**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**

**CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS**

**FACULDADE DE DIREITO**

# A LEI GERAL DE PROTEÇÃO DE DADOS E O CONSENTIMENTO: OS DESDOBRAMENTOS DO DIREITO DE PORTABILIDADE NO OPEN FINANCE

**LUIZ FERNANDO BATISTA NEVES**

**RIO DE JANEIRO**

**2022**

**LUIZ FERNANDO BATISTA NEVES**

# A LEI GERAL DE PROTEÇÃO DE DADOS E O CONSENTIMENTO: OS DESDOBRAMENTOS DO DIREITO DE PORTABILIDADE NO OPEN FINANCE

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do título de Bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Magalhães Martins**.

**RIO DE JANEIRO**

**2022**

CIP - Catalogação na Publicação

N5181

Neves, Luiz Fernando
A LEI GERAL DE PROTEÇÃO DE DADOS E O CONSENTIMENTO: OS DESDOBRAMENTOS DO DIREITO DE PORTABILIDADE NO OPEN FINANCE / Luiz Fernando Neves. -- Rio de Janeiro, 2022.
50 f.

Orientador: Guilherme Magalhães Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2022.

1. Evolução normativa da proteção de dados na história brasileira. 2. O direito à portabilidade de dados. 3. O que é Open Finance?. I. Magalhães Martins, Guilherme, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

**LUIZ FERNANDO BATISTA NEVES**

# A LEI GERAL DE PROTEÇÃO DE DADOS E O CONSENTIMENTO: OS DESDOBRAMENTOS DO DIREITO DE PORTABILIDADE NO OPEN FINANCE

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do título de Bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Magalhães Martins**.

Data da aprovação: 19/12/2022

Banca Examinadora:

_____

Prof. Dr. Guilherme Magalhães Martins

_____

Profa. Andreia F. Almeida Rangel

_____

Profa. Juliana Gomes Lages

**Rio de Janeiro**

**2022**

*"Se antes de cada ato nosso nos puséssemos a prever todas as consequências dele, a pensar nelas a sério; primeiro as imediatas, depois as prováveis, depois as possíveis, depois as imagináveis, não chegaríamos sequer a mover-nos de onde o primeiro pensamento nos tivesse feito parar.*

*Os bons e maus resultados dos nossos ditos e obras vão-se distribuindo, supõe-se que de uma forma bastante uniforme e equilibrada, por todos os dias do futuro, incluindo aqueles infindáveis, em que já cá não estaremos para poder comprová-lo, para congratular-nos ou pedir perdão. Aliás, há quem diga que isso é que é a imortalidade de que tanto se fala."*

*José Saramago (1922 – 2010)*

## AGRADECIMENTOS

Reservo estas páginas como espaço para demonstrar toda a gratidão que carrego comigo. Em primeiro lugar, sou grato à Deus, como humildade para reconhecer que se não fosse por Ele, nada disso seria possível. Por todas as coisas que não lhe roguei, mas que ainda assim me foram concedidas.

Sou grato pela proteção, não só minha, mas de todos que me são alicerce. No decorrer de 5 anos desta graduação presenciei diversas histórias trágicas que sobrevieram a amigos e conhecidos. Famílias que tiveram perdas devido à pandemia de COVID-19, entre outros acontecimentos fortuitos. Neste momento percebo o quão privilegiado eu sou por ter todos que amo com suas saúdes intactas. Obrigado Deus, pela saúde dos meus avós maternos, que puderam presenciar seu neto caçula se formando na faculdade. Para meus avós paternos, que já se foram, tenho a certeza de que se hoje estivessem conosco, estariam enormemente orgulhosos. Que do céu possam ver que, os valores guardados, semeados e regados floresceram.

A todos os meus avós, presentes em matéria ou espirito, todos de origem humilde e sem a mesma oportunidade e privilégio de poder estudar: que possam compartilhar dessa alegria e se sentirem orgulhosos, de onde pudemos chegar por meio de vocês. Todo o esforço não foi em vão, e o caminho dos justos foi recompensado. Seus netos, advogados e médicos, perpetuarão os valores da retidão e justiça, jamais se valendo do atual posto social para oprimir os que estão onde um dia nossos avós estiveram, honrando e jamais esquecendo nossas origens.

