LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Dioni Alves da Silva
Eva Matos Pinho
Geovane Aquino Diniz Guedes
Gustavo Oliveira Cardoso
Luan Barbosa Souza
Marco Antônio Junqueira Bersani
Maria Francisca Cruz de Souza
Manuella Santana da Silva
Tamires Ribeiro de Souza
William Marques

Resumo

A presente pesquisa teórica foi realizada com o objetivo de embasar a atividade extensionista que será realizada no âmbito da disciplina "Direito Digital", sob a orientação do Prof. Dr. Henrique Savonitti Miranda.

O constante aumento dos usuários e a crescente presença das empresas no campo virtual, fez da segurança de dados algo imprescindível. Com o alto fluxo de dados, notou-se também o grande número de ataques cibernéticos e o uso indiscriminado de informações sensíveis, tornou-se necessária a fiscalização afim de garantir um ambiente virtual seguro.

A diretriz tomada para estabelecer a segurança dos dados veio através da Lei Geral de Proteção de Dados Pessoais do Brasil (13.709/2018), para assegurar o tratamento responsável, o correto manuseio e armazenamento de informações pessoais de terceiros pelas empresas, e gerar transparência para o público.

Este regulamento deve ser levado a sério, e sendo assim, muitas empresas investem neste aperfeiçoamento a fim de seguir os requisitos estabelecidos em lei. É de suma importância compreender a LGPD (lei13.709/2018) e garantir que os requisitos propostos estarão em conformidade com o código.

1. Introdução

A Lei Geral de Proteção de Dados (LGPD) (lei 13.709/2018) tem como objetivo principal, garantir a proteção de direitos fundamentais como a liberdade e privacidade. Foca também em criar um cenário juridicamente seguro, padronizando regulamentos e práticas que promovem a proteção aos dados pessoais de qualquer cidadão em território brasileiro.

Como afirma Patrícia Peck Pinheiro:

> *"A Lei n. 13/709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica." (PINHEIRO, 2024, pág. 1 do Kindle).*

A referida lei foi aprovada em 2018, com entrada em vigor a partir de 2020.

Em 2022, a lei contou com modificações, que acresceram pontos que tratam de questões específicas referentes às pequenas empresas. As atualizações trazidas foram fundamentais para adequar as exigências de conformidade às pequenas empresas, permitindo maior flexibilidade no cumprimento da lei e considerando as particularidades dessas organizações.

De acordo com Leandro Cazeiro, “a menor rigidez das regras em determinados requisitos tem um papel importante para desburocratizar processos e viabilizar a adequação dos agentes de tratamento de pequeno porte.” (CAZEIRO, 2024).

O conteúdo desta lei norteia a definição de dados pessoais e determina quais tipos de dados devem receber cuidados específicos, como por exemplo, dados pessoais sensíveis assim como dados a respeito de crianças e

adolescentes. Elucida ainda que estão sujeitos à regulação, todos os dados tratados por meio físico ou digital.

Ademais, a aplicabilidade da Lei Geral de Proteção de Dados (LGPD) se dá independentemente da localização da sede da empresa ou, mesmo, da origem dos dados. Portanto, possui aplicabilidade extraterritorial.

De acordo com Daniel Donda:

> *"(...) a lei se aplica quando os dados estiverem sendo tratados em território nacional, ou se os dados tiverem sido coletados em território nacional, independentemente do país onde seja a sede da empresa ou do país onde estejam localizados os dados, sendo uma lei com alcance extraterritorial" (DONDA, 2020, pág. 17 do Kindle).*

2. O que é a Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) (Lei 13.709/2018) é o regulamento brasileiro que visa garantir a segurança de informações pessoais, através de normas acerca da coleta, manuseio, compartilhamento e armazenamento de dados, voltadas para empresas e negócios.

A Lei Geral de Proteção de Dados (LGPD) tem como propósito assegurar que dados pessoais sejam tratados de forma segura e transparente, respeitando os direitos dos indivíduos.

Patrícia Peck Pinheiro afirma que:

> *O espírito da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa de boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso de informação que identifique ou possa identificar uma pessoa e esteja relacionada a*

> *ela, incluindo a categoria de dados sensíveis (PINHEIRO, 2024, pág. 1 do Kindle)*

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), em seu artigo 6°, elenca os princípios de boa-fé a serem observados no tratamento de dados pessoais, conforme listados abaixo:

> *"I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*
>
> *II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*
>
> *III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*
>
> *IV - **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;*
>
> *V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*
>
> *VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*
>
> *VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;*
>
> *VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*

> *IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*
>
> *X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."*

Outrossim, conforme mencionado, a sua aprovação se deu em 2018, entrando em vigor apenas em 2020. O lapso temporal existente entre a publicação da lei e sua entrada em vigor buscou conceder tempo suficiente para que as organizações revisassem e adequassem suas práticas de tratamento de dados, assegurando uma transição suave.

