

## **PROCESSO DE ADEQUAÇÃO À LGPD: UM ESTUDO COMPARATIVO ENTRE A ISO 27.701 E A LEI 13.709/2018**

Aline Pons Alves Lisboa, discente de Pós-Graduação PPGCAP, Universidade Federal do Pampa, Campus Bagé  
Vinícius do Nascimento Lampert, docente, Universidade Federal do Pampa  
Érico Marcelo Hoff do Amaral, docente, Universidade Federal do Pampa

[alinelisboa.aluno@unipampa.edu.br](mailto:alinelisboa.aluno@unipampa.edu.br)

A falta de cuidado nas operações com dados pessoais causou exposição dos dados de 243 milhões de brasileiros, 3,75 bilhões de registros e 2,2 bilhões de credenciais foram expostas em vazamentos de dados no primeiro trimestre de 2021, publicado no relatório da Axur (2021). A União Europeia criou em 2016 o *General Data Protection Regulation (GDPR)* que serviu de inspiração para a criação da Lei Geral de Proteção de Dados (LGPD), aprovada em 2018 que elevou a proteção de dados pessoais a direito fundamental, entrando para o rol da Constituição Federal pela Emenda Constitucional nº 115/2022. O setor agropecuário lançou a Cartilha LGPD e uma pesquisa que identificou a dificuldade que as empresas enfrentaram na adequação à lei (ASBRAAP, 2022). No Brasil já existia a NBR ISO/IEC 27.001 relacionada a gestão de segurança da informação e a ISO/IEC 27.002 direcionada a boas práticas para gestão de segurança da informação. Após a LGPD e a GDPR, foi criada em 2019 a NBR ISO/IEC 27.701 para gerir a privacidade da informação. O objetivo do presente estudo é elaborar uma sumarização entre a lei brasileira e a norma, direcionada a realização de um processo de adequação, utilizando boas práticas e governança. Para o desenvolvimento deste estudo optou-se por utilizar uma metodologia de pesquisa baseada em autores que descrevem os procedimentos legais referentes a proteção de dados e normas técnicas para *compliance* no agronegócio. O comparativo entre as regras da LGPD e requisitos da ISO 27.701 foi possível de ser realizado a partir dos conhecimentos obtidos em dois cursos online, um direcionado para as questões de tecnologia e o outro sobre adequação à LGPD. Entendendo o funcionamento das regras da LGPD enquadra-se que o tratamento de dados deve seguir um conjunto de diretrizes encontrados no artigo 6º, tomando por base o princípio de conduta e boa-fé. Os princípios da LGPD para Gonçalves (2021) podem ser associados às ações para obter melhor desempenho na gestão de privacidade de dados. No princípio da Finalidade, é relevante utilizar a transparência no sentido de realizar o tratamento exatamente como está sendo informado ao titular. O princípio da Adequação também exige transparência quanto à finalidade e documentos dispostos aos titulares. Para o princípio da Necessidade ser atingido, pode ser necessário organizar os processos para o tratamento. Quanto ao princípio do Livre acesso, será preciso ter um canal de comunicação com os titulares e atender suas solicitações. O princípio da Qualidade dos dados, exige que os dados estejam corretos e atualizados, para isto pode ser disponibilizado um meio para que o titular consiga fazer essas ações. No princípio da Transparência, é interessante ter conteúdos e objetivos exatos. No princípio da Segurança, a empresa deve ter medidas eficazes e no princípio da Prevenção ter meios de prevenir que o incidente ocorra. Para o atendimento do

princípio da Não discriminação a empresa deve seguir os requisitos da lei sem tratar os dados de uma forma que traga prejuízos ao titular. Para atender ao princípio da Responsabilidade e prestação de contas, devem ser feitos registros que evidenciem as medidas utilizadas para alcançar o que a lei exige. Com o estudo da lei foi realizado em paralelo um estudo da norma, ISO 27.701, sendo feita uma descrição contendo indicadores de ambas as normas em cada artigo da lei para identificar pontos de atendimento dos requisitos em um processo de adequação, conforme Donda (2021) e Beux (2021) orientam em seus cursos. Nos fundamentos do Art. 2º, a subseção 6.3.1.1 da ISO/IEC 27.701 recomenda que exista um responsável pela proteção de dados e segurança da informação. O Art. 8º, além de coletar o consentimento de forma escrita ou que manifeste a vontade inequívoca, a subseção 5.6.2 indica a avaliação de riscos e a subseção 5.6.3 o tratamento de riscos de segurança da informação. No Art. 9º, deve ser garantido o livre acesso aos dados e estabelecer política de privacidade. No Art. 33, é preciso identificar se o país possui lei de proteção de dados, o nível de adequação e coletar o consentimento, e ainda, a subseção 6.13.1.2 recomenda a notificação de eventos de segurança da informação. Para o Art. 46, a subseção 6.9.6 indica a gestão de vulnerabilidades técnicas e no Art. 48, é indicado notificar o incidente para a ANPD. O Art. 50 é direcionado para a subseção 6.3.1.1 com definição de responsáveis e papéis, combinado com a subseção 6.13.1.2 notificação de eventos de segurança da informação. Por fim, no Art. 51, se recomenda adoção de padrões de acessibilidade de titulares ao controle de seus dados. O estudo comparativo entre a LGPD e a ISO 27.701, resultou em um conjunto de recomendações que podem ser apresentadas como auxílio para a tomada de decisão no processo de adequação de proteção de dados de empresas do agronegócio.

**Agradecimentos:** Este trabalho foi desenvolvido com apoio financeiro da CAPES/FAPERGS.

**Palavras-chave:** Proteção de Dados; ISO 27.701; Agronegócio.