PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DAS *FINTECHS*

ORIENTANDA: AMANDA ALVARES RODRIGUES

ORIENTADORA: PROFª DRA. GLACY ODETE RACHID BOTELHO

GOIÂNIA-GO
2020

AMANDA ALVARES RODRIGUES

LEI GERAL DE PROTEÇÃO DE DADOS ÂMBITO DAS *FINTECHS*

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.ª Orientadora: Dra. Glacy Odete Rachid Botelho

GOIÂNIA-GO
2020

AMANDA ALVARES RODRIGUES

LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DAS *FINTECHS*

Data da Defesa: 17 de novembro de 2020.

BANCA EXAMINADORA

_____

Orientadora: Profª: Dra. Glacy Odete Rachid Botelho..... Nota_____

_____

Examinador Convidado: Prof.: Ms. Frederico Gustavo Fleischer .....

Nota _____

“Mas porque a maioria de nossos desejos se reporta a coisas que não dependem todas de nós, nem todas do outro, devemos exatamente nelas distinguir o que só depende de nós, a fim de reportar nosso desejo unicamente a isso.”

(Descartes, *As paixões da Alma*)

Dedicatória

Esta obra é dedicada à minha família que sempre apoiou meus projetos e sonhos, contribuindo para que a realização desta fosse possível.

Agradecimentos

Primeiramente, agradeço à minha família, por caminhar comigo nessa trajetória, seja no declínio ou no progresso; pelo amparo e assistência e; pelo apoio em minhas escolhas; sem este não seria possível a conclusão desta obra, tampouco seria possível acreditar que meus sonhos e objetivos poderiam ser alcançados.
Aos meus amigos que me apoiaram em minhas decisões e vibraram comigo a cada passo acertado.
À minha orientadora profª Glacy Odete Rachid Botelho, pela paciência e ensinamentos, pelos conselhos e recomendações, pela confiança em mim depositada e por tornar possível a conclusão desta obra.
À professora Nuria Micheline Cabral, por vislumbrar a mim tamanha confiança e tornar possível o início de minha trajetória, por questionar minha primeira decisão, caso contrário não haveria a existência do presente trabalho.
Ao professor Frederico Gustavo Fleischer, por acudir minhas indagações relativas ao tema e por trazer o direito empresarial de forma fascinante e descomplicada.
À professora Larissa Priscila Reis Bareato, por trazer às aulas de direito empresarial, palestras inerentes à empresas de inovação tecnológica, fato que tornou possível minha motivação e paixão pela área.
A todos os professores do curso de bacharelado em Direito da Pontifícia Universidade Católica de Goiás, que me forneceram todas as bases necessárias para a realização deste trabalho, agradeço com profunda admiração pelo vosso profissionalismo.
À Nayara Cléver por me proporcionar tantos conselhos e dicas referentes ao tema e *lives* que forneceram melhor entendimento do assunto.
Agradeço a todos aqueles que, de alguma forma, tornaram possível o início, a trajetória ou a conclusão do presente artigo, seja com auxílio educacional, conselho ou apenas uma vibração positiva.

SUMÁRIO

RESUMO

Amanda Alvares Rodrigues[1]

O presente artigo buscou analisar a aplicação da Lei nº 13.709/18 – e sua nova redação – às *fintechs*, bem como seu processo de transição e contribuição social deste segmento com o recente ordenamento. Foi utilizado o método hipotético-dedutivo onde os problemas foram testados e confrontados bibliograficamente. Investigou-se o surgimento recente das *fintechs* no ordenamento jurídico e sua regularização em que também recente, resume-se na Lei 13.709/18. A necessidade da coleta de dados foi compreendida em razão da proteção e segurança do usuário, bem como a individualização do serviço prestado. Já a eficácia da fiscalização foi analisada através de dados internacionais em que o regulamento brasileiro se baseou para construção da presente lei.

Palavras-chave: Lei Geral de Proteção de Dados. *Fintechs*. Direito empresarial. Direito bancário. Direito digital.

[1]Aluna do Curso de Direito e Relações Internacionais da PUC-Goiás

INTRODUÇÃO

A presente pesquisa busca analisar e compreender o processo de transição das *fintechs* no âmbito da recente Lei Geral de Proteção de Dados – Lei nº 13.709/18, porém, com redação atualizada pela Lei nº 13.853/19. A ideia se originou a partir do interesse pela inovação somado ao Direito Empresarial, ocasionando a participação em *workshops* e palestras deste segmento.

A crescente mudança no meio empresarial gera consequências tanto econômicas quanto jurídicas. Portanto, a revolução deste sistema implica, também, em modificações jurídicas. Recentemente, as chamadas *startups*, empresas recém-criadas que utilizam como base a tecnologia, modificaram o cenário econômico e impulsionaram a chamada "4º Revolução Industrial", como aduz Klaus Schwab acerca deste fenômeno:

> A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo.
> [...]
> O que torna a quarta revolução industrial fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitas e biológicos. (SCHWAB, 2016, p. 20)

Destarte, os sistemas construídos sob base tecnológica fazem *jus* a esta recente revolução. Assim, o segmento que se abordará na presente pesquisa são as chamadas *fintechs,* que consistem em *startups* direcionadas ao segmento financeiro. Cabe ressaltar que as financeiras se incorporam ao Sistema Financeiro, e o Banco Central do Brasil se encarrega de sua regularização, ainda que normatizado pelo Conselho Monetário Nacional.

Embora o Banco Central do Brasil tenha regularizado as *fintechs* através das resoluções de nºs 4.656/18, 4.657/18 e 4.658/18, sendo a última relacionada à segurança cibernética, ainda havia pontos a serem consolidados e realçados pelo ordenamento jurídico. Desta forma, ainda no ano de 2018, foi aprovada a Lei Geral de Proteção de Dados, a qual dispõe, a partir do conceito de dados pessoais, e finaliza com a unidade fiscalizadora de segurança de dados, incrementada pela Lei nº 13.853/19.

Atualmente, as *fintechs* contam com inúmeros usuários, e consequentemente, inúmeros dados. Desta feita, resta evidente que a informação acerca do processo de

transição é imprescindível tanto aos usuários quanto às próprias organizações. Não se sabe, ao certo, o grau de dificuldade das *fintechs* na aplicação da LGPD, como também é hipotético que todo usuário tem a convicção de como são utilizados os dados repassados.

A presente pesquisa busca demonstrar como as *fintechs* ingressaram e se estabilizaram no Brasil, visto que estas procuram se adequar às mudanças de acordo com o cenário internacional. Essa adequação poderia ser causa para que o grau de dificuldade de transição para a Lei Geral de Proteção de Dados seja ainda menor.

Em suma, grande parte dos usuários que optam por este segmento buscam inovação e confiam cada vez mais na tecnologia e seus derivados, logo, aderir às *fintechs* pode resultar em facilidade e confiabilidade, haja vista que houve queda no número de indivíduos que aderem aos bancos físicos suscitando em uma transformação significante no cenário financeiro e, consequentemente, no jurídico.

Entretanto, as *startups* especializadas no segmento financeiro detém inúmeros dados pessoais dos usuários, sendo estes coletados no momento de adesão ao serviço. A Lei Geral de Proteção de Dados traz em seu artigo 6º, inciso III, o chamado princípio da necessidade, o qual expõe a verificação da necessariedade da quantidade dos dados coletados dos usuários pelas empresas, aduzindo que seja somente o essencial.

Juntamente com os dados, levanta-se outro apontamento: a segurança destes. Sabe-se que há a transferência de dados, podendo ser ainda internacionalmente, portanto é lícito que haja a fiscalização eficaz para que os dados sejam devidamente protegidos, assegurando, dessa forma, a privacidade e individualidade do indivíduo.

A proteção de dados já se faz presente há anos no cenário internacional, posto que a LGPD brasileira em muito se assemelha com a *GDPR* europeia *(General Data Protection Regulation),* nesse sentido se baseia o ordenamento jurídico em matéria de proteção de dados.

Há de se analisar a trajetória aplicada do regulamento europeu para que possa ser feita uma analogia diante da aplicação da lei no Brasil, em vista de suas semelhanças. Ressalta-se ainda que, a eficácia deverá ser testada em análise à Autoridade Nacional de Proteção de Dados viabilizando seu escopo e sua competência, posto ser o órgão nacional responsável pela fiscalização do tratamento de dados.