Da mesma forma, sou agradecido pela oportunidade que me foi dada, de poder viver esta experiência tão frutífera que foi estar nas salas de aula da Faculdade Nacional de Direito, a maior do Brasil, este ambiente foi fundamental para minha evolução pessoal, graças a seu corpo docente, seus eventos e palestras, sempre promovendo um ambiente plural e democrático, ensinando sempre a não perder o olhar crítico sobre o mundo e sobre

o direito. Dedico minha sensibilidade a todas as vezes que eu não apenas escutei, mas ouvi o que me era lecionado.

Agradeço a minha família, que me é sinônimo de força. Começo pelo meu pai, Fernando, que nunca deixou que eu pudesse tirar da sua existência qualquer impressão contrária da força. Sou muito orgulhoso da trajetória de vida dele, que se abdicou o máximo possível em prol de sua família, em todos os tempos de dificuldade. Essa característica me é preciosa e pretendo leva-la comigo. Que esta graduação, apenas um ponto da minha trajetória, lhe seja motivo de orgulho.

À minha mãe, Luciene, que também é sinônimo de força, posto que foi vitoriosa sobre um câncer mortal. Ela me é exemplo de sabedoria, fé e resistência sobre qualquer adversidade. Obrigado por todo apoio, e por demonstrar que obstáculos normalmente não são tão grandes quanto nossos olhos querem nos fazer crer e obrigado por todas as orações.

Sou grato também pela minha irmã, Ana Carolina, uma vez que me orgulha demais em sua caminhada, me fazendo enxergar que sonhos são possíveis. Sou grato pela vida dela, pela nossa relação de ajuda e orgulho mútuo, ambos em seus ofícios. Que um dia eu possa vencer a burocracia tão bem quanto ela salva vidas nas salas de cirurgia.

Gostaria de deixar meus agradecimentos à Eliane, que cuidou de mim por anos com carinho de segunda mãe e me proporcionou toda uma organização cuidadosa para que eu pudesse me preocupar somente com os estudos. Agradeço as orações e o zelo.

Gostaria de agradecer ao Professor Guilherme Magalhães Martins, que aceitou me orientar durante meu trabalho de conclusão de curso, obrigado pela honra.

Gostaria de deixar meus agradecimentos ao meu irmão de coração, Luiz Henrique, e a todos os meus amigos aqui representados por ele que fizeram da vida um trajeto mais leve. Amigos que seguiram outros caminhos, mas que nunca deixaram de estar presentes em minha vida, estando perto ou até mesmo em outros países. Também aos amigos que adquiri na Faculdade Nacional de Direito, e compartilharam comigo muitos momentos de frustração, ansiedade, stress e alegrias. Desejo-lhes o melhor futuro possível, cheio de realizações e alegrias no exercício deste oficio que escolhemos desempenhar pelo resto de nossas vidas. A nós, a sabedoria e a retidão para diligenciar problemas da vida alheia como se nossa, ou de nossos parentes fosse.

Agradeço a todos os professores que tive até hoje. Minha mãe enquanto professora me ensinou a valorizar todos os que se dedicam a ensinar. Sou grato por todos os estímulos, enquanto tábula rasa. Por todos os conteúdos e toda a curiosidade que foi incentivada e todo o conhecimento científico que me foi passado. Reconheço que, se hoje recebo elogios por qualquer traço de inteligência que me seja associada, também é mérito de quem um dia me ensinou que o conhecimento e a cultura são os bens mais preciosos que podemos ter conosco.

Por fim, aos mencionados e os não mencionados, que de alguma forma contribuíram com a minha caminhada, deixo o meu muito obrigado.

## RESUMO

Quando mais da metade da população do planeta utiliza a internet diariamente na era da *Big Data* necessita-se pensar os desafios do direito sobre como as pessoas estão empregando seus dados pessoais no ambiente virtual. O presente estudo analisou através de um breve panorama histórico as evoluções no tempo do instituto da portabilidade e da proteção de dados, e como estas mudanças permitiram que novas modalidades financeiras como o Open Finance pudessem ser implementadas, observando sua adequação jurídica à Lei Geral de Proteção de Dados. Por fim, analisou-se como estas mudanças podem ajudar a sociedade no parâmetro de inclusão financeira, observados o instituto da concorrência e como podem surgir novas ofertas de produtos e serviços. O recurso metodológico a ser utilizado foi sobre pesquisas exploratórias bibliográficas e documentais, apoiada na Análise Econômica do Direito.



