FACULDADE BAIANA DE DIREITO

CURSO DE GRADUAÇÃO EM DIREITO

MORENICE ANDRADE SILVA CALDAS DE ALMEIDA

OS IMPACTOS DA RESOLUÇÃO 41 DO COAF DIANTE DA REAL NECESSIDADE DO DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS DOS EMPREGADOS NAS EMPRESAS DE *FACTORING*

Salvador

2024

MORENICE ANDRADE SILVA CALDAS DE ALMEIDA

OS IMPACTOS DA RESOLUÇÃO 41 DO COAF DIANTE DA REAL NECESSIDADE DO DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS DOS EMPREGADOS NAS EMPRESAS DE *FACTORING*

Monografia apresentada ao curso de graduação em Direito, Faculdade Baiana de Direito, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientadora:

Salvador

2024

TERMO DE APROVAÇÃO

MORENICE ANDRADE SILVA CALDAS DE ALMEIDA

OS IMPACTOS DA RESOLUÇÃO 41 DO COAF DIANTE DA REAL NECESSIDADE DO DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS DOS EMPREGADOS NAS EMPRESAS DE *FACTORING*

Monografia aprovada como requisito parcial para obtenção do grau de bacharel em Direito, Faculdade Baiana de Direito, pela seguinte banca examinadora:

Nome:_____

Titulação e instituição:_____

Nome:_____

Titulação e instituição:_____

Nome:_____

Titulação e instituição:_____

Salvador,____/____/2024

RESUMO

A presente monografia tem por objetivo analisar os impactos da Resolução nº 41 do Conselho de Controle de Atividades Financeiras sobre a atividade empresarial do *factoring*, com enfoque particular no tratamento dos dados pessoais de empregados. À luz da Lei Geral de Proteção de Dados e do arcabouço constitucional de tutela da intimidade e privacidade, busca-se compreender em que medida as exigências normativas de prevenção à lavagem de dinheiro e financiamento do terrorismo, impostas às empresas de *factoring*, afetam o direito fundamental à proteção de dados daqueles que nelas laboram. A partir de pesquisa qualitativa e exploratória, pautada em revisão bibliográfica e análise normativa, a investigação pretende elucidar as tensões entre a necessidade de transparência e rastreabilidade de informações, exigidas pelo COAF, e a salvaguarda da privacidade dos sujeitos inseridos nessas relações laborais. Ao final, serão apresentadas conclusões que apontam para a necessidade de um equilíbrio normativo e interpretativo, capaz de compatibilizar o combate a práticas ilícitas com a tutela dos direitos fundamentais dos empregados.

Palavras-chave: Direitos Fundamentais; Factoring; Proteção de Dados; Prevenção à Lavagem de Dinheiro.

ABSTRACT

This monograph aims to analyze the impacts of Resolution No. 41 of the Financial Activities Control Council on the business activity of factoring, with a particular focus on the processing of employees' personal data. In light of the General Data Protection Law and the constitutional framework for the protection of intimacy and privacy, we seek to understand to what extent the regulatory requirements for preventing money laundering and terrorist financing, imposed on factoring companies, affect the law fundamental to the protection of data of those who work in them. Based on qualitative and exploratory research, based on a bibliographical review and normative analysis, the investigation aims to elucidate the tensions between the need for transparency and traceability of information, required by COAF, and the safeguarding of the privacy of subjects involved in these labor relationships. At the end, conclusions will be presented that point to the need for a normative and interpretative balance, capable of making the fight against illegal practices compatible with the protection of employees' fundamental rights.

KEYWORDS: Fundamental Rights; Factoring; Data Protection; Prevention of Money Laundering.

SUMÁRIO

1 INTRODUÇÃO

A sociedade contemporânea é marcada por um fluxo incessante de informações, resultante do desenvolvimento tecnológico e do aumento exponencial do número de transações comerciais e financeiras realizadas diariamente. O ambiente empresarial, ao longo das últimas décadas, tornou-se um ecossistema complexo, interconectado e altamente dinâmico, no qual dados pessoais e profissionais, sejam de clientes, fornecedores ou empregados, circulam em redes de informação e bancos de dados cada vez mais amplos. Neste contexto, o tema da proteção de dados pessoais emerge como uma das questões centrais dos debates jurídicos e regulatórios atuais, demandando maior atenção por parte de legisladores, empresas e operadores do Direito (DE SOUZA; CAMARGO, 2024).

Por outro lado, a realidade econômica brasileira, inserida em um cenário globalizado, é continuamente desafiada pela presença de atividades ilícitas, entre elas a lavagem de dinheiro e o financiamento ao terrorismo. O combate a tais práticas tornou-se prioridade para o Estado brasileiro e seus órgãos de controle, resultando em um arcabouço normativo multifacetado, do qual se destaca a atuação do Conselho de Controle de Atividades Financeiras. A Resolução nº 41 do COAF é um dos instrumentos regulatórios que visam garantir maior transparência e segurança nas operações econômicas, exigindo que as empresas adotem protocolos rigorosos de identificação, análise e comunicação de operações suspeitas (FLORENCIO; MARCO; ZANON, 2018).

A atividade de *factoring*, entendida como a aquisição de direitos creditórios e a prestação de serviços correlatos, ocupa um papel relevante no mercado nacional, sobretudo na concessão de liquidez e suporte a pequenas e médias empresas. As empresas de *factoring* manipulam dados sensíveis, não apenas relacionados aos clientes e fornecedores, mas também relativos a seus próprios empregados, haja vista o intenso fluxo de informação interna necessário para cumprir normativas de compliance e *due diligence*. Esse contexto impõe a necessidade de conciliar exigências regulatórias de combate a ilícitos financeiros com a preservação dos direitos fundamentais dos trabalhadores (FERNANDES; ZANI, 2022).

O direito fundamental à proteção de dados, consagrado no contexto nacional e internacional, adquire concretude a partir da Lei Geral de Proteção de Dados, Lei nº 13.709/2018. Essa norma estabelece princípios, direitos e obrigações para o

tratamento de dados pessoais em qualquer âmbito, público ou privado, e incide também sobre as relações de trabalho. Assim, o empregador, ao tratar dados de seus empregados, deve observar estritamente os parâmetros de licitude, finalidade, necessidade, transparência e segurança, evitando abusos que violem a privacidade e a dignidade da pessoa humana (BRASIL, 2018).

Este trabalho pretende investigar de maneira sistemática e aprofundada os impactos da Resolução nº 41 do COAF na dinâmica interna das empresas de *factoring*, especialmente quanto ao manejo de dados pessoais dos seus empregados. Busca-se compreender se as exigências impostas pela resolução, voltadas a identificar e notificar potenciais ilícitos, podem de alguma maneira tensionar ou conflitar com o direito fundamental à proteção de dados, ao impor a essas empresas a coleta, análise e eventual compartilhamento de informações sensíveis (FLORENCIO; MARCO; ZANON, 2018).

A hipótese central é a de que não se trata de uma colisão incontornável de normas, mas sim de um desafio interpretativo e prático, exigindo a aplicação de critérios como proporcionalidade, razoabilidade e harmonização de princípios constitucionais. Se a prevenção à lavagem de dinheiro é um imperativo para a proteção do sistema econômico e da ordem pública, a tutela da privacidade e a segurança no tratamento de dados são igualmente indispensáveis para assegurar a proteção do indivíduo enquanto trabalhador e titular de direitos fundamentais (FRAZÃO; TEPEDINO; OLIVA, 2019).

Assim, esta monografia parte de uma metodologia qualitativa, sustentada em pesquisa bibliográfica, documental e normativa. Serão analisadas doutrina, jurisprudência, legislações correlatas, bem como relatórios e recomendações de organismos internacionais (MARCONI; LAKATOS, 2011). O objetivo é captar não apenas o arcabouço formal, mas também os argumentos e princípios subjacentes ao debate, fornecendo ao leitor um quadro analítico robusto, capaz de orientar a aplicação do Direito em casos concretos.

O estudo encontra fundamento na própria evolução histórica do Direito do Trabalho e do Direito Empresarial. O tratamento de dados de empregados era outrora um assunto secundário ou restrito a algumas informações administrativas. Hoje, entretanto, à luz da LGPD, se insere em um contexto normativo rigoroso e complexo, no qual o titular dos dados possui direitos subjetivos que devem ser respeitados pelo empregador (TURESSI; DA PONTE, 2022).

Ao se examinar o factoring, é preciso compreender não apenas sua natureza jurídica, mas também a sua operacionalização prática. Esse ramo econômico envolve contato constante com informações sensíveis, seja para análise de crédito, gestão de riscos ou cumprimento de requisitos legais. A imposição de obrigações adicionais pelo COAF – como a identificação de transações suspeitas – pode exigir procedimentos internos que incorporem o exame de registros ou perfis de acesso de empregados, demandando cuidadoso planejamento no desenho dos processos internos (FERNANDES; ZANI, 2022).

Nesse sentido, é importante atentar para o fato de que nem sempre a simples observância literal da Resolução nº 41 do COAF será suficiente para evitar violações ao direito à privacidade. Uma empresa de factoring deverá avaliar se há outros meios menos invasivos de cumprir a resolução, optando por técnicas de minimização de dados, pseudonimização ou controles internos que reduzam o acesso indiscriminado às informações (FERNANDES; ZANI, 2022).

Esta pesquisa segue, portanto, uma linha argumentativa que busca o equilíbrio. Longe de defender a supremacia absoluta de um interesse sobre o outro, propõe-se a leitura constitucionalmente adequada da resolução do COAF, interpretando-a à luz dos valores fundamentais do ordenamento brasileiro. A prevenção à lavagem de dinheiro não é um fim em si mesmo, mas um meio para alcançar um mercado íntegro e confiável. Da mesma forma, a proteção de dados não pode ser vista como obstáculo intransponível às obrigações de compliance, mas sim como um conjunto de diretrizes que orientam a conduta empresarial (FRAZÃO; TEPEDINO; OLIVA, 2019).

O debate não se restringe ao plano teórico. Há impactos práticos evidentes na gestão de recursos humanos e na governança corporativa. Caso as empresas de factoring falhem em equilibrar esses interesses, podem estar expostas a sanções de natureza trabalhista, cível, administrativa e até mesmo penal, além de prejudicar sua imagem e reputação perante o mercado. A conformidade legal, nesse aspecto, torna-se elemento estratégico para a sustentabilidade do negócio (DOS SANTOS, 2020).

Ao longo do trabalho, buscar-se-á mapear a posição da Autoridade Nacional de Proteção de Dados, bem como de outras entidades reguladoras, com vistas a identificar uma possível convergência ou orientações que auxiliem as empresas de factoring na criação de protocolos internos mais eficientes e menos invasivos (SARLET; RUARO, 2021).

Não se pode ignorar que o tema da proteção de dados também ganhou destaque internacional, e o Brasil, ao se alinhar a padrões internacionais de governança da informação, se coloca em posição de dialogar com outras jurisdições. Assim, haverá espaço para comparações pontuais com a União Europeia, referência no assunto, para compreender se a experiência europeia pode fornecer insights para a realidade brasileira (UCHÔA, 2019).

A articulação entre o arcabouço de prevenção à lavagem de dinheiro e o regime de proteção de dados pessoais é, em última análise, um exercício de maturidade institucional. Mostra-se necessário que legisladores, reguladores e operadores do Direito compreendam a complexidade desse equilíbrio e trabalhem em conjunto para aperfeiçoar a normatização e a interpretação jurídica (UCHÔA, 2019).

A presente monografia pretende contribuir para esse debate, oferecendo análise crítica, sólida e fundamentada. Ao fazê-lo, espera-se auxiliar na elaboração de políticas internas por parte das empresas de Factoring, permitindo que essas não apenas cumpram suas obrigações perante o COAF, mas também respeitem a dignidade e os direitos fundamentais de seus empregados (TURESSI; DA PONTE, 2022).

Outro ponto importante é o reconhecimento da existência de possíveis conflitos entre o poder diretivo do empregador e os direitos do empregado. Embora o empregador tenha prerrogativas para organizar e fiscalizar a atividade econômica, incluindo controles sobre o acesso a sistemas, registros de logins e comunicações, tais medidas não podem se converter em um instrumento de vigilância excessiva e desproporcional (DOS SANTOS, 2020).

Assim, a análise aqui empreendida irá detalhar conceitos como minimização de dados, necessidade, adequação e segurança da informação, bem como explorar os remédios jurídicos cabíveis em caso de abusos. A ideia é fornecer um ferramental teórico-prático que permita identificar, na rotina empresarial, quais práticas estão em consonância com o ordenamento e quais devem ser revistas.

Ao final do estudo, longe de esgotar o tema, a monografia objetiva ser um ponto de partida sólido para futuras pesquisas e debates. A complexidade do assunto certamente demandará novas reflexões, especialmente à medida que a tecnologia evolui, e com ela as formas de tratar, analisar e compartilhar dados.

Portanto, a introdução aqui apresentada estabelece o panorama da pesquisa: há uma tensão latente entre as obrigações emanadas pela Resolução nº 41 do COAF

e o direito fundamental à proteção de dados dos empregados nas empresas de Factoring. Cabe a este trabalho não apenas descrever o problema, mas analisar criticamente as possíveis soluções, sempre com olhar atento para os princípios constitucionais, a legislação infraconstitucional e as boas práticas internacionais de proteção de dados (BRAGA, 2023).

Dessa forma, o desafio contemporâneo reside na capacidade das empresas, especialmente aquelas operando em setores economicamente estratégicos como o factoring, de implementarem práticas que conciliem as exigências regulatórias com os direitos fundamentais dos titulares de dados. O setor de factoring, caracterizado por sua atuação como fomentador econômico, depende intensamente do fluxo de informações sensíveis para análise de crédito, gestão de riscos e conformidade regulatória, o que amplia as responsabilidades dessas empresas diante das normativas vigentes. A Resolução nº 41 do COAF, ao estabelecer critérios rigorosos para identificação e comunicação de operações suspeitas, evidencia a necessidade de um aparato de compliance robusto, que deve ser complementado por medidas que assegurem a proteção à privacidade (SARLET; RUARO, 2021).

Nesse contexto, reconhece-se que o direito à proteção de dados, agora consagrado como direito fundamental pela Constituição Federal, impõe às empresas a adoção de políticas que respeitem os princípios da finalidade, necessidade e transparência. Essa análise se faz ainda mais relevante no atual cenário de globalização econômica e digitalização, onde o tratamento de dados pessoais se tornou intrínseco às atividades empresariais e alvo de crescente escrutínio público (DOS SANTOS, 2020).

Ademais, embora a LGPD defina limites claros para o processamento de dados, a Resolução no 41 impõe obrigações que podem ser interpretadas como intrusivas, principalmente em relação à coleta e avaliação de informações confidenciais de funcionários e terceiros. Portanto, o objetivo do trabalho é encontrar maneiras de harmonizar essas normas, sugerindo soluções que assegurem a segurança jurídica das empresas de factoring, sem negligenciar a salvaguarda dos direitos fundamentais dos indivíduos implicados (BRAGA, 2023).

Em conclusão, ressalta-se a relevância de entender o efeito da Resolução no 41 do COAF em um contexto mais abrangente, que englobe tanto a visão normativa quanto a função da governança corporativa na promoção de práticas de negócios éticas e claras. Esta pesquisa não só amplia o debate teórico acerca do equilíbrio entre

segurança econômica e proteção de dados, como também fornece sugestões práticas para a criação de políticas internas eficientes, que tenham como objetivo não só o cumprimento da lei, mas também a promoção da ética, inovação e confiança no cenário empresarial.

Assim, o objetivo é fornecer uma avaliação que não só apoie empresas e profissionais jurídicos a lidar com os desafios trazidos pela implementação simultânea da Resolução no 41 do COAF e da LGPD, mas também promova a discussão acadêmica e institucional sobre as melhores práticas em governança de dados e conformidade regulatória. A meta principal é auxiliar na criação de um ambiente de negócios mais balanceado, onde a luta contra a lavagem de dinheiro e a salvaguarda de dados pessoais possam coexistir de maneira harmônica e eficiente, fomentando o crescimento sustentável das empresas e a salvaguarda dos direitos individuais.