Isto posto, a pesquisa procurará realizar uma minuciosa análise da aplicação da Lei Geral de Proteção de Dados às *fintechs*, assim como seu processo de transição, e as diretrizes que devem ser tomadas pelos organismos empresarias e a atenção exigida dos usuários, bem como as possíveis consequências que poderão ser acarretadas caso haja descumprimento do regulamento.

1 CONTEXTO HISTÓRICO DAS *FINTECHS* NO BRASIL

Para iniciar os estudos acerca das denominadas *fintechs* e sua trajetória até os dias atuais, é necessário adentrar no sistema do qual essa modalidade empresarial faz parte. Sabe-se que as *fintechs* são *startups* especializadas em serviços financeiros, entretanto, cumpre esclarecer o que vem a ser *startups* e como são regidos tais serviços.

Estes organismos regem-se de acordo com o sistema financeiro, ainda assim, não são consideradas instituições bancárias. O Banco Central do Brasil esteve se adequando acerca destas especialidades, à medida em que foram surgindo no cenário brasileiro, tendo editado as resoluções de nº 4.656/2018, nº 4.657/2018 e nº 4.658/2018, todas de 26 de abril de 2018, as quais serão tratadas no decorrer deste capítulo. Ademais, cumpre investigar a trajetória da fase inicial de uma *fintech*, as chamadas *startups* especializadas em serviços financeiros.

1.1 DA INOVAÇÃO EMPRESARIAL – DAS *STARTUPS* ÀS *FINTECHS*

Doutrinadores e estudiosos de diversas localidades do mundo afirmam que atualmente vivemos em meio à era da quarta revolução industrial, em meio a tecnologias nos campos físicos, biológicos e digitais, que muitas das vezes se entrelaçam entre si.

Porém, o que rege a quarta revolução industrial não se baseia somente em tecnologia, mas também na rapidez em que é ofertada, na agilidade de informações e no grande compartilhamento e armazenamento de dados, bem como salienta Klaus Schawb, (2016, p. 20) sobre o impacto sistêmico que estas inovações causam, como modificam o cenário econômico, empresarial, jurídico, e toda a sociedade.

Dentro deste cenário de evolução e aprimoramento tecnológico, especificamente no campo digital, encontram-se as *startups*. Embora o conceito de *startup* não seja uníssono, a maior parte de seus doutrinadores optam por definirem como empresas emergentes no âmbito tecnológico, utilizando-se da tecnologia para aprimorar serviços e modificar aspectos no cotidiano de seus usuários. No âmbito deste modelo empresarial, Saulo Michiles (2016, p. 05) as conceitua em “organizações que buscam melhorar algum aspecto da vida das pessoas, se utilizando

da tecnologia para fazer isso de uma maneira inovadora, disruptiva e escalável.” Deste modo, entende-se que as *startups* são empresas que se utilizam da tecnologia para aprimorar o cotidiano social, seja em tarefas simples ou complexas.

No Brasil, o número de *startups* tem crescido espantosamente com média de 26,75% por ano, segundo site da Associação Brasileira de *Startups*, como demostrado no quadro:

Top 4 estados					Total de startups cadastradas
Ano	São Paulo	Minas Gerais	Rio Grande do Sul	Rio de Janeiro	Brasil
2015	1.320	365	183	343	4.451
2016	1.327	591	184	343	4.273
2017	1.668	714	223	446	5.147
2018	3.060	720	885	843	10.000
2019	3.780	1.094	918	839	12.727

*Fonte: **Startupbase***

Diante deste fenômeno, cumpre ressaltar que dentre o crescimento das mencionadas *startups*, encontram-se as *fintechs*, uma das modalidades *startup* com grande aumento de unidades. A revolução das *fintechs* no Brasil teve início com a chamada *Nubank*, a pioneira no ramo no país, surgindo no ano de 2013.

Adentrou neste campo, inicialmente, oferecendo apenas crédito para seus usuários, porém, inovando ao longo dos anos, criou assim, a função débito e a chamada *Nuconta,* entretanto esta não é a única *fintech* em crescimento. Em maio de 2019, segundo o estudo *Fintech Mining Report* – Distrito, foram contabilizadas 550 (quinhentos e cinquenta) *fintechs* no Brasil e estima-se que atualmente este número ultrapasse a 600 (seiscentos), assim como demonstrado no quadro abaixo (fonte: Distrito):

Embora seja um grande avanço tecnológico, as *fintechs* cresceram de forma instantânea gerando outra preocupação: a sua regularização. Ainda não havia respaldo jurídico que empregasse meio regulatório para empresas denominadas *startups* especializadas no âmbito financeiro. Com base nesta premissa, o Banco Central do Brasil tomou para si a responsabilidade regulatória, através de resoluções específicas.

1.2 DA TRAJETÓRIA NORMATIVA DAS *FINTECHS*

Inicialmente, cumpre esclarecer a que meio pertence o relator das citadas resoluções. O Banco Central é regido pelo Sistema Financeiro do Brasil, sendo formado por órgãos normativos como o Conselho Monetário Nacional – CMN), entidades supervisoras como o Banco Central – BC, e os operadores como instituições bancárias, cooperativas de créditos, administradoras de consórcios, corretoras, entre outros. O Banco Central é responsável por fiscalizar e supervisionar as normas impostas aos componentes do sistema financeiro. Deste modo, as *fintechs* compõem parte deste sistema, na forma de operadora.

No ano de 2018, o número crescente de *fintechs* ocasionou a edição de três resoluções do Banco Central do Brasil. A resolução nº 4.656/2018, de 26 de abril de 2018, disciplina a constituição e o funcionamento da Sociedade de Crédito Direto (SCD) e da Sociedade de Empréstimo entre Pessoas (SEP), tipos de *fintechs* operadoras de crédito. No mesmo ano, o BC editou a resolução nº 4.657/2018, de 26 de abril de 2018, regularizando as *fintechs* de forma que pudessem permitir recursos creditórios e securitização, sem instituição bancária ou financeira. Já na resolução nº

4.658/2018, também de 26 de abril de 2018, a regularização aduz acerca da proteção de informações repassadas pelos usuários, salientando pela segurança destas. Luiz Gabriel Monteiro Rodrigues, em seu artigo publicado no ano de 2018, no sítio do JusBrasil, afirmou:

> De acordo com o representante do Banco Central, a edição do texto normativo tem intenção de trazer segurança jurídica à atividade. Essa afirmação é de grande valia para o atual cenário pátrio, haja vista a recente liquidação extrajudicial do Banco Neon.

No mesmo ano, o Banco Neon foi liquidado extrajudicialmente, mesmo que a decisão não tenha sido válida para a *fintech* que realizava os pagamentos – a Neon Pagamentos – entretanto, também foi afetada indiretamente, como a dificuldade de acesso dos usuários à época. Situações como esta criaram a necessidade de uma regularização ainda mais complexa, ao longo dos anos.

Destarte, com o crescimento demasiado dessas novas modalidades empresariais, surgiu a necessidade da criação de lei reguladora, a Lei nº 13.709, de 14 de agosto de 2018, a chamada Lei Geral de Proteção de Dados, aduzindo especificamente sobre seus princípios norteadores e acerca dos dados pessoais dos usuários. Entretanto, em 2019, a LGPD foi acrescida da Lei nº 13.853, de 08 de julho de 2019, dando-lhe nova redação e regularizando a autoridade nacional de proteção de dados.

A base normativa da Lei Geral de Proteção de Dados espelha-se na Lei europeia GDPR *(General Data Protection Regulation),* porém, é composta por diversas diferenças, a começar pela forma com que ambas lidam com o compartilhamento de dados, a saber:

> A GDPR, em seu considerando 31, afirma que o tratamento pautado nessa base legal não implica que as autoridades possam compartilhá-los entre si; enquanto a LGPD permite tal compartilhamento no próprio inciso que trata dessa base legal, contanto que se atente às finalidades específicas de execução de políticas públicas nos termos do artigo 26. (LUZ, 2019, p. 30)

Outrossim, ainda que em sua base tenha semelhanças como princípios e foco no tratamento de dados, seu escopo é ainda mais amplo, sendo dotado de inúmeras divergências. Ainda assim, resta evidente que a criação da LGPD sucedeu em consequência da transformação do tratamento de dados no âmbito internacional, dessa forma a *GDPR* deu início aos primeiros passos jurídicos, no Brasil, para a regularização dos segmentos em questão.