**PALAVRAS-CHAVE:** Open Finance, Dados Pessoais, LGPD, Inclusão Financeira

## ABSTRACT

When half of the world citizenship uses internet daily in the Big Data era the law needs to think of challenges on how people are placing their personal data online. The present study analizes through a brief historical panorama the evolutions on the portability and data protection institutes, and how these changes allowed new financial models such as the Open Finance could be implemented, observing it's adequation to the Brazilian General Law of Data Protection. In the end, it analized how the changes could improve society's financial inclusion, considering the institute of concurrence, and how it can help bringing new products and services. The methodological resource used was upon several bibliographical and documentary researches, supported by the Economic Analysis of Law.



**KEYWORDS:** Open Finance, Personal Data, LGPD, Financial Inclusion

## LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

API – *Application Programming Interface*

BACEN – Banco Central

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

GDPR – *General Data Protection Regulation*

LGPD – Lei Geral de Proteção de Dados

MCI – Marco Civil da Internet

SFN – Sistema Financeiro Nacional

**SUMÁRIO**

# INTRODUÇÃO

Por centenas de anos a sociedade teve seus meios de propagação de informação limitados pelos recursos de sua respectiva época, tendo sido utilizado desde as pinturas rupestres e a forma oral para disseminação de histórias e acontecimentos, até o surgimento dos primeiros papiros. Mesmo após a evolução da linguagem e escrita, a quantidade de livros disponíveis e traduzidos eram ínfimas, haja visto que havia poucos estudiosos e todo o trabalho feito era manual, o que demandava um gasto excessivo de tempo para uma baixa produção. No século XVIII, a Revolução Industrial proporcionou novos meios de produção e com o desenvolvimento tecnológico a intensificação dos fluxos de informação tomou uma proporção nunca vista. No século XX, as empresas puderam investir em pesquisas na área da computação objetivando a redução do tamanho físico das máquinas, onde um computador chegava a ocupar todo um cômodo de um prédio, não tendo tanta capacidade de processamento. Agora, microchips e conexões *wireless* permitem que todo o tipo de conteúdo digitalizado possa ser transmitido e guardado em *HDs* ou nuvens, com *terabites* de capacidade de armazenamento.

Muitas destas informações que antes eram efêmeras e se perdiam com o tempo junto com pessoas que morriam, passaram a ter um papel fundamental no mundo globalizado do século XXI, onde tudo está conectado e o mesmo arquivo pode estar disponível na *internet* para ser acessado de diferentes partes do planeta ao mesmo tempo. A sensibilidade do tema é dada quando usuários passam a utilizar de diferentes formas em diversos contextos com finalidades prejudiciais, violando sistemas ou divulgando informações sensíveis e sem permissão do titular. Atualmente, onde mais da metade da população do planeta tem acesso à internet, enxerga-se a necessidade de pensar acerca dos desafios do direito com as novas tecnologias e nova realidade na Era da *Big Data.*

A autora Shoshana Zuboff inaugura o termo “capitalismo de vigilância”, que pode ser entendido como 1. uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado.

Ao debruçar-se sobre a forma como empresas que atuam na internet iniciaram sua jornada na transformação de dados pessoais em matéria prima, observou-se que o início deste processo se deu após um período de dificuldade econômica no ano 2002 que demandou que *start-ups* do Vale do Silício mudassem suas estratégias para se manterem vivos no mercado, como no caso da Google, essa gigante que conhecemos foi a pioneira em termos de sucesso financeiro criando um sólido alicerce para agir neste território virgem.

