Unisanta Science and Technology, **2022, August**
Published Online 2022 Vol. 11 nº2 http://periodicos.unisanta.br/index.php/sat

UNISANTA
Science and Technology
ISSN 2317-1316

A importância da Lei Geral de Proteção de Dados no contexto da privacidade de dados das pessoas físicas

Luiz Antonio Ferraro Mathias, Antonio Carlos Marques do Amaral Guerra, Ana Carolina Caetano Senger, José Avelino dos Santos Moura, Fernando José Cesílio Branquinho, Marcos Antonio Santos de Jesus, Fernando Augusto dos Santos Ribeiro.

UNISANTA– Universidade Santa Cecília – Faculdade de Ciências Exatas, Engenharia e Arquitetura – Bacharelado em Sistemas de Informação e Tecnólogo em Análise e Desenvolvimento de Sistemas
Rua Oswaldo Cruz, 277 - Santos-SP, Brasil - CEP: 11045-907

E-mail*:* lmathias@unisanta.br
Received June, 2022

Resumo: O presente artigo científico versa sobre a importância e a aplicabilidade da Lei Geral de Proteção de Dados - GPD, para proteção dos dados pessoais de pessoas naturais (físicas) cujo tratamento se dê em qualquer parte do território nacional. A proteção aos dados pessoais é tema muito discutido na atualidade e abarca desde direitos fundamentais como a proteção à intimidade e à vida privada, até ao seu entendimento de um direito autônomo enfrentando questões inéditas acerca de seu uso, decorrentes da introdução de novas tecnologias e da internet, além da mudança de paradigmas nas relações sociais e na economia. A exposição acentuada das pessoas usuárias nas redes sociais, na internet, bem como, o aumento exponencial da produção de dados possibilita que as organizações façam uso dessas informações das mais distintas formas. À medida que as violações dos dados pessoais das pessoas crescem na sociedade, principalmente no ambiente virtual, surge a necessidade de proteção jurídica. Neste contexto, a Lei 13.709/2018 (LGPD), veio como um grande avanço na regulamentação sobre o tratamento de dados pessoais no Brasil, com o objetivo de tutelar os direitos de personalidade, que decorre da dignidade da pessoa humana, consagrados pela Constituição Federal. Sancionada em 14 de agosto de 2018, a LGPD entrou em vigor em agosto de 2020 e afetou a maioria das empresas brasileiras, onde tem como principal objetivo, a proteção dos direitos fundamentais de liberdade e de privacidade e a permissão do livre desenvolvimento da personalidade da pessoa natural.

Palavras-chave: Lei de Proteção de Dados; privacidade; Internet.

The importance of the General Data Protection Law in the context of the privacy of individuals

Abstract: This scientific article deals with the importance and applicability of the General Data Protection Law - GPD, to protect the personal data of natural persons (individuals) whose processing takes place in any part of the national territory. The protection of personal data is a much-discussed topic today and ranges from fundamental rights such as the protection of intimacy and private life, to the understanding of an autonomous right facing unprecedented questions regarding its use, arising from the introduction of new technologies and the internet, in addition to changing paradigms in social relations and the economy. The accentuated exposure of users on social networks, the internet, as well as the exponential increase in data production allows organizations to make use of this information in the most different ways. As violations of people's personal data increase in society, especially in the virtual environment, the need for legal protection arises. In this context, Law 13,709/2018 (LGPD) came as a major advance in the regulation of the processing of personal data in Brazil, with the aim of protecting personality rights, which derive from the dignity of the human person, enshrined in the Federal Constitution. Sanctioned on August 14, 2018, the LGPD came into force in August 2020

Copyright © 2022 ISESC

and affected most Brazilian companies, where its main objective is the protection of fundamental rights to freedom and privacy and the permission of free development of the personality of the natural person.

Keywords: Data Protection Law; privacy; Internet.

1. Introdução

O mundo digital é uma realidade na atualidade, ficando praticamente impossível viver sem a internet, e atividades que antes eram costumeiras como ir ao banco, não se faz mais necessária, pois o aplicativo no smartphone ou computador leva o banco à pessoa; com isso os dados da pessoa como senhas, transações bancárias ficam nesse mundo digitalizado, e golpes são realizados, chamados também como crimes cibernéticos; dizer sobre essa "Era Tecnológica", serve também para designar os avanços tecnológicos advindos da Terceira Revolução Industrial, refletindo na difusão de um ciberespaço, claramente trouxe consigo a amplitude da capacidade do armazenamento e memorização de informações, dados e formas de conhecimentos. (NASCIMENTO, 2016).