2 O CONTEXTO NORMATIVO DA PREVENÇÃO À LAVAGEM DE DINHEIRO E A RESOLUÇÃO Nº 41 DO COAF

A prevenção à lavagem de dinheiro no Brasil constitui um pilar fundamental na proteção do sistema financeiro e na manutenção da integridade das transações econômicas. Este contexto normativo encontra-se alicerçado na Lei nº 9.613/1998, marco regulatório essencial que tipificou o crime de lavagem de dinheiro e estabeleceu diretrizes para o controle e a repressão dessas práticas ilícitas, com base em recomendações internacionais provenientes do Grupo de Ação Financeira Internacional. A criação do Conselho de Controle de Atividades Financeiras, órgão central no sistema de inteligência financeira brasileiro, resultou da necessidade de monitorar atividades financeiras e identificar operações suspeitas, demonstrando o compromisso do Brasil em combater práticas ilícitas (TURESSI; DA PONTE, 2022).

A Resolução nº 41 do COAF é um desdobramento desse arcabouço normativo, delineando obrigações específicas para setores não diretamente regulados por instituições financeiras tradicionais, como o de *factoring*. Este setor, caracterizado pela cessão de direitos creditórios e serviços correlatos, lida com fluxos financeiros que frequentemente demandam monitoramento cuidadoso para evitar o uso indevido de recursos financeiros. O contexto normativo brasileiro busca, portanto, alinhar-se às recomendações internacionais, adaptando mecanismos de controle ao cenário local sem comprometer a eficiência regulatória (FLORENCIO; MARCO; ZANON, 2018).

As obrigações impostas pela Resolução nº 41 incluem a identificação de clientes, a classificação de riscos e a comunicação de operações suspeitas ao COAF. Essas diretrizes refletem a adoção de uma abordagem baseada em risco, conforme preconizado pelo GAFI, permitindo que as empresas estabeleçam prioridades conforme a probabilidade de ocorrência de atividades ilícitas. No entanto, a aplicação rigorosa dessas normas apresenta desafios, especialmente no que tange à proteção de dados pessoais, uma vez que o tratamento e a análise de informações sensíveis podem entrar em conflito com os direitos fundamentais assegurados pela Constituição Federal e pela Lei Geral de Proteção de Dados (DE SOUZA; CAMARGO, 2024).

A integração normativa entre o combate à lavagem de dinheiro e a proteção de dados requer a harmonização de princípios fundamentais. A LGPD, por exemplo, enfatiza a necessidade, a finalidade e a transparência no tratamento de dados pessoais, enquanto a Resolução nº 41 exige o cumprimento de protocolos de

compliance que frequentemente envolvem a coleta de informações sensíveis. Empresas do setor de *factoring*, ao adotarem essas práticas, precisam equilibrar rigorosamente as exigências legais com os direitos fundamentais de seus empregados e clientes, evitando excessos que possam resultar em sanções regulatórias ou em ações judiciais (FERNANDES; ZANI, 2022).

Historicamente, o Brasil tem buscado se alinhar às melhores práticas internacionais, ratificando tratados e convenções relevantes, como a Convenção de Viena (1988), a Convenção de Palermo (2000) e a Convenção de Mérida (2003). Esses instrumentos influenciaram diretamente a construção do sistema preventivo nacional, promovendo a criação de unidades de inteligência financeira e a implementação de regras de compliance. A integração dessas normas ao ordenamento jurídico brasileiro reforça o compromisso do país em combater a lavagem de dinheiro, ao mesmo tempo que desafia as empresas a adequar suas práticas internas para cumprir tanto as exigências internacionais quanto as legislações locais (FLORENCIO; MARCO; ZANON, 2018).

A Resolução nº 41 do COAF representa, assim, um marco na regulamentação de atividades não bancárias, especialmente no contexto do *factoring*, ao impor a responsabilidade de identificar e comunicar operações que apresentem indícios de ilicitude. No entanto, esse controle rigoroso não pode ser dissociado das garantias constitucionais que asseguram a proteção da intimidade, da privacidade e dos dados pessoais. As tensões normativas que surgem dessa dualidade exigem soluções que considerem a proporcionalidade e a razoabilidade, especialmente diante da crescente digitalização e globalização das transações financeiras (CESPEDES, 2018).

Por fim, a harmonização entre a Resolução nº 41 e a LGPD não é apenas uma necessidade regulatória, mas também uma oportunidade para promover a governança corporativa e fortalecer a confiança nas relações de trabalho. Empresas que adotam práticas responsáveis de tratamento de dados, conciliando as exigências de compliance com os direitos fundamentais, não apenas mitigam riscos legais, mas também contribuem para a construção de um sistema financeiro mais ético e transparente. Esse equilíbrio normativo é, portanto, essencial para consolidar a posição do Brasil como um ator confiável no combate à lavagem de dinheiro, ao mesmo tempo em que protege os direitos fundamentais dos indivíduos (DE ALMEIDA; NETO, 2023).

2.1 O SURGIMENTO DO ARCABOUÇO NORMATIVO ANTILAVAGEM NO BRASIL

A legislação de combate à lavagem de dinheiro no Brasil nasceu em um momento de forte integração global no combate ao crime organizado. A promulgação da Lei nº 9.613/1998 foi um marco importante, representando a adesão do Brasil às recomendações do Grupo de Ação Financeira Internacional, entidade que estabelece padrões globais para o combate à lavagem de dinheiro e ao financiamento do terrorismo (TURESSI; DA PONTE, 2022).

Essa lei introduziu um novo regime jurídico, estabelecendo tanto a tipificação penal da lavagem de capitais quanto mecanismos administrativos e regulatórios para prevenir e reprimir essas práticas. Um dos pilares desse sistema foi a criação do Conselho de Controle de Atividades Financeiras, órgão encarregado de receber, examinar e identificar operações suspeitas, além de estabelecer normativas para setores considerados sensíveis (TURESSI; DA PONTE, 2022).

Desde sua criação, o COAF tem desempenhado um papel fundamental no fortalecimento da integridade do sistema financeiro brasileiro, monitorando transações atípicas e impondo padrões de diligência para diversos segmentos econômicos. Sua atuação é particularmente relevante em setores como o de factoring, onde o fluxo de recursos e informações exige atenção redobrada para prevenir o uso indevido do sistema econômico (FLORENCIO; MARCO; ZANON, 2018).

A evolução normativa que culminou na Resolução nº 41 do COAF refletiu a necessidade de ampliar os mecanismos de controle em setores não regulados por órgãos financeiros tradicionais. Essa resolução é um exemplo claro de como o arcabouço legal brasileiro vem se adaptando para enfrentar práticas ilícitas que utilizam lacunas regulatórias para dissimular recursos de origem criminosa (FLORENCIO; MARCO; ZANON, 2018).

Sobre o marco regulatório, a doutrina assevera:

> Desse modo, políticas públicas, a partir de uma perspectiva jurídica, podem ser compreendidas como ações governamentais decorrentes de um processo decisório regulado cujo objetivo é organizar esforços para a realização de objetivos socialmente importantes. Frise-se que, os marcos regulatórios não se confundem com as políticas públicas em si, de modo que o conjunto de leis de determinado ramo do direito representam apenas uma das expressões da política pública, a qual apresenta também outras medidas administrativo-financeiras. Diante de tais definições, verifica-se que um sistema de políticas públicas de prevenção e combate à lavagem de dinheiro implica em uma rede

> complexa de ações governamentais resultantes de um intrincado processo decisório regulado, o qual perpassa diversas dimensões e tem como uma das expressões de seu programa a edição de diplomas legais antilavagem. Particularmente em relação ao Brasil, verifica-se que a primeira influência externa que veio a corroborar para a construção do referido sistema data de 1991, quando o país se tornou signatário da Convenção de Viena, editada em 1988,incorporando suas normas ao direito pátrio por meio do Decreto nº 154/91. A referida convenção, de forma pioneira, ao tratar do tráfico ilícito de entorpecentes e substâncias psicotrópicas, apresentou uma definição sobre o crime de lavagem de dinheiro, hoje aceita mundialmente. Saliente-se que todos os países que ratificassem o tratado se obrigavam a criar um tipo penal visando à responsabilização pela ocultação de bens ou valores oriundos do tráfico internacional de drogas. Ainda, no tocante às normas internacionais que vieram a influenciar o tratamento do crime de lavagem de dinheiro no Brasil destacam-se a Convenção de Palermo, de 2000, ratificada pelo Brasil em 2004; e a Convenção de Mérida, de 2003, ratificada pelo Brasil em 2006. Note-se que a primeira apresentou conceitos relevantes sobre o crime organizado e fez referências à lavagem de dinheiro, em especial no que tange aos mecanismos de prevenção, além de trazer outros tipos penais que poderiam ser considerados crimes antecedentes, ampliando o objeto material do crime de lavagem e foi incorporada ao direito brasileiro pelo Decreto nº5015/04. A segunda, incorporada ao direito nacional por meio do Decreto nº 5687/06, embora tenha como escopo o combate à corrupção, apresentou pontos específicos relacionados à lavagem de dinheiro, quais sejam: necessidade de cooperação internacional para investigação; ênfase na regulamentação e fiscalização das instituições financeiras, bem como de valores e títulos que cruzam as fronteiras (FLORENCIO; MARCO; ZANON, 2018, p. 71 e 72).

Neste trecho, o autor, ao abordar a natureza das políticas públicas como instrumentos organizados para alcançar objetivos de relevância social, destaca sua estrutura enquanto ações governamentais reguladas e fruto de um processo decisório complexo. Nesse contexto, diferencia o papel dos marcos regulatórios, os quais, embora sejam uma das manifestações das políticas públicas, não se confundem com elas. Estes marcos representam um conjunto normativo de caráter jurídico, enquanto as políticas públicas abrangem uma ampla gama de medidas, incluindo ações administrativas e financeiras (FLORENCIO; MARCO; ZANON, 2018).

Esta diferenciação é necessária para compreensão do instituto, já que campo da prevenção e combate à lavagem de dinheiro, tal sistemática é caracterizada por uma rede integrada de ações governamentais que extrapola a simples edição de normas legais. No caso brasileiro, a base desse sistema foi influenciada por tratados internacionais, como a Convenção de Viena de 1988, que trouxe a primeira definição amplamente aceita do crime de lavagem de dinheiro, obrigando os Estados signatários a criarem tipos penais para responsabilizar aqueles que ocultassem bens ou valores oriundos de tráfico de drogas. Essa convenção, incorporada ao ordenamento jurídico

brasileiro pelo Decreto nº 154/91, marcou o início do alinhamento do país às práticas internacionais (FLORENCIO; MARCO; ZANON, 2018).

Outros importantes marcos internacionais, como a Convenção de Palermo e a Convenção de Mérida, complementaram e expandiram a abordagem brasileira. A primeira, incorporada pelo Decreto nº 5015/04, além de tratar do crime organizado, ampliou os mecanismos de prevenção à lavagem de dinheiro, destacando a importância da identificação de crimes antecedentes. Já a segunda, por meio do Decreto nº 5687/06, enfatizou o combate à corrupção e reforçou a necessidade de cooperação internacional, bem como a regulamentação e fiscalização das atividades financeiras e de transações transfronteiriças (FLORENCIO; MARCO; ZANON, 2018).

No que tange a eficácia das normas antilavagem, vejamos:

> É importante destacar a lógica que move essa normatização internacional de proteção integral aos direitos humanos, aqui incluídas as decisões da Corte Interamericana de Direitos Humanos (CIDH), como fontes do Direito, da qual a segura leitura da Lei nº 9.613/1998 não pode se distanciar: de um lado, respeito aos direitos e garantias individuais da pessoa acusada, mas, de outro, máxima efetividade na apuração do ilícito e atribuição de responsabilidades, sendo clara a ideia da assunção, pelos países signatários, de verdadeiras obrigações estatais de garantia da apuração do delito e, no limite, de que não há efetiva tutela de direitos fundamentais, de forma integral, sem a existência e aplicação de leis penais que confiram real proteção ao bem jurídico, de forma proporcional, vedando-se excessos, mas distanciando-se de uma proteção penal insuficiente. (TURESSI; DA PONTE, 2022, p. 319).

No entanto, o surgimento desse regime rigoroso de prevenção à lavagem de dinheiro trouxe consigo novos desafios, incluindo o impacto sobre os direitos fundamentais, como a privacidade e a proteção de dados pessoais. As obrigações impostas pelo COAF às empresas obrigadas incluem a coleta, o armazenamento e a análise de informações sensíveis, levantando questões importantes sobre os limites e as condições para o tratamento de tais dados (TURESSI; DA PONTE, 2018).

2.2 A RELAÇÃO ENTRE AS RECOMENDAÇÕES INTERNACIONAIS E O CONTEXTO NACIONAL

O Brasil, como membro ativo do GAFI, tem alinhado sua legislação às melhores práticas internacionais. Esse alinhamento é essencial para garantir a credibilidade do país no cenário global e para proteger sua economia contra os impactos negativos da lavagem de dinheiro. A implementação de resoluções como a nº 41 do COAF atende

a essas demandas, mas também gera implicações para o ambiente regulatório interno (CESPEDES, 2018).

No que diz respeito ao GAFI é importante trazer:

> O GAFI estabelece padrões de prevenção daquelas atividades ilegais e dos danos que causam à sociedade: as conhecidas 40 Recomendações elaboradas em 1990, em cuja adoção a abordagem baseada em risco é uma diretiva fundamental, sendo este o escopo da Recomendação 1 (GAFI, 2012). As Recomendações originais do GAFI foram revisadas várias vezes, a fim de refletirem um ambiente de PLD/FTP em constante mudança (NEWBURY, 2017, p. 2). O GAFI também conduz as chamadas avaliações mútuas16 sobre seus países e jurisdições membros (Anexo 2), a fim de gerar vontade política para a promoção das reformas legislativas e regulatórias domésticas necessárias à adoção de suas Recomendações. As avaliações são realizadas sob dois componentes: a) efetividade (incorporada à metodologia em 2013) – em que são exigidas evidências capazes de demonstrar o funcionamento das medidas adotadas na PLD/FTP e a geração dos resultados desejados; e b) cumprimento técnico – aborda o requerido nas 40 Recomendações, especialmente quanto aos instrumentos legais e institucionais relevantes, assim como poderes e procedimentos das autoridades competentes (LARRUBIA, 2023, p. 17 e 18).

Para atender as recomendações do GAFI, a Resolução nº 41 do COAF estabelece um conjunto de obrigações que se aplicam a pessoas jurídicas não reguladas por órgãos específicos. Essas obrigações incluem a necessidade de identificar clientes, classificar riscos, registrar operações e comunicar transações suspeitas. No setor de factoring, essas exigências são particularmente relevantes, devido ao volume de informações financeiras e pessoais tratadas nessas operações (DA SILVA NETO et al., 2022).

Quanto ao Grupo de Ação Financeira para a América do Sul, destacamos:

> O GAFISUD19 (*Financial Action Task Force of South America Against Money Laundering*) consiste numa projeção regional do GAFI para a América do Sul, com sede em Buenos Aires, agregando 10 membros (Argentina, Bolívia, Brasil, Chile, Colômbia, Equador, México, Paraguai, Peru e Uruguai), contando ainda com a participação da OEA – Organização dos Estados Americanos, CICAD – Comissão Interamericana contra o Abuso de Drogas), dos países observadores (França, Alemanha, Portugal, Espanha e Estados Unidos) e das organizações observadoras (Grupo de *Egmont*, BIRD – Banco Interamericano de Desenvolvimento, Nações Unidas e Banco Mundial). Sua criação se deu em 8 de dezembro de 2000, em Cartagena, Colômbia por meio de um Memorando de Entendimento pelos representantes dos governos de nove países sul-americanos, em atendimento a esforços de combate à lavagem de dinheiro na América do Sul (ANSELMO, 2010, p. 366).

