

ADEQUAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS AOS PROGRAMAS DE COMPLIANCE DO SETOR BANCÁRIO – Compartilhamento de dados cadastrais entre instituições financeiras

Felipe Santana Mariz Nogueira *

Maria Jamily Lima de Azevedo*

Mariane Galvão Montelo*

Resumo

O presente artigo analisa a importância da existência de uma adequação da LGPD nos programas já existentes de Compliance, trazendo um foco para as relações bancárias, e o seu sistema de compartilhamento de dados com demais instituições bancárias e centrais de risco.

Inicialmente, é realizada uma ligeira elucidação do que significa o termo “Compliance”, do Surgimento a sua atribuição para uma boa organização nas relações corporativas.

Posteriormente é adentrado no tema da Lei Geral de Proteção de Dados, descrevendo sua importância no contexto atual da sociedade, explanado a responsabilidade civil das empresas ao divulgarem sem autorização dados pessoais de clientes e colaboradores.

Por fim é explanado de forma sucinta a divulgação de dados bancários a luz da Lei Nº 13.709/2018, e demonstrando a importância de se haver um equilíbrio entre os termos do Compliance visando garantir a segurança empresarial, e o direito de proteção de dados pessoais que é garantida a pessoa humana.

* Orientador do Artigo. Graduado pela Universidade Católica de Pernambuco (2006). Especialista em Direito e Processo Civil (2013). Mestrando em Ciências Ambientais pela UFP – Universidade Federal do Pará. Oficial de Justiça do TRT8. Professor na FESAR – Faculdade de Ensino Superior da Amazônia Reunida.

* Acadêmica do Curso de Direito – 10º Período da Faculdade de Ensino Superior da Amazônia Reunida - FESAR. E-mail: jamilly.leal@outlook.com

* Acadêmica do Curso de Direito – 10º Período da Faculdade de Ensino Superior da Amazônia Reunida - FESAR. E-mail: marianegalvao09@gmail.com

Palavras-chave: Compliance, Lei Geral de Proteção de Dados, Dados bancários, Compartilhamento de Dados Cadastrais.

1 INTRODUÇÃO

A Lei de Proteção de Dados também conhecida como LGPD foi sancionada em agosto de 2018, e entrará em vigor assim que o artigo 4º da MP 959-20, que visava adiar a vigência da LGPD para 31 de dezembro, for retirado.

No entanto, é importante ressaltar que ela não é a primeira lei do Brasil que possui como finalidade proteger os dados pessoais das pessoas. Tal temática já vem chamando a atenção do Legislativo há muitos anos, antes de todo o engajamento dessa ideia através da internet e outros meios de comunicação.

Desde a criação da Constituição de 1988, já se constituíram diversos motivos para que se buscasse a proteção dos dados pessoais.

O programa de Compliance por sua vez vem ganhando cada vez mais notoriedade com o passar dos anos, estando muito em alta nos interesses da sociedade. O risco de uma empresa seguir sem possuir um programa de compliance ativo é, muito grande podendo trazer prejuízos financeiros e também legais.

Para que haja ética* nas instituições é imprescindível que se siga um código que descreva todas as ações aceitáveis ou não.

Uma empresa para estar de acordo com o compliance, o principal é que se tenha acesso a todos os dados pessoais de seus colaboradores e clientes, mas como garantir a proteção desses dados?

Com a vigência da LGPD as empresas para estarem em compliance devem ver os dados cadastrais não apenas como algo pessoal, mas também como um direito fundamental.

Quando toda essa ideia já fomentada está relacionada a instituições financeiras, tudo ganha uma proporção ainda maior.

* Ética: conjunto de regras e preceitos de ordem valorativa e moral de um indivíduo, de um grupo social ou de uma sociedade

Os bancos podem trocar compartilhar dados entre si, até mesmo para se comprovar a autenticidade e veracidade dos dados cadastrais.

Mas até onde essa compartilhamento é permitida e quais são os requisitos para que não se infrinja a Lei de Proteção de Dados? Essa é a principal questão a ser pensada e discutida. O programa de compliance também deve fazer mutações para que haja uma adequação de suas diretrizes com a garantia de proteção de cadastro e dados pessoais.

Assim, mediante todo o exposto se torna claro a necessidade de haver uma pesquisa que discuta sobre a relação da nova Lei de Proteção de Dados – LGPD e os programas compliance das instituições financeiras, explicando a linha tênue que existe entre algo que é permitido por Lei e a ética, portanto, a necessidade de adequação.