Em 2022, a Autoridade Nacional de Proteção de Dados publicou regulamentações específicas para agentes de tratamento de pequeno porte por meio da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Segundo matéria da Conjur, "o objetivo do regulamento é trazer equilíbrio para a adaptação de empresas de pequeno porte, microempresas e startups às regras da LGPD, e ao mesmo tempo garantir os direitos dos titulares dos dados" (CONJUR, 2022).

Quanto à territorialidade, a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) elenca regras para o tratamento de dados no Brasil, dispondo ainda de aplicabilidade extraterritorial, portanto, a lei deve ser respeitada independentemente de onde esteja localizada a sede da companhia ou origem dos dados.

A questão territorial é tratada no art. 3º Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018):

> *"Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:*
>
> *I - a operação de tratamento seja realizada no território nacional;*

> *II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)*
>
> *III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.*
>
> *§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.*
>
> *§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei."*

A LGPD teve influência direta da GDPR. A *General Data Protection Regulation* (GDPR) foi criada, na União Europeia, com entrada em vigor em 25 de maio de 2018. Com ela foram definidas regras para tratamento de dados pessoais, inclusive estabelecendo padrões mínimos de privacidade e proteção de dados para as empresas europeias que ao realizarem transferência internacional de dados para fora da Europa.

Assim, o Brasil, por ter interesse em ser membro efetivo da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), órgão voltado ao desenvolvimento econômico e à busca do bem-estar social por meio da cooperação entre seus países-membros, se viu com a necessidade de editar norma que passasse a regulamentar a proteção de dados pessoais.

Diante disso, com a "intenção de participar desse seleto grupo que recebe os dados oriundos da UE com maior facilidade, o Brasil passou a desenvolver uma norma protetiva de dados pessoais" (D'ÁVILA; SILVA; ARAÚJO, 2020, pág. 56 do Kindle).

Dentre as vantagens, obtendo o Brasil a Decisão de Adequação, as operações multinacionais no país poderão ser facilitadas, em especial quando europeias, possibilitando redução de custos de transação, gerada pela maior facilidade na transferência internacional de dados.

2.1 Dados Pessoais

A Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) traz a classificação dos dados regulados em categorias, como dados pessoais, dados sensíveis, dados anonimizados e dados pseudonimizados.

O artigo 5º define dados pessoais como informações relacionadas a uma pessoa natural identificada ou identificável, abrangendo elementos como nome, sobrenome, CPF, e-mail, endereço, data de nascimento, histórico de compras, dados de localização e identificadores eletrônicos.

A jurista Patrícia Peck Pinheiro define dados pessoais como:

> *"Toda informação identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva" (PINHEIRO, 2024, pág. 27 do Kindle).”*

Em suma, dados se referem a informações que podem vincular a identidade de uma pessoa viva, requerendo, dessa forma, um rigor maior ao ser tratado, conforme estabelece a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018).

Para que se faça o tratamento dos dados é imprescindível que haja o consentimento, devendo serem precisas as informações de como serão tratados os dados, sem que reste qualquer dúvida, não sendo permitido o “vício de consentimento” (BRASIL, 2018, art. 8º, § 3º).

De acordo com Daniel Donda, "a linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas” (PINHEIRO, 2024, pág. 37 do Kindle).

A LGPD exige que todos os dados que possam identificar uma pessoa devem ser tratados com um alto nível de proteção, de modo a garantir a privacidade e a segurança das informações pessoais.

Diante disso, a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) também traz uma categoria específica chamada de “dados sensíveis”, que envolvem informações delicadas, como origem racial ou étnica, convicções religiosas, posicionamento político, sindicalização ou filiação a organizações de caráter religioso, filosófico ou político, como também informações referentes à saúde, hábitos sexuais, dados referentes à genética ou biometria quando vinculados a uma pessoa natural (BRASIL, 2018, art. 5º, II).

Tal classificação objetiva garantir uma proteção maior, a fim de que esses dados não sejam mal utilizados, caso contrário, poderiam resultar em discriminação ou sérias violações de direitos individuais.

