

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

**LGPD NA PROTEÇÃO DE DADOS DOS CLIENTES DE AUTOMAÇÃO**

RESPONSABILIDADE DAS EMPRESAS NAS HIPÓTESES DE VAZAMENTO DE DADOS

ORIENTANDO - IAGO CARVALHEDO DE SOUSA
                      ORIENTADOR - PROF. ME JOSÉ HUMBERTO ABRÃO MEIRELES

  GOIÂNIA-GO
  2022

IAGO CARVALHEDO DE SOUSA

**LGPD NA PROTEÇÃO DE DADOS DOS CLIENTES DE AUTOMAÇÃO**

RESPONSABILIDADE DAS EMPRESAS NAS HIPÓTESES DE VAZAMENTO DE DADOS

    Projeto de Artigo Científico (ou Monografia Jurídica) apresentado à disciplina Trabalho de Curso I, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS). Prof. Orientador: ME José Humberto Abrão Meireles.

GOIÂNIA-GO

2022

IAGO CARVALHEDO DE SOUSA

 **LGPD NA PROTEÇÃO DE DADOS DOS CLIENTES DE AUTOMAÇÃO**

RESPONSABILIDADE DAS EMPRESAS NAS HIPÓTESES DE VAZAMENTO DE DADOS

 Data da Defesa: \_\_\_\_ de \_\_\_\_\_\_\_\_\_\_ de \_\_\_\_\_\_\_

BANCA EXAMINADORA

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Orientador: Prof. José Humberto Abrão Meireles Nota

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Examinadora: Goiacy Campos dos Santos Dunck

**LGPD NA PROTEÇÃO DE DADOS DOS CLIENTES DE AUTOMAÇÃO**

RESPONSABILIDADE DAS EMPRESAS NAS HIPÓTESES DE VAZAMENTO DE DADOS

Iago Carvalhedo de Sousa

O presente artigo científico surgiu como um produto da averiguação do atual cenário tecnológico que o mundo se encontra. Em face das alterações digitais, as diversas formas de armazenamento de dados sofreram algumas adequações tendo como objetivo, uma maior responsabilidade e buscando evitar vazamentos de dados pessoais e sensíveis de clientes. Diante dessa problemática, se fez necessário uma resposta por parte do Direito, com o objetivo de acautelar os princípios fundamentais estabelecidos na Carta Magna, sendo essa a Lei Geral de Proteção de Dados nas quais estabeleceu direitos e deveres a controladores e operadores dos sistemas de automação. Diante das expostas indagações este artigo científico vem analisar se as bases teóricas e práticas da LGPD poderão promover a coletividade o resguardo crucial de sua privacidade e dados, tal qual constatar se a mesma está em concordância com as atuais regras impostas pela modernização.

**Palavra-chave:** Automação. Segurança. Privacidade. Responsabilidade.

**SUMÁRIO**

**INTRODUÇÃO**...........................................................................................................06
**1. DA AUTOMAÇÃO E A LEGISLAÇÃO INTERNACIONAL**...................................08
1.1. DO MARCO CIVIL E A LGPD CONTEMPLANDO A AUTOMAÇÃO..................09

1.2. DA AUTOMAÇÃO E SUA SEGURANÇA............................................................11
1.2.1. DO ARMAZENAMENTO DE DADOS PESSOAIS...........................................14
**2. ANPD NA FISCALIZAÇÃO DOS SISTEMAS DE AUTOMAÇÃO**........................16
2.1. EFICÁCIA DA LGPD NA AUTOMAÇÃO.............................................................19
**3. DA RESPONSABILIZAÇÃO**..................................................................................20

**CONSIDERAÇÕES FINAIS**.......................................................................................22
**REFERÊNCIAS**..........................................................................................................24

**INTRODUÇÃO**

O presente artigo tem o objetivo de compreender a temática acerca da automação comercial no Brasil, sendo trabalhada com prioridade, a segurança de dados dos usuários com base na Lei Geral de Proteção de Dados. Os atuais avanços da tecnologia culminaram em uma busca de melhoria de vida dos indivíduos, ao qual podemos elevar a um alto grau de modernidade, pois aparelhos antes muito usados foram automatizadas, em decorrência desse processo tecnológico surgiu a era digital ao qual trouxe aparelhos modernos que possuem como principal funcionamento, o transporte de dados.