Pelo exposto, é de extrema importância que os dados sejam tratados da maneira correta, por isso o objetivo geral deste trabalho de pesquisa é expor a importância e a aplicabilidade da Lei Geral de Proteção de Dados - LGPD, analisar as legislações que visam a proteção de dados pessoais, identificar as possíveis violações aos direitos dos usuários, entender como os dados pessoais são tratados e quais as penalizações pelo tratamento incorreto, analisar como uma empresa busca garantir a integridade dos dados pessoais.

Para tal proteção, a LGPD submete a coleta e tratamento, ou seja, processamento, armazenamento e compartilhamento de dados do consumidor por controladores da pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados e operadores que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, a observância de vários princípios, dentre os quais necessidade, adequação, finalidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, seguindo sob as hipóteses do consentimento do titular e legítimo interesse da empresa.

Esta Lei representa o primeiro regulamento geral sobre proteção de dados pessoais no Brasil, onde o tema era tratado apenas por leis específicas, como o Código Brasileiro de Defesa do Consumidor (Lei 8.078/1990) e a Lei Brasileira da Internet (Lei 12.965/2014).

2 Desenvolvimento

2.1 Aspectos da proteção de dados

Estima-se que 4,1 bilhões de pessoas tenham acesso à internet no mundo e que 3,4 bilhões mantenham uma rede social (CIRIACO, 2018). Logo, grande parte da população tem suas informações na rede mundial. E todo esse banco de dados disponível na rede é utilizado pelas empresas (dada a facilidade de acesso). A facilidade com que podem e cada vez mais poderão ser obtidas informações pessoais lança, porém, uma sombra sobre a privacidade, capaz de gerar, como potencial consequência, a diminuição da esfera de liberdade do ser humano.

A concepção da proteção dos dados pessoais e sensíveis como um direito humano fundamental vem ganhando projeção no cenário jurídico. A preocupação em torno dos dados tem aumentado consideravelmente em decorrência do avanço tecnológico observado nas últimas décadas (MAGALHÃES E OLIVEIRA, 2021).

A disponibilização, o tratamento e a combinação de informações tornam-se cada vez mais intensos, a ponto de resultar em uma sociedade gradativamente orientada por dados. Na atualidade, as questões envolvendo violação da privacidade, da intimidade e dos dados são progressivamente presentes (PALETTA, 2020).

O direito à privacidade é constituído como direito fundamental conforme previsto no Artigo 5°, incisos X, XI e XII da Constituição Federal de 1988.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Copyright © 2022 ISESC

A privacidade está aliada ao princípio da exclusividade, onde ocorrer uma disposição de informações entres as partes, da qual estas não pode ser repassada sem consentimento, a terceiros. Sendo umas das primeiras leis, no Brasil, a prever mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados foi assim observado, na Lei nº 7.232, de 1984, que dispõe sobre a Política Nacional da Informação (DONEDA, 2019).

2.2 Características da LGPD

A LGPD oferece aos indivíduos maior controle sobre seus dados pessoais, garantindo maior transparência sobre a utilização dos dados e exige maior segurança e controles de proteção de dados. Tal Lei foi inspirada na Regulamento Geral de Proteção de Dados – GDPR (*General Data Protection Regulation*) europeu, que é geralmente visto internacionalmente como um modelo em questões de privacidade.

Esta lei impõe novas regras às empresas, ao poder público, às organizações sem fins lucrativos e outras organizações que (i) executam operações de processamento de dados em território brasileiro; (ii) oferecem bens e serviços às pessoas em território brasileiro ou que coletam e analisam dados relacionados às pessoas em território brasileiro; ou (iii) processam dados pessoais coletados em território brasileiro.

As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios, prevalecendo, portanto, sobre quaisquer outras leis municipais ou estaduais.

Os dados pessoais referem-se a qualquer informação relacionada a uma pessoa física identificada ou identificável. Isso inclui informações que, isoladamente ou em conjunto com outras, são capazes de identificar uma pessoa específica. Alguns exemplos de dados pessoais são:

a) Dados de identificação: Nome, sobrenome, número de identificação (como RG ou CPF), data de nascimento, entre outros.
b) Dados de contato: Endereço residencial, endereço de e-mail, número de telefone etc.
c) Dados sensíveis: Informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos, informações genéticas, dados biométricos, saúde, vida sexual, orientação sexual etc.
d) Dados de localização: Dados que identificam a localização geográfica de uma pessoa, como coordenadas GPS, endereço IP etc.
e) Dados de comportamento: Informações sobre hábitos de consumo, preferências, histórico de navegação na internet, interações em redes sociais, entre outros.