Conforme salienta Donda, "esses dados devem ter uma atenção maior, pois são muito pessoais e podem gerar atos discriminatórios e lesivos” (DONDA, 2020, pág. 17 do Kindle).

A classificação existente busca, ainda, que esses dados não sejam mal utilizados, prevenindo possíveis consequências negativas para os indivíduos afetados.

Também pode ser feita a anonimização de dados pessoais, dando maior ênfase aos dados sensíveis e informações críticas.

Como mencionado por Patrícia Peck Pinheiro, a anonimização é a “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” (PINHEIRO, 2024, pág. 29 do Kindle).

2.2 Bases legais da LGPD

O artigo 7º da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018) estabelece um arcabouço de princípios e situações onde é permitido o tratamento de dados pessoais, no qual se garante a proteção dos direitos dos titulares. Essas hipóteses abarcam uma série de contextos como consentimento explícito do titular, cumprimento de obrigações legais, realização de estudos por órgãos de pesquisa (com a anonimização devida dos dados), de modo a garantir

a privacidade dos participantes. Desse modo, os dados são utilizados de forma responsável e dentro de um marco regulatório.

O respeito às bases legais da Lei Geral de Proteção de Dados (LGPD) é necessário para que haja equilíbrio entre a inovação e a proteção de dados. À medida que se garanta que as informações sejam tratadas observados os princípios estabelecidos pela lei, organizações são capazes de promover maior segurança jurídica e confiabilidade nas suas operações, assegurando os direitos dos titulares e promovendo o uso ético dos dados (BRASIL, 2018).

2.3 Consentimento

A base legal do consentimento é a previsão de que o usuário, de forma inequívoca, declare sua concordância e permissão para que a empresa use seus dados pessoais. Portanto, “o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular” (BRASIL, 2018, Art. 7º, I).

Um exemplo atual são as inscrições para aulas grátis, já que para ter acesso, é necessário preencher um formulário com informações como nome completo, e-mail e telefone. A empresa obrigatoriamente deverá perguntar se você aceita receber e-mails com atualizações e promoções e se está de acordo com o acesso e armazenamento dos seus dados pela empresa. Tais exigências visam garantir o consentimento de forma clara e explícita.

Em todo o caso, o consentimento deve ser de manifestação livre, não podendo haver campos pré-marcados, como bem assevera Donda (2020):

> *“O consentimento deverá então ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Um claro exemplo desse tipo de manifestação é quando existe a necessidade de coleta de dados a partir de um website, em que a empresa deverá adotar o texto de consentimento e incluir uma checkbox que o titular irá marcar para expressar o consentimento. Essa checkbox não pode, de forma alguma, estar pré-marcada, e o titular deverá clicar nela para manifestar o seu consentimento.”*

2.4 Legítimo interesse

Trata-se de base legal para o tratamento de dados pessoais, conforme previsão contida no art. 10 Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018):

> *"Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:*
>
> *I - apoio e promoção de atividades do controlador; e*
>
> *II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.*
>
> *§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.*
>
> *§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.*
>
> *§ 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."*

Valida que as organizações processem dados sem necessitar de consentimento explícito do titular. Todavia, para tanto, "o interesse será considerado legítimo quando atender a três condições: (i) compatibilidade com o ordenamento jurídico; (ii) lastro em situações concretas; e (iii) vinculação a finalidades legítimas, específicas e explícitas." (ANPD, guia orientativo 2024, pág. 16).

Além disso, o interesse legítimo não pode ser colocado acima dos direitos e liberdades fundamentais do titular, havendo para este uma proteção especial.

Conforme destacado acima, o legítimo interesse é respaldo legal que autoriza o uso de dados que não necessitam necessariamente do consentimento do usuário. Por seu turno, as ações realizadas com essas informações não podem violar os direitos e liberdades dos usuários e deverão ser usados em ocasiões onde o serviço prestado beneficie o titular dos dados.

Tanto é assim que não há de se falar em tratamento por legítimo interesse de dados sensíveis. Conforme assevera Lima, “(...) não há a previsão da hipótese de tratamento em razão de interesse legítimo do controlador no caso de dados pessoais sensíveis, uma vez que se deve destacar o interesse do titular do dado” (LIMA, 2021, pág. 69 do Kindle).

Para se enquadrar no uso dessa base legal, a empresa deverá seguir uma série de regras para que a adoção dessa prática atenda os interesses da empresa tanto quanto respeite os direitos de seus titulares.