Em decorrência desse progresso tecnológico, ocorreu a popularização da Internet, que se constituiu nas mais diversas ferramentas, desde bancos até relacionamentos humanos. Desta forma, toda a sociedade sofreu adaptações que buscam melhorar o bem estar do indivíduo, o que ocasionou em uma comodidade ainda maior com os smartphones. Visando uma forma de inibir qualquer tipo de prejuízo, foram criados regulamentos e leis de proteção de dados ao redor do mundo. A primeira manifestação legal acerca deste tema foi criada na Alemanha em decorrência do grande processamento de dados dos computadores daquela época, o que veio a influenciar as legislações futuras ao redor do mundo.

Vale destacar que dados são responsáveis por todo tráfico de informação relacionado ao meio digital ou não. Partindo desse princípio, surgiu uma enorme preocupação acerca do princípio da inviolabilidade à segurança estabelecidos na Constituição Federal, se fez necessário trazer legislações pertinentes ao tráfico de dados conhecida como a Lei nº 12.965/2014, ao qual se chamamos de Marco Civil da Internet, onde estabeleceu a proteção da privacidade e dos dados pessoais e pode ser tratada como uma espécie de constituição das leis relativas à automação.

A metodologia a ser utilizada na elaboração da pesquisa envolverá o método dedutivo e a pesquisa teórica.

Tendo em vista o tema a ser tratado, o trabalho será realizado com a finalidade de um estudo com o objetivo de compreender os sistemas de automação, quanto às hipóteses nos casos de vazamento de dados, e qual seriam seus efeitos jurídicos com base na Lei Geral de Proteção de Dados.

1. **DA AUTOMAÇÃO E A LEGISLAÇÃO INTERNACIONAL**

A principal referência para a LGPD se encontra no Regulamento Geral de Proteção de Dados Europeu 2016/679 e seu texto aborda todas as situações pertinentes ao tratamento de dados, impondo regras a operadores e controladores, fomentando a padronização dos sistemas de segurança e governança dos dados, assegurando às empresas e indivíduos.

No que tange a automação e todos os controladores de dados, estes devem seguir as seguintes práticas em conforme o art. 11 do Regulamento Geral de Proteção de Dados Europeu:

A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros. (UNIÃO EUROPEIA,2016, Art.11)

A adequação dos agentes controladores de dados ao RGPD é de caráter obrigatório para todos os Estados Membros, pois tendo em vista o poder econômico e social da União Europeia, em um possível ataque virtual, ou vazamento de dados de forma acidental, teríamos consequências e danos de caráter universal, uma vez que a mesma detém 15% do comércio mundial de mercadorias, e se valendo dessas hipóteses dispões no art.19 da RGPD:

A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos. Todavia, os dados pessoais tratados pelas autoridades competentes ao abrigo do presente regulamento deverão ser regulados, quando forem usados para os efeitos referidos, por um ato jurídico da União mais específico, a saber, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (1). Os Estados-Membros podem confiar às autoridades competentes na aceção da Diretiva (UE) 2016/680 funções não necessariamente a executar para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, de modo a que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do presente regulamento. (UNIÃO EUROPEIA,2016, Art.19)

Dessa forma, sistemas de automação devem ser exemplos de boas práticas e de políticas de caráter ético, um exemplo seria as ISO’s, que é a sigla de *International Organization for Standardization*, ou Organização Internacional para Padronização, tem como objetivo principal aprovar normas internacionais em todos os campos técnicos, como normas técnicas, classificações de países, normas de procedimentos e processos, e etc. No Brasil, a ISO é representada pela ABNT (Associação Brasileira de Normas Técnicas).