2.3 Pilares da LGPD

Os pilares da LGPD são os princípios e diretrizes fundamentais que orientam o tratamento de dados pessoais no Brasil. Esses pilares são essenciais para garantir a privacidade, transparência e segurança das informações pessoais dos cidadãos. São eles:

a) A regulamentação de qualquer operação executada com "dados pessoais", como aquisição, armazenamento, uso e compartilhamento de dados pessoais. Dados pessoais têm uma definição muito ampla na LGPD: qualquer dado que se refira a uma pessoa física identificada ou identificável;
b) Uma pessoa natural é identificável quando "*possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular*.".
c) Os indivíduos têm o direito de saber se uma organização está processando seus dados pessoais e de compreender o motivo deste processamento, assim como têm o direito de ter seus dados excluídos ou corrigidos, de pedir que não sejam mais processados, de recusar mala direta, e de revogar o consentimento de determinados usos dos seus dados. O direito à portabilidade de dados fornece aos indivíduos o direito de mover seus dados para outro lugar e de receber ajuda para fazê-lo;
d) Há exigência de que as organizações protejam dados pessoais de acordo com sua sensibilidade. No caso de violação de dados, controladores de dados, geralmente, devem notificar a autoridade correta dentro de um prazo razoável. Além disso, se a violação puder resultar em grandes riscos aos direitos e liberdade de indivíduos, as organizações também deverão notificar os indivíduos assim que possível;
e) É preciso que haja uma base legal para o processamento de dados pessoais. Nos casos em que o consentimento seja esta base legal, ele deve ser "*fornecido de forma voluntária, consciente e não ambígua para propósitos específicos*". Há exigências específicas da LGPD para o consentimento com a finalidade de proteger crianças;
f) As organizações devem executar avaliações sobre o impacto da proteção de dados, por exigência da Agência Nacional de Proteção de Dados (ANPD), para prever os impactos de privacidade dos projetos e aplicar medidas corretivas quando preciso. Registros de atividades de processamento, consentimentos para processar dados e conformidade com a LGPD devem ser mantidos;

Copyright © 2022 ISESC

g) A conformidade com a LGPD não é uma atividade pontual, mas sim um processo contínuo. A não conformidade com a LGPD pode resultar em elevadas sanções administrativas e multas. Para garantir a conformidade com a LGPD, as organizações devem ser encorajadas a abraçar a cultura da privacidade para proteger os interesses dos indivíduos em seus dados pessoais.

2.4 Aplicabilidade da LGPD

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, excetuando-se aquelas cujos dados pessoais foram provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei;
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
iii. Os dados pessoais objeto do tratamento, tenham sido coletados no território nacional (cujo titular se encontre no momento da coleta).

2.5 Não aplicabilidade da LGPD

Esta Lei não se aplica às hipóteses de tratamento de dados:

i. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
ii. Realizado para fins exclusivamente: jornalístico e artísticos; ou acadêmicos (para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais);
iii. Realizado para fins exclusivos de (e regido com base em legislação específica que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular, bem como opiniões técnicas ou recomendações da ANPD): segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais.

2.6 Princípios do tratamento de dados

A LGPD traz em seu rol, princípios como publicidade, finalidade, exatidão, livre acesso e segurança física e lógica. Esses princípios são comumente vistos em legislações de proteção de dados pessoais, e em ordenamentos jurídicos de vários graus. Esses estão disseminados, mas podem ser encontrados em variadas normativas, também são centro de pautas e questionamentos, no qual os ordenamentos jurídicos buscam para solucionar e garantir a eficácia da proteção de dados pessoais (DONEDA, 2019).

Neste contexto, as atividades de tratamento de dados pessoais, segundo a LGPD, deverão observar a boa-fé e os seguintes princípios:

Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

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

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;

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.

O rol de princípios citado deve ser seguido para que haja controle dos dados, logo estará em conformidade com

Copyright © 2022 ISESC

a LGPD, caso não esteja em conformidade, logo também, não atenderá aos princípios redigidos em lei. Vale ressaltar que um dos pontos essenciais para aplicação do tratamento de dados é o consentimento do titular.

2.7 O tratamento de dados pessoais

É importante destacar que a LGPD estabelece regras específicas para o tratamento de dados pessoais, exigindo o consentimento do titular para a coleta e o uso dessas informações, além de garantir direitos aos titulares, como o acesso aos seus dados, a correção de informações incorretas e a exclusão de dados desnecessários ou que não estejam em conformidade com a lei.