A relação entre as recomendações internacionais e o contexto normativo brasileiro é marcada por um equilíbrio delicado entre transparência e privacidade. Enquanto as exigências de identificação e rastreamento de operações buscam

garantir a integridade do sistema financeiro, elas também exigem cuidados para evitar a exposição indevida de dados sensíveis (DE SOUZA; CAMARGO, 2024).

A experiência internacional demonstra que a eficácia das normas antilavagem de dinheiro depende da colaboração entre os diferentes atores envolvidos, incluindo empresas, reguladores e autoridades judiciais. No Brasil, essa colaboração tem sido fortalecida pela atuação do COAF e pela integração de suas políticas com as normas da LGPD, que estabelecem diretrizes claras para o tratamento de dados pessoais (FERNANDES; ZANI, 2022).

Diante das transformações da modernidade e do aumento das interações globais, a lavagem de dinheiro se consolida como um fenômeno transnacional de extrema relevância, impulsionando a adoção de convenções e mecanismos de cooperação internacional voltados à sua prevenção e repressão, senão vejamos:

> Conforme lições do sociólogo alemão Ulrich Beck, a sociedade contemporânea é fruto de transformações que são consequências não planejadas da própria modernidade, a qual acabou se modificando. A primeira modernidade –simples, linear e industrial –indica as sociedades embasadas nos Estados-Nação, nas quais as relações, redes sociais e comunidades eram entendidas em um sentido, essencialmente, territorial. Noções como controlabilidade, certeza e segurança são fundamentais na primeira modernidade e isso tanto no sentido técnico-científico quanto político-jurídico (Beck, 2002, p. 1-3 e 115). O crescimento econômico e tecnológico contínuo, entretanto, não mais se contêm nas fronteiras estatais, porque cria possibilidades novas para os indivíduos e gera novas formas de risco. Surge, então, a segunda modernidade, na qual cinco processos inter-relacionados ocorrem: a globalização, a individualização, a revolução dos gêneros, o subemprego e os riscos globais (como a crise ecológica e o colapso dos mercados financeiros globais) (Beck, 2002, p. 2). Os movimentos de integração supranacional propiciados, por um lado, pela consolidação do liberalismo econômico no âmbito dos países ocidentais e, por outro, pelo avanço das novas tecnologias, deram ensejo a um cenário político-social marcado pela instabilidade. A lógica da produção industrial acompanha um universo de perigos, observa Beck (1998, p. 42), assim como a evolução tecnológica propiciou uma verdadeira revolução nas comunicações e, por conseguinte, nos mais diferentes mercados, entre eles o financeiro, estruturante do modelo econômico liberal sobre o qual está ancorada a sociedade ocidental. Nesse cenário, a lavagem de dinheiro transnacional exsurge como uma grande geradora de riscos na sociedade pós-industrial. Com a evolução da tecnologia e o crescente aumento do fluxo de pessoas, bens e valores entre países, os atos de lavagem de dinheiro têm se espalhado para fora das fronteiras dos países, mediante sucessivas e complexas transações financeiras ou empresariais, de modo a afastar as autoridades nacionais de sua persecução e garantir a fruição do produto e do proveito de atividades criminosas. Essa prática começou a gerar preocupação no mundo, e os Estados e os organismos internacionais começaram a discutir o assunto e a celebrar diversos tratados bilaterais e multilaterais prevendo formas efetivas de cooperação jurídica internacional para a prevenção e o enfrentamento de crimes de lavagem de dinheiro transnacional.No plano internacional, Convenção das Nações Unidas contra o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas (Convenção de Viena), de 19.12.1988, foi a primeira a prevê-lo expressamente (artigo 3º).

> Posteriormente, a Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), de 15.11.2000, também fez referência ao crime de lavagem de dinheiro e previu novos tipos penais que pudessem figurar como crimes antecedentes. A Convenção das Nações Unidas contra a Corrupção (Convenção de Mérida), de 31.10.2003, por sua vez, dispôs sobre uma série de medidas para prevenção e repressão da lavagem de dinheiro3.No âmbito do sistema preventivo, a Convenção das Nações Unidas contra o Crime Organizado Transnacional introduziu uma inovação ao estipular a criação, pelos Estados signatários (artigo 7º, 1, b), de um "serviço de informação financeira", que deve funcionar como um centro nacional para coleta, análise e disseminação de informações sobre possíveis atividades de lavagem de dinheiro. Portanto, é identificada aqui a obrigação desses Estados de estabelecer unidades de investigação de crimes de lavagem, conhecidas como Unidades de Inteligência Financeira (UIF). O sistema preventivo também é fortalecido pela criação de regras de conformidade (*compliance*), conforme estabelecido no artigo 7º, 1 da Convenção (DE SOUZA; CAMARGO, 2024, p. 84 e 85).

A sociedade contemporânea, fruto de transformações da modernidade, caracteriza-se pela globalização, individualização e riscos globais, especialmente no âmbito financeiro, marcando uma nova era de incertezas e desafios. Nesse cenário, a lavagem de dinheiro emerge como uma prática transnacional que aproveita os avanços tecnológicos e a integração econômica para se desenvolver além das fronteiras estatais, dificultando a atuação das autoridades nacionais (DE SOUZA; CAMARGO, 2024).

A resposta internacional a essa problemática incluiu a celebração de convenções como a de Viena, Palermo e Mérida, que estabeleceram medidas para a prevenção e repressão à lavagem de dinheiro, incluindo a criação de Unidades de Inteligência Financeira e a implementação de sistemas de compliance. Tais medidas buscam fortalecer a cooperação internacional e garantir mecanismos efetivos de controle e combate a essas práticas ilícitas, fundamentais para a estabilidade econômica e social na sociedade globalizada (DE SOUZA; CAMARGO, 2024).

Sobre o tema, a doutrina assevera:

> Da mesma forma, o seguro manejo da Lei nº 9.613/1998, no plano jurisprudencial, também não pode se dar ao arrepio da normativa internacional que, combatendo o surgimento de paraísos jurídico-penais, busca enfrentar o fenômeno global da lavagem de dinheiro de maneira uniforme, notadamente da Convenção das Nações Unidas contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas (Convenção de Viena), e, antes disso, das ações afirmativas (positivas) dos direitos humanos extraídas de outros importantes textos internacionais vinculantes, no exercício de um verdadeiro e necessário controle da convencionalidade das leis. De fato, para além do apoio nos Tratados, Convenções e Diretivas internacionais que disciplinam especificamente a lavagem de dinheiro, a aplicação da Lei nº 9.613/1998 também deve se fundar na existência de um verdadeiro sistema interamericano de proteção aos direitos humanos, com

> especial destaque para a Carta da Organização dos Estados Americanos (OEA), de 1948, conhecida como Carta de Bogotá, e para a Declaração Americana dos Direitos e Deveres do Homem (DADH), que culminou com a Convenção Americana dos Direitos Humanos (CADH), de 1969 (Pacto de São José da Costa Rica) , extraindo-se dessa normativa internacional verdadeiras obrigações processuais penais positivas, identificadas por Fischer e Pereira (2019, p. 93) no dever assumido pelos Estados partes de adotarem todas as medidas e providências necessárias para a apuração de ilícitos penais e responsabilização de seus autores, de forma vinculante, a fim de tornar o sistema jurídico-penal célere, eficiente e eficaz (TURESSI; DA PONTE, 2022, p. 319).

Contudo, é preciso reconhecer que o cumprimento das obrigações regulatórias por parte das empresas de factoring exige investimentos significativos em tecnologia, treinamento e auditorias internas. Essas exigências muitas vezes geram custos adicionais, mas também contribuem para a construção de um ambiente de negócios mais seguro e confiável.

2.3 HARMONIZAÇÃO ENTRE DIFERENTES NORMAS E IMPLICAÇÕES PRÁTICAS

A coexistência entre a Resolução nº 41 do COAF e outras normas relevantes, como a LGPD, apresenta desafios interpretativos e práticos. Por um lado, há uma pressão para que as empresas atendam às exigências de prevenção à lavagem de dinheiro. Por outro, é necessário respeitar os limites impostos pela legislação de proteção de dados, que busca evitar o uso excessivo ou inadequado de informações pessoais (FERNANDES; ZANI, 2022).

Essa dualidade normativa exige que as empresas adotem uma abordagem sistêmica para o compliance, considerando não apenas os requisitos específicos de cada norma, mas também os princípios constitucionais que garantem a dignidade e a privacidade dos indivíduos. No caso das empresas de factoring, isso significa desenvolver políticas internas que conciliem as demandas regulatórias com os direitos dos empregados (GOMES, 2019).

Um exemplo prático desse desafio está na coleta e análise de dados de empregados envolvidos em operações sensíveis. Embora essas práticas sejam necessárias para atender às exigências do COAF, elas devem ser realizadas de forma proporcional, garantindo que os dados sejam utilizados apenas para os fins previstos e com medidas adequadas de proteção (GOMES, 2019).

As implicações práticas dessa harmonização incluem a necessidade de revisar continuamente as políticas internas das empresas de factoring, garantindo que estejam alinhadas tanto às exigências do COAF quanto aos princípios da LGPD. Isso pode envolver desde a implementação de sistemas de anonimização de dados até a realização de treinamentos específicos sobre proteção de dados (FERNANDES; ZANI, 2022).

Ao discutir sobre o tema, Oliveira (2016, 423) aduz:

> Em nosso país, por intermédio da Lei n° 9.613, de 3 de março de 1998, foi autorizada a criação do Conselho de Controle de Atividades Financeiras , unidade de inteligência financeira do Brasil, subordinada ao Ministério da Fazenda, cujo objetivo institucional consiste em recepcionar, analisar e retransmitir (na forma de relatórios de inteligência), aos órgãos públicos competentes para investigação e persecução criminal, informações estratégicas que configurem indícios de cometimento do crime de lavagem de dinheiro. Desse modo, a implantação da política de prevenção e repressão aos mecanismos de lavagem de dinheiro, no Brasil, depende da colaboração de entidades públicas e particulares, com vistas a que auxiliem nesta tarefa, mediante a comunicação de atitudes suspeitas, principalmente em atividades relacionadas a bancos, corretores, comerciantes de bens de alto valor e atividades semelhantes. Em razão da promulgação da Lei n°12.683, de 9 de julho de 2012, a discussão em torno do delito de lavagem de dinheiro auferiu novos contornos, uma vez que o referido diploma normativo pretende tornar mais eficaz a persecução penal para esse tipo de atividade delitiva. O Coaf, por sua vez, depois da entrada em vigor da referida lei, emitiu resoluções destinadas a regulamentar a colaboração de pessoas físicas e jurídicas no combate à lavagem de dinheiro, especialmente relacionadas às atividades de comercialização de joias, pedras e metais preciosos, distribuição de dinheiro e de quaisquer bens, na exploração de atividades de loterias e relativas a empresas que atuem no ramo de fomento comercial. As resoluções impõem a obrigação de comunicar ao Coaf as operações que, consideradas as partes e o modo de realização, possam configurar sérios indícios de lavagem de dinheiro. Tais diplomas, no entanto, não definem, de forma objetiva e clara, em que consistem tais indícios. Constam, também, determinações de que os procedimentos de apuração devem ser recorrentes, inclusive com a realização de outras diligências não previstas nas resoluções, o que enseja grande insegurança jurídica para as pessoas obrigadas, nos termos da legislação.

Outro ponto relevante é o papel das autoridades reguladoras na mediação dessas questões. A ANPD, em particular, pode contribuir para esclarecer como as empresas devem interpretar e aplicar as normas de proteção de dados no contexto do compliance regulatório. Esse diálogo entre reguladores é essencial para promover maior segurança jurídica e eficiência no cumprimento das obrigações (DE ALMEIDA; NETO, 2023).

No plano internacional, há exemplos que podem servir de inspiração para o Brasil. A União Europeia, por exemplo, desenvolveu diretrizes específicas para

setores regulados, permitindo que as empresas atendam às exigências de compliance sem comprometer os direitos fundamentais. A adoção de práticas semelhantes no Brasil pode ajudar a superar os desafios enfrentados pelas empresas de Factoring (CARLINI, 2024).

Ainda sobre a experiencia da União Europeia é possível verificar que:

> Os desenvolvimentos recentes da União Europeia demonstram a prioridade conferida à matéria penal na construção comum, com o surgimento de instrumentos normativos que impactam diretamente as legislações penais dos Estados-membros. E tal situação é fundamental para consolidar o espaço comum europeu: além da integração econômica, há objetivos mais vastos que demandam um enquadramento sancionatório que, por vezes, necessita ser penal. Assim, nos últimos anos, a independência do direito penal frente ao direito europeu tem-se relativizado. Evidencia-se que o primeiro não ficou imune à influência do segundo, mesmo a matéria penal sendo considerada manifestação última da soberania nacional, uma vez que cada vez mais é observado uma cooperação internacional e europeia no âmbito político-criminal. Embora a UE não detenha uma competência penal em si, certo é que determinadas incriminações nacionais e a utilização de instrumentos sancionatórios penais evidenciam uma realidade dos EM em unir esforços para a proteção dos interesses em causa no espaço comum (UCHÔA, 2019, p. 17).

É importante destacar que a harmonização entre diferentes normas não é apenas uma questão jurídica, mas também uma oportunidade para promover a inovação e a ética nas práticas empresariais. Empresas que tratam dados de forma responsável e eficiente podem se destacar no mercado, fortalecendo sua reputação e atraindo investidores (FERNANDES; ZANI, 2022).

A Resolução nº 41 do COAF, ao mesmo tempo em que impõe desafios significativos para as empresas, também representa uma oportunidade para aprimorar a governança corporativa. Quando interpretada e aplicada de forma equilibrada, ela pode contribuir para a construção de um ambiente de negócios mais transparente e ético (FERNADES; ZANI, 2022).

Quanto a atuação do COAF com outras normativas regulatórias, Cespedes (2021, p. 84) aduz:

> Em 2018, o Coaf também atuou com outros órgãos do Estado na negociação para o encaminhamento do Projeto de Lei 10.431, de 18 de junho de 2018, que visa aprimorar as medidas de congelamento de bens ligados a terroristas em cumprimento às resoluções do Conselho de Segurança das Nações Unidas. A atuação do órgão no aperfeiçoamento da legislação sobre o assunto é importante na medida em que ele possui informações de inteligência capazes de fazer diferença na formulação de medidas legislativas e judiciais mais efetivas no combate à lavagem de dinheiro. O PL 10.431/2018 se transformou na Lei 13.810, de 8 de 2019.

O contexto normativo da prevenção à lavagem de dinheiro no Brasil, embora complexo, oferece possibilidades concretas de harmonização com os direitos previstos na LGPD. O sucesso dessa integração depende, em grande medida, da atuação conjunta de empresas, reguladores e sociedade civil, na busca por soluções que conciliem eficiência regulatória e respeito aos direitos fundamentais (FERNADES; ZANI, 2022).

3 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS E SUA INCORPORAÇÃO AO ORDENAMENTO BRASILEIRO

Diante a globalização e o avanço desenfreado da tecnologia, a temática envolvendo a segurança das informações pessoais e corporativas vem se tornando cada vez mais questionada. Ataques *hacker's* e situações nas quais empresas utilizam dados pessoais de clientes sem o consentimento destes, vem se tornando bastante frequentes não só em território nacional, mas em todo o planeta (FINKELSTEIN; FINKELSTEIN, 2019; DINIZ, 1982).

Na atual fase do avanço da tecnologia, com as redes sociais, a informação compreende em um dos maiores bens aos indivíduos, de tal maneira merece ser devidamente preservada e protegida. O direito à privacidade, constitucionalmente previsto nos incisos X, XI e XII, do artigo 5º da Constituição Federal de 1988, tem uma importância tão vasta que serve de pilar para a proteção do direito de personalidade, visando preservar e garantir o desenvolvimento do indivíduo, evitando situações que possam atingir sua identidade intelectual, física e moral (FINKELSTEIN; FINKELSTEIN, 2019; DINIZ, 1982).