Não se trata de um novo tema em discussões internacionais, posto que a União Europeia postulou a Diretiva 95/46/CE que estabeleceu regras sobre o tratamento de dados e direito dos usuários membros do bloco dada à alteração no cenário bancário, ensejando em novos meios de pagamentos (*fintechs*) e compras (*e-commerce*), e, ainda, a junção destes em apenas um, visto que diversas plataformas de compras *online* também possuem seu próprio meio de pagamento, a exemplo, o *e-commerce* Mercado Livre e o meio de pagamento Mercado Pago.

Retornando a questão da *GDPR*, a aplicação extraterritorial desta ocasionou a necessidade de adaptação das empresas inclusive em outros territórios, tornando imprescindível a criação de ordenamento à égide do compartilhamento de dados pessoais. Tal respaldo atinge a todas as modalidades empresariais, sobretudo às *fintechs* considerando sua operação específica e precisa de dados de usuários, em vista ainda dos serviços financeiros prestados, ensejando a utilização de dados sensíveis.

Com o supracitado novo ordenamento jurídico como ferramenta imprescindível para o regular funcionamento destes organismos, o desafio se posiciona em outro questionamento: a criação da Lei Geral de Proteção de Dados acarreta dificuldade de adaptação às *fintechs*?

1.3 DA ADAPTAÇÃO DAS *FINTECHS* À LEI GERAL DE PROTEÇÃO DE DADOS

Como analisado anteriormente, as *fintechs* tiveram seu escopo tecnológico baseado internacionalmente, deste modo essas modalidades no âmbito nacional precisavam se manter antenadas às mudanças constantes em qualquer objeto que ocasionasse uma extensa modificação em territórios internacionais.

Com vastas opções ligando a inovação ao custo-benefício, as *fintechs* conquistaram rapidamente o público, sendo que os usuários aderiram aos serviços simplesmente pela facilidade, agilidade e, ainda, confiabilidade das finanças. Tal processo resultou na atenção destes organismos para com o cenário atual como um todo, visando problemas futuros e engajando soluções, apenas visando aos acontecimentos internacionais. Deste modo, ao passo que a Lei Geral de Proteção de Dados adentrou ao cenário jurídico empresarial, mesmo com sua entrada em vigor

somente no segundo semestre de 2020, muitas *startups* na modalidade *fintechs* já se mostram preparadas para receber a LGPD.

O setor em que as *fintechs* atuam, considera-se de risco, isto porque o campo financeiro lida diariamente com dados pessoais sensíveis e dados bancários dos usuários, deste modo, a segurança deste dados há de ser respaldada, garantida, e para que coexista a confiabilidade do usuário juntamente com a real segurança, tal elemento deve estar presente no momento de sua criação como empresa, implicando apenas no seu aperfeiçoamento no meio jurídico.

Entretanto, o maior problema em meio à era digital é justamente a invasão de dados, com os chamados *hackers*. A vulnerabilidade resulta da presente inovação tecnológica no nosso cotidiano, sendo chamada de tecnologia ubíqua. Neste cenário, a Lei Geral de Proteção de Dados busca combater exatamente essa fragilidade no que diz respeito aos dados, principalmente de empresas que lidam diretamente com a tecnologia, e esta última, em consonância com dados bancários, necessita de uma proteção ainda mais consolidada. A regulamentação das *fintechs* na nova lei têm ocorrido antes mesmo da sua entrada em vigor, a exemplo, a *Nubank* e a *Next* atualizaram sua política de segurança e de privacidade há poucos meses, estando à frente da entrada em vigor da LGPD.

Cumpre ressaltar que a adequação da empresa à lei também advém para oferecer ao usuário maiores informações diante destes organismos, posto que as políticas de segurança e privacidade não são sempre claras em seu escopo, caso em que a autora Ana Frazão tem premeditado:

> Certamente que muitas discussões surgirão em relação aos contratos eletrônicos, já que os agentes envolvidos deverão tomar as devidas providências para a obtenção, o registro e a comprovação de que houve o consentimento do titular em observância a todas as exigências legais. (FRAZÃO, 2018, p. 02)

Portanto, ainda que as *fintechs* estejam preparadas para a adaptação da Lei Geral de Proteção de Dados, esta se faz extremamente necessária em vista da regularização destas novas modalidades empresariais, para que qualquer lacuna no âmbito do tratamento de dados seja preenchida.

2 DA NECESSIDADE DA COLETA DE DADOS PESSOAIS

Atualmente, a coleta de dados pessoais tornou-se requisito primordial para a contratação da maioria dos serviços e compra de produtos, entretanto com a criação da Lei nº 13.709, em 14 de agosto de 2018, restaram estabelecidos limites impostos acerca da quantidade e finalidade do requerimento de determinados dados visando a segurança do titular.

Baseando-se na Constituição Federal de 1988, a Lei nº 13.709/18 prevê, em seu art. 2º, fundamentos acerca da proteção de dados, os quais versam acerca do respeito à privacidade; à liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da hora e da imagem; o desenvolvimento econômico, a livre iniciativa e a defesa do consumidor, dentre outros. Embora a mencionada lei objetive a proteção dos dados dos usuários, também estabelece maior segurança às empresas que necessitam da coleta de dados para o oferecimento de serviços, já que não havia qualquer amparo jurídico perante este segmento.

Ainda que a atual legislação verse sobre a proteção individual dos usuários e estabeleça amparo jurídico empresarial, há ainda um campo maior visado pela LGPD: a proteção da segurança pública. Bem como preconiza Patrícia Peck Pinheiro:

> [...] há sempre necessidade de equilibrar a proteção da privacidade (como um direito individual) e a proteção da segurança pública (como um direito coletivo), especialmente diante da obrigação de fortalecer o combate ao crime organizado, à fraude digital e ao terrorismo. (PINHEIRO, 2020, p. 78)

Destarte, a solução primordial para as diversas inseguranças amparadas no cenário atual seria a implementação de normas regulatórias acerca dos dados pessoais, posto que a coleta destes dados não deixará de ocorrer e os riscos tendem a aumentar diante da exigente adaptação tecnológica à qual se induz.

Diante deste fato, a Lei Geral de Proteção de Dados introduziu princípios para regulamentação destes organismos, dispostos no art. 6º, a saber, princípio da finalidade, da adequação, da necessidade, do livre acesso, da qualidade, da transparência, da segurança, da prevenção, da não-discriminação, da responsabilização e prestação de contas. Os princípios elencados, em sua literalidade, são autoexplicativos, como o princípio da não-discriminação, o qual consiste em não utilizar dados pessoais, principalmente dados sensíveis, de forma

discriminatória ou de modo que possa induzir outrem a isso, como por exemplo, em campanhas publicitárias.

Ainda que a coleta de dados seja necessária, esta precisa ter sua finalidade fundamentada, adequando-se ao serviço prestado pela empresa, utilizando apenas os dados necessários para o prosseguimento da relação de titular e controlador (“a quem competem as decisões referentes ao tratamento de dados”, art. 5º, inciso VI, LGPD/18).

Isto posto, pretende-se compreender a coleta de dados, especificadamente realizada pelas *fintechs,* visando a contribuição na melhora de prestação dos serviços perante os princípios enumerados na Lei nº 13.709/18.