2. Como Surgiu o Termo Compliance e Qual Sua Função no Ambiente Corporativo

2.1 Explicando o Termo Compliance

O termo “ Compliance” vem do verbo ‘to comply’* que traduzido em palavras e ações significa estar de acordo com as normas, procedimentos e regulamentos de determinado lugar. Não se comete infrações quando as ações são baseadas na legalidade.

Ser ou Estar em Compliance é ter o dever de cumprir normas e procedimentos, estar em conformidade como que é proposto e fazer cumprir regulamentos internos e externos impostos às atividades da instituição. No entanto existe uma grande diferença entre ser ou estar em Compliance.

Ser Compliance é ter conhecimento sobre as normas e seguir os procedimentos, todas as ações do indivíduo são voltadas para o senso ético, sabendo que é essencial viver com idoneidade.

Estar em Compliance por outro lado, é apenas estar em conformidade com leis e regulamentos internos e externos. Por isso que o mais importante do que estar, é ser compliance.

Para Carla Veríssimo (2018)

* To Comply: cumprir com, obedecer

Compliance é um substantivo que significa concordância com o que é ordenado, compliant é aquele que concorda com alguma coisa, e to comply with significa obedecer.

Tudo surge com uma ideia de como garantir transparência e segurança para uma empresa, tais ideias são formuladas em ações e essas ações são cobradas de todos os seus colaboradores. A empresa que possui Compliance exige um padrão ético a ser seguido, e como cada ser humano possui um diferente senso do que é ética é imprescindível que para que haja organização, todos os regulamentos sejam expressos e rigorosamente cobrados.

Imagine uma linha reta que é passada de um lugar até o outro para seguir de guia e assim ninguém se perca...é exatamente isso que o Compliance significa! É o caminho a ser seguido por todos dentro de uma empresa para que ninguém se perca em suas ações e comportamentos perante o mercado que que atue, seja ele qual for.

A definição de Compliance para Christian Karl de Lamboy é:

Quando se houve a palavra “Compliance”, tentamos traduzir e entender o que significa, o que abrange, do que se trata. O termo “Compliance” vem do verbo inglês “to comply”, que significa cumprir, executar, concordar, adequar-se, satisfazer o que lhe foi imposto.

Ou seja, estar em Compliance significa cumprir as normas baseadas em valores éticos, estando sempre em constante vigilância para garantir os resultados da empresa. Portanto, é uma forma de se prevenir irregularidades.

Christian complementa ainda:

Compliance é o dever de cumprir e estar em conformidade com diretrizes estabelecidas na legislação, normas e procedimentos determinados, interna e externamente, para uma empresa, de forma a mitigar riscos relacionados a reputação e a aspectos regulatórios.

Seguindo o pensamento de Karl, se esclarece que a empresa possui o dever de cumprir decretos, leis, regulamentos e instruções aplicáveis à atividade da empresa, para que se diminua os riscos financeiros.

Em um estabelecimento que segue diretrizes de Compliance se observa tanto a direção da empresa que deve estar sempre comprometida com o planejamento das ações, como também sua execução. Para que tudo isso aconteça, é investido recursos adequados para a manutenção do programa de Compliance, elegendo uma pessoa ou grupo que será responsável pelo programa, que possuirá autonomia para tomar medidas necessárias;

2.2 Breve Histórico da Criação do Compliance no Brasil e no Mundo

Agora que já ficou claro sobre o que é o Compliance surge a dúvida mais comum: Mas de onde surgiu esse termo?

O Compliance ficou mais conhecido após o caso Watergate*, que ocorreu nos EUA em 1974. Em 1977 o país instituiu a Lei Americana FCPA que tem por escopo combater as irregularidades comerciais no âmbito internacional.

Em 2010, o Reino Unido instituiu o Bribery ACT, que é uma Lei Britânica de combate e prevenção de irregularidades nas empresas, que é uma das legislações mais rígidas do mundo.

No Brasil, o Compliance só surgiu em 1998, vindo a ser formalmente instituído em 2013 através da Lei Anticorrupção que é regulamentada pelo decreto nº 8420/2015. A Lei Anticorrupção trata sobre a responsabilização de empresas de forma Objetiva, Administrativa e Civil pela prática contra a Administração Pública nacional ou estrangeira.

Na década de 90 o Brasil queria se alinhar ao mercado mundial que é altamente competitivo por isso se viu a necessidade de criar regras de segurança além de incrementar as já existentes. Muitas instituições se viram falidas por não conseguirem competir com outras empresas mais organizadas, e consequentemente as empresas brasileiras foram perdendo cada vez mais espaço no mundo.

* O caso Watergate foi um dos grandes escândalos políticos de corrupção ocorridos nos Estados Unidos, que teve como resultado a renúncia do então presidente republicano Richard Nixon. O episódio teve início no ano de 1972, com a invasão do Comitê Nacional do Partido Democrata, situado no conjunto de edifícios Watergate.