Levando em conta a omissão legislativa em torno do assunto e da grande relevância em torno da proteção aos dados pessoais, no dia 14 de agosto de 2018 foi promulgada a Lei nº 13.709, intitulada como Lei Geral de Proteção dos Dados Pessoais ou Marco Civil da Internet, a qual regulamenta acerca de medidas preventivas, proativas na manutenção e também privacidade dos dados de terceiros (BRASIL, 2018).

A referida lei compreende em um marco histórico na regulamentação acerca do tratamento de dados pessoais no território nacional, estando disponíveis tanto em meio físico quanto em meios digitais. A regulamentação modifica completamente a maneira como as empresas devem coletar, armazenar e disponibilizar informações referentes a seus usuários/clientes (FRAZÃO; TEPEDINO; OLIVA, 2019).

Depois de publicada, o Conselho Nacional de Justiça veio a editar a Recomendação 73/2020, com o objetivo de orientar os órgãos do Poder Judiciário a se adequarem às normas da LGPD (FRAZÃO; TEPEDINO; OLIVA, 2019).

Em seu artigo 1º, a Lei prevê que o referido ordenamento objetiva tratar a respeito dos dados pessoais, inclusive sob os meios digitais, tanto por pessoa natural quanto jurídica de direito privado ou público, com respaldo aos direitos fundamentais

constitucionalmente previstos, como a liberdade, a privacidade e a livre personalidade da pessoa natural (BRASIL, 2018).

Em continuação a referida legislação dispõe que as informações nela contidas são de interesse coletivo e deverão ser seguidas pela União, Estados, Distrito Federal e Municípios. A título de fundamentos, a LGPD prevê além do direito à liberdade e privacidade, a autodeterminação informativa, além da liberdade expressão, informação, comunicação e opinião, inviolabilidade da intimidade, honra e imagem, desenvolvimento da economia, tecnologia e também da informação, liberdade à iniciativa, à concorrência e a defesa do consumidor, e, aos direitos humanos (BRASIL, 2018).

Tratando-se de uma situação hipotética que dispõe acerca da realização de uma operação de tratamento de dados por uma pessoa jurídica de direito público, através de um meio eletrônico, e de modo que os dados ou informações pessoais consistidas nos objetos da operação, que tenham sido coletados em território nacional, mas que encontram-se em outro país, é possível enaltecer que este contexto encontra-se previsto na Lei nº13.709/2018 (Lei Geral de Proteção a Dados Pessoais) (BRASIL, 2018).

Mais especificamente, em seu artigo 3º, inciso III, a LGPD prevê que a Lei estará cabível a qualquer operação de tratamento que tenha sido realizada por pessoa natural ou por pessoa jurídica, seja de direito público ou privado, independente do meio, do país de sua sede ou do país onde estejam localizados os dados, sob a observação de três hipótese (BRASIL, 2018).

A primeira hipótese obriga que a operação de tratamento seja realizada no território nacional, até então, a situação hipotética se enquadra ao respaldo. A segunda hipótese prevê que a atividade de tratamento objetive a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território, a situação hipotética condiciona a uma atividade de tratamento sob a finalidade de tratar dados de pessoas localizadas em território nacional, se adequando à legislação. Por fim, o último inciso prevê a hipótese que os dados pessoais, que compreendem nos objetos da operação de tratamento, tenham sido coletados em território nacional, mais uma vez adequando a situação hipotética à proteção do respaldo legal (FRAZÃO; TEPEDINO; OLIVA, 2019).

A legislação em questão dispõe sobre a diferenciação entre alguns termos de importante relevância no estudo sobre a proteção aos dados. Para a Lei, o dado

pessoal está condicionado à informação referente à pessoa natural identificada ou indentificável (art. 5º, I, da LGPD) (BRASIL, 2018).

Já o dado pessoas sensível está condicionado àqueles dados que dispõem de informações pessoais dos indivíduos, que abordem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou até mesmo político, no que compreende à saúde ou à vida sexual, dado genérico ou biométrico, quando circulado a uma pessoa natural (art. 5º, inciso II). O banco de dados compreende no conjunto de dados pessoais (art. 5º, inciso III) (BRASIL, 2018).

A importância em torno dos dados já justifica a relevância em torno da implementação da referida Lei no ordenamento jurídico brasileiro. A proteção à dados pessoais, além de pregar pelo respeito a integridade, à dignidade humana e à honra, ainda é responsável por evitar a ocorrência de fraudes, uma vez que, infelizmente ataques hacker's e a utilização de dados pessoais por empresas, sem o consentimento dos indivíduos vem se tornando situações bastante frequentes no cotidiano não só do brasileiro, mas de toda a população mundial. Com o respaldo legal, os criminosos poderão ser devidamente identificados e punidos pelas condutas ilícitas as quais vieram a cometer (FRAZÃO; TEPEDINO; OLIVA, 2019).

3.1 FUNDAMENTAÇÃO CONSTITUCIONAL E O RECONHECIMENTO DA PROTEÇÃO DE DADOS

A proteção de dados pessoais, embora tenha ganhado destaque recente no ordenamento jurídico brasileiro, está enraizada nos princípios constitucionais de 1988. A Constituição Federal consagra, em seu artigo 5º, diversos direitos fundamentais que asseguram a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Esses preceitos fornecem a base para a garantia da proteção de dados, mesmo antes da existência de uma legislação específica (BRASIL, 1988).

Com a promulgação da Emenda Constitucional nº 115/2022, o direito à proteção de dados pessoais foi elevado ao status de direito fundamental autônomo, consagrado no inciso LXXIX do artigo 5º:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se 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:

> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.
> § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.
> § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.
> § 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais.
> § 4º O Brasil se submete à jurisdição de Tribunal Penal Internacional a cuja criação tenha manifestado adesão (BRASIL, 1988).

Essa emenda reflete a evolução das necessidades sociais e tecnológicas, reconhecendo a importância de salvaguardar informações pessoais em um mundo interconectado e digital (BRASIL, 1988).

A inclusão do direito à proteção de dados na Constituição fortalece as garantias individuais, ao mesmo tempo em que impõe limites à atuação do Estado e das empresas. Essa evolução demonstra a relevância do tema na agenda política e jurídica, alinhando o Brasil a tendências internacionais e ampliando o alcance das garantias fundamentais (SARLET, 2020).

O avanço da digitalização trouxe inúmeros impactos para todos os âmbitos da sociedade, especialmente na proteção de dados. Por essa razão é importante destacar:

> O avanço da digitalização (que, todavia, não se restringe ao problema da proteção de dados, como sabido), de certo modo, tem impactado não apenas o direito positivo, ou seja, a produção legislativa e normativa em geral, mas também “contaminado” a dogmática e a metodologia jurídicas, ademais de estender os seus tentáculos para os domínios da administração pública e labor dos Tribunais, os quais, cada vez mais, são compelidos a achar soluções criativas e suficientes a dar conta dos problemas concretos que lhes são submetidos. Assim, não é à toa que já há tempos se fala em um processo de digitalização dos direitos fundamentais (ou de uma dimensão digital dos direitos fundamentais), bem como de uma digitalização do próprio direito4 (daí se falar também de um direito digital), o que, à evidência, inclui – mas de longe não só isso! – o reconhecimento gradual, na esfera constitucional e no âmbito do direito internacional, de um direito humano e fundamental à proteção de dados, assim como de outros princípios, direitos (e deveres) conexos, mas também de uma releitura de direitos fundamentais “clássicos”. Outrossim, nada obstante o problema da proteção dos dados não se restrinja aos dados armazenados, processados e transmitidos na esfera da informática e por meios digitais, pois em princípio ela alcança a proteção de todo e qualquer dado pessoal independentemente do local (banco de dados) e do modo pelo qual é armazenado, cada vez mais os dados disponíveis são inseridos em bancos de dados informatizados. A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social.6 É por tais razões que se pode acompanhar o entendimento de Carlos Alberto Molinaro e

> Gabrielle Bezerra S. Sarlet, de que a proteção de dados pessoais – e o reconhecimento de um direito fundamental correspondente –, de certo modo, “confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes” (SARLET, 2020, p. 180 e 181).

No contexto das relações de trabalho, os princípios constitucionais relacionados à proteção da dignidade da pessoa humana (art. 1º, III) e ao valor social do trabalho (art. 1º, IV) complementam a proteção à privacidade. Esses princípios formam a base para a interpretação de normas que visam equilibrar o poder diretivo do empregador com os direitos fundamentais dos empregados (BRASIL, 1988).

Sobre a proteção de dados no Brasil, destaque-se:

> No caso do Brasil, como já antecipado, a Constituição Federal de 1988 (CF), embora faça referência, no art. 5º, XII, ao sigilo das comunicações de dados (além do sigilo da correspondência, das comunicações telefônicas e telegráficas), não contempla expressamente um direito fundamental à proteção e livre disposição dos dados pelo seu respectivo titular, sendo o reconhecimento de tal direito algo ainda relativamente recente na ordem jurídica brasileira. A proteção dos dados pessoais, por outro lado – para além da referência ao sigilo da comunicação de dados – também encontra salvaguarda parcial e indireta mediante a previsão da ação de habeas data (art. 5º, LXXII, da CF), ação constitucional, com status de direito-garantia fundamental autônomo, que precisamente busca assegurar ao indivíduo o conhecimento e mesmo a possibilidade de buscar a retificação de dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, ao mesmo tempo em que se trata de uma garantia procedimental do exercício da autodeterminação informacional.

O avanço da tecnologia, aliado à crescente complexidade das relações econômicas, ampliou os desafios relacionados à proteção de dados. Com isso, o direito à privacidade, antes associado a aspectos mais limitados da vida pessoal, passou a abranger também o controle sobre informações digitais e sensíveis, justificando a criação de um marco regulatório específico, como a Lei Geral de Proteção de Dados.

3.2 DIREITOS DOS TITULARES E APLICAÇÃO DA LGPD NAS RELAÇÕES DE TRABALHO

A LGPD, promulgada pela Lei nº 13.709/2018, representou um divisor de águas na proteção de dados no Brasil. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia, a LGPD estabelece um conjunto de direitos para os titulares de dados, como o acesso, a retificação, a exclusão e a portabilidade de informações

pessoais. Esses direitos reforçam a autonomia dos indivíduos sobre seus dados, impondo limites à coleta e ao uso indiscriminado de informações (CARLINI, 2024).

No âmbito das relações trabalhistas, a LGPD tem implicações diretas. Empregadores, ao coletar e tratar dados de seus empregados, devem justificar tais práticas com base nas hipóteses legais previstas na lei, como a execução de contrato, o cumprimento de obrigações legais ou o legítimo interesse. Contudo, a aplicação dessas hipóteses deve respeitar os princípios de necessidade e finalidade, evitando abusos (SANTOS; DUARTE, 2022).

> A LGPD além de trazer em seu artigo 2º alguns direitos e garantias fundamentais que estão previstos no artigo 5º da Constituição Federal, teve com a promulgação da Emenda Constitucional 115/2022, de 10 de fevereiro de 2022, seu objeto principal, a Proteção de Dados Pessoais, inserido na Constituição Federal de 1988 como direito fundamental. A proteção de dados passou a ser um direito fundamental, tendo a União, competência privativa para legislar sobre a proteção de dados. A LGPD passou a ser estudado em nível constitucional, estando inserido no texto da Constituição Federal em seus artigos 5º, 21 e 22. No qual o caput do art. 5º da Constituição Federal passou a vigorar acrescido do seguinte inciso LXXIX: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (BRASIL, 19881).No que diz respeito a competências, o caput do art. 21 da Constituição Federal passou a vigorar acrescido do seguinte inciso XXVI: “organizar e fiscalizar a proteção de dados pessoais, nos termos da lei” (BRASIL, 1988).Já o caput do art. 22 da Constituição Federal que trata da competência privativa da União, passou a vigorar acrescido do seguinte inciso XXX: “proteção e tratamento de dados pessoais” (BRASIL, 1988). A proteção de dados como um direito fundamental é muito importante, pois aumenta ainda mais a segurança jurídica em relação ao assunto, permitindo que outros países tenham mais um motivo para investir e manter relações com empresas brasileiras (SANTOS; DUARTE, 2022, p. 2678)

Dados pessoais coletados para fins específicos, como o pagamento de salários ou a gestão de benefícios, não podem ser utilizados para outras finalidades sem o consentimento expresso do titular. Esse entendimento reforça a importância de políticas claras de proteção de dados nas empresas, especialmente em setores regulados, como o de factoring (FERNANDES; ZANI, 2022).

A LGPD também classifica alguns dados como "sensíveis", exigindo maior rigor no tratamento dessas informações:

> Art. 5º Para os fins desta Lei, considera-se:
> 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 [...] (BRASIL, 2018).

Entre os dados sensíveis estão aqueles relacionados à saúde, origem racial, convicções religiosas, biometria e orientação sexual. No contexto trabalhista, o manuseio desses dados deve ser feito com especial cautela, dada a possibilidade de discriminação ou violação da privacidade (BRASIL, 2018).

No entre os dados sensíveis é necessário trazer à baila que:

> As informações relacionadas à saúde dos empregados são dados sensíveis e, embora já protegidas pelo sigilo médico (o código de ética médica, no art. 73), merecem muita atenção quanto ao armazenamento e divulgação de informações como: divulgação de doenças, atestados, exames médicos, divulgação de informações de compra de medicamentos, convênios e utilização do plano de saúde, por exemplo, além do armazenamento seguro das informações sensíveis por parte do empregador(controlador). Aplica-se a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, no caso em análise(empregado), ressalvado o disposto em legislação específica (ALCASSA, 2020).Segundo Cartaxo (2010), o Repertório de Recomendações Práticas de Proteção de Dados Pessoais do Trabalhador da Organização Internacional do Trabalho – OIT (1997) sugere que a coleta de dados médicos deve se restringir às informações que são necessárias para determinar se o trabalhador está apto para determinado posto de trabalho; se pode cumprir com os requisitos de segurança e saúde do trabalho; e, mais, se pode ter direito a prestações sociais (DOS SANTOS, 2020, p. 148).

Um dos desafios enfrentados pelas empresas é a conciliação entre a necessidade de tratar dados para atender a obrigações regulatórias e o respeito aos direitos dos empregados. A LGPD exige que as empresas implementem medidas técnicas e administrativas que garantam a segurança dos dados, prevenindo acessos não autorizados e vazamentos (DOS SANTOS, 2020).

3.3 GOVERNANÇA, FISCALIZAÇÃO E ALINHAMENTO INTERNACIONAL

A governança de dados é um dos pilares da LGPD. Empresas de todos os setores, incluindo as de factoring, são obrigadas a implementar programas de compliance específicos para a proteção de dados. Esses programas incluem políticas internas, designação de encarregado (DPO – *Data Protection Officer*), realização de avaliações de impacto e treinamento de colaboradores.

> Considerando que a relação de trabalho constitui uma fonte inesgotável de dados pessoais tratados, é dever do empregador fazer uso correto deles. Isso é aplicável em dados de empregados, prestadores de serviços, fornecedores, clientes, entre outros. O uso adequado dos dados deve ser uma prioridade para qualquer empreendedor, empresa ou instituição. A Lei Geral de Proteção de Dados não é aplicável somente nas relações de trabalho e sim em todas as relações envolvendo o tratamento de 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 (DOS SANTOS, 2020, p.146).

A Autoridade Nacional de Proteção de Dados, criada pela LGPD, desempenha um papel fundamental na fiscalização e orientação das práticas empresariais. Cabe à ANPD emitir diretrizes, aplicar sanções em caso de descumprimento da lei e promover a conscientização sobre a importância da proteção de dados pessoais (SARLET; RUARO, 2021).