2.1 DA CONCEITUAÇÃO DOS DADOS ATRAVÉS DA LEI Nº 13.709/18

Vislumbrando um melhor entendimento, cumpre ressaltar, primeiramente, o conceito do que vem a ser dado pessoal, o que esclarece a Lei nº 13.709 /18, em seu art. 5º, inciso I, quando aduz “dado pessoal: informação relacionada a pessoa natural identificada ou identificável”. Deste modo, dado pessoal é todo aquele relacionado à pessoa, visando identificar o indivíduo, podendo ser desde o nome do titular até informações relativas ao computador ou máquina utilizada, como Endereço de IP (Protocolo da Internet). Adentrando ao tema, há ainda a classificação de dados sensíveis prevista no art. 5º, inciso II, do mesmo diploma legal citado, o qual expõe:

> 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;

Os dados sensíveis encontram-se dentro de um parâmetro além do pessoal, com uso ainda mais estrito pela lei que o versa, de modo que as hipóteses de sua utilização se restringem apenas em casos indispensáveis, como por exemplo, para garantir a segurança do titular, prevenindo a fraude contra este. Sabe-se que os dados considerados sensíveis muitas vezes versam conhecimento sobre características físicas, psicológicas e comportamentais do indivíduo, devendo ser altamente

protegidos para resguardar a individualidade do titular. Como bem salienta Ana Frazão:

> Acresce que discussões mais recentes apontam para a ocorrência de fenômeno de publicidade comportamental voltado à formação de perfis de consumo, fato que se relaciona diretamente à regulação do tratamento de dados pessoais, em especial os dados sensíveis. (FRAZÃO, 2018, p. 02)

Portanto, para evitar os transtornos e inseguranças que permeiam os dados sensíveis fez-se necessário abordá-los de forma diferente dos dados pessoais comuns. Destarte, o art. 12, § 2º, da Lei Geral de Proteção de Dados, determina que também são considerados dados pessoais "aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada".

Ademais, os organismos citados fazem parte de um banco de dados estruturado e estabelecido em um ou vários locais, podendo ser em suporte eletrônico ou físico (art. 5º, inciso IV, Lei nº 13.709/18), entretanto, dados anonimizados não agrupam este segmento, posto que são dados os quais não se pode identificar o titular, "aquele incapaz de revelar a identidade de uma pessoa, e por isso, não apresenta necessidade de proteção legal" (VAINZOF, 2018, p. 37).

Dispõe a LGPD que somente utilizará os dados anonimizados caso o processo de anonimização ao qual foram submetidos for revertido (art. 12), restando visível a titularidade dos dados, estes serão considerados dados pessoais.

Embora a lei não trate sobre isso, existe, ainda, a pseudoanonimização que consiste na descentralização dos dados perante o titular, ou seja, os dados coletados são tratados a não dispor de titularidade precisa. A criptografia e a tokenização (gerador de código identificador digital exclusivo) são exemplos claros de pseudoanonimização.

O ramo empresarial que versa sobre as *fintechs* consiste inteiramente na coleta de dados dos usuários, haja vista tratar de serviços financeiros, os quais exigem extrema segurança da identidade e finanças destes consumidores. Embora seja comum o uso de *internet banking*, financeiras e bancos inteiramente digitais, a segurança pautada pelo titular dos dados transferidos a estes organismos é de extrema importância, tanto ao usuário quando à empresa, visto a onda de notícias nos anos anteriores a respeito do vazamento de dados de empresas, principalmente digitais.

2.2 DO TRATAMENTO DE DADOS REALIZADO PELAS *FINTECHS*

Desde o surgimento das *fintechs* são utilizadas coletas de dados dos usuários para uma experiência mais segura e individualizada, de modo que o serviço oferecido é moldado mediante o perfil do consumidor. Dispõe a Lei nº 13.709/18, em seu artigo 5º, que o tratamento é conceituado como:

> Art. 5º [...]
> X – tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Embora seja ao controlador a quem competem as decisões relacionadas ao tratamento de dados pessoais dos titulares, a figura do operador se encontra presente, pois este realiza o procedimento em nome do controlador. Ademais, a Lei nº 13.853, de 08 de julho de 2019, modificou o inciso VIII, da Lei nº 13.709/18, incumbindo o encarregado para atuar como canal de comunicação entre o controlador, titulares dos dados e a Autoridade de Proteção de Dados (ANPD). Entretanto, os agentes de tratamento abordam apenas o controlador e operador, visto que estes realizam diretamente o tratamento dos dados pessoais.

Outrossim, para que o tratamento seja realizado, é necessário seguir restritas regras para requisição dos dados pessoais previstas no ordenamento. Embora seja de suma importância o consentimento do titular, esta não é a única alternativa, posto que o próprio titular, muitas vezes, disponibiliza dados pessoais publicamente podendo ser utilizados por organismos empresariais visando, principalmente, o *marketing,* sem a necessidade de consentimento*.* Ainda assim, vale rememorar:

> [...] **é importante ressaltar que são exceções à regra do consentimento os dados tornados manifestamente públicos pelo titular. Todavia, mesmo nesses casos, o tratamento de tais dados continua sujeito ao respeito aos direitos deste.** Com efeito, enquanto o § 3º do art. 7º da LGPD dispõe que "O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização" o § 4º do mesmo artigo prevê que "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei" (FRAZÃO, 2018, p. 01) (Grifo nosso)

Evidencia-se que, mesmo quando os dados são disponibilizados pelo próprio titular publicamente, é indispensável que sejam tratados conforme dispõem os princípios elencados em lei, posto que neste caso o titular pode opor-se ao tratamento realizado se houver descumprimento ao disposto no ordenamento jurídico pertinente. Portanto, a LGPD, em seu art. 7º, salienta as hipóteses em que o tratamento poderá ser efetuado:

> Art. 7º **O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:**
>
> **I - mediante o fornecimento de consentimento pelo titular;**
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> **V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;**
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> **X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.** (Grifo nosso)

No momento em que o usuário aceita os serviços oferecidos pela empresa, deve ser disponibilizado contrato de serviço informando como será realizado o tratamento, especificando os dados pessoais que serão coletados, bem como a finalidade da coleta, estes contratos são os chamados “Termos de uso e serviço”. Desta forma, faz-se necessário o consentimento expresso para o recolhimento dos dados pessoais inerentes ao titular, tratando-se de contrato vinculado ao controlador por serviço prestado.

Lado outro, os serviços prestados pelas *fintechs* são de caráter financeiro, por isso entende-se que a coleta de determinados dados remete à proteção do crédito do usuário. Deste modo, além dos dados específicos e necessários à prestação do serviço, posteriormente poderão ser solicitados dados opcionais não obrigatórios, como a biometria do titular. Tal requisição consiste, geralmente, na proteção de

finanças do usuário, entretanto o titular poderá revê-los, possuindo o direito de abstê-los da empresa.

Portanto, visando a atual normativa, as *fintechs* têm adequado políticas que facilitam o entendimento dos usuários para que esteja claro o consentimento, ensejando apenas em atos positivos, de modo que as *startups* deste segmento permaneçam imunes na confiança e praticidade que buscam transmitir. Rememora-se, ainda, que o consentimento deve se referir a finalidades determinadas, haja visa que as autorizações genéricas serão consideradas nulas. Salienta a doutrinadora Ana Frazão sobre o tema:

> Certamente que muitas discussões surgirão em relação aos contratos eletrônicos, já que os agentes envolvidos deverão tomar as devidas providências para a obtenção, o registro e a comprovação de que houve o consentimento do titular em observância a todas as exigências legais. (FRAZÃO, 2018, p. 02)

Cumpre ressaltar que o consentimento não será válido se houver vício de vontade (art. 8º, §3º, LGPD), ou seja, a vontade do titular deve ser expressamente comprovada. Outrossim, ainda em observância às novas regras, qualquer mudança no tratamento dos dados, ou necessidade de compartilhamento de dados pessoais com outros controladores, deverá ser comunicado ao titular para obtenção do consentimento para este fim, exceto para os dados tornados manifestamente públicos pelo titular, resguardando a finalidade, a boa-fé e o interesse público que justificaram a disponibilização dos mencionados dados.

Vale ressaltar que o mesmo não se aplica aos dados pessoais sensíveis, os quais poderão ser objeto de vedação se compartilhados para obter vantagem econômica, e caso for inerente à saúde do titular, salvo se consistir em assistência à saúde. Entretanto, a Lei nº 13.709/18 especifica algumas hipóteses em relação aos dados pessoais sensíveis, em seu art. 11, inciso II, alínea “g”, salientando que não será necessário o consentimento do titular quando tratar-se de:

> Art. 11 - [...]
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Nota-se a aplicabilidade da mencionada alínea no âmbito das *fintechs*, visto que a proteção dos dados dos usuários é medida imprescindível para um bom funcionamento das referidas unidades, posto a exposição ao ambiente digital, aumentando o risco de fraudes mediante a vulnerabilidade da empresa. É imperioso que sejam desenvolvidos meios e modos de garantia à segurança dos usuários de serviços financeiros eletrônicos, e para tornar possível, faz-se necessário o uso de demais dados pessoais, bem como a proteção destes.