Conforme salienta Donda:

> *"(...) é complexa a aplicação dos interesses legítimos como fundamento legal para tratamento de dados pessoais e, por isso, o apoio especializado de profissionais da área será fundamental neste ponto para mitigar o risco de ilicitude” (DONDA, 2020, pág. 24 do Kindle).*

Diante disso, torna-se necessário que a empresa avalie com cuidado se os benefícios esperados são compatíveis com os riscos, de modo a garantir a privacidade dos dados.

De acordo com o que é estipulado pela Lei Geral de Proteção de Dados (LGPD), o uso de dados pessoais com fundamento no legítimo interesse deve ser "estritamente necessário para a finalidade almejada" (BRASIL, 2018, Art. 10, § 3º), reforçando o compromisso com o uso ético e transparente das informações dos titulares.

2.5 Contrato

Sua base legal está ancorada na garantia de cumprimento de uma obrigação prevista em contrato e tem como objetivo validar ou registrar o início de vigência de um acordo através do processamento dos dados de um usuário.

Ao ceder e autorizar o tratamento de seus dados, o usuário e a empresa criam um vínculo por meio deste contrato.

Desse modo, é criado um respaldo legal ao tratamento de dados pessoais, sendo parte essencial para a execução de obrigações entre as partes envolvidas.

De acordo com a Lei Geral de Proteção de Dados (LGPD), no país, "o tratamento de dados pessoais deverá observar a boa-fé e seguir os princípios de finalidade, adequação e necessidade" (Lei nº 13.709/2018, Art. 6º).

Para tanto, firma-se um contrato formal quando o usuário cede e autoriza o tratamento de dados para a empresa, gerando para ambos responsabilidades.

Ademais, para que se possa tratar o dado, é indispensável que ocorra o livre consentimento do titular dos dados, com o intuito de dar legitimidade do processo.

Como ensina a jurista Patrícia Peck Pinheiro, "a linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas" (PINHEIRO, 2024, pág. 39 do Kindle).

Um dos pilares fundamentais para fortalecer a confiança entre as partes é a existência de transparência no tratamento de dados pessoais. Há muitas situações em que o seu uso vai além do cumprimento de obrigações contratuais, podendo envolver dados de terceiros, ou até mesmo finalidades comerciais.

Assim, faz-se necessário que tais questões estejam claramente definidas nos termos dos contratos, bem como no consentimento concedido pelo

usuário, com a finalidade de se evitar que sejam violados os direitos do titular dos dados.

Nas palavras de Patrícia Peck Pinheiro, o consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (PINHEIRO, 2024, pág. 28 do Kindle).

Cabe pontuar que o responsável pelo tratamento dos dados, é responsável por protegê-lo de usos indevidos e, até mesmo, vazamentos de informações. Assim, cabe as empresas adotarem medidas de segurança e proteção, de modo a garantir a integridade e confiabilidade dos dados tratados. Nesse sentido, as empresas devem recorrer à adoção de tecnologias avançadas, a exemplo da criptografia e anonimização de dados, tais medidas são essenciais para mitigar riscos e assegurar o cumprimento das obrigações contratuais.

Nesse sentido, importante registrar o posicionamento em decisão do Superior Tribunal de Justiça:

> *“O Superior Tribunal de Justiça (STJ) entendeu que bancos de dados que compartilham informações de consumidores devem informá-los previamente acerca da utilização desses dados, sob pena de terem que pagar indenização por danos morais [...] o fato de as informações serem fornecidas pelo consumidor no ato de uma compra, ou até mesmo divulgadas em redes sociais, não afasta a responsabilidade do gestor do banco de dados de previamente comunicar o seu compartilhamento [...] uma empresa gestora de dados, que foi condenada a indenizar um consumidor em R$ 8 mil pela comercialização indevida de informações pessoais e sigilosas. [...].”*

Conclui-se, dessa forma, que o tratamento de dados observa várias normas que visam garantir a proteção dos direitos dos titulares. O contrato é o documento que vincula como se dará o tratamento de dados e deve observar os limites da legislação vigente, com transparência e segurança.

2.6 Assegurando boas práticas de LGPD

Com a crescente globalização e expansão da tecnologia pelo mundo, a proteção de dados ganhou significativa importância, sendo reconhecido como um ativo de alta relevância.

Nesse sentido, é crescente a necessidade de garantir a proteção dos dados pessoais daqueles que utilizam de serviços, compras ou que realizem qualquer tipo de transação em meio eletrônico.