> No Brasil, após emblemática tramitação legislativa, foi criado um corpo estatal incumbido de expressar garantias às múltiplas e atuais projeções do humano nesse novo contexto, sobretudo no que toca ao âmbito digital: a Autoridade Nacional de Proteção de Dados Pessoais (doravante ANPD). A ansiedade que antecedeu o seu pleno e independente funcionamento não surpreende. De acordo com dados de 2019 divulgados pelo IBGE, 82,7% dos domicílios brasileiros tem hoje acesso à internet, o que representa um aumento de 3,6% em relação a 2018, e com avanços em todos os grupos etários (BARROS, 2021). O fenômeno pode ser visto como positivo, na medida em que promove mais acesso à informação, mas, por outro lado, também ativa um dever estatal de proteção e, nessa medida, de educação quanto aos riscos que habitam este novo *locus* do debate público. Exemplo disso são os inúmeros incidentes e vazamentos de dados que acompanharam a parcial entrada em vigor da Lei Geral de Proteção de Dados Pessoais, em setembro de 2020, e que foram adensados em 2021 em relação à aplicabilidade dos seus dispositivos punitivos. Uma vez promulgada a Emenda Constitucional n. 115/2022, pacificou-se o tema quanto ao reconhecimento do direito fundamental à proteção de dados pessoais, inserindo no rol do artigo 5º o novo inciso LXXIX, segundo o qual é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (SARLET; RODRIGUEZ, 2022, p.220)

A interação entre a ANPD e outros reguladores, como o COAF, é essencial para promover a harmonização normativa. Essa interação pode evitar conflitos interpretativos e garantir que as exigências de compliance regulatório não sejam implementadas de maneira desproporcional ou contrária aos direitos fundamentais (SARLET; RUARO, 2021).

O alinhamento da legislação brasileira com padrões internacionais, como o GDPR, contribui para a inserção do Brasil no mercado global. Empresas que demonstram conformidade com normas internacionais de proteção de dados tendem a ganhar a confiança de parceiros comerciais e investidores, consolidando sua competitividade (SARLET; RUARO, 2021).

No entanto, o alinhamento normativo exige adaptações práticas, especialmente em setores que lidam com grandes volumes de dados. A implementação de

tecnologias de anonimização e criptografia, por exemplo, é uma das formas mais eficazes de reduzir riscos e garantir a segurança das informações (SARLET; RUARO, 2021).

No contexto das empresas de factoring, a governança de dados deve levar em conta as especificidades do setor. Como essas empresas lidam com informações financeiras e contratuais de clientes, fornecedores e empregados, é crucial que os processos internos sejam estruturados para evitar excessos e atender às exigências da LGPD (DE FARIAS; COLARES, 2024).

> Concluiu-se que são necessárias as adoções de segurança e de boas práticas para a governança de dados dos funcionários com o intuito de não os deixarem em uma posição de vulnerabilidade para evitar passivos trabalhistas perante a justiça do trabalho e fiscalizações dos órgãos reguladores. Todos os esforços devem representar uma verdadeira mudança de paradigma, adaptando a "Cultura" da empresa à nova realidade ditada pela sociedade dos dados, geração 4.0, havendo real mudança de hábitos e costumes de todos os envolvidos no processo, sendo imperiosa a adoção de uma governança de dados dos empregados, evitando prejuízos de ordem moral e material a empresa (DOS SANTOS, 2020, p.150).

A prática de realizar auditorias internas regulares é altamente recomendada, pois permite identificar falhas e implementar melhorias contínuas nos processos de tratamento de dados. Essas auditorias devem ser conduzidas por equipes qualificadas, que possam avaliar não apenas os aspectos técnicos, mas também a conformidade legal (D OLIVEIRA *et al.*, 2024).

4 A ATIVIDADE DE FACTORING E O TRATAMENTO DE DADOS DE EMPREGADOS

4.1 NATUREZA DO FACTORING E FLUXO DE INFORMAÇÕES

O factoring é uma atividade comercial voltada para a aquisição de direitos creditórios e a prestação de serviços correlatos, como gestão de créditos, consultoria financeira e cobrança. Embora não seja classificado como uma atividade financeira tradicional, o factoring tem grande importância no mercado, especialmente para pequenas e médias empresas que necessitam de capital de giro (DE ALMEIDA; PEREIRA, 2023).

O conceito de factoring apresentado pela doutrina majoritária consiste em:

> Logo, podemos conceituar o contrato de factoring como o negócio jurídico de prestação de serviços de atividade de assessoria e gerenciamento financeiro e de créditos por parte do faturizador, a envolver análise dos riscos da atividade do faturizado, através do exame e estudo da sua carteira de créditos futuros, compra destes direitos ou de parte deles, por intermédio do instituto da cessão civil, mediante pagamentos ou antecipação de parte dos valores dos títulos cedidos, além do exercício de cobrança dos recebíveis frente aos terceiros devedores. Fábio Ulhôa Coelho define o factoring como: Contrato pelo qual um empresário (faturizador) presta a outro (faturizado) serviços de administração do crédito concessão e garantia do pagamento das faturas emitidas (maturity factoring). É comum, também, o contrato abranger a antecipação do crédito, numa operação de financiamento (convencional factoring). Além de socialmente típico, o factoring pode ser classificado como contrato bilateral/sinalagmático, oneroso, comutativo, misto e empresarial. Bilateral ou sinalagmático, por quanto estabelece direitos e deveres recíprocos entre as partes, com equivalência de prestações. É contrato oneroso, pois para ambas as partes remanescem proveitos e sacrifícios em relação às prestações pactuadas. Comutativo, porque as partes, de antemão, já sabem quais são e em que momento suas prestações são de ser adimplidas. É misto porque envolve diversas espécies de contratos, nomeados ou não, numa mesma relação jurídica complexa. É empresarial, pois seu objeto é o fomento mercantil, através da prestação de serviço de análise dos negócios empreendidos pelo faturizado para escorreita avaliação dos riscos dos créditos a serem adquiridos pelo faturizador através de cessão civil (DE ALMEIDA; PEREIRA, 2023, p. 63 e 64).

No que diz respeito a sua natureza, o autor assevera que há controvérsias, porém, a doutrina majoritária concorda que a natureza do factoring é de natureza real e bancária. Por sua natureza, o factoring lida com informações sensíveis, não apenas relacionadas a clientes e fornecedores, mas também aos empregados que participam da execução de suas operações. Esse fluxo de dados inclui informações financeiras,

comerciais e operacionais, o que exige mecanismos robustos de gestão e proteção (DE ALMEIDA; PEREIRA, 2023).

O setor de factoring, ao não ser regulado diretamente por órgãos como o Banco Central, está sujeito às normativas do Conselho de Controle de Atividades Financeiras. A Resolução nº 41 do COAF impõe a essas empresas a responsabilidade de identificar, registrar e comunicar operações suspeitas de lavagem de dinheiro, o que aumenta a complexidade da gestão de dados (BRAGA, 2023).

O tratamento de dados de empregados no contexto do factoring ocorre principalmente em processos relacionados à segurança e ao compliance. Exemplos incluem o registro de acessos a sistemas, monitoramento de atividades realizadas e análise de histórico profissional. Esses dados, embora necessários para cumprir obrigações legais e regulatórias, devem ser tratados com rigor para evitar violações aos direitos fundamentais (RODRIGUES, 2023).

4.2 MONITORAMENTO INTERNO, COMPLIANCE E PROTEÇÃO DE DADOS

O monitoramento interno nas empresas de *factoring*, orientado pelo critério do COAF, envolve a coleta e análise de informações sensíveis, como registros de atividades dos empregados, dados financeiros e acessos a sistemas corporativos. Essas práticas são fáceis para identificar e relatar operações suspeitas, mas levantam questões relacionadas à proporcionalidade e à legalidade no tratamento dos dados (DE ALMEIDA; NETO, 2023). Nesse sentido, o compliance desempenha um papel central ao estabelecer políticas que conciliem as demandas regulatórias com a proteção dos direitos fundamentais dos trabalhadores.

A LGPD, promulgada pela Lei nº 13.709/2018, estabelece diretrizes claras para o tratamento de dados pessoais, exigindo que as empresas observem os princípios de necessidade, específicas e segurança (BRASIL, 2018). No contexto do monitoramento interno, isso significa que as informações dos funcionários só devem ser coletadas e processadas na medida de restrição necessária para atender às exigências do COAF. Além disso, as empresas devem implementar medidas de segurança robustas para evitar acessos não autorizados e garantir a integridade dos dados (FERNANDES; ZANI, 2022).

Outro aspecto importante é a transparência. Os funcionários devem ser informados sobre os tipos de dados coletados, as especificidades do tratamento e as

medidas de segurança exigidas. Essa prática está em conformidade com o princípio da transparência prevista pela LGPD e contribui para fortalecer a confiança entre trabalhadores e empregados (DOS SANTOS, 2020). A ausência de clareza nas políticas de monitoramento interno pode gerar conflitos trabalhistas e até mesmo avaliações administrativas, conforme apontado por Fernandes e Zani (2022).

A tensão entre as normas do COAF e a LGPD pode ser mitigada por meio de uma abordagem equilibrada e proporcional, que leva em conta os direitos dos trabalhadores e as obrigações regulatórias das empresas. Ferramentas como a pseudonimização e a anonimização de dados são estratégias recomendadas para reduzir os riscos associados ao tratamento de informações sensíveis (SARLET; RUARO, 2021). Essas práticas garantem que os dados utilizados para fins de conformidade sejam suficientemente despersonalizados, minimizando o impacto sobre a privacidade dos indivíduos.

Além disso, a criação de um programa interno de governança de dados, incluindo a designação de um encarregado de proteção de dados (DPO), é fundamental para garantir a conformidade com a LGPD e a Resolução nº 41 do COAF. O DPO pode atuar como intermediário entre a empresa e as autoridades reguladoras, garantindo que as práticas de monitoramento interno sejam aprovadas de forma legal e ética (DE ALMEIDA; NETO, 2023).

A interação entre reguladores, como o COAF e a Autoridade Nacional de Proteção de Dados, é essencial para promover uma harmonização normativa. Essa colaboração pode fornecer diretrizes mais claras para as empresas de *factoring*, ajudando-as a navegar pelas complexidades das questões regulatórias sem comprometer os direitos fundamentais dos trabalhadores (SARLET; RUARO, 2021). No âmbito internacional, o Regulamento Geral de Proteção de Dados da União Europeia pode servir como referência para o desenvolvimento de práticas de conformidade que respeitem a privacidade e a segurança das informações.

De tal maneira, as auditorias internacionais regulares desempenham um papel crucial no fortalecimento das políticas de conformidade e proteção de dados. Essas auditorias permitem identificar falhas, avaliar a conformidade com a LGPD e o COAF, e implementar melhorias contínuas nos processos internos (DOS SANTOS, 2020). A implementação de uma cultura organizacional focada na proteção de dados não apenas reduz os riscos legais, mas também fortalece a confiança das empresas de *factoring* no mercado.

A integração efetiva entre monitoramento interno, compliance e proteção de dados exige que as empresas de factoring adotem uma abordagem que vá além do cumprimento normativo superficial, estruturando processos internos que protejam simultaneamente os interesses institucionais e os direitos dos indivíduos dos empregados. Este equilíbrio, embora desafiador, é essencial para garantir tanto a integridade operacional quanto o respeito às garantias fundamentais previstas no ordenamento jurídico brasileiro.

A Resolução nº 41 do COAF impõe obrigações específicas às empresas de *factoring* no que diz respeito à identificação, registro e comunicação de operações suspeitas. Contudo, a implementação dessas práticas não pode desconsiderar os limites e as diretrizes impostas pela LGPD, especialmente em relação ao tratamento de dados sensíveis. Segundo De Souza e Camargo (2024), a conformidade normativa eficaz depende da adoção de medidas que proporcionem ao risco identificado, minimizando interferências desnecessárias na privacidade dos funcionários.

O compliance, nesse cenário, é o mecanismo central que conecta os critérios regulatórios à operação prática das empresas. A criação de políticas internas claras, a realização de treinamentos regulares e a definição de processos auditáveis são ferramentas fundamentais para garantir que as empresas estejam alinhadas às expectativas tanto do COAF quanto da ANPD (SARLET; RUARO, 2021). Além disso, a introdução de protocolos de monitoramento que utilizam métodos como pseudonimização, criptografia e controle de acesso ajuda a mitigar os riscos associados ao tratamento de dados pessoais.

No âmbito ambiental, o monitoramento interno não pode extrapolar os limites definidos pelos princípios da necessidade, adequação e especificamente, consagrados na LGPD. Os dados encontrados para atender às exigências do COAF, como registros de acesso a sistemas ou análises de atividades suspeitas, devem ser tratados de forma restrita ao objetivo específico, evitando que informações sejam utilizadas para outros fins sem consentimento o expresso do titular (BRASIL, 2018). Assim, as empresas devem se comprometer a estruturar políticas claras de uso de dados, abrangendo desde a coleta até a exclusão ou arquivamento seguro dessas informações.

Outro aspecto relevante é a transparência no relacionamento com os trabalhadores. A comunicação clara e acessível sobre as políticas de proteção de dados, os direitos garantidos pela LGPD e os procedimentos de monitoramento

interno é essencial para construir confiança e evitar conflitos. Além disso, a disponibilização de canais seguros para que os funcionários possam exercer seus direitos de acesso, correção ou exclusão de dados pessoais reforça a proteção da empresa e demonstra comprometimento com a conformidade legal (DOS SANTOS, 2020).

As auditorias internacionais são instrumentos indispensáveis para avaliar a eficiência das políticas de conformidade e proteção de dados. Realizadas periodicamente, essas auditorias permitem identificar vulnerabilidades, verificar o cumprimento das normas aplicáveis e implementar melhorias contínuas nos processos organizacionais. É importante que essas auditorias sejam fornecidas por equipes competentes e imparciais, capazes de analisar não apenas os aspectos técnicos, mas também a conformidade jurídica e ética das práticas exigidas (FERNANDES; ZANI, 2022).

A relação entre as normas do COAF e os princípios da LGPD também destaca a necessidade de uma interpretação sistemática e integrada das legislações aplicáveis. De acordo com Sarlet e Ruaro (2021), o diálogo entre reguladores é uma estratégia essencial para evitar conflitos normativos e promover uma aplicação coerente e harmoniosa das normas. Esse diálogo pode incluir, por exemplo, a emissão de guias ou orientações conjuntas pelo COAF e pela ANPD, estabelecendo critérios claros para o cumprimento da exigência de monitoramento e proteção de dados.

No âmbito internacional, experiências como o Regulamento Geral de Proteção de Dados da União Europeia fornecem insights importantes para a construção de uma governança de dados eficaz no Brasil. A adoção de práticas recomendadas, como avaliações de impacto à privacidade e design de processos centrados na proteção de dados, pode ajudar as empresas de *factoring* a atender às exigências locais enquanto se alinham aos padrões globais (CARLINI, 2024). Essa harmonização não apenas fortalece a competitividade das empresas brasileiras no mercado global, mas também contribui para a consolidação de um sistema financeiro mais ético e transparente.

Assim, o monitoramento interno, quando alinhado aos princípios de conformidade e proteção de dados, transcende a mera conformidade legal, tornando-se um elemento estratégico para a sustentabilidade e a confiança das empresas de *factoring*. Ao equilibrar rigor regulatório e respeito aos direitos fundamentais, essas empresas não apenas cumprem suas obrigações perante o COAF e a LGPD, mas também demonstram um compromisso genuíno com a transparência, a ética e a

segurança das informações, contribuindo para a construção de um ambiente corporativo e regulatório mais confiável e equilibrado.

4.3 DESAFIOS NA RELAÇÃO EMPREGADOR-EMPREGADO NO CONTEXTO DO FACTORING

A relação entre empregador e empresário no setor de factoring apresenta desafios únicos, exacerbados pelas exigências normativas do Conselho de Controle de Atividades Financeiras e pelas disposições da Lei Geral de Proteção de Dados. A natureza dinâmica e sensível das operações de factoring, que envolve a manipulação constante de dados pessoais e financeiros, exige que os funcionários adotem medidas rigorosas para garantir o cumprimento das obrigações legais, ao mesmo tempo que protegem os direitos fundamentais dos empregados. Nesse cenário, surgem graves consequências, que exigem uma abordagem equilibrada e bem estruturada para evitar conflitos e garantir um ambiente de trabalho ético e seguro (FERNANDES; ZANI, 2022).