Ainda para a autora:

> "As matérias-primas que haviam sido usadas com o único intuito de melhorar a qualidade da busca agora seriam usadas também a serviço de dirigir a publicidade a usuários individuais. Alguns dados continuariam a ser aplicados no aprimoramento do serviço, mas os crescentes depósitos de sinais colaterais seriam reaproveitados para melhorar a lucratividade de anúncios tanto para o Google quanto para seus anunciantes. Esses dados comportamentais disponíveis para usos além de melhorias nos serviços constituíam um superávit, e foi na força desse superávit comportamental que a jovem companhia encontraria a solução para "lucro constante e exponencial", que seria necessário para a sobrevivência. Graças à percepção de estado de emergência, uma nova mutação começou a ganhar forma e se esgueirou, tomando o contrato social implícito orientado para a proteção da relação original da companhia com seus usuários."
>
> (**A era do capitalismo de vigilância.** Shoshana Zuboff – Rio de Janeiro: Intrínseca, 2019)

Os dados pessoais, Para Tepedino, Frazão e Oliva (2019, p.26), "são os principais recursos econômicos da nossa época, revelam importante ponto de partida para a compreensão da necessidade de proteção dos dados pessoais". São comparados de forma análoga como a água que bebemos, e o ar que respiramos, explicitando como as informações pessoais se transformaram em insumos da *data-driven economy*.

A devida atenção a ser tomada é quando muitas das vezes concedemos um consentimento aos termos e condições de uso sem nos dar conta de onde estamos depositando nossas informações, aceitando um contrato de adesão que demandaria horas

para que fosse lido na íntegra, o que configura prática desleal para o consumidor, haja vistos os perigos que podem estar maquiados. Uma das possíveis teorias que explicam esta tomada de decisão é a da utilidade subjetiva, onde o ser humano tende a focar nos benefícios imediatos, representado pelo acesso a um produto ou serviço *on-line*, em detrimento dos possíveis prejuízos à privacidade que estão temporariamente distantes e uma vez feita tal escolha, é pouco provável que o sujeito volte atrás, revogando o consentimento para o tratamento dos dados pessoais. (BIONI, 2018)

Enquanto sobrepesa-se a lógica do consentimento ficcional, uma empresa pode ter a sua disposição dados que identificam sujeitos como pessoa individual, traçando o perfil do que a pessoa gosta, quais seus hábitos de consumo, localização geográfica, e que podem ser disponibilizados livremente com empresas terceiras. Em forma de um monitoramento completo, muitas vezes estas ferramentas são utilizadas, em suas formas legais, para aperfeiçoamento de marketing estratégico, e mesmo que eventualmente os consumidores dispusessem do conhecimento técnico específico para controlar seus dados pessoais, o mercado desenvolve novas ferramentas, conhecidas como *evercookie* para driblar essa escolha. Dessa maneira, fica demonstrado a vulnerabilidade do consumidor, incapaz de desempenhar por si próprio a proteção de suas informações pessoais (BIONI, 2018).

Em seu livro Shoshana Zuboff alerta que mesmo em um estudo empírico onde 543 participantes eram familiarizados com assuntos jurídicos de privacidade e vigilância, 74% destes optaram pela “adesão rápida” quando solicitados a aderir a um serviço online, passando por cima dos acordos de termos e serviços e política de privacidade.

É necessário que se façam considerações acerca dos institutos legais envolvidos em questão. No uso de websites e aplicativos e na contratação de serviços e produtos, estamos a todo momento concedendo informações que são compartilhadas num fluxo intenso entre diferentes companhias. Este primeiro contato de acordo entre as partes, na maioria dos casos é regido e condicionado pelo aceite do usuário a Termos e Condições de uso, que é um contrato de adesão imposto pela contratada nessa relação de consumo. A não concordância do contratante com estes termos e com as políticas de privacidade da empresa implica a não utilização ou limitação dos recursos dos websites ou serviços.

Os Termos e Condições são as regras as quais os visitantes estão concordando, como os deveres e obrigações do usuário, a fim de eximir a culpa da empresa contratada de algumas responsabilidades, como por exemplo na culpa em caso de prejuízo por problemas no serviço e a Política de Privacidade é utilizada para informar aos usuários do *site* que suas informações serão coletadas, armazenadas, compartilhadas e/ou vendidas para outras empresas parceiras. Assim, os termos que regularão o comportamento dos usuários serão decididos unilateralmente e fornecidos por meio de uma plataforma, podendo ser considerados como "*law of the plataform"* (De Filippi, 2012).