No que tange às práticas de segurança da informação, as empresas têm de se fundar nos regulamentos dos melhores padrões de notabilidade global, tal como a ISO26 e o NIST27, no qual fazem parte de uma série de certificações de boas práticas dos sistemas de informação. É imperativo destacar que as grandes empresas de automação no Brasil já adotam a ISO como padrão como referência internacional para a gestão da Segurança da informação, o que, além de trazer uma certificação de qualidade de gestão ética de dados, trazem vantagens comerciais.

* 1. DO MARCO CIVIL E A LGPD CONTEMPLANDO A AUTOMAÇÃO

Toda matéria que envolve a proteção de dados tem garantia constitucional no art. 5º inciso X, ao qual visa o princípio da inviolabilidade à segurança, dispondo que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado, em seguida o Marco Civil, ao qual dispõe sobre o tema nos seguintes artigos:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Dessa forma, após escândalos que envolveram a segurança de privacidade de dados do Facebook, no qual a empresa Cambridge Analytica coletou informações pessoalmente inidentificáveis de até 87 milhões de usuários, com a finalidade de influenciar na opinião política da eleição de Donald Trump. Diante da preocupação acerca dessa problemática, era notória a necessidade de uma legislação nacional referente à matéria, pois mesmo a Constituição Federal e o Marco Civil não eram capazes de abordar de forma técnica e sucinta os tópicos referentes os dados no país vigente.

Por consequência desses fatores, em 2018 foi sancionada e publicada a Lei Geral de Proteção de Dados, tendo como finalidade garantir o direito à privacidade dos indivíduos, abordar direitos e deveres das pessoas naturais e jurídicas que fazem o tratamento de dados e aplicar as devidas sanções a estes que descumprirem as regras estabelecidas em lei. Sob essa ótica, as empresas de automação, no qual na maioria das vezes são operadoras e controladoras de dados, estariam suscetíveis às adequação em lei, com base no art.5º, inciso X, da Lei Geral de Proteção de Dados:

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

Portanto, entendendo-se a automação como todo tipo de serviço que visa a menor interferência humana e busca de forma automática alcança sua finalidade, todas essas operações citadas acima corroboram a ratificar o principal papel da automação, sendo operador e às vezes controlador de dados. Desse modo, a LGPD estabelece princípios de boas práticas aos agentes responsáveis pelos dados, tendo base no art.6º nos respectivos incisos:

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.

Deste modo, deve as empresas responsáveis pelo tratamento de dados adotar essas medidas, com a finalidade de prevenir possíveis danos a indivíduos de natureza física ou jurídica. Assim como citado acima, existem normas, como a ISO 27001, no qual são certificações reconhecidas mundialmente, que visam a boa prática e padronização dos sistemas de informação. Ainda que de forma breve, torna perceptível a correlação do direito brasileiro com automação, pois toda forma de tratamento de dados, não deve violar princípios constitucionais e deve seguir as determinadas práticas de boa-fé.

* 1. DA AUTOMAÇÃO E SUA SEGURANÇA

São várias as etapas que visam a segurança das empresas de automação para com os dados dos clientes, uma delas é a estrutura física da empresa, pois uma provável invasão na sede de tratamento desses dados, traria consequências que ferem os critérios estabelecidos em lei, tendo em vista que se encontra toda a estrutura de servidores e computadores. Portanto, as empresas devem investir em estratégias de segurança que dificultem o acesso e controle do fluxo de funcionários.

Em seguida, vale ressaltar as políticas de boas práticas e governança das empresas elencados na LGPD nos seguintes dispositivos:

Art. 50. 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.

§ 1º 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.

a) 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;

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

 A adequação à Lei Geral de Proteção de Dados é a principal ferramenta para uma eficácia da segurança dos sistemas de automação, no qual, tendo em vista o aumento de vazamento de dados frequentes no país. Um exemplo a esse assunto é do comércio eletrônico de artigos esportivos Netshoes, em que, por consequência de ataques cibernéticos, teve seu banco de dados comprometido e, em decorrência desse episódio, quase dois milhões de clientes tiveram dados como data de nascimento, CPF e e-mail expostos. Conforme esses acontecimentos vêm se sucedendo, mister se faz inibir qualquer tipo de invasão ou vazamento de dados nos sistemas de automação, as medidas possíveis devem ser tomadas conforme o art. 6º da Lei Geral de Proteção 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.