Paralelo a tudo isso o ato terrorista nos EUA em 2001* e os escândalos financeiros em Wall Street em 2002* mostraram a importância de ter regulamentações mais eficientes que se apliquem em todos os países para prever os riscos a que as instituições estão sujeitas.

Foi no meio de toda essa inovação que se destacou o tema Compliance, que já estava incorporado em outros países a um bom tempo, e se mostrou tão importante.

Depois de devidamente inserido no mercado brasileiro, o Compliance tem mostrado cada vez mais seu valor, cumprindo sua missão de assegurar o cumprimento de normas e procedimentos, e por consequência gerando credibilidade as instituições que seguem o seu sistema.

2.3 Para que serve o Sistema de Compliance ?

A principal função de um sistema de Compliance é corrigir desvio que venham trazer prejuízos para o negócio, e corrigir eventuais falhas que venham acontecer.

Ademais, o programa deve analisar todos os possíveis riscos que determinado negócio pode ter, criando um manual com todas as normas a serem seguidas na empresa e realizando sempre que necessário, auditorias.

Através de um Compliance, também é possível conhecer as Leis que podem ser aplicadas ao negócio de forma positiva e negativa;

* Os **ataques ou atentados terroristas de 11 de setembro de 2001** (às vezes, referido apenas como **11 de setembro**) foram uma série de ataques suicidas contra os Estados Unidos coordenados pela organização fundamentalista islâmica al-Qaeda em 11 de setembro de 2001. Na manhã daquele dia, dezenove terroristas sequestraram quatro aviões comerciais de passageiros.^{[1][2]} Os sequestradores colidiram intencionalmente dois dos aviões contra as Torres Gêmeas do complexo empresarial do World Trade Center, na cidade de Nova Iorque, matando todos a bordo e muitas das pessoas que trabalhavam nos edifícios.

* O laboratório **Merck**, em meados de 2002 registrou como receita de uma das suas subsidiárias (Medco) **12.400 milhões de dólares que não recebeu**, a fim de equilibrar as contas, mas a renda não lhe pertencia, por isso adotou o valor apenas para inflar os ganhos. Embora a contabilidade da Merck não fosse tecnicamente considerada uma fraude, a Merck sofreu uma semana muito tensa em Wall Street até que pudesse esclarecer a situação.

O Compliance de uma empresa administra os controles internos e externos, alcançando dessa maneira, melhorias para os negócios, se torna portanto, uma maneira de compartilhar a cultura do Compliance com todos os colaboradores.

Para Carla Veríssimo (2018) A missão do Compliance é:

O Compliance tem objetivos tanto preventivos como reativos. Visa a prevenção de infrações legais em geral assim como a prevenção de riscos legais e reputacionais aos quais a empresa está sujeita, na hipótese de que essas infrações se concretizem. Além disso, impõe à empresa o dever de apurar as condutas ilícitas em geral, assim como as que violam as normas da empresa, além de adotar medidas corretivas e entregar os resultados de investigações internas às autoridades, quando for o caso.

Para a associação de bancos ABBI e FEBRABAN, é função do Compliance dentro da empresa: Assegurar quanto a aplicação das leis, princípios Éticos e Normas de Conduta, regulamentos e Normas, demonstrar os procedimentos e Controles internos, também é responsável pelo Sistema de Informações, planos de Contingência, segregação de funções, relatório do sistema de controles internos (Gestão de Compliance) e Políticas Internas.

Assim, Compliance tem a missão de assegurar que os controles internos da empresa funcionem de forma sistemática, buscando a redução dos riscos com base no modelo de negócios e a complexidade dos mesmos. Também deve disseminar a cultura de controles internos em toda organização de forma a assegurar o cumprimento das leis, normas, regulamentos internos e externos existentes.

De qualquer forma o principal é que o programa de Compliance seja desenvolvido por uma boa equipe, que tenha cargos específicos voltados para esse fomento, para que o programa de Compliance abranja não apenas as regras e procedimentos da empresa, mas também os valores éticos de seus colaboradores.

3. Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/18)

3.1 Aspectos da nova Lei de Proteção de dados

A nova lei de dados – Lei Geral de Proteção de Dados (LGPD) – foi sancionada em agosto de 2018 e entrou em vigor em agosto de 2020. As empresas e as organizações terão grandes responsabilidades em relação à proteção de todos os dados pessoais de seus funcionários, fornecedores e clientes.