Em outro estudo tivemos que o número de consumidores que lê os contratos de adesão antes de aceitar é entre 0.5% e 0.22% onde, para quem resolver realizar esta leitura deverá dispender de aproximadamente 4 horas e 30 minutos de uma leitura que não garante uma compreensão íntegra devido sua linguagem técnica, jurídica e da ciência da computação (BAKOS, et. Al, 2014).

Atualmente, o contrato de adesão é o instrumento muito adotado nas relações de consumo por garantir economia e agilidade na execução dos negócios, conforme versa o art. 54 do Código de Defesa do Consumidor. Em muitos dos casos, sites e aplicativos de acesso gratuito cobram seu preço de forma indireta, quando grande parte dos seus dados são a moeda de pagamento. Nesse momento, depreende-se a vulnerabilidade do consumidor e põe em voga as cláusulas manifestamente abusivas destas empresas de tecnologia.

O instituto da portabilidade de dados no marco regulatório geral brasileiro sobre proteção de dados pessoais vem sendo alvo de debate, quando postos em contraposição o direito da titularidade dos dados e autodeterminação do indivíduo com a postura reticente das empresas em aderir à essa transferência a outro agente de tratamento, justamente pelo fato do texto da norma não apresentar uma delimitação específica, de forma que inviabiliza o exercício desse direito. Como se lê do art. 18 da LGPD:

> O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> (...)

> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> (Redação dada pela Lei nº 13.853, de 2019).

Desta maneira, a redação do presente diploma legal não restringe o alcance aos dados fornecidos na portabilidade, o que gera instabilidade jurídica acerca de como esse instituto será regulado. Esta insegurança acarretaria no compartilhamento de dados que já passaram por um processo ou foram complementados através da atividade do controlador, o que infere na violação do segredo comercial e industrial da forma como estas companhias de tecnologia tratam estes dados.

Apesar de alguma postura temerária, é notável que a portabilidade pode promover uma série de benefícios não somente para o consumidor quanto para o mercado concorrencial, pois os obstáculos para a troca de prestador de serviços se reduziriam, visto que haveria uma mitigação dos chamados *switching costs*, que reduziria o aprisionamento de dados a um só prestador de serviços quando outras empresas fornecem serviços mais vantajosos e incentivaria a entrada de novos *players* no mercado, estimulando uma concorrência saudável. (CRAVO, 2020)

Um exemplo é a iniciativa do Banco Central do Brasil, ao implementar o Sistema Financeiro Aberto ou *Open Finance*, que é um sistema de compartilhamento de dados financeiros de forma padronizada através de uma plataforma única e integrada onde diferentes instituições poderão ter acesso a dados de clientes por meio de APIs (*Application Programming Interface*), para oferecer produtos únicos e personalizados para seus clientes, atraindo-os de forma mais vantajosa para suas realidades financeiras. O objetivo da pesquisa será esclarecer as formas de obtenção do consentimento nas hipóteses dos dois casos supracitados.

À luz de nossa Lei 13.709/18, discorrer-se-á acerca do uso adequado e da responsabilidade civil nos casos de compartilhamento de dados no funcionamento do Open Finance no Brasil, que eventualmente sejam prejudicados ou favorecidos através dessa iniciativa, a fim de observar os impactos positivos e negativos desta política financeira do Banco Central, para estarem em conformidade com os princípios expressos

no art. 3º do Marco Civil da Internet e os dispositivos da Constituição da República Federativa do Brasil de 1988 (CRFB/88) referentes ao direito fundamental à privacidade.

Tomando como referência os diplomas legais supracitados, o objetivo do presente trabalho é investigar, à luz da LGPD, os limites do direito de portabilidade e quais os possíveis estímulos e desafios a serem enfrentados para que essa proposta venha a ser frutífera tanto para o ecossistema bancário quanto para os clientes consumidores mediante consentimento, permeando o paradigma da autodeterminação e a garantia efetiva da proteção dos direitos fundamentais envolvidos nos casos de portabilidade de dados entre empresas.