Além dos dados pessoais, a LGPD também trata dos dados anonimizados, que são aqueles que não permitem a identificação direta ou indireta do titular, e dos dados pseudonimizados (processados de forma a substituir elementos de identificação direta por um identificador alternativo, chamado de pseudônimo), que são dados que passaram por um processo técnico que impossibilita a identificação direta do titular sem o uso de informações adicionais.

Portanto, a LGPD busca proteger não apenas os dados pessoais diretamente identificáveis, mas também promover uma gestão responsável e ética de todas as informações que possam impactar a privacidade e os direitos das pessoas. Neste sentido, a Lei estabelece que o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

i. Mediante o fornecimento de consentimento pelo titular;
ii. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
iii. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições em capítulo específico da LGPD;
iv. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
v. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
vi. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
vii. Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
viii. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
ix. Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
x. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

2.8 O consentimento para tratamento de dados

No contexto da Lei Geral de Proteção de Dados (LGPD), o consentimento refere-se a uma das bases legais que legitimam o tratamento de dados pessoais. O consentimento é uma manifestação livre, informada e inequívoca do titular dos dados, por meio da qual ele concorda com o tratamento de suas informações pessoais para uma finalidade específica. O consentimento é fundamental porque garante que o titular tenha controle sobre seus dados e possa decidir de forma consciente se deseja ou não autorizar o uso de suas informações por parte da empresa ou organização. Além disso, o consentimento deve ser obtido de forma clara, transparente e fácil de entender, sem qualquer tipo de coerção ou pressão sobre o titular. Alguns aspectos importantes sobre o consentimento na LGPD incluem:

a) Manifestação livre: o consentimento deve ser dado de forma voluntária, sem qualquer forma de coação, ameaça ou indução por parte da empresa. O titular deve ter liberdade para decidir se deseja ou não consentir com o tratamento de seus dados;
b) Informação clara e transparente: antes de obter o consentimento, a empresa deve fornecer informações claras e transparentes sobre o tratamento de dados que será realizado, incluindo a finalidade, a forma de uso, os responsáveis pelo tratamento, os direitos do titular, entre outras informações relevantes;
c) Consentimento específico: o consentimento deve ser específico para cada finalidade de tratamento de dados. Isso significa que a empresa não pode utilizar o consentimento dado para uma finalidade para justificar o tratamento de dados para outra finalidade diferente daquela para a qual o consentimento foi obtido;
d) Revogação do consentimento: o titular dos dados tem o direito de revogar seu consentimento a qualquer momento, de forma fácil e acessível. Após a revogação do consentimento, a empresa deve interromper o tratamento dos dados para a finalidade consentida, salvo se houver outra base legal que justifique o tratamento;
e) Registro do consentimento: a empresa deve manter registros adequados que demonstrem que o consentimento foi obtido de acordo com as exigências da

Copyright © 2022 ISESC

LGPD, incluindo informações sobre como o consentimento foi obtido, a data, a finalidade, entre outros detalhes;

f) Em resumo, o consentimento no contexto da LGPD é um elemento crucial para garantir a proteção da privacidade e dos direitos dos titulares de dados, assegurando que o tratamento das informações pessoais seja realizado de forma ética, transparente e respeitando a vontade dos indivíduos.

Na hipótese em que o consentimento é requerido, esse 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;

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

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos (confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados etc.). Neste caso, o controlador deve informar claramente ao titular sobre os produtos e serviços a que ele deixará de ter acesso caso não forneça o consentimento. Dessa forma, garante-se a plena ciência do titular e seu discernimento sobre aceitar ou não o tratamento de seus dados para os fins propostos.

2.9 O tratamento de dados pessoais sensíveis

No contexto da LGPD, dados pessoais "sensíveis" são categorias especiais de informações que requerem um cuidado adicional no seu tratamento devido ao seu potencial de causar danos ou discriminação ao titular dos dados. Esses dados são considerados mais sensíveis por revelarem aspectos íntimos da vida de uma pessoa. A Lei os define como aqueles referentes a:

Origem racial ou étnica: dados que revelam a raça ou etnia de uma pessoa, como cor da pele, ascendência, nacionalidade etc.

Convicções religiosas ou filosóficas: informações relacionadas às crenças religiosas, filosóficas ou morais de um indivíduo, incluindo filiação a grupos religiosos.

Opiniões políticas: dados que indicam as opiniões políticas, ideológicas ou partidárias de uma pessoa.

Filiação sindical: informações sobre a afiliação a sindicatos ou associações profissionais.

Dados genéticos: informações relacionadas ao DNA, características genéticas e predisposições genéticas de uma pessoa.