Dessume, o tratamento de dados alcançará seu fim mediante: a perca da necessidade de uso dos dados coletados; fim do período de tratamento, comunicação do titular, inclusive para revogar seu consentimento; e, ainda, por determinação legal havendo violação da lei (art. 15, Lei nº 13.709/18). E, consequentemente, serão eliminados após o término, salva a conservação mediante as hipóteses em que visa o cumprimento de obrigação legal ou regulatória pelo controlador; o estudo por órgão de pesquisa, possibilitando de preferência, a anonimização dos dados pessoais; transferência a terceiro, desde que em consonância com a lei; e para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

2.2.1 Da adequação da política das *fintechs* ao regular tratamento de dados – *nubank*

Muitas empresas têm se adequado à Lei nº 13.709/18, inclusive a *fintech* pioneira do ramo no Brasil, *nubank*, atualizou, há alguns meses, a política de privacidade da empresa, se adequando às normas regidas pela lei. Detalhando os dados informados pelo titular e por terceiros e, especificando sua adequação ao contrato almejado pelo consumidor do serviço. Como, por exemplo, o recolhimento de dados da máquina utilizada pelo usuário consiste na navegação do titular no sistema da empresa, haja vista tratar-se de um organismo completamente digital.

Ainda assim, são recolhidos dados pessoais sensíveis, almejando a segurança do indivíduo, bem como dispõe em lei, como aduz trecho da Política de Privacidade, item 3, da referida empresa ao tratar da finalidade dos dados biométricos: “prevenção à fraude e garantia da sua segurança nos processos de identificação e autenticação de cadastro e de novo dispositivo” (Termos de Uso e Serviços *Nubank*, 2020). Bem como salienta a Lei nº 13.709/18:

> Art. 9º **O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:**
>
> **I - finalidade específica do tratamento;**
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> **IV - informações de contato do controlador;**
> **V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;**
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (Grifo nosso)

Em consonância com este dispositivo, os termos de uso e serviços da *nubank* dispõem das informações de contato do controlador, o qual, como titular dos dados, poderá entrar em contato a qualquer momento, para solicitar dispensa de consentimento, obter conhecimento de quais dados estão sendo tratados, solicitar a exclusão de dados desnecessários, informações de compartilhamento, entre outras, disponibilizando acesso simples para o usuário do sistema. Dessume, a LGPD salienta acerca da importância de proteção dos dados pessoais, desta forma, vislumbra a referida *fintech* sobre as medidas de segurança que permeiam os dados pessoais dos usuários, visando a garantir a integridade destes, posto ainda serem necessários, para adesão de serviço financeiro, consequentemente, mais seguro.

2.3 DOS DIREITOS DOS TITULARES DOS DADOS MEDIANTE A LEI nº 13.709/18

Cumpre rememorar que, como mencionado, os princípios tratados na Lei nº 13.709/18 encontram-se baseados na Constituição Federal de 1988, garantindo ao titular dos dados os direitos fundamentais de liberdade, de intimidade e de privacidade. Isto posto, os direitos vislumbrados pautam-se na obtenção de informações e quesitos que podem ser exigidos pelo titular ao controlador, em relação aos dados por ele tratados, obedecendo aos princípios da transparência, qualidade e livre acesso.

A propósito, pode o titular requisitar: a confirmação da existência de tratamento, bem como seu acesso aos dados e a correção destes, caso se encontrem incompletos, inexatos e desatualizados; podendo ainda exigir a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou em desconformidade

com a lei, bem como a eliminação de dados tratados, mesmo com consentimento, em casos expressos em lei; requerer informação das entidades públicas e privadas em que foram compartilhados os dados pelo controlador, e sobre a possibilidade de não fornecer o consentimento e as consequências desta ação, bem como a revogação do consentimento nos termos da lei; e acrescentado pela Lei nº 13.853/2019, o direito à portabilidade dos dados a outro fornecedor de serviço ou produto (art. 18, LGPD, 2018).

Observa-se que os direitos inerentes ao titular dos dados baseiam-se nos princípios primordiais da Lei nº 13.709/18, dispostos no art. 6º, como já mencionados. A adequação das *fintechs* aos termos expostos têm sido realizada ao longo dos últimos dois anos, como são empresas que tem como base as mudanças mundiais, seja tecnológica ou jurídica, tal modificação não se apresentou como uma impossibilidade à política empresarial deste segmento, procurando se atentar às tendências internacionais, visto que em outros países, há anos, aplica-se a proteção de dados.

Em continuidade, os direitos dos titulares encontram-se dispostos por diversos artigos da Lei nº 13.709/2018, já demonstrado em seções anteriores, não se limitando, apenas, ao art. 18, como ilustra a doutrinadora Ana Frazão:

> Por essa razão, há que se considerar que a descrição do art. 17 é meramente exemplificativa e precisa ser interpretada em conformidade com os artigos anteriores da lei que tratam da questão, especialmente no que diz respeito ao livre desenvolvimento da personalidade, à autodeterminação informativa, à dignidade da pessoa humana e ao exercício da cidadania. (FRAZÃO, 2018, p. 1)

Outrossim, todo e qualquer dos direitos expressos na referida lei serão exercidos mediante requisição do titular aos controladores, caso não seja possível o imediato cumprimento, deverá informar motivos e causas da não providência da requisição, estabelecida em apenas duas hipóteses: não for este o agente de tratamento e, desta forma, indicá-lo; indicar fatos ou direitos que impeçam a adoção imediata da providência. Não fundamentado em lei ou direito do controlador ou agente de tratamento, o titular poderá peticionar perante a autoridade nacional de dados (ANPD), podendo ser exercido, também, perante os organismos de defesa do consumidor, de forma individual ou coletiva.

As informações deverão ser disponibilizadas de forma clara, segura e de modo acessível às necessidades do titular, rememorando que o indivíduo poderá

rever as decisões de consentimento a qualquer tempo, incluindo a solicitação de revisão de dados pessoais que afetem seus interesses, inclusive “decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou de aspectos de sua personalidade” (art. 20, LGPD, 2018), bem como poderá opor a tratamento fundamento nas hipóteses de dispensa de consentimento, caso descumprimento da lei.

Cumpre ressaltar que o exercício do direito do titular relativo aos seus dados pessoais não poderá ser usado para prejudicá-lo, ou seja, este ato não poderá ser utilizado para traçar seu perfil perante quaisquer órgãos, em especial às empresas que dependem da coleta de dados para seu funcionamento, como organismos publicitários.

3 DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Criada em 26 de agosto 2018, a Lei nº 13.709 prevê em seu diploma legal a criação da Autoridade Nacional de Proteção de Dados (ANPD) e o seu regimento organizacional, estipulada pela Medida Provisória nº 859/2018, foi posteriormente modificado pela Lei nº 13.853/19, arguindo nova redação à Lei Geral de Proteção de Dados. Entretanto, a criação da ANPD somente foi vislumbrada através do Decreto nº 10.474, de 26 de agosto de 2020.

O caminho legislativo para criação da autoridade competente, embora turbulento, resta necessário, tendo em vista o cenário atual, o qual emerge à quarta revolução industrial, com evidentes mudanças tecnológicas. Tais mudanças despertam a iniciativa jurídica a se adequar e, com a Autoridade Nacional de Proteção de Dados não poderia ser diferente. Isto posto, deve manter em aberto a possibilidade de posteriores modificações, sejam jurisprudenciais ou dispositivos próprios em lei, atentando-se ao surgimento de novos segmentos ou políticas organizacionais que precisarão ser analisadas minuciosamente.

Neste sentido, o Decreto nº 4.474/2020, de 26 de agosto de 2020, estabelece o conceito jurídico da Autoridade Nacional de Dados bem como dispõe de sua competência, senão vejamos:

> Art. 1º A Autoridade Nacional de Proteção de Dados - ANPD, órgão integrante da Presidência da República, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem o

> objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na Lei nº 13.709, de 14 de agosto de 2018.