O principal desafio nesse contexto é o equilíbrio entre as necessidades regulatórias e o respeito aos direitos dos trabalhadores. A Resolução nº 41 do COAF exige que as empresas de factoring implementem mecanismos internos de monitoramento e compliance para identificar e reportar operações suspeitas de lavagem de dinheiro. Essa obrigação implica a coleta e o processamento de dados sensíveis, como registros de atividades e acessos de trabalho, informações financeiras e até mesmo dados comportamentais, necessários para cumprir as políticas de "conheça seu cliente" (*Know Your Customer* - KYC) e de diligência de vida. Contudo, a LGPD estabelece limites específicos para o tratamento de dados pessoais, priorizando os princípios de necessidade, especificamente, minimização e transparência (BRASIL, 2018).

A aplicação prática dessas diretrizes pode gerar atritos na relação empregador-empregado. Por exemplo, o monitoramento constante das atividades dos trabalhadores, mesmo quando justificável sob a ótica do compliance, pode ser percebido como uma violação da privacidade, especialmente se as políticas internacionais não forem claras ou se a comunicação sobre essas práticas for insuficiente. Esse conflito é ainda mais acentuado quando os empregados não são informados sobre os dados encontrados, os propósitos desse tratamento e as medidas

de proteção inovadoras pela empresa (DOS SANTOS, 2020). Assim, a transparência e o diálogo aberto tornam-se fundamentais para mitigar percepções negativas e evitar possíveis litígios trabalhistas.

Outro desafio significativo é a proteção de dados sensíveis dos trabalhadores. A LGPD classifica como informações sensíveis que revelam origem racial, convicções religiosas, filiação a sindicatos, saúde, vida sexual ou dados biométricos, entre outros (BRASIL, 2018). No contexto das empresas de factoring, dados relacionados com a saúde, por exemplo, podem ser processados em programas de compliance ou em iniciativas de bem-estar organizacional. Contudo, qualquer uso indevido dessas informações pode resultar não apenas em avaliações administrativas, mas também em danos à confiança da empresa e na transparência dos direitos dos empregados (SARLET; RUARO, 2021).

Além disso, o poder diretivo do empregador, que inclui a prerrogativa de supervisão e gerenciamento das atividades laborais, enfrenta limites impostos importantes pelos princípios da dignidade da pessoa humana e do valor social do trabalho, consagrados na Constituição Federal de 1988 (BRASIL, 1988). Esse equilíbrio é particularmente desafiador em setores como o factoring, onde a segurança das operações muitas vezes exige níveis elevados de controle e monitoramento. O abuso dessas prerrogativas, seja por falta de clareza nas políticas internas ou por excesso de fiscalização, pode caracterizar desrespeito aos direitos fundamentais dos trabalhadores, desencadeando litígios trabalhistas, impactos negativos para a organização (DE ALMEIDA; NETO, 2023).

No âmbito do compliance, a implementação de programas práticos que respeitem os direitos dos trabalhadores exigem investimentos em treinamento e capacitação. Empregados bem informados sobre as normas de proteção de dados e compliance têm maior probabilidade de compreender a importância das políticas internacionais e de aderir às melhores práticas de segurança e ética organizacional. Por outro lado, a ausência de capacitação adequada pode gerar resistência às medidas de monitoramento, aumentar a sensação de invasão de privacidade e dificultar a implementação de uma cultura organizacional alinhada aos preceitos legais (FERNANDES; ZANI, 2022).

Além disso, as empresas de *factoring* enfrentam o desafio de criar mecanismos internos para responder às interrupções dos trabalhadores no exercício de seus direitos previstos na LGPD, como o acesso, a retificação ou a exclusão de dados. A

criação de canais eficientes para atender essas demandas é crucial para fortalecer a confiança dos trabalhadores na empresa e para garantir a conformidade com as disposições legais. Esse tipo de iniciativa contribui para minimizar os riscos de prejuízos e prejuízos à remuneração da organização (DOS SANTOS, 2020).

Outro ponto relevante é o impacto das práticas de governança de dados sobre o clima organizacional. Políticas de compliance mal projetadas, que impõem controles excessivos ou práticas de monitoramento desproporcionais, podem gerar insatisfação entre os trabalhadores e prejudicar o engajamento e a produtividade. Por isso, as empresas devem adotar abordagens equilibradas e garantir que as medidas de controle sejam inovadoras de maneira justa e respeitosa, promovendo um ambiente de trabalho positivo e motivador (SARLET; RUARO, 2021).

Finalmente, a harmonização entre os critérios regulatórios do COAF e os direitos assegurados pela LGPD exige que as empresas de factoring adotem uma postura proativa e inovadora. A utilização de tecnologias como anonimização e pseudonimização de dados, bem como a implementação de auditorias regulares e independentes, são práticas recomendadas para minimizar riscos e garantir a segurança das informações (DE ALMEIDA; NETO, 2023). Além disso, o diálogo com reguladores contínuos, como o COAF e a ANPD, é essencial para esclarecer ambiguidades normativas e promover a implementação de soluções que equilibrem eficiência e proteção de direitos.

Os desafios na relação empregador-empregado no contexto do factoring refletem a complexidade de conciliar as exigências de compliance com a proteção dos direitos fundamentais dos trabalhadores. Para superá-los, as empresas devem investir em políticas transparentes, treinamento contínuo e tecnologias de proteção de dados, além de cultivar um ambiente organizacional baseado no respeito e na ética. Ao fazer isso, não apenas atenderão às suas obrigações legais, mas também promoverão uma cultura corporativa mais sólida, alinhada aos valores de responsabilidade social e respeito à dignidade humana (DE ALMEIDA; NETO, 2023).

A resolução dos desafios inerentes à relação entre empregadores e empregados no setor de factoring também requer a formulação de políticas internas que equilibrem a eficiência operacional com o respeito às normas legais e aos direitos fundamentais. Uma dessas políticas é a delimitação clara de responsabilidades e limites no uso de ferramentas de monitoramento, como sistemas de registro de atividades e logs de acesso. Esses sistemas devem ser projetados para coletar

apenas os dados estritamente necessários para atender às exigências normativas do COAF, reduzindo a coleta excessiva de informações e evitando a exposição indevida dos trabalhadores (BRASIL, 2018).

Além disso, as empresas devem priorizar a implementação de um programa robusto de governança de dados, no qual todas as práticas relacionadas ao tratamento de informações sejam supervisionadas por um encarregado de proteção de dados (DPO). O DPO atua como uma ponte entre a empresa, seus empregados e os órgãos reguladores, garantindo que os procedimentos internos estejam em conformidade com a LGPD e promovendo a conscientização dentro da organização. Sua atuação é essencial para identificar riscos, estabelecer protocolos de segurança e responder rapidamente a incidentes ou solicitações dos titulares de dados (SARLET; RUARO, 2021).

Outro ponto fundamental é a criação de uma cultura organizacional que valorize a proteção de dados como um princípio ético e estratégico. Essa transformação cultural pode ser alcançada por meio de campanhas internas, treinamentos periódicos e iniciativas de sensibilização, que mostrem aos empregados a importância da proteção de dados não apenas para a empresa, mas também para eles como indivíduos. Um ambiente em que a proteção de dados é percebida como um valor compartilhado reduz a resistência a práticas de compliance e estimula a colaboração na implementação de medidas de segurança (DOS SANTOS, 2020).

Ainda no aspecto cultural, as lideranças organizacionais desempenham um papel importante na superação desses desafios. Gestores e supervisores precisam ser capacitados para atuar como agentes de conformidade e proteção de dados, aplicando as normas de maneira justa e proporcional, enquanto demonstram, na prática, o compromisso da empresa com o respeito aos direitos dos empregados. A liderança ética e transparente tem o potencial de fortalecer a confiança dos trabalhadores e aumentar a adesão às políticas internas (DE ALMEIDA; NETO, 2023).

Os desafios enfrentados pelas empresas de *factoring* no Brasil também podem ser analisados à luz das melhores práticas internacionais. Na União Europeia, por exemplo, o Regulamento Geral de Proteção de Dados enfatiza a necessidade de realizar avaliações de impacto à privacidade (*Privacy Impact Assessments* – PIAs) antes de implementar qualquer prática de tratamento de dados que possa implicar riscos elevados aos titulares. Essa abordagem preventiva é um exemplo que as empresas brasileiras podem adotar para antecipar e mitigar possíveis conflitos ou

violações (CARLINI, 2024).

Adicionalmente, a interação entre reguladores e empresas pode ser aprimorada por meio da criação de guias setoriais específicos para o setor de *factoring*, elaborados de forma conjunta entre o COAF, a ANPD e representantes das empresas. Esses guias podem oferecer orientações práticas e exemplos de boas práticas que ajudem a alinhar os requisitos regulatórios às particularidades do setor, promovendo uma aplicação mais uniforme e eficiente das normas (SARLET; RUARO, 2021).

No que se refere às consequências de uma gestão inadequada desses desafios, é importante destacar que falhas na proteção de dados ou no cumprimento das exigências regulatórias podem resultar em penalidades significativas, tanto na esfera administrativa quanto judicial. Além das sanções previstas na LGPD, as empresas podem enfrentar ações trabalhistas por violação dos direitos à privacidade e à dignidade dos empregados, bem como danos à sua reputação corporativa. Por outro lado, empresas que investem em conformidade e proteção de dados não apenas minimizam esses riscos, mas também ganham a confiança de seus stakeholders, fortalecendo sua posição no mercado (FERNANDES; ZANI, 2022).

Finalmente, cabe ressaltar que os desafios na relação empregador-empregado no setor de *factoring* não são estáticos, mas evoluem à medida que novas tecnologias e regulamentações são introduzidas. Assim, as empresas devem adotar uma abordagem dinâmica e adaptável, revisitando periodicamente suas políticas e processos para garantir que permanecem alinhados às melhores práticas e às expectativas regulatórias. A busca por soluções inovadoras, como o uso de inteligência artificial para a análise de dados de forma anonimizada, pode ser um diferencial estratégico para lidar com as complexidades do setor, mantendo o foco no respeito aos direitos dos empregados e na eficiência operacional.

Dessa forma, ao abordar os desafios da relação empregador-empregado de maneira proativa e ética, as empresas de *factoring* não apenas atendem às suas obrigações legais, mas também criam um ambiente de trabalho mais justo, seguro e alinhado aos princípios de responsabilidade social. Essa abordagem contribui para o fortalecimento do setor como um todo, promovendo a confiança nas operações e nos relacionamentos que sustentam sua atividade.

5 A TENSÃO ENTRE AS NORMAS: PREVENÇÃO À LAVAGEM DE DINHEIRO E PROTEÇÃO DE DADOS PESSOAIS

A contradição entre as regras que controlam a prevenção à lavagem de dinheiro e a salvaguarda de dados pessoais no Brasil evidencia uma questão legal e operacional que confronta empresas de várias áreas, especialmente aquelas que manipulam informações delicadas, como é o caso do setor de *factoring*. Por um lado, temos a Resolução no 41 do COAF, que define diretrizes estritas para identificar, documentar e notificar transações financeiras suspeitas, demandando um alto nível de transparência e rastreabilidade das informações. Por outro lado, a Lei Geral de Proteção de Dados, que salvaguarda a privacidade e a segurança das informações pessoais, estabelece restrições claras ao uso dessas informações, fundamentadas nos princípios de necessidade, minimização e finalidade (BRASIL, 2018). Essa dualidade normativa impõe às empresas o desafio de harmonizar suas práticas internas para atender simultaneamente às exigências de ambas as legislações, sem comprometer direitos fundamentais ou obrigações regulatórias.

A Resolução no 41 do COAF destaca a relevância da supervisão no sistema financeiro como ferramenta de luta contra delitos graves, como a evasão fiscal e o apoio ao terrorismo. Para alcançar essa meta, as empresas precisam coletar e examinar minuciosamente dados pessoais, financeiros e comportamentais de clientes, parceiros e, frequentemente, funcionários. Essas informações servem para reconhecer padrões ou transações incomuns, constituindo um instrumento crucial para a prevenção de condutas ilegais (DE SOUZA; CAMARGO, 2024). No entanto, a extensão das informações requeridas pela resolução suscita dúvidas sobre a equidade das ações e a sua conformidade com os direitos fundamentais de privacidade e proteção de dados garantidos pela LGPD.

Por outro lado, a LGPD reconhece a proteção de dados como um direito essencial e determina que a manipulação de informações pessoais deve seguir critérios estritos de legalidade, necessidade e segurança. Ela estabelece penalidades para ações que infrinjam a privacidade dos titulares, além de enfatizar a autodeterminação informacional como um alicerce fundamental nas interações entre empresas e pessoas (BRASIL, 2018). Neste cenário, a intersecção das demandas do

COAF com os princípios da LGPD pode resultar em situações conflitantes, principalmente quando o monitoramento e a recolha de dados excedem os limites estritamente necessários para o cumprimento das obrigações regulatórias.

O principal ponto de tensão surge da aparente contradição entre a necessidade de transparência, imposta pelas normas de prevenção à lavagem de dinheiro, e o direito à privacidade, protegido pela LGPD. Enquanto o COAF exige que as empresas sejam vigilantes e proativas na coleta e análise de informações, a LGPD busca restringir o uso de dados a propósitos específicos e claramente definidos, exigindo a minimização e a proteção contra acessos não autorizados (FERNANDES; ZANI, 2022). Esse paradoxo normativo não significa que as duas legislações sejam irreconciliáveis, mas sim que sua aplicação requer uma abordagem cuidadosa, baseada na harmonização e no equilíbrio entre interesses coletivos e individuais.

A resposta a essa tensão envolve a implementação de princípios constitucionais como a proporcionalidade e a razoabilidade. Estes princípios indicam que a observância de uma regra não deve impedir a implementação de outra, e que a avaliação de valores deve visar a salvaguarda máxima dos direitos em jogo. Em relação à prevenção da lavagem de dinheiro e à proteção de dados, isso implica que as organizações devem estabelecer políticas de conformidade que deem prioridade à segurança das informações e restrinjam a coleta de dados ao estritamente necessário, prevenindo ações intrusivas ou desproporcionais (SARLET; RUARO, 2021).

A pseudonimização e a anonimização de dados são métodos que auxiliam as organizações a atender às demandas do COAF sem prejudicar os direitos assegurados na LGPD. Essas estratégias possibilitam o tratamento de informações sensíveis para minimizar os perigos de identificação dos proprietários, preservando a integridade dos dados para monitoramento e avaliação de conformidade (DE ALMEIDA; NETO, 2023). Ademais, as organizações precisam implementar medidas de segurança sofisticadas, tais como criptografia, gerenciamento de acessos e auditorias constantes, assegurando que as informações manipuladas estejam salvaguardadas contra acessos não autorizados e eventuais vazamentos.

Um aspecto crucial na administração dessa tensão é a função das entidades reguladoras, tais como o COAF e a ANPD. A colaboração entre esses organismos pode auxiliar na elucidação de ambiguidades normativas e na definição de orientações que simplifiquem a implementação simultânea das normas. Por exemplo, guias práticos coletivos podem fornecer às organizações diretrizes sobre como tratar dados

de maneira alinhada à LGPD, ao mesmo tempo que atendem às demandas de prevenção à lavagem de dinheiro (SARLET; RUARO, 2021). Esta colaboração entre reguladores não só diminui as divergências interpretativas, como também proporciona maior segurança jurídica para as empresas, que precisam de termos claros para ajustar suas práticas às diversas demandas.