Dados biométricos: dados físicos, fisiológicos ou comportamentais que podem ser usados para identificar uma pessoa de maneira única, como impressões digitais, reconhecimento facial, entre outros.

Dados de saúde: informações sobre a saúde física ou mental de uma pessoa, incluindo histórico médico, tratamentos realizados, exames clínicos, entre outros.

Vida sexual: dados relacionados à vida sexual de uma pessoa, como orientação sexual, histórico de relacionamentos, entre outros.

O tratamento dessas categorias de dados sensíveis exige um cuidado maior por parte das organizações e empresas que os coletam, armazenam ou utilizam. A LGPD estabelece que o tratamento de dados pessoais sensíveis só pode ocorrer nas seguintes situações:

i. Com o consentimento específico e destacado do titular;
ii. Para o cumprimento de obrigações legais ou regulatórias pelo controlador;
iii. Em caso de proteção da vida ou da incolumidade física do titular ou de terceiros;
iv. Para a tutela da saúde, em procedimento realizado por profissionais da saúde ou por entidades sanitárias;
v. Quando necessário para a execução de políticas públicas pelo poder público;
vi. Para fins de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
vii. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Essas medidas visam proteger a privacidade e a integridade dos titulares dessas informações, assegurando que o tratamento dos dados pessoais sensíveis seja realizado de maneira ética, transparente e respeitando os direitos e garantias previstos na LGPD.

2.10 Término do tratamento de dados

O direito ao apagamento dos dados, também conhecido como “direito ao esquecimento” ou “direito a ser esquecido”, previsto no artigo 17 do LGPD, consiste no direito que o titular tem de obter do responsável pelo tratamento o apagamento dos seus dados pessoais em algumas situações, entre elas, quando deixarem de ser necessários para a finalidade que motivou o seu recolhimento, quando o consentimento para o tratamento for retirado ou, ainda, quando os dados forem tratados ilicitamente (VILELA E LAIA, 2021).

Copyright © 2022 ISESC

De acordo com a LGPD, o término do Tratamento de dados pessoais ocorrerá nas seguintes hipóteses: verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; fim do período de tratamento; comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou determinação da ANPD, quando houver violação ao disposto nesta Lei.

Diante das situaçoes expostas, os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;
b) Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
c) Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos da LGPD; Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (para fins estatísticos, por exemplo).

2.11 Direitos dos titulares dos dados pessoais

Assim, uma vez identificado o titular dos dados pessoais, o artigo 18 da LGPD estabelece um rol de direitos a serem exercidos, a qualquer momento e mediante requisição, em face do controlador. Nessa perspectiva, o titular dos dados pessoais tem direito à confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a anonimato, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e a revogação do consentimento (SANTOS, 2021).

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da LGPD (não importa o que seja pedido no consentimento ou qual seja o tratamento; dados pessoais são individuais e intransferíveis e sempre pertencerão à pessoa a que se referem).

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

i. confirmação da existência de tratamento;
ii. acesso aos dados;
iii. correção de dados incompletos, inexatos ou desatualizados;
iv. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
v. portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD, observados os segredos comercial e industrial;
vi. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas na LGPD;
vii. informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
viii. informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
ix. revogação do consentimento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

O titular dos dados pessoais tem o direito, ainda, de peticionar em relação aos seus dados contra o controlador perante a ANPD, bem como opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

2.12 Os agentes de tratamento dos dados pessoais

A fim de controlar, garantir que todos os agentes de tratamento de dados estejam em conformidade e cumpram todas as normas determinadas pela LGPD, esta dispõe de uma série de ações para autuar e penalizar aqueles que cometerem infrações. As empresas, entidades e órgãos públicos que coletam dados pessoais dos seus clientes e/ou usuários tiveram de observar as disposições da Lei, sob pena de incorrer em sanções administrativas (SANTOS, 2021).

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

A ANPD poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Este

Copyright © 2022 ISESC

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

O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Complementarmente, a ANPD poderá dispor sobre padrões de interoperabilidade (capacidade de sistemas e organizações operarem entre si) para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

2.13 O papel do encarregado de dados

O Encarregado de Proteção de Dados (*Data Protection Officer* - DPO) desempenha um papel crucial no contexto da Lei Geral de Proteção de Dados (LGPD). O DPO é uma figura designada pela empresa ou organização responsável pelo tratamento de dados pessoais para garantir o cumprimento das disposições da LGPD e promover a proteção dos direitos dos titulares dos dados. Seu papel inclui diversas responsabilidades e atribuições, tais como:

Monitoramento do cumprimento da LGPD: é responsável por assegurar que a empresa esteja em conformidade com as exigências da LGPD no que diz respeito ao tratamento de dados pessoais. Isso inclui a verificação do cumprimento das normas, diretrizes e princípios estabelecidos pela Lei;

Orientação e aconselhamento: oferece orientação e aconselhamento aos colaboradores e à alta administração da empresa sobre as práticas adequadas de proteção de dados, ajudando a garantir que todas as atividades de tratamento de dados estejam em conformidade com a LGPD;

Registro de atividades de tratamento: é responsável por manter um registro das atividades de tratamento de dados realizadas pela empresa, incluindo informações sobre os tipos de dados processados, as finalidades do tratamento, as medidas de segurança adotadas, entre outros detalhes.