A Lei Geral de Proteção de Dados (LGPD), em seu art. 2º, especifica os fundamentos a serem observados para a proteção dados, quais sejam:

> *"Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:*
> *I - o respeito à privacidade;*
> *II - a autodeterminação informativa;*
> *III - a liberdade de expressão, de informação, de comunicação e de opinião;*
> *IV - a inviolabilidade da intimidade, da honra e da imagem;*
> *V - o desenvolvimento econômico e tecnológico e a inovação;*
> *VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e*
> *VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."*

Outrossim, estabelece princípios a serem observados no tratamento de dados:

> *"Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:*
> *I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - 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;

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

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

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

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

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

Diante disso, percebe que é essencial averiguar se as empresas com as quais você mantém vínculos estão agindo de acordo com os princípios norteados pela Lei Geral de Proteção de Dados (LGPD), sempre aprimorando as práticas e ações visam assegurar o correto desenvolvimento dos procedimentos já adotados.

Para além disso, a fim de se avaliar a conformidade com a LGPD, verifica-se a necessidade de mudança de cultura, conforme bem assinalado abaixo:

> *"**Para o devido processo de conformidade à Lei Geral de Proteção de Dados, é necessário que haja, não apenas, a implementação de um sistema de governança de dados na empresa, mas também, a mudança de cultura**. Questão interessante pode ser posta da seguinte maneira: de que adiantaria haver um sistema eletrônico completamente de acordo à LGPD, se o funcionário, ao sair de seu posto de trabalho, não bloqueia a tela inicial do computador, deixando-o aberta para qualquer um ter acesso? Vale ressaltar, porém, que essa mudança não se restringe aos funcionários. Deve abranger todo o ambiente empresarial." (Grifo nosso) (DeServ Tecnologia e Serviços et al., 2024, posição 94 do Kindle)*

É interessante que as companhias tenham um setor, ou colaboradores treinados que estejam alinhados com a Lei Geral de Proteção de Dados (LGPD), no intuito de fortalecer o compromisso de transparência e segurança de seus usuários.

Além de estar em conformidade com a lei, deve-se identificar possíveis riscos à segurança, de modo a antecipar as ações cabíveis aos ataques ou vazamento de dados.

Desse modo, é necessário que seja implementada, como parte da análise de risco, a avaliação de risco. De acordo com Donda a avaliação de risco "é um método de identificar vulnerabilidades e ameaças para avaliar os possíveis impactos e determinar como implementar controles de segurança" (DONDA, 2020, pág. 83 do Kindle).

Nessa perspectiva, a Lei Geral de Proteção de Dados (LGPD) não se trata apenas de uma implementação para evitar multas ou penalidades. Mas sim, um conjunto de ações que visam garantir um ambiente seguro e adequado a todos.

O presente estudo tem como objetivo analisar a Lei Geral de Proteção de Dados (LGPD) e os cuidados necessários que os usuários devem

adotar. Assim, a seguir serão apresentadas algumas das estratégias para a prevenção de dados pessoais.

2.6.1 Como proteger informações e dados pessoais com o uso de credenciais de acesso

Na atualidade, o avanço tecnológico caminha de forma extremamente ágil e, na mesma velocidade, aumentam as ameaças cibernéticas, as quais se dão cada vez mais sofisticadas.

A proteção de dados e de informações têm se tornado prioridade para empresas e clientes. Dessa forma, é fundamental a proteção e o uso adequado de credencias de acesso, senhas chaves de segurança, bem como outros meios de barreiras contra invasão e roubo de dados sensíveis.

Donda aborda em sua obra, inclusive, a importância de políticas de senhas e afirmar que:

> *"Apesar de existirem muitos mecanismos novos que podem ser usados para autenticação, como biometria ou tokens, ainda dependemos quase sempre de senhas definidas por usuários, que muitas vezes são criadas de maneira insegura, permitindo que pessoas mal-intencionadas possam identificar ou quebrar essas senhas muito facilmente. Há também o fato de que muitos usuários possuem a mesma senha para diversos recursos, o que também oferece grande risco ao ambiente corporativo." (DONDA, 2020, pág. 63 do Kindle)*

A seguir, encontram-se relacionadas algumas formas de proteger informações e dados pessoais com o uso de credencias de acesso:

- Quando disponível, ative a autenticação em dois fatores no seu dispositivo;
- Não disponibilize sua senha para terceiros;