Esses princípios estabelecem relações diretas com as políticas de governanças das empresas e as associam com uma segurança dentro dos parâmetros da LGPD, a fim de destacar critérios ao qual devem ser seguidos, garantindo os deveres éticos e legais dos controladores, operadores e agentes de tratamento desses dados. Visando evitar possíveis consequências aos titulares dos dados, se faz necessário usar políticas que priorize o bem estar do indivíduo, e que traga uma harmonia entre o poder público e empresas de automação, se faz imperativo acatar medidas relacionadas à segurança, dessa forma a Secretaria de Segurança dispõe as seguintes medidas institucionais:

* O incentivo a medidas de [gestão de riscos](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/gestao-riscos) e às [melhores práticas internacionais](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/melhores-praticas-internacionais);
* A promoção de [oficinas, cursos e outros eventos](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/treinamento-desenvolvimento-eventos);
* A divulgação de informações sobre [órgãos](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/orgaos-atividades-projetos) e [legislação](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/legislacao-federal);
* A interação constante com outros órgãos e entidades federais para dialogar, promover trabalhos técnicos conjuntos e disseminar boas práticas de segurança da informação e de proteção de dados pessoais.

Portanto, tratar dados é assumir [riscos](https://getprivacy.com.br/lgpd-protecao-de-dados-principais-riscos-de-seguranca-para-empresas/). Na prática, quanto mais dados pessoais a organização trata e quanto mais sensíveis são esses dados, maior é a responsabilidade. Por consequência, a cobrança também é maior, assim como as sanções em casos de erros e falhas. É fundamental ter isso em mente ao tratar ou cogitar o tratamento de dados sensíveis. Considerando o risco que eles representam para a organização e para o próprio titular caso sejam expostos ou utilizados de forma indevida, dados sensíveis só devem ser tratados em caso de real necessidade. (PRIVACY, 2020)

Essas e outras medidas são derivadas da LGPD, para prover uma maior maturidade de segurança e privacidade por parte das empresas para não ocorrer certa comodidade e sensação de inviolabilidade dos sistemas de informação e dados. Vale ressaltar que nenhum sistema de banco de dados ou de informação é 100% seguro, porém devem ocorrer auditorias a cerca infraestrutura operacional, tático e organizacional devem ser revisadas com frequência, a fim de evitar uma possível invasão ou vazamento de dados.

1.3. DO TRATAMENTO DE DADOS SENSÍVEIS

No que tange a dados sensíveis, a  [LGPD](https://ndmadvogados.jusbrasil.com.br/artigos/606197608/a-nova-lei-de-protecao-de-dados-pessoais-e-a-seguranca-das-informacoes) define no art. 5º inciso II:

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

Por se tratar de dados sensíveis, o armazenamento desses dados devem adotar medidas de segurança, técnica e administrativa que possam coibir a infringência do princípio da dignidade da pessoa humana e do direito à privacidade. Diante disso, Viviane Porto entende da seguinte forma:

1. *Mediante o consentimento: A base legal do consentimento para tratamento de dados pessoais sensíveis, além de ter que observar todos os requisitos da hipótese de consentimento de dados pessoais não sensíveis, isto é, o consentimento tem que ser dado de forma livre, inequívoca e específica, deverá ser, ainda, específico e destacado, seguindo as demais obrigações que constam na lei, como indicar a finalidade específica do tratamento, o prazo de duração, o compartilhamento de dados, dentre outros. O consentimento para autorizações dado de forma genérica é considerado nulo.(PORTO, 2020)*

*II) Sem o consentimento: O artigo 11 da LGPD previu a possibilidade de tratamento de dados pessoais sensíveis, sem o consentimento do titular do dado, nos casos:* *a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.(PORTO, 2020)*