A experiência internacional, como a aplicação do GDPR na União Europeia, oferece insights valiosos sobre como lidar com a coexistência de normas de conformidade financeira e proteção de dados. O GDPR, por exemplo, enfatiza a necessidade de realizar avaliações de impacto à privacidade antes de implementar práticas que possam gerar riscos elevados aos titulares de dados. Esse tipo de abordagem preventiva pode ser adotada no Brasil, especialmente por empresas de *factoring*, para antecipar conflitos e ajustar seus processos às exigências legais (CARLINI, 2024).

Outro aspecto importante é o treinamento e a capacitação dos colaboradores. As empresas de *factoring* devem garantir que seus funcionários compreendam as obrigações impostas tanto pelo COAF quanto pela LGPD. Treinamentos periódicos e programas de sensibilização podem ajudar a promover uma cultura organizacional que valorize tanto a integridade financeira quanto a proteção da privacidade (FERNANDES; ZANI, 2022). Esse investimento em capacitação reduz a possibilidade de erros operacionais e fortalece o compromisso ético da empresa.

Ademais, a aplicação de políticas internas transparentes e passíveis de auditoria é crucial para atender às demandas normativas. Estas diretrizes precisam especificar os tipos de dados que podem ser encontrados, de acordo com as especificações específicas do processamento e as medidas de proteção que serão específicas. É igualmente crucial implementar sistemas de supervisão que sejam proporcionais e protejam os direitos dos empregados e demais detentores de dados (DOS SANTOS, 2020). Aclarar as políticas não apenas previne interpretações dúbias, mas também aumenta a confiança dos interessados na organização.

Um outro aspecto significativo é a administração dos incidentes de segurança, que não está ligada à tensão entre as normas. A LGPD requer que as organizações comuniquem prontamente à ANPD e aos proprietários dos dados sobre possíveis vazamentos ou acessos não permitidos. Contudo, as obrigações de sigilo do COAF podem, em determinados casos, restringir a divulgação de informações sobre operações suspeitas ou incidentes. Neste cenário, torna-se imprescindível que as

organizações elaborem protocolos de resposta que levem em conta ambos os aspectos e que sejam aptos a tratar os incidentes de maneira eficiente e de acordo com as normas legais (SARLET; RUARO, 2021).

Finalmente, as implicações jurídicas de não harmonizar essas normas podem ser significativas. Empresas que não cumprem a Resolução nº 41 do COAF estão sujeitas a prejuízos administrativos e possíveis repercussões criminais, enquanto a não conformidade com a LGPD pode levar a multas severas e danos reputacionais. Além disso, conflitos trabalhistas podem surgir caso os funcionários sintam que seus direitos à privacidade foram desrespeitados por práticas invasivas de monitoramento interno (FERNANDES; ZANI, 2022). Dessa forma, o custo da inobservância dessas normas transcende as avaliações financeiras, impactando diretamente a sustentabilidade e a confiança organizacional.

Portanto, o conflito entre as regras de prevenção à lavagem de dinheiro e a proteção de dados pessoais não é intransponível, porém requer uma estratégia e um tratamento meticuloso por parte das organizações. Ao implementar medidas que equilibrem segurança e privacidade, fomentando uma governança de dados sólida e investindo em tecnologia e formação, as organizações podem não só cumprir suas responsabilidades legais, mas também consolidar sua posição no mercado. A harmonização das normas, fundamentada nos princípios de proporcionalidade e razoabilidade, é a estratégia mais eficiente para enfrentar os obstáculos apresentados por este complexo ambiente regulatório, assegurando tanto a salvaguarda do sistema financeiro quanto os direitos básicos dos indivíduos.

5.1 EXIGÊNCIAS DO COAF VERSUS PRINCÍPIOS DA LGPD

O Conselho de Supervisão de Atividades Financeiras obriga as empresas de várias áreas, incluindo o *factoring*, a cobrar, examinar e divulgar informações financeiras e pessoais em certas situações, particularmente em relação a transações duvidosas. Contudo, essas demandas podem colidir com os princípios básicos da LGPD, que tem como objetivo assegurar a privacidade e a proteção dos dados pessoais dos indivíduos.

A Resolução nº 41 do COAF, como uma das normativas que orientam a prevenção à lavagem de dinheiro, exige que as empresas implementem sistemas de monitoramento e vigilância para identificar e relatar atividades financeiras suspeitas.

Nesse contexto, as empresas precisam coletar uma vasta gama de dados pessoais e financeiros, incluindo informações sobre clientes, fornecedores e, em algumas situações, sobre seus funcionários. Esses dados são essenciais para a identificação de padrões de comportamento financeiro atípicos que podem indicar envolvimento com atividades ilícitas, como lavagem de dinheiro ou financiamento ao terrorismo (DE SOUZA; CAMARGO, 2024). A coleta de dados abrangente e, muitas vezes, intrusiva, é uma exigência que visa garantir a transparência e a integridade das transações econômicas, mas levanta questões sobre o tratamento ético e legal dessas informações.

Em contrapartida, a LGPD, que começou a vigorar em 2020, define um conjunto estrito de princípios para o processamento de dados pessoais, que abrange a necessidade de seguir os princípios de necessidade, especificamente, proporcionalidade, transparência e segurança. Por exemplo, o princípio da necessidade determina que os dados pessoais só devem ser incluídos e processados quando forem necessários para atingir um objetivo específico, proibindo a coleta de informações desnecessárias ou sem relevância. Este princípio colide diretamente com o critério do COAF, que muitas vezes demanda a coleta de informações extensas e minuciosas, frequentemente indo além do necessário para a realização de uma transação financeira legal (BRASIL, 2018).

O princípio específico da LGPD determina que os dados devem ser recolhidos apenas para propósitos específicos, claros e legítimos, e não podem ser manipulados de forma incompatível com esses propósitos. Por exemplo, em empresas de *factoring*, o processamento de informações de colaboradores e clientes deve ser realizado para a avaliação de riscos ou para a realização de contratos. No entanto, o COAF requer que essas empresas usem essas informações para monitorar e prevenir delitos financeiros, como a lavagem de dinheiro. Esta dualidade de objetivos - um propósito legítimo de cumprimento e um propósito específico de processamento de dados - pode criar um impasse para as empresas, que devem assegurar a conformidade entre os dois conjuntos de normas aplicáveis (FERNANDES, 2014).

O princípio da proporcionalidade, um dos pilares fundamentais da LGPD, requer que o processamento de dados seja apropriado, pertinente e não exagerado em relação aos objetivos para os quais os dados são coletados. Contudo, as demandas do COAF costumam levar a práticas de supervisão constante, obtenção de informações extras e análise de padrões de comportamento que podem ser

excessivas e, em alguns casos, intrusivas. Apesar de tais ações poderem ser justificadas pelo combate à lavagem de dinheiro, elas podem infringir o princípio da proporcionalidade da LGPD, que visa salvaguardar os direitos individuais contra o processamento de dados desmedido ou desnecessário (SARLET; RUARO, 2021).

A clareza, um dos fundamentos da LGPD, requer que as organizações comuniquem aos titulares de dados de forma transparente e compreensível como seus dados serão manipulados, qual a finalidade específica desse tratamento e quem terá acesso a essas informações. No entanto, para atender às demandas do COAF, pode ser necessário coletar e analisar dados sem o consentimento do titular, particularmente ao se tratar de detectar atividades suspeitas. Apesar do COAF autorizar o processamento de dados sem o consentimento explícito do proprietário, a LGPD requer que as organizações assegurem que seus colaboradores e clientes sejam devidamente informados sobre o uso de seus dados. Esse desequilíbrio entre a exigência de confidencialidade e a necessidade de transparência coloca as empresas em uma posição exigida, pois elas precisam equilibrar o cumprimento das obrigações regulatórias com o dever de garantir a confiança dos titulares de dados (DOS SANTOS, 2020).

A proteção de dados, também crucial na LGPD, é outro campo crucial de segurança que surge quando as organizações tentam harmonizar as demandas do COAF com as da LGPD. A Resolução no 41 do COAF requer que as corporações instalem sistemas sólidos para a supervisão de transações e guarda de informações financeiras confidenciais, o que resulta em uma quantidade considerável de dados que precisam ser resguardados contra acessos não autorizados. A LGPD intensifica a necessidade de implementar medidas de segurança severas para salvaguardar dados pessoais contra falhas de segurança, vazamentos ou acessos não autorizados. Assim, as empresas devem criar estruturas de segurança que atendam tanto aos critérios de vigilância financeira do COAF quanto às medidas de proteção de dados da LGPD, o que exige investimentos em tecnologias, auditorias e práticas organizacionais que atendam aos mais altos padrões de segurança (FERNANDES; ZANI, 2022).

Por fim, a harmonização entre as exigências do COAF e os princípios da LGPD exige que as empresas de *factoring* e outros setores regulamentados adotem uma abordagem equilibrada, que considere tanto a necessidade de cumprir com as obrigações de prevenção à lavagem de dinheiro quanto os direitos dos titulares de

dados. Isso pode ser alcançado por meio de medidas como a pseudonimização e a anonimização de dados, que permitem a análise e o monitoramento sem comprometer a identidade dos indivíduos. Além disso, as empresas devem revisar periodicamente suas práticas e políticas de tratamento de dados, garantindo que sejam sempre cumpridas com as normas vigentes e com as melhores práticas de governança e compliance (DE ALMEIDA; NETO, 2023).

Assim, o equilíbrio entre as exigências do COAF e os princípios da LGPD representa um desafio complexo, mas não insuperável. Ao adotar políticas de compliance transparentes, tecnologias de proteção de dados robustas e uma abordagem ética e proporcional ao tratamento das informações, as empresas podem garantir que cumpram com as normas legais, ao mesmo tempo em que respeitam os direitos fundamentais dos indivíduos.

5.2 PRINCÍPIOS DE NECESSIDADE, MINIMIZAÇÃO E TRANSPARÊNCIA

A lei brasileira de proteção de dados pessoais baseia-se nos princípios de necessidade, minimização e transparência, particularmente sob a vigência da Lei Geral de Proteção de Dados, Lei n° 13.709/2018. Estes princípios orientam a atividade de processamento de dados pessoais, particularmente no ambiente corporativo e, em particular, no setor de *factoring*, onde a gestão de informações sensíveis é uma exigência regulatória resultante de normas como a Resolução no 41 do COAF. Portanto, a avaliação desses princípios é crucial para entender a necessidade de um equilíbrio entre a observância das obrigações jurídicas e o respeito aos direitos básicos dos titulares de dados.

O princípio da necessidade é claramente estabelecido no artigo 6o, inciso III, da LGPD, que determina que o processamento de dados pessoais deve ser restrito ao mínimo necessário para atingir seus objetivos. Este preceito visa garantir que somente os dados indispensáveis sejam recolhidos e processados, minimizando, assim, os perigos de exposição indevida ou uso impróprio de informações sensíveis (BRASIL, 2018). No contexto do *factoring*, este princípio requer que as organizações estabeleçam precisamente quais informações dos seus colaboradores são necessárias para atender às demandas regulatórias estabelecidas pelo COAF, prevenindo a coleta em massa e desnecessária de dados.

Alinhado ao princípio da necessidade, o princípio da minimização enfatiza que

os dados pessoais devem ser manipulados de maneira proporcional e estritamente ligada ao objetivo estabelecido. Isso implica que a organização precisa estabelecer procedimentos que restringem o acesso a esses dados, utilizando soluções tecnológicas, como pseudonimização e anonimização, sempre que viável, para minimizar os riscos de vazamentos ou acessos não permitidos (FERNANDES; ZANI, 2022). Essas práticas ganham especial relevância em um cenário de regulamentações estritas, como as estabelecidas pela Resolução no 41, que requer o acompanhamento constante e o registro de transações tidas como suspeitas.

Por outro lado, o princípio da transparência, estabelecido no artigo 6o, inciso VI, da LGPD, exige que os titulares de dados tenham total compreensão de como seus dados estão sendo recolhidos, processados e guardados. Este princípio é crucial para garantir que o processamento de dados pessoais seja realizado de maneira ética e responsável, fomentando a confiança entre os colaboradores e a empresa (DE ALMEIDA; NETO, 2023). No ramo de *factoring*, isso implica que os colaboradores precisam ser adequadamente esclarecidos acerca do motivo pelo qual seus dados estão sendo recolhidos, as ações de segurança postas em prática e os procedimentos disponíveis para o exercício de seus direitos como proprietários de dados.

Esses princípios, quando aplicados conjuntamente, criam um arcabouço normativo robusto que busca harmonizar os interesses das empresas com a proteção dos direitos fundamentais dos empregados. A Resolução nº 41 do COAF impõe às empresas de *factoring* a obrigação de implementar medidas de controle para identificar e comunicar transações suspeitas, o que muitas vezes implica no tratamento de dados pessoais dos empregados (BRAGA, 2023). No entanto, essas medidas devem ser projetadas para respeitar os princípios da LGPD, sob pena de configuração de ilegalidade e violação de direitos fundamentais.

Para colocar esses princípios em prática, é necessário implementar soluções tecnológicas e administrativas que incentivem a governança e a proteção dos dados pessoais. Programas de conformidade, capacitações constantes e auditorias internas são exemplos de ferramentas que podem garantir que as empresas de *factoring* cumpram a legislação em vigor. Ademais, a transparência deve ser fomentada não somente através de políticas transparentes, mas também através de uma comunicação confiável com os colaboradores acerca de seus direitos e a maneira como seus dados são resguardados.

Sob o enfoque do princípio da necessidade, é fundamental que as empresas

realizem avaliações de impacto sobre a proteção de dados (*Data Protection Impact Assessment* - DPIA) antes de implementar novos processos ou sistemas que envolvam o tratamento de informações pessoais. Essa prática permite identificar possíveis riscos e estabelecer medidas preventivas que assegurem a conformidade legal e a segurança das informações (CARLINI, 2024).

Em relação ao princípio da minimização, é igualmente crucial que as organizações se empenhem em limitar ao mínimo o acesso e a partilha de dados. As normas internas devem limitar o acesso somente a profissionais diretamente envolvidos nas tarefas de conformidade, assegurando que informações confidenciais não sejam compartilhadas de maneira descontrolada. Esta estratégia auxilia na formação de um ambiente de negócios seguro e alinhado aos princípios de proteção de dados.

O princípio da transparência requer um esforço constante para assegurar que os detentores de dados entendam de maneira clara os objetivos e os procedimentos de tratamento de seus dados. Isso engloba não só a disponibilização de políticas de privacidade pormenorizadas, mas também a execução de campanhas de sensibilização interna na empresa, com o objetivo de fomentar uma cultura de respeito aos direitos básicos dos funcionários.

Para concluir, é crucial seguir os princípios de necessidade, minimização e transparência para que as empresas de *factoring* funcionem conforme a LGPD e as diretrizes do COAF. Esses princípios não só auxiliam na defesa dos direitos básicos dos funcionários, como também incentivam a ética e a responsabilidade no manejo de informações pessoais, reforçando a confiança e a imagem da empresa no mercado. Ao implementar práticas em conformidade com esses princípios, as empresas não só cumprem seus deveres legais, como também colaboram para a criação de um ambiente de negócios mais transparente e seguro para todos os participantes.

5.3 CAMINHOS PARA A HARMONIZAÇÃO NORMATIVA

A procura por um equilíbrio normativo entre as normas de prevenção à lavagem de dinheiro e a salvaguarda de dados pessoais é um desafio que requer respostas jurídicas, técnicas e institucionais unificadas. No cenário brasileiro, onde convivem legislações como a Resolução no 41 do COAF e a Lei Geral de Proteção de Dados, é imprescindível a harmonização para prevenir conflitos normativos e fomentar um

ambiente regulatório balanceado, que satisfaça tanto as demandas de segurança financeira quanto os direitos básicos dos proprietários dos dados.

A primeira etapa para a harmonização é definir orientações claras que possibilitem a implementação coordenada das normas em discussão. A Autoridade Nacional de Proteção de Dados e o Conselho de Supervisão de Atividades Financeiras devem trabalhar em conjunto, incentivando a criação de normas adicionais que clarifiquem as responsabilidades das empresas no processamento de dados pessoais em atividades regulamentadas. Essa colaboração entre instituições pode minimizar interpretações divergentes e assegurar maior proteção jurídica para os participantes econômicos (FERNANDES; ZANI, 2022).

