proteção durante todo o ciclo de vida dos dados: não deve haver lacuna da proteção dos dados e nem na prestação de contas.

6. Visibilidade e Transparência: garantindo que as promessas da empresa são passíveis de verificação.

7. Respeito pela privacidade do usuário: prezar ao máximo pelos interesses do indivíduo, mantendo o usuário no controle dos seus dados pessoais.

Por fim, o Privacy by Design e seus 7 princípios devem estar presentes em toda tecnologia, processos, cultura e governança da empresa, ou seja, deve ser parte do DNA da empresa, oferecendo o máximo grau de privacidade e que a proteção dos dados pessoais seja automática em qualquer sistema ou prática de negócio.

7.2. Controle de Acesso, anonimização, pseudoanimização

O controle de acesso, anonimização e pseudoanimização são boas práticas que devem ser seguidas. É importante lembrar que quanto mais sensíveis são as informações, menos pessoas devem ter acesso a esses dados, ou seja, uma empresa precisa ter controle de acesso em toda fase do ciclo de vida do tratamento de dados pessoais, para que se possa mitigar riscos.

Além disso, a LGPD aduz que as técnicas de anonimização e pseudoanonimização devem ser utilizadas, sempre que possível, no tratamento dos dados pessoais. A própria Lei determina o conceito de dado anonimizado, sendo:

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

A partir do momento em que o dado foi anonimizado, ele sai do escopo da legislação, por não se tratar mais de um dado pessoal. No entanto, se o dado considerado anonimizado tem possibilidade de reversão do processo e permitir novamente a identificação do titular de dados, estaremos diante da pseudoanonimização, e por isso, ainda estará no escopo da Lei Geral de Proteção de Dados. Por exemplo, a criptografia é um dos métodos de pseudoanonimização, e é mais uma forma de proteger os dados pessoais, pois só poderá acessá-los quem conhecer a chave, sem ela, os dados são ininteligíveis.

8. BOAS PRÁTICAS PARA TRATAR DADOS PESSOAIS NO PBDOC

Ao utilizar a ferramenta PBdoc, alguns pontos precisam de atenção para que dados pessoais não sejam expostos de forma desnecessária e sem embasamento legal. Desse modo, quando documentos/processos forem elaborados no sistema, é importante que se colete ou insira somente os dados pessoais realmente necessários para atender a determinada finalidade, seguindo o princípio da necessidade da LGPD.

Quando se tratar de documentos públicos, assim como portarias, designações e outros, uma boa forma de proteger os dados pessoais é com o uso de tarjas e/ou descaracterização dos mesmos, a não ser que exista previsão legal quanto à publicidade/exposição de tais dados. Por exemplo:

CPF: 000.000.000-00 x

CPF: ***.000.000-** ✓

Matrícula: 000000000 x

Matrícula: ******000 ✓

Além disso, na criação de processos ou documentos, é importante estabelecer o nível de acesso, podendo ser público, restrito ou sigiloso. O art. 31, da Lei n° 12.527/2011, a LAI, aduz que no tratamento de dados ou informações pessoais o nível de acesso deve ser restrito sob a hipótese legal de “Informação Pessoal”.

Em qualquer caso, é importante que o servidor promova o equilíbrio entre a transparência e a proteção dos dados pessoais, analisando cada caso separadamente, se porventura houver a necessidade de disponibilizar os processos ou documentos a usuários externos.

9. BOAS PRÁTICAS AO USAR OS EQUIPAMENTOS DA CODATA

9.1 O bom uso dos computadores da CODATA

O uso dos computadores da CODATA também merecem atenção, visto que, se utilizados da maneira errada, podem gerar brechas para que dados pessoais sejam acessados por pessoas não autorizadas. Dessa forma, algumas práticas merecem atenção:

- Ao se ausentar da sua mesa, lembre sempre de bloquear o seu computador, evitando acesso não autorizado;
- Evite ao máximo baixar arquivos pessoais dentro do computador, para que não venham acompanhados de malwares e para que seus dados não fiquem expostos. Caso seja extremamente necessário baixar, lembre-se de excluí-los logo em seguida;

- Evite tirar prints, fotos ou gravar vídeos da tela do computador que contenha algum dado pessoal, opte por encaminhá-los por algum canal de comunicação oficial.

9.2 O bom uso das impressoras da CODATA

Assim como os computadores, as impressoras também precisam ser usadas de maneira responsável para que se evite alguma brecha no acesso aos dados pessoais. Portanto, é recomendável que:

- No momento em que o servidor imprimir documentos que contenham dados pessoais, deve lembrar de retirá-los da impressora logo em seguida;
- No caso da necessidade de descartar tais documentos, recomenda-se procurar técnicas para que os dados não sejam identificados, por exemplo, triturar o documento ou até mesmo riscar os dados pessoais de forma que se torne ilegível;
- Os documentos impressos que tiverem dados pessoais devem ser guardados em locais seguros, por exemplo, em um armário com chave;
- Quando deixar tais documentos em sua mesa, é preferível que vire o anverso das folhas para baixo, para que os dados pessoais não sejam vistos por qualquer pessoa.

9.3 O uso de ferramentas oficiais da CODATA

A CODATA utiliza a plataforma de e-mail corporativo chamada Zimbra, por isso, é preciso que a troca de e-mails contendo dados pessoais ocorra apenas através desse canal de comunicação, evitando que seja realizado por e-mails pessoais dos colaboradores.

9.4 O uso seguro das senhas

A proteção e a segurança das suas senhas é outro ponto importante para proteger os dados pessoais que estão na empresa, por isso, recomenda-se:

- Nunca compartilhe suas senhas com outras pessoas. A princípio, você é o responsável por tudo que ocorre com o uso de sua senha;
- Se você não consegue memorizar sua senha e precisar anotá-la, não a deixe em locais visíveis, expostas em cadernos ou marcadores em sua mesa de trabalho.