Atendimento aos titulares dos dados: é o ponto de contato para os titulares dos dados exercerem seus direitos previstos na LGPD, como o acesso aos seus dados, a correção de informações incorretas, a exclusão de dados desnecessários, entre outros;

Avaliação de impacto à proteção de dados: realiza avaliações de impacto à proteção de dados (Data Protection Impact Assessments - DPIA) sempre que forem realizadas atividades de tratamento de dados que possam representar um risco elevado para os direitos e liberdades dos titulares dos dados;

Treinamento e conscientização: promove a conscientização e o treinamento dos colaboradores da empresa sobre a importância da proteção de dados e as melhores práticas a serem seguidas para garantir a conformidade com a LGPD;

Relacionamento com a ANPD: atua como ponto de contato entre a empresa e a ANPD, a autoridade responsável pela aplicação da LGPD, facilitando a comunicação e a cooperação em questões relacionadas à proteção de dados.

Em resumo, o Encarregado de Proteção de Dados desempenha um papel fundamental na garantia da conformidade com a LGPD e na promoção de uma cultura de proteção de dados dentro da empresa, assegurando o respeito aos direitos dos titulares dos dados e a segurança das informações pessoais tratadas pela organização.

2.14 Boas práticas e governança

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Na aplicação dos princípios de segurança e prevenção, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

a) Implementar programa de governança em privacidade que, no mínimo:

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

Copyright © 2022 ISESC

ii. seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
iii. seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
iv. estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
v. tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
vi. esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
vii. conte com planos de resposta a incidentes e remediação; e
viii. seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

b) Demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da ANPD ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento da LGPD.

2.15 O papel da ANPD

Outra participante da relação de processamento de dados pessoais é a Autoridade Nacional Proteção de Dados (ANPD). Teixeira (2020) descreve, de acordo com a estrutura definida pelo Decreto n° 10.474/2020, que a ANPD exerce quatro funções básicas:

i. Normativa: edição de normas que regulamentem a proteção de dados pessoais;
ii. Educativa: estabelecimento de diretrizes para a adequada aplicação da lei, promovendo na população o conhecimento das normas e das políticas públicas;
iii. Fiscalizatória: zelar pela proteção de dados pessoais, fiscalizando as atividades de tratamento;
iv. Sancionatória: aplicação de sanções, na hipótese de tratamento de dados pessoais realizado em desacordo com a legislação.

A Lei, por si só, não basta como instrumento regulatório, sem que essa seja harmonicamente interpretada e tendo sua aplicação efetivada, portanto, compreende-se a fundamental existência da ANPD, para que seja fomentada a cultura de proteção de dados, pois a autoridade é um instrumento de garantia da lei (SANTI, 2020).

A criação da ANPD foi fundamental para se estabelecer vinculação entre o titular de dados ao setor privado e público. Ainda, a ANPD, tem como papel de alinhar com demais autoridades de fiscalização e regulação, e com os poderes do país, dentre outras funções que foram determinadas na LGPD (SANTI, 2020).

Também será um articulador com órgãos públicos, como os Procons, demais agências reguladoras e o Ministério Público, a fim de gerar segurança jurídica ou mesmo mitigar conflito de competências na aplicação das normas, da mesma forma articulando com os setores privados. Assim, a LGPD atribuiu à autoridade nacional, o papel de ser o órgão central para interpretação da Lei, cabendo exclusivamente a este, esclarecer qualquer ponto incontroverso (TEIXEIRA, 2020).

3. Materiais e métodos

A ANPD, conforme exposto anteriormente pode aplicar sanções em caso de descumprimento das disposições da LGPD. As sanções previstas pela LGPD podem ser aplicadas tanto a agentes de tratamento de dados (como empresas, organizações e órgãos públicos) quanto a encarregados pelo tratamento de dados, podendo incluir: advertência, multa simples, multa diária, publicização da infração: pode determinar a publicização da infração após processo administrativo, divulgando informações sobre a natureza, gravidade e consequências do descumprimento das normas de proteção de dados, bloqueio dos dados pessoais, eliminação dos dados pessoais.