Uma tática eficiente para a convergência é o uso de programas de conformidade que atendam aos requisitos da LGPD e da Resolução no 41. Esses programas precisam ser elaborados com base em uma avaliação de risco completa, que detecte os pontos de convergência e tensão entre as normas. A adoção de ações como a pseudonimização de dados, o gerenciamento de acessos e a revisão constante dos processos pode auxiliar as organizações a cumprir as demandas de rastreabilidade e transparência, sem prejudicar a privacidade dos proprietários dos dados (CARLINI, 2024).

Além disso, é crucial que as empresas de *factoring* apliquem recursos em tecnologia e capacitação para aprimorar sua governança de dados. A aquisição de instrumentos que possibilitem o acompanhamento seguro e eficaz das operações financeiras, juntamente com a formação de funcionários em assuntos como proteção de dados e prevenção à lavagem de dinheiro, são ações fundamentais para o cumprimento das normas. Essas ações também auxiliam na formação de uma cultura corporativa fundamentada na ética e na responsabilidade (DE ALMEIDA; NETO, 2023).

Outra abordagem relevante é a realização de consultas públicas e audiências que permitam a participação de diferentes setores da sociedade na formulação de diretrizes normativas. Esse processo participativo pode auxiliar na identificação de soluções práticas para os desafios enfrentados pelas empresas, além de fomentar um entendimento mais amplo e integrado sobre a importância da harmonização entre as legislações vigentes (BRAGA, 2023).

No cenário global, a vivência da União Europeia com o Regulamento Geral de Proteção de Dados pode fornecer percepções valiosas para a situação brasileira. É

eficaz na Europa a aplicação de normas setoriais que ajustam os princípios gerais de proteção de dados às particularidades de setores como o financeiro. No Brasil, a implementação de soluções similares pode auxiliar na formação de um cenário regulatório mais consistente e eficaz (UCHÔA, 2019).

Em última análise, é fundamental incentivar a educação e a sensibilização acerca da relevância da proteção de dados e da prevenção contra a lavagem de dinheiro. Campanhas de conscientização direcionadas ao público interno e externo podem ampliar a compreensão dos benefícios da harmonização das normas, além de envolver todos os interessados na criação de soluções integradas e sustentáveis.

6 CONCLUSÃO

Esta dissertação realizou uma avaliação minuciosa dos efeitos da Resolução no 41 do COAF na administração de informações pessoais de funcionários em empresas de *factoring*, considerando os direitos básicos de privacidade e proteção de dados, além das consequências práticas do cumprimento das obrigações legais de prevenção à lavagem de dinheiro. O estudo mostrou que, apesar da regulamentação representar um progresso notável na luta contra delitos financeiros, ela apresenta desafios significativos para as empresas, particularmente em áreas não regulamentadas por instituições financeiras convencionais, como o *factoring*, ao demandar métodos rigorosos de identificação, monitoramento e comunicação de informações confidenciais.

A pesquisa começou com a constatação de que a Resolução no 41 do COAF está inserida em um cenário normativo nacional e internacional que está em conformidade com as melhores práticas de prevenção à lavagem de dinheiro. Através da implementação de normas internacionais, como as orientações do Grupo de Ação Financeira Internacional, o Brasil visa reforçar a integridade do sistema financeiro e prevenir ações ilegais que possam prejudicar a economia do país. Contudo, a execução dessas ações se dá em um contexto de normatização cada vez mais complexa, intensificada pela entrada em vigor da Lei Geral de Proteção de Dados, que reafirma o direito básico à proteção de dados pessoais e define normas estritas para a manipulação dessas informações.

A pesquisa revelou que a convergência entre a Resolução no 41 e a LGPD é um desafio complexo, demandando das empresas de *factoring* a implementação de estratégias inovadoras e unificadas. Por um lado, as regras do COAF estabelecem obrigações de conformidade que exigem a coleta, o armazenamento e a divulgação de informações pessoais em situações delicadas, como a avaliação de transações financeiras e a detecção de operações que possam ser suspeitas. Em contrapartida, a LGPD estabelece restrições precisas sobre a finalidade, a necessidade e a proporcionalidade no processamento de dados, obrigando as empresas a implementarem medidas de segurança para assegurar a salvaguarda da privacidade de seus colaboradores e demais detentores de dados.

Assim, constatou-se que a implementação simultânea dessas normas necessita de uma interpretação constitucional apropriada, guiada pelos princípios de

proporcionalidade, razoabilidade e harmonização de interesses. Apesar de ser crucial para a proteção do sistema financeiro, a prevenção à lavagem de dinheiro não deve ser aplicada de maneira que infrinja direitos básicos, tais como dignidade, privacidade e a autodeterminação informativa dos colaboradores. Portanto, é crucial que as organizações elaborem políticas internas sólidas e que estejam em conformidade tanto com as demandas do COAF quanto com as diretrizes da LGPD.

Ademais, o estudo enfatizou a relevância de incentivar a formação contínua dos profissionais envolvidos na aplicação dessas normas, particularmente em áreas como a *factoring*, onde há um fluxo elevado de dados sensíveis. A execução de formações e o estabelecimento de uma cultura corporativa focada na proteção de dados podem auxiliar na redução de riscos legais e reputacionais, enquanto reforçam a confiança dos funcionários e parceiros de negócios. A implementação de tecnologias como anonimização, pseudonimização e criptografia, juntamente com a execução de auditorias internas frequentes, também foi citada como uma estratégia eficiente para assegurar a segurança e a conformidade no processamento de dados pessoais.

Outro aspecto importante discutido foi a função das entidades reguladoras, tais como o COAF e a Autoridade Nacional de Proteção de Dados, na resolução de conflitos normativos entre a prevenção da lavagem de dinheiro e a salvaguarda de dados. A ação conjunta desses órgãos é crucial para estabelecer orientações precisas e garantir a segurança jurídica na implementação das regras, fomentando um ambiente regulatório mais eficaz e balanceado. A experiência global, em particular o Regulamento Geral de Proteção de Dados da União Europeia, foi ressaltada como inspiração para o Brasil, apontando estratégias para a harmonização entre conformidade regulatória e direitos fundamentais.

A avaliação também destacou que a convergência entre a Resolução no 41 do COAF e a LGPD constitui uma chance para aprimorar a governança corporativa. As empresas que implementam práticas éticas e transparentes no processamento de dados não só se protegem de penalidades legais, como também se sobressaem no mercado, consolidando sua imagem e atraindo investidores. Esta perspectiva destaca a relevância da responsabilidade social corporativa no contexto atual, onde a segurança dos dados se torna cada vez mais crucial para a continuidade dos negócios.

Assim, conclui-se que, apesar de parecerem conflitantes, a Resolução no 41 do COAF e a LGPD podem ser interpretadas e implementadas de maneira

complementar, desde que as empresas de *factoring* adotem uma atitude proativa e estratégica em relação ao cumprimento das regulamentações. Esta atitude deve incluir não só a aplicação de ações técnicas e organizacionais para assegurar a proteção das informações, mas também a dedicação ética à salvaguarda dos direitos básicos dos funcionários e demais detentores de dados.

Assim, o estudo enfatiza a importância de um equilíbrio entre os interesses públicos e privados envolvidos na prevenção da lavagem de dinheiro e na salvaguarda de informações pessoais. Este equilíbrio não é somente um requisito legal, mas também uma chance de fomentar a inovação, a competitividade e a segurança no cenário empresarial. Ao cumprir suas responsabilidades normativas de maneira responsável e em conformidade com os direitos básicos, as empresas de *factoring* têm a capacidade de auxiliar na criação de um sistema financeiro mais equitativo, transparente e seguro, estabelecendo o Brasil como um líder mundial na luta contra práticas ilegais e na defesa da proteção de dados pessoais.

REFERÊNCIAS

ANSELMO, M. A. O ambiente internacional do combate à lavagem de dinheiro. **Revista de Informação Legislativa**, Brasília, DF, v. 47, n. 188, p. 357-358, 2010. Disponível em: https://www2.senado.leg.br/bdsf/item/id/198729. Acesso em: 09 dez. 2024.

BRAGA, J. R. B. **Análise comparativa da implementação das normas de combate à lavagem de dinheiro e ao financiamento ao terrorismo nos países do Mercosul**. 2023. 138 f., il. Dissertação (Mestrado Profissional em Economia) — Universidade de Brasília, Brasília, 2023. Disponível em: http://repositorio2.unb.br/jspui/handle/10482/47886. Acesso em: 09 dez. 2024.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Diário Oficial da União, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 nov. 2024.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988. Diário Oficial da União: Poder Legislativo, Brasília, DF, 5 out. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao. htm. Acesso em: 28 out. 2024.

CESPEDES, C. P. Coaf e controles internos: prevenção e combate à lavagem de dinheiro no sistema financeiro. **Revista da Procuradoria-Geral do Banco Central**, v. 15, n. 1, p. 76-93, 2021. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1098. Acesso em: 09 dez. 2024.

D OLIVEIRA, N. P. C. *et al.* **Política e gestão da informação no contexto da LGPD: a perspectiva da auditoria de informação para o registro do tratamento de dados pessoais**. 2024. 160 f. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal da Bahia, Instituto de Ciência da Informação, Salvador, 2024. Disponível em: https://repositorio.ufba.br/handle/ri/39921. Acesso em: 12 nov. 2024.

DA SILVA NETO, C. A. *et al.* A comunicação empresarial no combate à lavagem de dinheiro: Corporate communication in the fight against money laundering. **Studies in Social Sciences Review**, v. 3, n. 2, p. 546-567, 2022. Disponível em: https://studiespublicacoes.com.br/ojs/index.php/sssr/article/download/539/541. Acesso em: 08 dez. 2024.

DE ALMEIDA, B. M. P.; NETO, J. A. M. Mecanismos de Controle de Proteção de Dados Pessoais: Uma Análise Netnográfica da Maturidade das Organizações Contábeis do Ceará À Lei Geral De Proteção De Dados. **THEMIS: Revista da Esmec**, v. 21, n. 1, p. 205-246, 2023. Disponível em: https://revistathemis.tjce.jus.br/THEMIS/issue/view/72. Acesso em: 09 dez. 2024.

DE ALMEIDA, M. E. M.; PEREIRA, F. B. O contrato de factoring como meio de fomento à atividade empresarial no mundo globalizado. **Revista de Direito Internacional e Globalização Econômica**, v. 2, n. 02-Ext, p. 60-72, 2023.

Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/download/64537/43671/206966. Acesso em: 09 dez. 2024.

DE FARIA, N. L.; COLARES, A. C. V. Análise da representação contábil em empresas de capital aberto nas operações de risco sacado com base no ofício circular CVM nº 01/2016. **CAFI**, v. 7, n. 2, p. 229-251, 2024. Disponível em: https://revistas.pucsp.br/index.php/CAFI/article/view/67553. Acesso em: 20 nov. 2024.

DE SOUZA, C. M.; CAMARGO, F. D.'E. Padrões internacionais de prevenção à lavagem de dinheiro transnacional em transações comerciais e sua aplicação no Brasil. **Revista Insigne de Humanidades**, v. 1, n. 1, p. 79-98, 2024. Disponível em: https://insigneacademica.com.br/ojs/index.php/revistainsignedehumanidades/article/view/7?articlesBySimilarityPage=2. Acesso em: 10 nov. 2024.

DINIZ, M. H. **Curso de Direito Civil Brasileiro** - Teoria Geral do Direito Civil. 1. vol. São Paulo: Ed. Saraiva, 1982.

FERNANDES, A.; ZANI, J. Análise e detecção dos indícios de lavagem de dinheiro por instituições financeiras: construção de uma ferramenta para identificação e mitigação dos riscos decorrentes da utilização de dados compartilhados/Analysis and detection of evidence of money. **Revista Científica do CPJM**, v. 1, n. 04, p. 152-179, 2022. Disponível em: https://rcpjm.cpjm.uerj.br/revista/article/download/102/120/201. Acesso em: 20 nov. 2024.

FINKELSTEIN, M. E.; FINKELSTEIN, C. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343. Acesso em: 09 dez. 2024.

FLORÊNCIO, F.; MARCO, A.; ZANON, P. B. Políticas Públicas de Prevenção e Combate à Lavagem de Dinheiro no Brasil: COAF e Arranjo Institucional. **Revista Pensamento Jurídico**, São Paulo, Brasil, v. 12, n. 2, 2018. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/382. Acesso em: 8 dez. 2024.

FRAZÃO, A. N. A.; TEPEDINO, G.; OLIVA, M. D. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 3ª ed. São Paulo: Thomson Reuters Brasil, 2019.

GOMES, D. Análise econômica da instituição de programas de compliance a partir das multas punitivas do COAF. **Direito UNIFACS–Debate Virtual-Qualis A2 em Direito**, n. 229, 2019. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/6326/3867. Acesso em: 11 nov. 2024.

LARRUBIA, R. B. **Como a supervisão realizada pelo COAF afeta a conformidade dos seus regulados?** 2023. 74 f. Dissertação (Mestrado em Administração Pública) – Escola Brasileira de Administração Pública e de Empresas, Centro de Formação

Acadêmica e Pesquisa, Rio de Janeiro-RJ, 2023. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/5e1ec41a-2825-4d30-ba66-f7b8de2494c6/content. Acesso em: 07 dez. 2024.

OLIVEIRA, B. Q. As Limitações impostas pelo Princípio da Legalidade ao Poder Regulamentar do Conselho de Controle de Atividades Financeiras. **Revista Justiça do Direito**, *[S. l.]*, v. 30, n. 3, p. 422-441, 2017. DOI: 10.5335/rjd.v30i3.6242. Disponível em: https://seer.upf.br/index.php/rjd/article/view/6242. Acesso em: 8 dez. 2024.

SANTOS, F. A lei geral de proteção de dados pessoais e a exposição de dados sensíveis nas relações de trabalho. **Revista do Tribunal Regional do Trabalho da 10ª Região**, v. 24, n. 2, p. 145-151, 14 jan. 2021. Disponível em: https://revista.trt10.jus.br/index.php/revista10/article/view/419. Acesso em: 09 dez. 2024.

SARLET, G. B. S.; RODRIGUEZ, D. P. A Autoridade Nacional de Proteção de Dados: elementos para uma estruturação independente e democrática na era da governança digital. **Revista Direitos Fundamentais & Democracia**, v. 27, n. 3, p. 217-253, 2022. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2285. Acesso em: 09 dez. 2024.

SARLET, G. B. S.; RUARO, R. L. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados –L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/download/2172/694/5371. Acesso em: 06 dez. 2024.

SARLET, I. W. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. **Revista Brasileira de Direitos Fundamentais & Justiça**, *[S. l.]*, v. 14, n. 42, p. 179–218, 2020. DOI: 10.30899/dfj.v14i42.875. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 9 dez. 2024.

TURESSI, F. E.; DA PONTE, A. C. Direitos humanos, mandados de criminalização e as obrigações processuais penais positivas: perspectivas e desafios na busca pela efetividade do regime antilavagem de dinheiro no Brasil. **Meritum: Revista de Direito da Universidade FUMEC**, v. 17, n. 2, 2022. DOI: https://doi.org/10.46560/meritum.v17i2.8860. Disponível em: https://revista.fumec.br/index.php/meritum/article/view/8860. Acesso em: 09 dez. 2024.

UCHÔA, C. de N. **A Gestão Responsiva do Risco Penal Empresarial: A Responsabilidade Penal da Empresa e os Programas de Compliance em um Ambiente Integrado e Colaborativo**. 2019. 159 f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de Coimbra, Coimbra, 2019. Disponível em: https://estudogeral.uc.pt/bitstream/10316/90377/1/DISSERTAÇÃO_2_CICLO_CARO

LINA_DE_NOVAES_UCHOA_2017192674_docx.pdf. Acesso em: 09 dez. 2024.