A LGPD demanda esforços para garantir a proteção e confidencialidade de dados sensíveis e regulamenta o uso e tratamento dos dados pessoais, tanto pela iniciativa privada quanto do poder público, na tentativa de protegê-los contra vazamentos e uso indevido. Por isso, promover uma governança fortalecida e baseada em uma postura transparente de privacidade se traduz em usuário mais confiantes no momento de compartilhar suas informações.

De acordo com Oscar Valente Cardoso, por conter, na sua maior parte, normas de direito material, a entrada em vigor da LGPD produz efeitos gerais e imediatos, respeitados o ato jurídico perfeito, o direito adquirido e a coisa julgada (art. 6º da Lei de Introdução às Normas do Direito Brasileiro – Decreto-Lei nº 4.657/42).

A partir da LGPD não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Ou seja, as empresas devem explicar para que usarão cada um dos dados pessoais.

Essas finalidades também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular.

Além disso, a empresa não está autorizada a modificar a finalidade durante o tratamento. Se seu startup solicita o e-mail do cliente para a finalidade específica de login na plataforma, você não pode automaticamente utilizar esse mesmo e-mail para enviar publicidade ou ofertas.

Com o objetivo de garantir privacidade, controle e segurança no uso dos dados de pessoas físicas nos mais diversos meios, a Lei Geral de Proteção de Dados (LGPD) traz o desafio de

adequar a política de tratamento dessas informações sensíveis por meio da adaptação de processos e sistemas em conformidade com a lei, assim como a GDPR. A LGPD permeia sua aplicação em uma extensão extraterritorial, ou seja, tratando de dados de cidadãos brasileiros ou estrangeiros residentes, a organização deve se comprometer com a regularização em todas as etapas do processo — incluindo empresas parceiras.

A jornada de Compliance com a LGPD - e também com a lei europeia, a GDPR - representa uma oportunidade para endossar sua postura de privacidade a fim de preservar e fortalecer a confiança e o engajamento de seus clientes e consumidores. Assumir o compromisso com as obrigações e o uso adequado dos dados, além de reduzir consideravelmente o risco potencial de brechas capazes de viabilizar exposições e vazamentos, pode impulsionar uma vantagem competitiva real a partir do aprimoramento de seus negócios sob uma perspectiva ética e responsável.

3.2 Responsabilidade Civil no âmbito da Proteção de Dados

A responsabilidade civil, se entendida numa visão ampla de obrigação de reparar um dano antijuridicamente causado a um terceiro, pode ser compreendida em duas modalidades. A primeira delas é a decorrente de danos resultantes do inadimplemento, má execução ou atraso no cumprimento de obrigações contratuais, denominada de responsabilidade contratual. A segunda, também chamada de responsabilidade civil extracontratual, diz respeito à obrigação de reparação de danos resultantes da violação de outros direitos alheios, como os direitos da personalidade.

A responsabilidade civil extracontratual é, portanto, diretamente ligada à violação de um direito. Assim, aquele que viola um direito e ocasiona dano a outrem será responsável pela reparação do dano causado. No Código Civil, a responsabilidade civil é fundada em dois conceitos, o de ato ilícito (art. 186) e o de abuso de direito (art. 187).

Para que exista a responsabilidade civil é necessária a conjugação de três pressupostos, quais sejam a conduta, o nexo de causalidade e o dano. A conduta pode ser ação ou inação; comissiva ou omissiva; própria ou de terceiros; lícita ou ilícita; derivada de fato, coisa, produto ou animal. O nexo de causalidade liga a conduta do agente ao dano sofrido pela vítima. Para que surja o dever de indenizar é preciso que o dano verificado seja consequência da ação ou omissão do agente. O dano é a lesão a um bem jurídico.

A LGPD, a seu turno, define a responsabilidade dos agentes de tratamento de dados, que são os controladores e os operadores, pelos danos causados em razão do exercício da atividade de

tratamento, de forma semelhante à sistemática do Código de Defesa do Consumidor (CDC), na seção III do Capítulo VI. A Lei, conforme art. 43, exime de responsabilidade os agentes quando provarem que: não realizaram o tratamento de dados em questão; que não houve violação à legislação; ou que houve culpa exclusiva do titular dos dados ou de terceiro pela ocorrência dos danos.

A LGPD, entretanto, não adota o risco como critério de imputação da responsabilidade civil e, tampouco, a culpa pode ser compreendida como elemento adequado de imputação na LGPD.

O ilícito geral na LGPD pode ser compreendido pela falta ao dever de segurança em termos similares aos da disciplina jurídica do Código de Defesa do Consumidor (CDC) para a responsabilidade civil pelo fato do serviço. No direito do consumidor o dever geral de segurança está fundado no elemento defeito, pois o produto ou serviço é considerado defeituoso e, assim, ensejador da responsabilidade civil do fornecedor, quando não oferece a segurança que legitimamente se pode esperar.