Visando aos princípios elencados no disposto acima, dentre as competências inerentes à ANPD, deve ser zelada a proteção dos dados pessoais, bem como a elaboração de diretrizes para a Política Nacional de Dados Pessoais e da Privacidade e ainda, devem ser editadas normas e orientações de caráter incremental para microempresas e *startups,* ou empresas de inovação, para que possam se adequar ao disposto na LGPD, entre outras disposições elencadas no art. 2º, do mesmo diploma legal. Ademais, qualquer que seja a medida tomada pelo referido órgão deve-se atentar pela preservação do segredo empresarial e do sigilo das informações.

Para regulamentação e segurança, a autoridade nacional poderá determinar ao controlador dos dados que elabore relatório de impacto à proteção de dados pessoais, inclusive sensíveis, referente a suas operações de tratamento. Este relatório deverá conter a descrição dos tipos de dados coletados e a metodologia utilizada para tratamento, para que seja garantida a segurança das informações.

Já o encarregado atua como meio de comunicação entre o titular dos dados e a autoridade nacional, como a aceitação de reclamação dos titulares, devendo prestar esclarecimentos e adotar providências, e ainda, deve receber comunicações da autoridade nacional bem como adotar as devidas providências, e, da mesma forma, deve orientar os funcionários da entidade a respeito das práticas estabelecidas em favor da proteção dos dados pessoais.

Outrossim, para que esteja assegurada a privacidade do indivíduo, as medidas adotadas devem se mostrar eficazes frente à proteção de dados dos usuários. Em vista da existência do compartilhamento de dados internacionalmente, resta estritamente necessária a garantia da segurança dos mesmos.

3.1 DA GARANTIA DE SEGURANÇA NO COMPARTILHAMENTO INTERNACIONAL DE DADOS

Convém ressaltar que o crescimento demasiado de informações em meio ao atual cenário norteado de novas plataformas digitais e tecnologias de ponta, em consonância com o compartilhamento desenfreado de informações, se faz estritamente necessária a proteção exigida aos dados pessoais. Entretanto, sabe-se

que a maioria das empresas de prestação de serviços ou até mesmo de venda de produtos utilizam os dados de seus usuários ou clientes para melhor garantia do serviço. Portanto, é necessário equilíbrio entre as partes, para que não haja prejuízo para ambos, a privacidade do titular deve ser pautada assim como a segurança econômica das empresas, leciona Patrícia Peck Pinheiro:

> Precisamos aprender a usar a tecnologia de forma ética, segura e legal. A liberdade não pode se tornar uma bandeira para proteção de criminosos. O anonimato, por si só, estimula prática de ilícitos. Há necessidade de que o Estado tenha uma atuação social forte, mas que garanta a livre-iniciativa com o mínimo de intervenção possível. (PINHEIRO, 2013, p. 49)

Destarte, o controle de proteção de dados deve atender aos princípios constitucionais de garantia à liberdade e a privacidade, atentando-se a ambas as partes. É evidente a vulnerabilidade dos dados pessoais, principalmente sensíveis, em meio a diversidade tecnológica, o surgimento de novos organismos propiciou maior levantamento de dados, entretanto empresas utilizam dados de cliente há muito tempo, antes mesmo de qualquer inovação tecnológica.

No mesmo sentido, as *fintechs* fazem o uso de dados de seus usuários, e assim como qualquer outra empresa, o uso é necessário para levantamentos econômicos, tributários, bem como cadastros e oferecimento de demais produtos e serviços que se encaixam no perfil do usuário. Porém, a lei prevê que podem ser realizados compartilhamentos de dados com terceiros e estabelece critérios para tal feito, cujo conceito se encontra disposto no art. 5º, inciso XVI, da Lei nº 13.709/18, a saber:

> Art. 5º. [...]
>
> XVI – Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

Deste modo, o controlador deve obter consentimento específico do titular para que seja possível o compartilhamento dos dados com terceiros ou outros controladores. Caso o consentimento tenha sido obtido mediante um primeiro serviço, deve o controlador comunicar ao titular sobre o compartilhamento. Como já dito anteriormente, a Lei Geral de Proteção de Dados poderá vetar o compartilhamento de dados pessoais sensíveis entre controladores que tenham como objetivo a vantagem

econômica, estando terminantemente vedado o compartilhamento de dados sensíveis referente à saúde que seja com o objetivo de obter vantagem econômica. Vale lembrar que o titular possui o direito de se informar das entidades com as quais o controlador realizou compartilhamento de dados. O artigo 30, da Lei nº 13.709/18, aduz que a autoridade nacional poderá editar normas complementares em relação ao uso dos dados de modo a garantir sua eficiência e segurança.

No mesmo sentido, evidencia-se o compartilhamento de dados internacionalmente, dispondo de regras que deverão ser observadas pela autoridade nacional e, se for o caso, aplicar as devidas sanções. Salienta o art. 33, da Lei nº 13.709/18, sobre os meios permissivos de compartilhamento internacional de dados, dentre os quais poderão ser realizados para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto em lei, caso a transferência seja necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros, e quando a autoridade nacional autorizar a transferência, entre outras.

Isto deve ser feito de modo que a autoridade nacional analise atentamente a eficiência de proteção de outros países, para que possa ocorrer a transferência de dados, e assim, garantir a segurança da privacidade do titular bem como a liberdade econômica da empresa, bem como salienta a doutrinadora:

> [...] a ANPD será incumbida de tornar a LGPD mais clara, acessível e palatável, tanto para os titulares de dados quanto para os agentes de tratamento, garantindo maior segurança jurídica às transações que envolvem o tratamento das informações pessoais, já que essas são uma das competências da Autoridade, conforme o art. 55-J da Lei Geral de Proteção de Dados. (PINHEIRO, 2020, p. 55)

Portanto, de acordo com sua competência, a ANPD visa a garantir maior égide ao tratamento e para que o nível de seguridade seja eficiente, a Lei Geral de Proteção de Dados propõe que medidas coercitivas sejam tomadas, resultando nas sanções dispostas na seção I, do Capítulo VIII, da Lei nº 13.709/2018, que devem ser aplicadas pela Autoridade Nacional de Proteção Dados.

3.2 DAS SANÇÕES IMPOSTAS PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

O Decreto nº 4.474/2020 determina em seu art. 2º, inciso IV, que compete à Autoridade Nacional “fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso”. Dessarte, alerta o §5º, que devem ser respeitados os segredos empresariais e o sigilo das informações. Desta forma, o art. 52, da Lei nº 13.709/18, juntamente com dispositivos adicionados através da Lei nº 13.853/19, dispõe sobre as sanções que poderão ser aplicadas caso haja descumprimento da lei, a saber:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total a que se refere o inciso II;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Observa-se que há punições brandas e severas com multas de valores variáveis, deve se atentar que tais medidas deverão ser aplicadas com base no princípio da proporcionalidade e razoabilidade, a depender do caso concreto. Isso porque a Autoridade é órgão nacional, dito isso, deve ser regida pelos princípios norteadores da Administração Pública, visando a privacidade do titular e a liberdade

do controlador. Vale rememorar, ainda, que a autoridade deverá regular tempo hábil para a adequação dos bancos de dados à LGPD, observando a natureza das informações e sua complexidade.

Neste cenário, destacam-se as empresas de inovação tecnológica, como as *fintechs*, que devem ter suas ações pautadas diante do risco que suas atividades agregam, rememorando que tais organismos demandam inúmeros dados para seu funcionamento e, por isso, necessitam de adequação precisa. O risco resulta da vulnerabilidade que possuem os dados, ora necessários, para o serviço financeiro prestado, podendo ser alvo de ataques cibernéticos, fato que ocasionaria prejuízos imensuráveis tanto à empresa quanto aos usuários do sistema. A propósito explica a doutrinadora:

> [...] o fiscalizador da nova regulamentação também deve levar em consideração alguns critérios que possam agravar ou amenizar a aplicação da sanção, visto que a possibilidade de ocorrência de uma violação de dados a partir de uma violação de segurança é altíssima no contexto digital atual, até por uma grande carência de investimentos no combate ao crime organizado que opera na Internet e que já se utiliza de recursos sofisticados para atacar indivíduos e instituições de todo e qualquer porte. (PINHEIRO, 2020, p. 133)

Contudo, mesmo a empresa aderindo às práticas de segurança e de acordo com a lei, pode ocorrer o incidente de vazamento de dados pessoais, por isso deve ser levado em conta os riscos da atividade no momento de aplicação da sanção. Assim, mesmo que a Autoridade Nacional permeabilize a utilização de medidas coercitivas é necessário um maior alcance para o combate de crime organizado cibernético, tal ação deve partir de outras entidades de segurança visando maior anteparo aos titulares e controladores.