Pode se afirmar que o direito à privacidade deve ser inviolável no que tange a dados sensíveis, pois os mesmos podem conter informações quanto à etnia, religião opção sexual ou dado genético. Por isso se fez necessário uma preocupação acerca destes, uma vez que dados vazados colocarão em risco a honra e dignidade de indivíduos ao qual possam comprometer suas vidas pessoais e profissionais. Outro problema que a LGPD demonstra preocupação é o fato de que o controlador possa usar dados sensíveis dos titulares com algum intuito financeiro. Destacamos que é explícita a proibição dessa prática e cabe a ANPD aplicar as devidas sanções administrativas nessas hipóteses.

Diante dessa problemática, a Agência Nacional de Proteção de Dados solicitará a qualquer momento os relatórios de impactos, que visam proteger os dados do titular e buscar conformidades com a lei para com as empresas. Ainda que breve, a ANPD dispõe de guias orientativos para agentes de tratamentos com instruções necessárias para o manuseio desses dados, pois gozam de proteção especial da LGPD. A Lei Geral de Proteção de Dados ainda estipula medidas de segurança que dificultem a identificação do titular, usando a pseudonimização ou anonimização de dados. Um exemplo dessa situação seria a técnica de criptografia dos dados sensíveis ao qual dispões em seus seguintes dispositivos:

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. (BRASIL, 2018)

Pseudonimização como explica o parágrafo 4º do Art. 13 ocorre quando um dado pessoal ou sensível só pode ser atrelado a um indivíduo se houver acesso também a alguma outra informação — que deve ser mantida em separado e em total segurança. Dessa forma, se alguém conseguir acesso apenas aos dados originalmente tratados, não conseguirá relacioná-lo a nenhum indivíduo. (GONZALEZ, 2020)

Por ser tratar de dados sensíveis, é papel das empresas propor a transparência e finalidade do tratamento de dados, tendo em vista o cenário político e econômico que se encontra invasões e vazamentos possíveis, colocaria em risco a dignidade da pessoa humana e traria consequências comerciais catastróficas as empresas de automação e agentes de tratamento de diversos segmentos.

**2. ANPD NA FISCALIZAÇÃO DOS SISTEMAS DE AUTOMAÇÃO**

A Agência Nacional de Proteção de Dados é um órgão da administração pública federal, integrante da Presidência da República, ao qual tem como papel de zelar e elaborar políticas de proteção dos dados pessoais e da privacidade, fiscalizar a aplicação da LGPD determinando sanções para casos de infrações dentre outras atribuições listadas em lei. Dessa forma, a ANPD deve fomentar políticas de segurança e boas práticas dentre os agentes de tratamento de dados e demais empresas que operam dados com finalidades comerciais lícitas, editando regulamentos e procedimentos que abordam segurança e privacidade de dados pessoais, assim como relatórios de impactos à proteção de dados para hipóteses nas quais o tratamento representar altos riscos à garantia dos direitos protegidos em lei.

Com a recente aprovação do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador por meio da Resolução CD/ANPD Nº 1, de 28 de outubro de 2021 ao qual trouxe segurança jurídica e papéis como fiscalizador.

Isso porque o objetivo do documento é de estabelecer as regras e procedimentos de fiscalização no âmbito do processo administrativo sancionador, o que compreende desde as atividades de monitoramento, atuação preventiva e orientação, até a efetiva aplicação pela ANPD das sanções previstas na legislação. Dentre os múltiplos papéis a serem exercidos pela Autoridade Nacional de Proteção de Dados, para além de suas atividades repressivas, destaca-se o de promoção de conscientização acerca da proteção de dados pessoais. No âmbito da Resolução, os artigos 27 a 29 dedicam-se a estabelecer as atividades de orientação da ANPD que visam a conscientização e a educação dos Agentes de Tratamento, dos titulares, dos titulares de dados e dos demais integrantes ou interessados no tratamento de dados pessoais, a fim de se evitar irregularidades. (BLUM, 2022)

Conforme a resolução, a ANPD terá papel de fundar guias, modelos de documentos relativos a maturidade de segurança e privacidade, cursos e oficinas que tenham como objetivo a publicidade das políticas de boas práticas e governança das empresas. Dessa forma, todas essas atividades deverão estar atreladas ao processo de fiscalização como um todo, pois fazem parte da Política Nacional de Proteção de Dados Pessoais e Privacidade, criando o hábito de prover o desempenho maduro referente a proteção de dados pessoais e sensíveis no país.