Do mesmo modo, mantendo a coerência sistemática, o tratamento irregular previsto no artigo 44 da LGPD ocorre quando da quebra de legítimas expectativas quanto à segurança dos processos de tratamento de dados. Poderia se falar, por conseguinte, de um defeito no tratamento de dados pessoais ou, caso se queira manter a nomenclatura da própria LGPD, de um tratamento irregular.

O mais relevante é perceber que além dos ilícitos específicos, o sistema estabeleceu uma forma de ilícito geral própria do sistema de proteção de dados pessoais, fundamentada na responsabilidade civil do agente que realizar um tratamento irregular (ilícito), seja por violar algum dever específico imposto pela legislação ou seja por violar o dever geral de segurança no tratamento de dados pessoais.

4 Relação entre o Compliance e a Lei Geral de Compartilhamento de dados

Com o advento da Lei de Proteção de Dados a área que será mais afetada será a do Compliance, pois como é ele que garante que a empresa esteja de acordo com a lei, será considerado, portanto o guardião da LGPD.

Para que uma empresa esteja de acordo com a LGPD a primeira coisa a se fazer será criar um comitê de Compliance se este ainda não existir, e nomear uma pessoa como fiscal das condutas éticas da empresa.

Na LGPD, o encarregado de proteção de dados se chama Data Protection Officer* (DPO), que é um profissional que tem que ter um amplo conhecimento em Compliance.

A função do DPO, está expresso no artigo 41 da LGPD, já no primeiro inciso é descrito o compromisso a ser realizado assim que nomeado o encarregado dos dados pessoais de clientes e colaboradores:

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

A razão desse inciso é trazer ainda mais segurança aos dados fornecidos, pois o encarregado terá acesso a todas as informações contidas no sistema, informações essas de caráter pessoal, destarte a necessidade da transparência da identidade do representante principal.

No inciso 2º é apontado a atribuição do encarregado como zelador de todos os dados movimentados pela empresa:

§ 2º As atividades do encarregado consistem em:

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

II - Receber comunicações da autoridade nacional e adotar providências;

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

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

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado,

* Na tradução literal do Inglês para a língua portuguesa, **Data Protection Officer** significa “Oficial de proteção de dados.”

inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Uma empresa tem que demonstrar que está preocupada com a segurança dos dados de seus clientes, e não basta ser falado, tem que ser comprovado os processos e políticas internas desenvolvidos para esse fim. A Lei não deixa claro que processos são esses que devem ser seguidos, mas é presumido que eles devem ser baseados no Compliance. Pelo Compliance possuir como um dos objetivos principais proteger as pessoas do uso indevido de seus dados pessoais, em muito ele se assemelha aos propósitos da Lei de Proteção de Dados. Através do poder da LGPD, o programa de Compliance possui ainda mais proteção ao fiscalizar as informações pessoais da qual tem acesso, se utilizando do embasamento de estar protegendo a instituição.

Ao mesmo tempo em que a LGPD concede o aval para Compliance realizar a fiscalização, exige como uma forma de freio a esse poder, a necessidade de se ter uma autorização expressa do titular das informações, sob o ônus de se configurar invasão de privacidade. Além de precisar do consentimento do indivíduo, ainda devem ser ofertados pelas empresas a opção da própria pessoa realizar a alteração dos dados já presentes, ou acrescentar algum que considere relevante a aquela situação. Se necessário, deve ser permitido inclusive a exclusão dos dados ali existentes na plataforma.

Com a Lei 13.719/18 em vigor, todas as empresas são obrigadas a realizar a atualização os Códigos de Condutas utilizados, alterando as normas de procedimentos internos e de proteção de dados.

5. COMPARTILHAMENTO DE DADOS CADASTRAIS BANCÁRIOS ENTRE INSTITUIÇÕES FINANCEIRAS E CENTRAIS DE RISCOS

5.1 Hipóteses que justificam o compartilhamento de dados cadastrais segundo a LGPD

Caso as instituições financeiras precisem compartilhar os dados pessoais de seus clientes com terceiros ou centrais de riscos, em regra é necessário que primeiramente haja um

consentimento expresso do titular, e que seja deixado claro também que esse consentimento é para a finalidade de compartilhamento de dados.

Entretanto existem situações em que a Lei de Proteção de Dados dispensa tal autorização.

A principal situação de permissão de compartilhamento de dados, é quando os dados cadastrais já se tornaram públicos pelo próprio titular, isento sempre os direitos e princípios previstos na LGPD.