# CAPÍTULO 1 - EVOLUÇÃO NORMATIVA DA PROTEÇÃO DE DADOS NA HISTÓRIA BRASILEIRA

## 1.1. Constituição Federal

O Brasil goza de um status internacional privilegiado por ter legislações avançadas em matérias como leis ambientais, de direitos humanos e civis, quando comparadas as legislações de outros países sul americanos, e até quando comparados com países norte americanos e europeus. Dessa forma, podemos concluir que a modernização e digitalização do nosso sistema financeiro só foi possível devido a esses estágios legislativos avançados que regulamentaram e permitiram que toda essa nova realidade virtual pudesse ser entendida e esclarecida no âmbito jurídico, tanto em esferas penais nos casos de crimes cibernéticos quanto nas esferas civis com todos os desdobramentos decorrentes da nossa vida pessoal que se estendeu para a vida virtual (CRAVO, 2018). Essa relação de dependência criou uma necessidade para que o direito pudesse entender e resolver eventuais conflitos decorrentes dessa nova forma de viver, trabalhar, estudar, acessar conteúdos e realizar negócios comerciais.

Mediante uma rápida análise acerca da privacidade e dados na Constituição Federal de 1988, a legislação já demonstrava uma preocupação com a garantia do direito à privacidade. Neste diapasão, o reconhecimento do direito à proteção de dados pessoais efetiva-se através de diversos dispositivos da Constituição da República que protegem a

intimidade, a vida privada, a honra e a imagem, à partir da proteção da intimidade (art. 5º, X, da Constituição Federal), que abrange a proteção à própria imagem, em face inclusive dos meios de comunicação de massa; do direito à informação (art. 5º, XIV); do direito ao sigilo das comunicações e dados (art. 5º, XII); da inviolabilidade do domicílio (art. 5º, XI); do direito a receber dos órgãos públicos informações de seu interesse ou de interesse coletivo ou geral, com exceção daquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 5º, XXXIII); ou da garantia individual ao conhecimento e correção de informações sobre si pelo habeas data (art. 5º, LXXII). Entende-se como a distinção entre esferas público e privada. (FERREIRA, 2020).

Para a doutrina, "é nesse sentido que se compreende a privacidade como direito de ser deixado só, estar a salvo de interferências alheias, do segredo ou sigilo que são direitos calibrados pela dicotomia das esferas pública e privada. A pessoa tem o direito de retrair aspectos da sua vida do domínio público.". Como exemplo de garantia de proteção temos a inviolabilidade a casa, a correspondência, as comunicações. (BIONI, 2019)

Em diálogo com a privacidade temos o direito à proteção de dados que passa a ser admitido como a tutela autônoma do indivíduo sobre as informações públicas, mas que sensíveis e passíveis de revelar detalhes precisos de uma pessoa de maneira que esta pessoa possa ser identificada e identificável.

Nesse sentido:

> "Por exemplo, fatos públicos, que a priori não gerariam preocupação atinente à vida privada, podem, quando agregados a outros fatos (dados), revelar detalhes precisos sobre a personalidade de um indivíduo. O mesmo com relação à agregação de dados triviais que permite a extração de informações sensíveis, e portanto, mais intrusivas dos indivíduos. A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Propugnar que o direito à proteção de dados pessoais seria uma mera evolução do direito à privacidade é uma construção dogmática falha que dificulta sua compreensão."
>
> (**Proteção de dados pessoais: a função e os limites do consentimento** / Bruno Ricardo Bioni – Rio de janeiro: Forense, 2019.)

Com a preocupação em reconhecer constitucionalmente este direito, o legislador trouxe uma grande conquista recente que foi a criação da Emenda Constitucional nº 115 de 2022, que alterou a Constituição Federal para incluir no rol do artigo 5º a proteção de dados pessoais como direito autônomo e garantia fundamental, dispondo sobre a competência privativa da União para legislar sobre a proteção e o tratamento destes. Vigorou a alteração do inciso LXXIX para constar "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 2022), a qual demonstrou uma grande evolução normativa do ordenamento jurídico brasileiro acerca deste direito fundamental.

A ideia era tornar o país internacionalmente mais competitivo e atraente para o mercado econômico, uma vez que as empresas multinacionais aumentaram seus fluxos internacionais de dados e essa regulação afastaria uma insegurança jurídica sobre o tema. Parte dessa pressão se deu a partir da aprovação da *General Data Protection Regulation* (GDPR), que foi a lei pioneira no assunto aprovada na União Europeia que fez com que outros países se adaptassem à uma sociedade cada vez mais movidas a dados (MARTINS, 2021).