- Evite escrever sua senha em locais públicos, ou que propiciem um fácil acesso como por exemplo, em papéis ou arquivos desprotegidos no seu dispositivo;
- Evite digitar senhas em locais com muitas pessoas em volta, principalmente se o meio de digitação for um teclado físico. Tenha certeza de que não está sendo observado ao digitar sua senha;
- Ao usar equipamentos compartilhados, prefira usar a guias ou abas anônimas para acessar sites que queiram o uso de senhas, ou se certifique de encerrar sua sessão (*logout*[1]) após usar o site;
- Não utilize dados pessoais ou sequências numéricas de teclado como senhas. O ideal de uma senha considerada forte envolve o uso de letras maiúsculas e minúsculas, números, caracteres especiais e ter pelo menos 10 (dez) dígitos;
- Utilize senhas diferentes para cadastros e acessos aos sistemas;
- Renove suas senas periodicamente;
- Altere sua senha caso desconfie que ela foi descoberta, vazada ou usada em dispositivos invadidos ou infectados;
- Atente-se para usar conexões seguras (https) ao acessar um site, ou quando for necessário fornecer credenciais de acesso.

2.6.2 Protegendo seus aplicativos e sistemas operacionais

Vive-se um momento em que a tecnologia se integra cada vez mais ao dia a dia da sociedade, o que traz uma preocupação constante para a proteção de aplicativos e sistemas operacionais, a fim de se evitar o roubo de informações pessoas e, até mesmo, o comprometimento de redes inteiras.

---

[1] *Logout é o processo de finalizar o acesso a um sistema ou serviço online. Tem como objetivos principais garantir a privacidade e a segurança do usuário, além de otimizar o uso dos recursos do sistema, como memória, processamento e armazenamento. <https://www.dic.app.br/2003/01/logout.html>*

Como destaca o relatório da Kaspersky, sistemas operacionais são alvos reiterados de *malwares*[2], pois "os cibercriminosos continuam a explorar vulnerabilidades para comprometer a segurança das plataformas e obter acesso não autorizado" (Kaspersky, 2024).

Dessa forma, meios de garantir a segurança são imprescindíveis, de modo que a adoção de boas práticas é premente, seja com a atualização de *softwares* de forma regular, pelo uso de antivírus e *firewalls*[3], ou mesmo de uma configuração adequada dos sistemas operacionais, a fim de se mitigar riscos.

Em sua obra Donda enfatiza que:

> *"é importante manter um antivírus ativo e atualizado. Em estações com Windows, é possível utilizar o software antivírus integrado ao Windows 10 chamado Windows Defender, que oferece proteção em tempo real contra ameaças de softwares (...)." (DONDA, 2020, pág. 62 do Kindle)*

Diante do exposto, propõe-se, a seguir, algumas sugestões de como se proteger utilizando aplicativos e sistemas operacionais:

- Atualize constantemente seus aplicativos e sistemas operacionais;
- Não abra links recebidos aleatoriamente de desconhecidos;
- Desconfie de *links*[4] desconexos encaminhados por pessoas próximas, e na dúvida, pergunte do que se trata;
- Ao instalar um novo aplicativo, busque por fontes seguras como as lojas oficiais. Leia a avaliação de outros usuários e busque pelo aplicativo com a melhor avaliação;
- Use apenas programas e sistemas operacionais originais.

2.6.3 **Prevenção contra *malware***

---

[2]

[3] *Firewalls são programas de software ou dispositivos de hardware que filtram e examinam as informações provenientes da sua conexão com a Internet. < https://www.mcafee.com/pt-br/antivirus/firewall.html>*

[4] *Link é um canal de direcionamento para um site na internet. < https://definicao.net/link-significado/>*

Em sendo a conectividade uma realidade da atualidade, é crescente a ocorrência de ameaças de *softwares*[5] maliciosos que podem causar danos a dispositivos e redes, podendo comprometer a integridades de sistemas e, com isso, gerar prejuízos financeiros e operacionais.

Conforme destacado em relatório da Kaspersky, em 2023, "mais de 400 mil arquivos maliciosos foram detectados diariamente, evidenciando a crescente sofisticação dos ciberataques" (Kaspersky, 2024).

Diante disso, torna-se necessário implementar formas de proteção a dados sensíveis, de forma a evitar a interrupção nas operações.

Nesse sentindo, buscou-se relacionar alguns exemplos de como se prevenir contra *malware*[6], conforme a seguir:

- Mantenha seu antivírus atualizado sempre que estiver conectado à internet;
- Crie o hábito de fazer varreduras periódicas completas nos seus sistemas operacionais;
- Desabilite a função de reprodução automática de dispositivos removíveis.