Caso se tenha o intuito de proteger o detentor dos dados de fraudes, também é admissível o compartilhamento de dados, sempre observando o direito à transparência e informação, para resguardar a integridade física ou a vida do titular dos dados.

Também se justifica o compartilhamento de dados, nas situações em que para a proteção da saúde seja necessário repassar informações a profissionais da área para realização de procedimentos, ou quando esses dados forem essenciais para o cumprimento das funções do regulamentador.

No geral, em qualquer hipótese de compartilhamento de dados cadastrais, sejam elas com ou sem autorização do titular, devem sempre observar os princípios dispostos no art. 6º da LGPD, que são os princípios da Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos Dados, Transparência, Segurança, Prevenção, Não Discriminação, e Prestação de Contas.

5.2 Proteção trazida pela Lei de Proteção de Dados contra o Compartilhamento de Dados Cadastrais Bancários

De acordo com uma pesquisa que foi realizada pela PG advogados com 36 segmentos da economia, apenas 30% deles já estão em conformidade com a Lei de Proteção de Dados, apesar de que a implantação da Lei nos bancos seja considerada simples pelo setor já se preocupar bastante com a segurança da informação.

O banco Bradesco realizou várias pesquisas com especialistas de outros países para implementar planos de ações eficientes para esse fim. Já foram analisados também uma relação de setores que sofrerão abalos com as novas mudanças que ocorrerão para entrar em conformidade com a LGPD.

Com a LGPD, as instituições financeiras ficam proibidas de compartilhar dados referentes a saúde para a finalidade de se obter vantagens econômicas, como por exemplo, no caso de solicitação de planos de saúde. Da mesma forma, os bancos não podem utilizar informações

relacionadas a saúde que lhe foram repassadas para aceitar ou excluir beneficiários na contratação de qualquer plano.

Outrossim, o titular dos dados também pode a qualquer momento mediante uma solicitação, receber a relação dos dados pessoais que estão sendo realizadas o compartilhamento, tanto com entidades públicas como privadas.

O possuente também possui o direito de requerer a correção de dados que estejam incorretos, além de bloqueá-los perante a instituições financeira e por consequência, perante a qualquer outro terceiro com o qual seus dados foram também compartilhados.

5.3 OPEN BANKING – Compartilhamento de Dados de Clientes com Integração de Plataformas

Através da plataforma Open Banking*, as instituições compartilharão dados de clientes, produtos e serviços com outras instituições financeiras, mas com o diferencial de que esses dados pertencerão aos clientes e não às instituições.

A principal finalidade desse sistema virtual é fornecer mais liberdade aos clientes e como consequência aumentar a competitividade financeira entre as empresas.

A implementação do Open Banking começou no dia 24 de Setembro de 2020 pelo Banco Central, sendo publicado o comunicado 33.455 que estabelece as suas diretrizes e procedimentos.

Nessa plataforma digital, os clientes de bancos poderão através de um único aplicativo visualizar um extrato de todas as suas contas bancárias, no entanto para que isso ocorra é necessário que haja o compartilhamento dados cadastrais dos clientes como nome, número de inscrição no Cadastro de Pessoas Físicas – CPF, endereço, etc. Além de dados pessoais se faz necessário também que se compartilhe dados transacionais relacionados a contas de depósito, a operações de crédito, a demais produtos e serviços contratados pelos clientes, etc.

Com todos esses dados salvos na plataforma digital, se por acaso o cliente quiser mudar de banco futuramente, não será necessário iniciar todo o procedimento do zero, pois somente será preciso consultar as informações presentes no Open Banking.

O Banco Central desenvolveu a ideia do Open Banking para garantir que as Instituições em Compliance seguissem um único modelo de plataforma e com isso assegurassem a eficiência

* Na tradução literal, open banking significa “**banco aberto**”, ou “**sistema bancário aberto**”.

dessas instituições financeiras. Seguindo a ideia do compliance, os bancos terão ainda mais transparência nos seus negócios, diminuindo os riscos financeiros. Ou seja, o Open Banking é um exercício de Compliance.

Entretanto, por causa da finalidade desse novo aplicativo, e procedimentos que devem ser seguidos, existe uma inerente incompatibilidade dele com a Lei de Proteção de Dados, uma vez que para que esse programa alcance êxito é essencial que haja o compartilhamento não apenas de dados cadastrais dos clientes bancários, mas também de seus dados transacionais.