As sanções aplicadas pela ANPD têm o objetivo de garantir a conformidade com a LGPD e proteger os direitos dos titulares dos dados, promovendo a segurança e a privacidade das informações pessoais tratadas pelas empresas e organizações no Brasil. Neste sentido, é importante que as empresas estejam cientes das obrigações impostas pela LGPD e adotem as medidas necessárias para garantir o cumprimento das normas de proteção de dados.

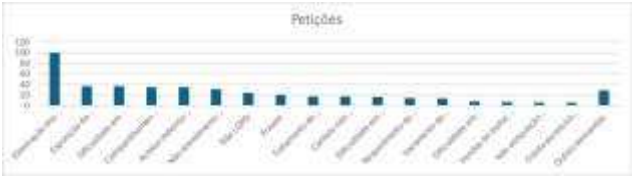
A seguir, serão apresentados os dados coletados da pesquisa. Segundo a ANPD, foram recebidos, em 2022, 1.045 requerimentos (entre denúncias e petições de titulares) e 287 comunicações de incidentes de segurança, além de terem sido instaurados 15 processos de fiscalização e 8 processos administrativos sancionadores.

Do total de requerimentos recebidos, aproximadamente 43,2% (452) foram classificados como petições de titulares (Figura 1. Todas as petições relacionam-se a solicitações de exercício dos direitos previstos nos arts. 9º, 18 ou 20 da LGPD.

Copyright © 2022 ISESC

procedimentos envolvem tanto agentes de tratamento do setor público quanto do setor privado.

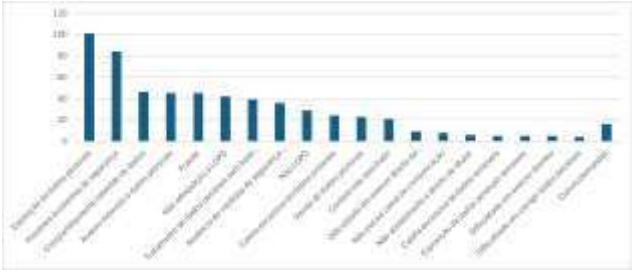
Figura 1 – Petições de titulares



Fonte: ANPD (2022).

A ANPD também recebeu denúncias de possíveis violações à LGPD. As denúncias são assim classificadas quando a violação de direitos inerentes à LGPD atinge toda uma coletividade e não necessariamente direitos individuais previstos nos art. 9º, 18 ou 20, da LGPD. Cerca de 56,8% (593) dos requerimentos recebidos foram classificados como denúncia (Figura 2). As principais denúncias versavam sobre exposição de dados pessoais e sobre tratamento e divulgação, por plataformas, de dados pessoais disponíveis publicamente e sobre possíveis incidentes de segurança com dados pessoais (vazamento de dados pessoais).

Figura 2 – Denúncias registradas



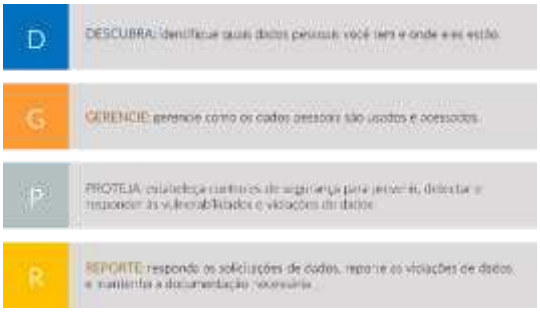
Fonte: ANPD (2022).

Além dos requerimentos recebidos e relatados na seção anterior, de janeiro a dezembro de 2022, 15 procedimentos de fiscalização foram iniciados, dos quais 6 foram concluídos. Outros 3 procedimentos iniciados em 2021 foram concluídos em 2022, totalizando, dessa forma, 9 processos encerrados. A maior parte dos procedimentos instaurados em 2022 (9 dos 15) são relativos a órgãos públicos. Outros 4 procedimentos instaurados dizem respeito a controladores privados e outros 2

4. Resultados e discussão

Em resumo, a implementação da LGPD envolve uma jornada complexa e multifacetada, que requer comprometimento, planejamento estratégico e ações coordenadas em toda a organização. É um processo contínuo de aprimoramento e adaptação às exigências regulatórias e às melhores práticas de proteção de dados pessoais. A jornada de implementação da LGPD pode ser dividida em diferentes fases (Figura 3), cada uma com suas próprias atividades e desafios.

Figura 3 – Passos rumo a conformidade com a LGPD



Fonte: O autor (2022).