Porém, o processo de fiscalização se divide em algumas partes, sendo este monitoramento, orientação e prevenção. O monitoramento por sua vez, entende-se como uma atividade responsável pela observação de informações e dados pertinentes para a tomada de decisões da ANPD, com o objetivo de zelar pelo direito dos titulares e dos sistemas de automação. A orientação é compreendida como métodos didáticos que vise a ética no tratamento de dados, ao qual busca prezar pelo princípio da boa fé. A prevenção é uma atividade de atuação que visa a boa comunicação entre a ANPD, o qual é exercida pelo encarregado vide art. 5º, inciso VII da LGPD, dispondo da seguinte forma:

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

A função do encarregado é primordial para a prevenção de iminentes riscos à privacidade dos dados, tendo como atividades estipuladas no Art. 41, § 2º da LGPD:

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

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Ainda se tratando de prevenção, é imperativo citar os relatórios de impacto que consistem em uma obrigação legal, que deve ser exigida pela ANPD para com os controladores sempre que alguma manipulação de dados ameaçarem a liberdade e direito fundamentais dos indivíduos. Se valendo dessa premissa, caso ocorra alguma infração de natureza danosa aos titulares dos dados, caberá sanções administrativas assim como estabelecidas no Art. 52, ao qual prevê multa simples de 2%(dois por cento) do faturamento bruto mais multa diária, com limite de R$ 50.000.000,00 ( cinquenta milhões ) por infração.

Outra sanção é a publicidade da infração após apurada e confirmada sua ocorrência, considerada danosa o suficiente para corroborar uma reputação negativa quanto ao seu tratamento de dados, no qual trará vantagens comerciais aos seus concorrentes que oferecem serviços em conformidade com a lei. Terá ainda a empresa infratora, o bloqueio e suspensão parcial do banco de dados, da atividade de tratamento de dados ao qual poderá impedir o exercício de função da empresa.

Vale ressaltar que as devidas sanções são empregadas de forma progressiva. Com o intuito de medir o grau do dano, assim estipulado no Art. 52, § 1º da LGPD:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

Deverá ainda ser levada em conta a atuação do agente na infração, se este cooperou diretamente para a proporção do dano causado, ou a aplicação de medidas corretivas para a reparação do dano. Todos esses critérios são exemplos de boas práticas e governança por parte dos sistemas de automação, que devem abordar princípios e técnicas elencadas em lei.

2.1 DA EFICÁCIA DA ANPD NA AUTOMAÇÃO

Com a vigência da Lei Geral de Proteção de Dados, os sistemas de automação sofreram mudanças positivas no âmbito de tratamento de dados, ao qual prioriza zelar os princípios fundamentais para a manutenção da privacidade dos indivíduos. Sob essa ótica, é possível esperar uma expectativa que faça instituições públicas e privadas se adequarem e almejarem uma melhora significativa em suas estruturas, fomentando a conscientização e a cultura de proteção de dados. Segundo as pesquisas da Fundação Dom Cabral (FDC) realizada em 2020, somente 40% de 207 empresas priorizou a adequação para o ano seguinte.

É notória uma preocupação acerca da adequação dessas empresas, pois grande parte das mesmas é de pequeno porte e fazem tratamento de dados na prestação de serviços e não se sujeitam a uma política de gestão mais segura. Porém, após dois anos de vigência da LGPD, somente em janeiro de 2022 a ANPD iniciou a fiscalização nos sistemas de informação e trouxe uma preocupação acerca da seriedade no que tange a privacidade e segurança dos indivíduos.