2.6.4 Uso de correio eletrônico

O uso de correio eletrônico se tornou essencial, é comum para que se faça qualquer acesso no meio eletrônico a exigência de informar o e-mail, para cadastro inicial, para troca de dados e informações, exigindo que sejam observadas formas de garantir a proteção de dados pessoais e privacidade, em

---

[5] *Softwares são programas, dados e instruções que comandam o funcionamento de um computador, smartphone, tablet e outros dispositivos eletrônicos. < https://www.significados.com.br/software/>*

[6] *Malware ou software mal-intencionado é todo e qualquer programa ou arquivo que seja prejudicial a um usuário de computador. < https://juristas.com.br/foruns/topic/definicao-de-malware-software-malicioso/>*

conformidade com os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD).

A não observância a tais princípios, cautelas necessárias, pode levar ao compartilhamento não autorizado de informações pessoais e, consequentemente, graves prejuízos às partes envolvidas.

Vale destacar que:

> *"Com o avanço da tecnologia, os cibercrimes estão cada vez mais constantes e sofisticados – causando prejuízos não apenas a empresas, como também a pessoas físicas.* ***Grande parte desses ataques são feitos por meio de e-mails, que são a maior porta de entrada para os cibercriminosos****.*
>
> *Segundo um estudo conduzido pela consultoria alemã Roland Berger, o Brasil tem sido um dos principais alvos globais desse tipo de crime. O levantamento aponta que, apenas no primeiro semestre de 2022, o país já ultrapassou o número de ataques ocorridos no ano passado: foram 9,1 milhões de ocorrências no período. Com esse resultado, o Brasil está em quinto lugar em ranking de cibercrimes – atrás de Estados Unidos, Reino Unido, Alemanha e África do Sul.*
>
> *Neste cenário, o e-mail segue como a maior porta de entrada para os cibercriminosos – que costumam atacar com alguma espécie de malware ou ransomwares.* ***Assim, eles conseguem acesso a dados bancários ou pessoais, bitcoins e até "sequestram" essas informações em troca de pagamentos.****" (Grifo nosso) (NETSAFE, 2023)*

Assim, deve o correio eletrônico ser utilizado de forma a garantir sua proteção e em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Pela visão do usuário, buscou-se destacar dois dos cuidados a serem observados no uso de correio eletrônico de forma regular, destacados abaixo:

- Verifique a procedência de todos os e-mails recebidos. Observe atentamente o cabeçalho e o conteúdo da mensagem. Em caso de dúvida, não clique em nenhum link ou anexo. Desconfie sempre!
- Caso desconfie de alguma mensagem, consulte o Catálogo de Fraudes da Rede Nacional de Pesquisa (https://catalogodefraudes.rnp.br/) que tem como objetivo conscientizar a comunidade sobre os principais golpes que estão em circulação na internet, identificando e divulgando fraudes reportadas pela comunidade ou coletadas por seus sensores.

3. Considerações finais

Conforme a definição dada pela Lei de Geral de Proteção de Dados – LGPD, os dados pessoais abarcam informações relacionadas a pessoas naturais identificadas ou identificáveis, englobando várias informações, como nomes, CPFs, e-mails, endereços, históricos de compras entre outros. Por sua natureza, esses dados exigem uma proteção mais rigorosa durante seu tratamento.

A Lei de Geral de Proteção de Dados – LGPD trata como dados sensíveis certas informações, mais delicadas, a exemplo da origem racial, convicção religiosa, opinião política entre outras informações para as quais se exige uma proteção adicional devido ao elevado risco de discriminação e demais violações dos direitos individuais.

As bases legais estabelecidas pela LGPD para o tratamento de dados pessoais são bastante claras e incluem o consentimento do titular, o cumprimento de obrigações legais, uso para fins de pesquisa, execução de contratos e a proteção da vida, saúde, crédito, entre outros. Tais bases, tem por objetivo o equilíbrio entre a necessidade de proteger os direitos dos titulares de dados com as necessidades legítimas das organizações.

É importantíssimo que as empresas compreendam e adotem essas bases legais trazidas pela LGPD, no qual garantem de forma ética e legal o tratamento dos dados.

Para tanto, a implementação requer práticas de proteção de dados, com a correta obtenção de consentimento levando em consideração os interesses legítimos conforme os requisitos contratuais.