5. Considerações finais

O desenvolvimento desta pesquisa permitiu constatar que a Lei Geral de Proteção de Dados (LGPD) representa um marco significativo na proteção dos direitos fundamentais das pessoas físicas em relação ao tratamento de seus dados pessoais. A importância dessa legislação não pode ser subestimada, pois ela estabelece diretrizes claras e rigorosas para o uso responsável e ético das informações pessoais, garantindo a privacidade, transparência e segurança dos dados dos cidadãos brasileiros.

Ao longo deste estudo, analisou-se os principais pilares da LGPD, destacando a necessidade de obtenção de consentimento, a transparência no tratamento de dados, a garantia de segurança das informações, o respeito aos direitos dos titulares dos dados e a adoção de medidas para evitar práticas discriminatórias ou abusivas.

Além disso, foi possível compreender a função do Encarregado de Proteção de Dados (DPO) e a possibilidade

Copyright © 2022 ISESC

de aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD) em caso de descumprimento das normas da LGPD. Esses mecanismos são essenciais para garantir a eficácia da lei e para incentivar as empresas e organizações a adotarem boas práticas de proteção de dados.

Diante do cenário de crescente digitalização e uso intensivo de dados pessoais, a LGPD se torna ainda mais relevante, promovendo a confiança dos cidadãos nas instituições que lidam com suas informações e estimulando a inovação de forma ética e responsável.

Conclui-se, portanto, que a LGPD desempenha um papel fundamental na sociedade contemporânea, fortalecendo os direitos individuais e contribuindo para um ambiente digital mais seguro, justo e transparente para todos. É imperativo que empresas, organizações e indivíduos se familiarizem e cumpram as disposições da Lei para garantir o respeito à privacidade e à dignidade das pessoas no mundo digital.

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasil, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 jan. 2022.

CIRIACO, D. Internet é usada por 4,1 bilhões de pessoas em todo o mundo, aponta estudo. Blog TecMundo. 2018. Disponível em: <https://www.tecmundo.com.br/internet/135281-internet-usada-4-bilhoes-pessoasmundo-aponta-estudo.htm>. Acesso em: 27 fev. 2022.

DONEDA, D. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MAGALHÃES, R.A.; OLIVEIRA, E.C.R.N. O direito à privacidade na Era Digital. Revista Jurídica da FA7, v. 18, n. 1, p. 55-70, 2021. Disponível em: <https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1173>. Acesso em: 30 mar. 2022.

NASCIMENTO Leonardo Fernandes. A Sociologia Digital: um desafio para o século XXI. 2016. Disponível em: https://www.scielo.br/j/soc/a/y9gtcQSrjjXVyRfryrKpXBk/?lang=pt. Acesso em: 20 mai. 2022.

SANTOS, L.S. A Lei 13.709/2018 – Lei Geral de Proteção de Dados: o direito à privacidade e os princípios que asseguram a proteção de dados. 2021. 36f. TCC (Graduação) – Escola de Direito, Comunicação e Negócios, Pontifícia Universidade Católica, Goiás, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2566/1/MONOGRAFIA%20-%20LARISSA%20SOARES%20-%20VF.pdf>. Acesso em: 29 mar. 2022.

PALETTA, F.C. Desafios na gestão da informação na Era Digital no contexto da Ciência da Informação. Informação & Amp; Sociedade: Estudos, v. 30, n. 4, p. 1–11, 2021. Disponível em: < https://periodicos.ufpb.br/index.php/ies/article/view/57795>. Acesso em: 30 mar. 2022.

SANTI, L. Lei nº 13.709/2018: análise à Lei Geral de Proteção de Dados Pessoais (LGPD). 2020. 60f. TCC (Graduação) – Universidade do Sul de Santa Catarina, Tubarão, 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/6086/3/Monografia%20-%20Leandro%20Santi%20-%2024.06.2020.pdf>. Acesso em: 01 jun. 2022.

TEIXEIRA, G.C. O papel social da Lei Geral de Proteção de Dados no Brasil. 2020. 59f. TCC (Graduação) – Universidade do Sul de Santa Catarina, Araranguá, 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/7514/1/Monografia%20Guilherme%20Cardoso%20Teixeira.pdf>. Acesso em: 01 jun. 2022.

VILELA, A.C.; LAIA, F. A efetividade da Lei Geral de Proteção de Dados Pessoais para a tutela do direito ao esquecimento. 2021. 25f. Artigo (Graduação) – Universidade do Sul de Santa Catarina, Blumenau, 2021. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/13259>. Acesso em: 15 mai. 2022.

Copyright © 2022 ISESC