O Banco Central alega que toda a regulamentação do Open Banking foi desenvolvida em conformidade com a LGPD. No tópico 6 do comunicado 33.455 está expresso:

O compartilhamento de dados cadastrais e transacionais dos clientes, bem como de serviços de pagamento, depende de prévio consentimento do cliente. Os procedimentos para viabilizar tal consentimento devem ter como diretriz a promoção de uma experiência simples, eficiente e segura para o cliente. Além disso a regulamentação poderá incluir outros dados, produtos e serviços mínimos no escopo mencionado no parágrafo anterior.

Barbosa (2014, p. 237) menciona o questionamento de Ronaldo Porto Macedo Júnior:

"Acerca da abusividade existente na comercialização de banco de dados, Ronaldo Porto Macedo Júnior questiona se a venda de informações pessoais contidas num cadastro de consumidores fornecido a uma empresa por outra configuraria uma violação do direito à privacidade e demandaria uma reparação com base nos princípios de privacidade constitucionalmente assegurados."

O questionamento do autor, é se o compartilhamento no banco de dados se configura ou não uma violação no direito de privacidade que são assegurados pela constituição.

No entanto, como é possível analisar os dados dos clientes para perceber o comportamento do consumidor e com isso evitar fraudes, sem ferir os direitos e a experiência do usuário? Indiscutivelmente é difícil manter o equilíbrio.

5.4 LGPD - Constitucionalidade do Compartilhamento de Informações Bancárias entre o Ministério Público e a Unidade de Inteligência Financeira

Em um julgamento do Recurso Extraordinário 105594, o Supremo Tribunal Federal decidiu ser constitucional o compartilhamento com o Ministério Público e as autoridades policiais, dados bancários e fiscais do contribuinte obtidos pela Receita Federal e pela Unidade de Inteligência Financeira (UIF), na existência de investigação criminal sem observar a autorização prévia do Poder Judiciário, ou da pessoa possuinte dos dados.

De acordo com o relator Dias Toffoli, é recepcionado que no momento em que forem detectados indícios da prática de delitos criminais, a Receita Federal e a Unidade de Inteligência Financeira compartilhem dados que são protegidos pela lei do sigilo bancário e pela LGPD, mesmo sem ter prévio consentimento do titular da conta, ou autorização judiciária.

Todavia, levando em conta a Lei 13.709/18, é plausível o questionamento sobre a Constitucionalidade do julgamento do recurso ordinário, isso porque as informações bancárias e fiscais de pessoas físicas são também dados pessoais de acordo com o artigo 5º, inciso I da LGPD:

Art. 5º Para os fins desta Lei, considera-se:

I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Ou seja, de acordo com esse inciso, informações bancárias e fiscais são protegidas pela Lei Geral de Proteção de Dados, por serem informações relativas a pessoa física. O embasamento do STF é de que a própria LGPD traz no seu dispositivo essa possibilidade de compartilhamento de dados, quando se visar proteger a eficácia das investigações e a segurança pública, como dispõe o art. 4º, III, da referida Lei. De fato, o compartilhamento de informações bancárias e fiscais nesses casos se torna aceitável tencionar identificar infrações no sistema Financeiro do país.

É tudo uma questão de ótica que deve ser analisada sucintamente no caso concreto, por causa da possível inconformidade do recente julgado do STF e a Lei de Proteção de Dados.

5.5 Consequências Administrativas e Cíveis Cabíveis em razão do compartilhamento indevido de dados cadastrais de Bancos entre Instituições Financeiras.

A Lei geral de Proteção de Dados trouxe vários dispositivos no que diz respeito a responsabilidade dos agentes a serem tratados, e várias dessas responsabilidades podem ser aplicadas a instituições financeiras.

Segundo o artigo 52 da Lei nº 13.709/2018 podem ser aplicados como sanções administrativas no descumprimento da LGPD, advertência, com indicação de prazo para adoção de medidas corretivas, multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, limitada, no total, a 50 milhões por infração, multa diária, observando o limite total a que se refere o inciso II, divulgação da Infração após apurada e confirmada a sua ocorrência, bloqueio dos dados pessoais a que refere a infração até a sua regularização e a eliminação dos dados pessoais a que se refere a infração.

Quanto a possibilidade dos bancos serem responsabilizados por danos morais em decorrência de compartilhamento indevido de dados, a LGPD trouxe no seu artigo 42, caput o seguinte:

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

Da mesma forma também é garantido a indenização por dano moral coletivo, nos termos do parágrafo 3º desse mesmo artigo citado anteriormente.