Com a morosidade da fiscalização dos sistemas de informação, houve consequências danosas a empresas que trabalham com o tratamento de dados. Um exemplo seria a Serasa que expôs seu banco de dados, evidenciando a fragilidade do sistema e fez com que indivíduos de má fé divulgassem CPF, foto de rosto, endereço, telefone, e-mail, score de crédito, salário e mais de 200 milhões de brasileiros na dark web. Vale salientar que esse caso ocorreu em 2021, após 2 anos de vigência da LGPD.

Somente após o incidente, a ANPD manifestou “estar apurando tecnicamente informações sobre o caso e atuará de maneira cooperativa com os órgãos de investigação competentes”. Isso demonstra déficit de prevenção na proteção de dados e de fiscalização dos agentes de tratamento e sistema de automação. Diante disso, cabe às instituições privadas trazer departamentos jurídicos especializados na proteção de dados, e diminuição de riscos de vazamentos elaborando relatórios de impacto que prezam pela segurança dos titulares dos dados.

**3. DA RESPONSABILIZAÇÃO**

É imperativo, ainda, os agentes de tratamento tomarem ciência sobre as suas responsabilidades para com os dados dos titulares, e no tocante a isso o Art. 42 da LGPD dispõe da seguinte forma:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Diante do dispositivo legal elencado acima, é perceptível que o operador e o controlador terão responsabilidade solidária nas hipóteses destacadas do caput já que se entende que caberá ao titular dos dados acionar judicialmente, tanto o controlador, como o operador de dados para a reparação do dano causado. De certo modo, isso traz uma condição benéfica ao titular dos dados, pois o mesmo não terá obrigação de consultar os agentes de tratamento para comprovar quem deu a motivação para o dano sofrido, sendo imperativo destacar a inversão de ônus da prova, em que será de responsabilidade dos agentes de tratamento, comprovar que não houve nexo de causalidade.

Portanto, tendo o titular dos dados uma relação jurídica de consumo, entende-se também como consumidor, assim como consta no caput do Art. 2º do Código de Defesa do Consumidor:

Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.

Desse modo, responderá também o controlador e operador pelo dano causado, pois os mesmos se classificam como fornecedores de serviços pelo Código de Defesa do Consumidor no Art. 3º:

Art. 3° Fornecedor é toda pessoa física ou jur ídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

 § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

Dessa maneira, poderá o titular dos dados aplicar também sanções administrativas e civis dispostas no Código de Defesa do Consumidor ou em legislações específicas, ao qual pode ser fundada ações judiciais, individuais ou coletivas de natureza indenizatória com o intuito de zelar pelo princípio constitucional do direito à privacidade, defesa do consumidor e da proteção dos dados dos titulares estipulado na Lei Geral de Proteção de Dados.

**CONSIDERAÇÕES FINAIS**

Durante a construção dessa monografia foram analisadas as referências históricas para a elaboração da Lei Geral de Proteção de Dados correlacionando na proteção de dados dos sistemas de automação. Torna-se evidente a proteção da privacidade e dos dados dos titulares, a fim de evitar possíveis vazamentos e trazer uma melhora significativa no tratamento de dados por parte dos sistemas de automação no Brasil.

Pode-se dizer que a base teórica da LGPD é didática, dando ênfase às responsabilidades dos agentes de tratamento, porém não pode ficar somente no papel, e boas práticas de governança de dados devem ser salientadas e ampliadas a fim de garantir uma gestão segura. Entretanto, dados sensíveis precisam de base legal rigorosa, e seu tratamento deve ser feito com total responsabilidade e maturidade por parte dos sistemas de automação, a fim de evitar possíveis danos à vida pessoal e profissional dos indivíduos.

Cabem à ANPD, uma fiscalização e acompanhamento da gestão de dados de vários sistemas de informação no país vigente, pois essa entidade ainda é imatura e tem a obrigação legal de fomentar as boas práticas, acompanhar riscos e impactos do mau tratamento de dados, ao qual não exerce com eficiência. Diante disso, é dever dos sistemas de automação agir por conta própria no quesito de segurança e boas práticas, a fim de evitar possíveis sanções administrativas milionárias e danosas.