Outrossim, o desenvolvimento tecnológico tem se mostrado engajado diante de políticas de proteção, visto que diversos meios de segurança já foram criados para elaboração de atividades que utilizem dados por meio digital, a exemplo disso é a tokenização, bastante utilizada na área financeira digital, consistindo em gerar um código identificador digital exclusivo, aleatório e temporário para proteger dados sensíveis. Salienta o doutrinador Nelson Abrão:

> O avanço tecnológico traz em seu bojo o mecanismo da incorreção de maiores invasões das redes e das concentrações de recursos, no sentido de eliminar falhas, consertar as adversidades, oferecendo ao cliente consumidor um serviço funcional e de qualidade segura. (ABRÃO, 2018, p. 294)

Embora o escopo tecnológico das *fintechs* possa agregar riscos às atividades financeiras, este mesmo escopo serve de parâmetro para proteção das informações, diante de medidas de segurança viabilizadas somente por meio do avanço digital. A cooperação de cientistas de inovação tecnológica com a Autoridade Nacional de Proteção de Dados poderá proporcionar mais segurança para o uso digital em diversas plataformas, possibilitando maior confiabilidade a este meio, oportunizando o uso de novas ferramentas propostas pelas empresas de inovação tecnológica.

3.3 DO GRAU DE EFICIÊNCIA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Como já dito anteriormente, a Lei Geral de Proteção de Dados baseia-se na *General Data Protection Regulation* (*GDPR*) ou, Regulamento Geral de Proteção de Dados da União Europeia, que teve entrada em vigor no ano de 2018, 02 (dois) anos após sua criação. Para ter ciência da eficácia da Autoridade Nacional, cumpre observar os resultados consequentes da ação da *GDPR* no âmbito de seu poder, como ensina Patrícia Peck Pinheiro (2020, p. 51) que, “o que se pode esperar da atuação da ANPD no Brasil pode ser espelhado na experiência em outros países”.

Dessume, a LGPD em muito se assemelha com a *GDPR*, a aplicação de sanções iniciou-se juntamente com o vigor do regulamento e, mesmo havendo dois anos de criação da lei, uma das penalidades mais aplicada foi justamente a inadequação das empresas às diretrizes de tratamento e segurança dos dados. No Brasil, as sanções entram em vigor somente no segundo semestre de 2021, oportunidade para melhor adequação, tanto de empresas, quanto de titulares ou, até mesmo, para profissionais da área.

Assim, tanto o regulamento europeu quanto o regulamento brasileiro de dados buscam efetivar a proteção e a privacidade dos dados, garantir confiabilidade ao titular, e em consonância, garantir à empresa diretrizes em que possa solucionar problemas e obter maior segurança jurídica, visto que anteriormente não havia qualquer regulamento próprio que viabilizasse a forma e o uso de tratamento de dados.

Outrossim, o site *http://www.enforcementtracker.com/* demonstra como têm sido a aplicação do Regulamento Geral de Proteção de Dados, indicando as penalidades impostas a partir do caso concreto e de acordo com as diretrizes expostas

pelo regulamento. O quadro abaixo denota as violações que ocorrem em maior número e respectivamente a soma das multas impostas:

Violação	Número de multas
Base jurídica insuficiente para o processamento de dados	**156** (com soma total de € 128.919.040)
Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	**83** (com soma total de € 335.201.807)
Não conformidade com os princípios gerais de processamento de dados	**64** (com soma total de € 17.571.565)
Cumprimento insuficiente dos direitos dos sujeitos de dados	**41** (com soma total de € 9.534.197)
Cumprimento insuficiente das obrigações de informação	**20** (com soma total de € 568.305)
Cooperação insuficiente com autoridade fiscalização	**15** (com soma total de € 135.211)
Cumprimento insuficiente das obrigações de notificação de violação de dados	**9** (com soma total de € 220.725)
Falta de nomeação de oficial de proteção de dados	**4** (com soma total de € 136.000)
Acordo de processamento de dados insuficiente	**2** (com soma total de € 14.380)
Cooperação insuficiente com autoridade fiscalização	**1** (com soma total de € 4.400)
Cumprimento insuficiente das obrigações de violação de dados	**1** (com soma total de € 286)
Desconhecido	**1** (com soma total de € 500)

Observa-se que, como já premeditado anteriormente, o maior número de violações decorre da falta de técnicas que possam garantir a segurança de dados, como também, da insuficiência de base jurídica para o processamento das informações. Para tanto, em um panorama brasileiro, esta violação pode ser alvo de inúmeras sanções diante da lacuna profissional para adoção de medidas que intensifiquem a base jurídica da empresa em relação ao tratamento de dados.

Entretanto, muitas empresas de inovação tecnológica, bem como os profissionais atuantes no direito digital, têm se adequado às diretrizes do regulamento brasileiro, antes mesmo do vigor da lei. Tal ponto pode ser demonstrado diante das atualizações da política de privacidade das referidas empresas, como já demonstrado pela *Nubank* e outras *fintechs* brasileiras.

Vislumbra-se, através da Lei nº 13.709/18, que a Autoridade Nacional de Proteção de Dados traz consigo a missão de regulamentar as diretrizes apontadas pela lei, isso porque não poderia ser demonstrada qualquer eficácia se não houvesse medidas coercitivas. Aduz a doutrina majoritária que:

> De maneira geral, pode-se afirmar que a constituição da ANPD é essencial para que o *enforcement* da Lei Geral de Proteção de Dados seja possível, ou seja, é esse regulamento que torna a aplicação da lei possível. Isso ocorre

> porque **um regulamento com previsão de sanções sem órgão fiscalizador não tem efetividade nem garantia de funcionamento**. (PINHEIRO, 2020, p. 56) (Grifo nosso)

Imperioso afirmar que a eficácia da autoridade pode ser comprovada através de sua própria competência para o feito, a fiscalização permite confiabilidade e garantia de maior segurança para ambas as partes, contudo a aplicação do regulamento europeu com as devidas sanções tem tornado o tratamento de dados mais seguro e eficaz entre os países componentes da União Europeia. Isto posto, cumpre ressaltar a importância da Autoridade Nacional de Dados para a Lei nº 13.709/18, a eficácia de ambas pode ser presumida pela missão da autoridade.

CONCLUSÃO

No ano de 2019 foram contabilizadas 550 (quinhentos e cinquenta) *fintechs* no Brasil, e atualmente este número ultrapassa a 600 (seiscentos). Era visível que estes e demais organismos necessitavam de base jurídica própria, era preciso um regulamento que assegurasse tanto as empresas quanto os usuários.

Ressalta-se que a atuação das *fintechs* no Brasil iniciou no ano de 2013, com a pioneira em serviços financeiros, *Nubank,* e, em seguida, surgiram diversos organismos no mesmo segmento, compulsando ao Banco Central do Brasil à edição de medidas regulatórias em torno da atividade tecnológica financeira que prestava.

Entretanto, no mesmo ano de edição das resoluções do BACEN, foi editada a Lei nº 13.709/18, conhecida por Lei Geral de Proteção de Dados – LGPD, ditando princípios e diretrizes ao tratamento de dados, contendo artigos autoexplicativos, trazendo em seu escopo o conceito de titular, controlador, dados pessoais, dados sensíveis, banco de dados e outros. E, posteriormente, o referido diploma legal sofreu modificações resultando atualmente na Lei nº 13.853/2019, trazendo nova redação principalmente no que diz sobre a Autoridade Nacional de Proteção de Dados.