Reforçando o que foi dito no curso deste trabalho, conclui-se que LGPD não serve só para evitar penalidades ou multas, mas para promover confiabilidade nos negócios e estabelecer vínculos de confiança com os clientes.

É crucial que as empresas invistam em profissionais especializados em proteção de dados, que possam localizar dados disponíveis, identificar riscos na segurança e promover a implementação de medidas afim de repelir ataques ou o uso indevido dos dados.

No âmbito das organizações, apresenta-se imprescindível a adoção de políticas de proteção de dados, capazes de responder a possíveis ameaças. Assim, faz-se necessário que invistam em tecnologias de segurança, a exemplo de criptografia e sistemas de detecção de intrusões. Tais providências auxiliam para que não sejam vazados dados sensíveis dos clientes.

Por fim, se faz necessário criar um ambiente digital que forneça a devida proteção de dados. A colaboração e a adoção de medidas de segurança por parte dos usuários é a complementação ideal, na qual torna seguro tanto o fornecimento quanto o tratamento dos dados.

Referências

BRASIL. **Lei nº 13.709, de 4 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 set. 2024.

DICAS de Segurança da Informação e Proteção de Dados Pessoais. Instituto Federal do Sudeste de Minas Gerais. Disponível em: https://www.ifsudestemg.edu.br/hotsites/processo-seletivo-2024-1/capa/index.html/acessoainformacao/protecao-de-dados-pessoais-no-if-sudeste-mg/dicas. Acesso em: 31 ago. 2024.

Lei Geral de Proteção de Dados. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd. Acesso em: 29 ago. 2024.

OUVIDORIA ANPD. **Autoridade Nacional de Proteção de Dados.** Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/ouvidoria. Acesso em: 02 set. 2024.

Dados do Consumidor. Disponível em: https://valor.globo.com/legislacao/noticia/2020/02/27/20f1f083-destaques.ghtml. Acesso em: 09 ago. 2024.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** 4. ed. São Paulo: Saraiva, 2024. E-book Kindle.

DONDA, Daniel. **Guia prático de implementação da LGPD.** 1. ed. São Paulo: Labrador, 2020. E-book Kindle.

D'ÁVILA, Ana Viória Germani; SILVA, Bruna Fabiane da; ARAÚJO, Thiago Volpi de. **LGPD: muito além da lei (atualizado): uma análise do direito em conjunto com a segurança da informação.** São Paulo: [Editora], 2020. E-book Kindle.

DALVI, Afonso Henrique Figueiredo; DALVI, Afonso. **Guia prático LGPD & Compliance Digital: referências, conceitos, estratégias e ações de segurança cibernética.** São Paulo: Labrador, 2020. E-book Kindle.

DeSERV TECNOLOGIA E SERVIÇOS; SILVA, Bruna Fabiane da; ARAÚJO, Thiago Volpi; D'ÁVILA, Ana Vitória Germani; PEREIRA, Thiago Guedes. **LGPD: muito além (atualizado): uma análise do direito em conjunto com a segurança da informação.** 2024. E-book Kindle.

CAZEIRO, Leandro. **Novas regras da LGPD para pequenas empresas.** Disponível em: TANGERINO https://tangerino.com.br/blog/novas-regras-da-lgpd/. Acesso em: 09 out. 2024.

ANPD. **Resolução CD/ANPD nº 2/2022.** Disponível em: Conjur https://www.conjur.com.br/2022-jan-28/anpd-regulamenta-aplicacao-lgpd-empresas-pequeno-porte/. Acesso em: 09 out. 2024.

ANPD - Autoridade Nacional de Proteção de Dados. **Guia orientativo: hipóteses legais de tratamento de dados pessoais - legítimo interesse.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 21 out. 2024.

LIMA, Cíntia Rosa Pereira de (Coord.). **ANPD e LGPD: desafios e perspectivas.** São Paulo: Almedina, 2021. E-book Kindle.

KASPERSKY. **Mais de 400 mil malware foram descobertos por dia em 2023.** Disponível em: https://www.kaspersky.com.br/about/press-releases/kaspersky-mais-de-400-mil-malware-foram-descobertos-por-dia-em-2023. Acesso em: 09 out. 2024.

NETSAFE. **Você sabia que o e-mail é a maior porta de entrada para os cibercriminosos?** Disponível em: https://netsafecorp.com.br/voce-sabia-que-o-e-mail-e-a-maior-porta-de-entrada-para-os-cibercriminosos/. Acesso em: 09 out. 2024.