LGPD ON AUTOMATION CLIENT DATA PROTECTION

RESPONSIBILITY OF COMPANIES IN CASES OF DATA LEAKAGE

**ABSTRACT**

The present scientific article emerged as a product of the investigation of the current technological scenario that the world is in. In several changes of digital data, such as different ways of storing personal data, greater responsibility and some adjustments to avoid customer data. In this problematic way, it was necessary to respond to this problem, with the fundamental principles of data protection Magna parte, with the fundamental principles of data protection Magna parte in which the fundamental principles of data protection are fundamental and the fundamental principles of data protection Magna part in which the fundamental principles must be protected of rights and mechanisms of protection systems. . In view of the scientific inquiries analyzed as theoretical and practical bases of LGPD, they can promote collectivity and data, as well as verifying whether it is in accordance with modernization.

Keyword: Automation: Safety. Privacy. Responsibility.

**REFERÊNCIAS BIBLIOGRÁFICAS**

# *ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber. 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml. Acesso em: 04 de Fevereiro de 2022*

*BLUM, Renato. O processo de fiscalização da Lei Geral de Proteção de Dados pela ANPD e o seu papel preventivo e orientativo. Disponível em: https://noomis.febraban.org.br/especialista/renato-opice-blum/o-processo-de-fiscalizacao-da-lei-geral-de-protecao-de-dados-pela-anpd-e-o-seu-papel-preventivo-e-orientativo Acesso em: 14 de Março de 2022*

*BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]. Disponível em:* [*http://www.planalto.gov.br/ccivil\_03/constituicao/constituicao.htm*](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm)*. Acesso em 02 fev. 2021.*

*BRASIL. (abr de 2014). Lei n. 12.965 de 23 de abr. de 2014. Marco civil da Internet . Acesso em: 11 de Março de 2022*

*BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: . Acesso em: 22 out. 2019.*

*BRASIL. (out de 2021. RESOLUÇÃO CD/ANPD Nº 1. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Disponível em:*

*https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513*

*CAMPELLO, Tatiane. LGPD: aspectos gerais para uma política de privacidade eficaz https://www.demarest.com.br/lgpd-aspectos-gerais-para-uma-politica-de-privacidade-eficaz/#:~:text=No%20momento%2C%20segundo%20uma%20pesquisa,uma%20das%20prioridades%20para%202021.*

*CASTELLS, M. (2018). O poder da identidade: a era da informação, volume 2. São Paulo: Paz & Terra.*

*DE ARAUJO PORTO, VIVIANE. Descomplicando a Lei Geral de Proteção de Dados (p. 23). Edição do Kindle.*

*GONZALÉZ, Mariana. LGPD COMENTADA. ID WALL. 2020. Disponível em:* [*https://guialgpd.com.br/lgpd-comentada/*](https://guialgpd.com.br/lgpd-comentada/) *Acesso em: 11 de Março de 2022.*

*NEGRI, Patrick. O que é automação e quais os benefícios para as empresas?. IUGU. 2018. Disponível em:* [*https://www.iugu.com/blog/o-que-e-automacao*](https://www.iugu.com/blog/o-que-e-automacao) *Acesso em: 10 de Janeiro de 2022:*

*UNIÃO EUROPEIA Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em:* [*https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT*](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT)*. Acesso em: 10 de Janeiro de 2022.*

*BRASIL. Código de defesa do consumidor. Lei 8.078 de 11/09/90. Brasília, Diário Oficial da União, 1990.*

# *SANTOS SOARES, FERNANDA. A responsabilidade civil na Lei Geral de Proteção de Dados. LAGE E PORTILHO. 2021. Disponível em: https://lageportilhojardim.com.br/blog/responsabilidade-civil-na-lgpd/#:~:text=Ele%20prev%C3%AA%20a%20responsabilidade%20dos,de%20prote%C3%A7%C3%A3o%20de%20dados%20pessoais / Acesso em:10/06/2022.*