Internacionalmente, já era previsto regulamento próprio para o tratamento de dados pessoais, e, como evidenciado, as *fintechs* foram construídas baseando-se nas tendências internacionais. Estes segmentos estiveram atentos às mudanças normativas e tecnológicas aduzidas em territórios nacionais, por isso, a aplicação da Lei nº 13.709/18 não demandou muita dificuldade. Dada a localização de risco em relação ao setor em que exerce sua atividade, o ordenamento jurídico trouxe mais segurança e confiabilidade às finanças.

Por conseguinte, restou claro que o uso de dados pessoais deve estar em consonância com os princípios estipulados em lei, como o princípio da necessidade, o qual versa somente pela utilização de dados essenciais ao serviço. As referidas empresas de tecnologia necessitam da coleta de diversos dados para prestação do serviço financeiro, entretanto se atualizaram conforme as regras estabelecidas respeitando os direitos do titular, além de proporcionar maior proteção aos dados pessoais e sensíveis, existe ainda a viabilidade de personalização do serviço de acordo com as preferências do usuário.

Isto posto, foi evidenciado que para a realização da coleta de dados, e posteriormente, a prestação do serviço, é indispensável o consentimento do titular,

devendo ser expressamente comprovada a sua vontade e que esteja ciente de quais dados deverão ser repassados à empresa. Portanto, a necessidade da coleta de dados foi compreendida em razão da proteção e segurança do usuário, bem como a individualização do serviço prestado.

A presente obra também buscou verificar a eficácia da fiscalização mediante a Autoridade Nacional de Proteção de Dados tendo em vista o compartilhamento e transferência internacional de dados. Entretanto, a ANPD somente poderá aplicar as sanções no âmbito de sua competência, no ano de 2021, dito isso, foi necessário observar a aplicação do regulamento europeu, posto que este resultou na base do regulamento brasileiro de proteção de dados.

Observada a aplicação internacional e a efetividade das medidas coercitivas adotadas, restou claro o efeito positivo que o regulamento trouxe à União Europeia, de mesmo modo resultará êxito nas aplicações brasileiras.

Cabe destacar que a figura da Autoridade Nacional é o que torna a Lei Geral de Proteção de Dados suscetível de realização de suas diretrizes, a fiscalização e as sanções mediante descumprimento, torna o ordenamento seguro e traz proteção tanto aos usuários quanto às empresas, posto que agora possuem regularização própria, facilitando a base jurídica empresarial.

Em continuidade, este estudo buscou analisar a aplicação da Lei nº 13.709/18 – Lei Geral de Proteção de Dados no âmbito das *fintechs*, tendo em vista sua atividade financeira no meio digital que denota extremo risco, necessitando de base regulatória, bem como de segurança tanto quanto à organização, quanto aos dados pessoais e sensíveis dos usuários.

A Lei nº 13.709/18 pôs em prática as diretrizes elencadas, trazendo às *fintechs* maior confiabilidade, posto o destaque de tais organizações em contribuir socialmente com a sociedade em termos inovadores, mais eficazes, de melhor acesso, facilidade e menos burocracia no tratamento das finanças, e ainda colaborando para o crescimento econômico brasileiro, resultando em um dos setores de maior investimento no país.

ABSTRACT

GENERAL DATA PROTECTION LAW IN THE FRAMEWORK OF FINTECHS

This article sought to analyze the application of Law No. 13.709/18 - and its new wording - to fintechs, as well as its transition and social contribution process in this segment with the recent ordering. The hypothetical-deductive method was used where the problems were tested and compared bibliographically. The recent emergence of fintechs in the legal system was investigated and their regularization, which is also recent, is summarized in Law No. 13.709/18. The need for data collection was understood due to the protection and safety of the user, as well as the individualization of the service provided. The effectiveness of the inspection was analyzed using international data on which the Brazilian regulation was based for the construction of this law.

Keywords: General Data Protection Law. Fintechs. Business law. Banking law. Digital law.

REFERÊNCIAS

ABRÃO, Nelson. **Direito Bancário**. 17. ed. São Paulo: Saraiva, 2018.

BRASIL. Decreto Nº 10.474, de 26 de agosto de 2020. Aprova a estrutura regimental da Autoridade Nacional de Proteção de Dados. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 26 ago. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 14 ago. 2018.

Banco do Brasil. Resolução nº 4.656, de 26 de abril de 2018. Dispõe sobre a sociedade de crédito direto e a sociedade de empréstimo entre pessoas e dá outros provimentos. **Conselho Monetário do Brasil**, Brasília, DF, 26 abr. 2018.

Banco do Brasil. Resolução nº 4.657, de 26 de abril de 2018. Altera a Resolução nº 4.606 de 19 de outubro de 2017. **Conselho Monetário do Brasil**, Brasília, DF, 26 abr. 2018.

Banco do Brasil. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a política cibernética e dá outros provimentos. **Conselho Monetário do Brasil**, Brasília, DF, 26 abr. 2018.

CARRILO, Ana Flávia**. Crescimento das Startups: veja o que mudou nos últimos anos**. Disponível em: https://abstartups.com.br/crescimento-das-startups/. Acesso em: 03 jun. 2020.

DISTRITO. **Fintech Mining Report**. Distrito, São Paulo: p. 10-25, 2019.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte III.** Disponível em: http://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consetimento-para-o-tratamento-dos-dados-pessoais-12092018. Publicado em: 12 set. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte IV.** Disponível em: https://www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018. Publicado em: 19 set. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte V.** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Publicado em: 26 set. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte VII.** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-termino-do-tratamento-de-dados-10102018. Publicado em: 10 out. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte VIII.** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-os-direitos-dos-titulares-de-dados-pessoais-17102018. Publicado em: 17 out. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte IX.** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direitos-dos-titulares-de-dados-pessoais-24102018. Publicado em: 24 out. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte IX.** Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direito-de-anonimizacao-bloqueio-ou-eliminacao-de-dados-31102018. Publicado em: 24 out. 2018.

FRAZÃO, Ana. **A Nova Lei Geral de Proteção de Dados Pessoais: parte XVIII.** Disponível em: Link: <https://www.jota.info/?pagename=paywall&redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-balanco-preliminar-da-mp-869-2018-06022019.> Publicado em: 06 fev. 2019.

LUZ, Baptista advogados. **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos**. Baptista Luz Advogados, São Paulo: p. 14-23, 2019.

MICHILES, Saulo. **Advogando para Startups**. Dr. Startup, Brasília: 03-21, 2016.

PAGAMENTOS, Grupo Nu. **Política de Privacidade do Nubank**. Disponível em: https://nubank.com.br/contrato/politica-privacidade/. Acesso em: 09 set. 2020.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed. São Paulo: Saraiva, 2013.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais – comentários à Lei N. 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva, 2020.

RODRIGUES, Luiz Carlos Monteiro Gabriel. **Fintechs de crédito e sua regulamentação pelo BACEN.** Disponível em: <https://luizgabrielmr.jusbrasil.com.br/artigos/581898659/fintechs-de-credito-e-sua-regulamentacao-pelo-bacen-tudo-o-que-voce-precisa-saber-parte-1?ref=feed.> Acesso em: 03 jun. 2020.

SCHAWB, Klaus. **A Quarta Revolução Industrial**. 1. ed. São Paulo: Édipro, 2016.

TAX, CMS Law. **Rastreador de Execução do GDPR**. Disponível em: https://www.enforcementtracker.com/. Acesso em: 26 de set. 2020.

VAINZOF, Rony. **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. São Paulo: Thomson Reuters Brasil, 2018.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL

Av. Universitária, 1069 | Setor Universitário

Caixa Postal 86 | CEP 74605-010

Goiânia | Goiás | Brasil

Fone: (62) 3946.3081 ou 3089 | Fax: (62) 3946.3080

www.pucgoias.edu.br | prodin@pucgoias.edu.br

RESOLUÇÃO n°038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Amanda Alvares Rodrigues do Curso de Bacharelado em Direito, matrícula 2016.2.0001.0050-7, telefone: (62) 9 9363-2305, e-mail amandaalvares_@outlook.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Lei Geral de Proteção de Dados no âmbito das *fintechs*, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 20 de novembro de 2020.

Assinatura do(s) autor(es): Amanda Alvares Rodrigues

Nome completo do autor: Amanda Alvares Rodrigues

Assinatura do professor-orientador: GRBotelho

Nome completo do professor-orientador: Glacy Odete Rachid Botelho