Nota-se a possibilidade de responsabilização pelos danos da violação da segurança dos dados não apenas as instituições financeiras, mas também os agentes de tratamento, o que é ainda mais reforçado no artigo 44 da mesma lei, que com o caput esclarece as hipóteses de responsabilização quando:

- (i) Há uma violação de segurança dos dados

- (ii) Não forem adotadas as medidas de segurança previstas no art. 46 da LGPD

A Constituição Federal assegurou como um direito fundamental, a privacidade de qualquer indivíduo, e é sim uma violação da privacidade compartilhar dados cadastrais sem a permissão do titular dos dados, e muitas vezes também, mesmo que houve uma permissão prévia da pessoa.

Quanto a possibilidade da aplicação do danos morais, Marcel Leonardi (2012,p.225) comenta que acordo com um estudo relevante realizado anteriormente, os motivos para se enquadrar uma atitude em dano moral, deve ser considerado dentre vários fatores, se existe culpa, a posição social da pessoa que está sendo ofendida, a gravidade da ofensa que foi imposta, a situação econômica da pessoa ofensora, e principalmente, a gravidade da ofensa, pois é ela que define a quantificação psicológica da vítima do dano.

É a mesma coisa que expressa um julgado do TJ no Estado de São Paulo, como transcrito a seguir:

"RESPONSABILIDADE CIVIL - Ação de indenização por danos morais - Cerceamento de defesa - Inocorrência - Ré que repassou dados cadastrais acerca dos rendimentos do autor a terceira estranha e com fins sem qualquer ligação a outra relação de consumo - Abuso do objeto cadastral em detrimento da privacidade do autor -Dano moral in re ipsa - Quantum que não merece reparo - Correção monetária, por outro lado, que deve incidir a partir da data em que o valor foi arbitrado - Incidência de juros mantida a partir da citação - Encargos da sucumbência Reciprocidade - Inocorrência - Gratuidade processual que não pode ser revogada com base em futura indenização - Litigância de má-fé -Inocorrência - Recurso provido em parte. (TJSP - AC: 3.55.607400-0, Relator: De Santi Ribeiro, Órgão julgador: 1ª Câmara de Direito Privado Data de Julgamento: 02/07/2009, Data de Publicação: 18/08/2009)"

Como foi mostrado no julgado, a empresa ré da ação de indenização por danos morais foi condenada por repassar dados cadastrais a terceiros, gerando o dever de indenizar, com o fundamento de ter sido violada a privacidade do autor pela atitude abusiva da empresa.

Chega-se a conclusão, portanto, que a privacidade é um direito essencial a qualquer pessoa, por isso, com o advento de tantas inovações vem surgindo cada vez mais a necessidade de se garantir a segurança dos indivíduos.

Para garantir a segurança das empresas, surgiu o Compliance, e para proteger os clientes e colaboradores foi criada a Lei Geral de Proteção de Dados com todas as suas diretrizes.

Os bancos como uma instituição financeira, vão muito além na sua importância de proteger os dados pessoais de seus clientes, e até mesmo como uma forma de estar em Compliance, existe a necessidade de compartilhamento de dados para a proteção corporativa. No entanto sempre deve se proteger acima de tudo, o direito a privacidade, não somente por ser um direito fundamental, mas essencial de toda a sociedade.

Referências

BARBOSA, Fernanda Nunes. Informação e consumo: a proteção da privacidade do consumidor no mercado contemporâneo da oferta. *In*: MARTINS, Guilherme Magalhães (coordenador). **Direito privado e Internet**. São Paulo: Atlas, 2014.

CARDOSO, Oscar Valente. [Lei Geral de Proteção de Dados e diálogo das fontes - 4\) Lei do Sigilo Bancário](#). **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, [ano 25, n. 6259](#), [20 ago. 2020](#). Disponível em: <https://jus.com.br/artigos/84714>. Acesso em: 28 ago. 2020.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988

DUTRA, Vitor Martins. [LGPD: a lei que mudará a relação empresa/instituição e usuário/cliente](#). **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, [ano 24, n. 5844](#), [2 jul. 2019](#). Disponível em: <https://jus.com.br/artigos/75087>. Acesso em: 28 ago. 2020

_____. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

13 FEBRABAN – FEDERAÇÃO BRASILEIRA DE BANCOS, Função de Compliance, 2009.

Lei 13.709/2018 – Lei Geral de Proteção de Dados.

LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.

MORAES, Ana Paula .LGPD - Lei Geral de Proteção de Dados: sua empresa está pronta? Editora: Literare Books International – 1 edição – 152 páginas – 2020.

_____. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães (coord.). Direito privado e internet. São Paulo: Atlas, 2014

VERÍSSIMO, Carla. Compliance: Incentivo a adoção de medidas anticorrupção. Carla Veríssimo.- São Paulo: Saraiva, 2017.

Manual de Compliance / Coordenador Christian Karl de Lamboy. – São Paulo(SP): Via ética (2018) 1061 p.