## 1.2. **Código de Defesa do Consumidor**

Em 1990 surge o Código de Defesa do Consumidor, que defende e tutela todos os direitos envolvidos em relações de consumo em que o consumidor seja vulnerável, na forma do artigo XXXII da CF/88. A legislação trouxe então em seu texto uma seção específica sobre cadastros e bancos de dados, permitindo que o consumidor acessasse seus dados de posse da empresa controladora com a finalidade de pedir a retificação dos mesmos, caso houvessem incompatibilidade com os dados atualizados desse sujeito, conforme artigo 43, §3º deste código. Observa-se que, até então a preocupação com o direito do consumidor era legítima, porém o entendimento que prevalecia era que os dados pessoais de um indivíduo detinham um caráter público, como consta no parágrafo quarto.

Esse caráter público refere-se ao livre acesso do consumidor aos bancos de dados, mas subjetivamente implica que a titularidade destes dados é de quem os detém e os

armazena, em dissonância com o entendimento atual. A intenção do legislador é aproximar o consumidor do controle sobre a circulação de seus dados, garantindo seu acesso e exatidão de tais informações, conferindo ao mesmo a autonomia e autodeterminação sobre seus dados, assumindo que todo consumidor seja capacitado para reivindicar seus direitos, caso haja práticas dissonantes da lei; exemplo este seria a não comunicação ao consumidor para quando fosse aberto um banco de dados pessoais por ele solicitado, conforme parágrafo segundo deste artigo.

Para Bioni:

> "A referida transparência só tem razão de ser porque o operador dos bancos de dados terá, simetricamente, os deveres de: i) garantir o seu acesso pelo consumidor (art. 43, caput, do CDC); ii) exatidão de tais informações; iii) que o banco de dados se restrinja para finalidades claras e verdadeiras e, por fim; iv) que seja observado o limite temporal de cinco anos para o armazenamento de informações negativas (art. 43, § 1º, do CDC). Por esse arranjo, o consumidor poderá demandar a imediata correção-cancelamento de uma informação errônea ou que tenha superado tal limite temporal (art. 43, § 3º, do CDC). Tais direitos (acesso, retificação e cancelamento) e princípios (transparência, qualidade [exatidão] e limitação temporal) 86 gravitam em torno da figura do consumidor, para que ele, na condição de titular dos dados pessoais, exerça controle sobre suas informações pessoais. Em suma, o Código de Defesa de Consumidor buscou conferir a autodeterminação informacional 87, o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento."
> (**Proteção de dados pessoais: a função e os limites do consentimento** / Bruno Ricardo Bioni – Rio de janeiro: Forense, 2019.)

Porém, o mesmo autor ressalta a importância do direito em estar sempre se atualizando para que os direitos dos consumidores estejam sempre tutelados, uma vez que cada vez mais a participação social está diretamente associada ao fluxo de dados pessoais nos ambientes virtuais, como se psicologicamente estivesse intrínseco o sentimento de que o "não compartilhamento" de seus dados implicasse numa segregação na sociedade da informação.

A complexidade do ecossistema que compõe a indústria dos dados se dá pelas inúmeras ações cooperativas que interligam vários players por meio do compartilhamento de informações para que chegue a uma finalidade comum. Neste ínterim, muito se questiona se o titular dos dados realmente tem a plena consciência de todos estes atores envolvidos nestes processos sobre seus dados.

Assim:

> "as habilidades cognitivas do ser humano são limitadas. (...) Já se faz impossível memorizar os inúmeros atores que compõe a referenciada rede social de publicidade, quanto mais compreender como os dados pessoais serão por eles tratados, já que cada um deles tem as suas respectivas políticas de privacidade. Soma-se, ainda, o complicador da compreensão de como a agregação dos dados pessoais desenrolar-se-á a ponto de extrair informações mais detalhadas sobre seus titulares. A complementar tal quadro problemático, há barreiras psicológicas que mistificam por completo a capacidade de o indivíduo controlar as suas informações pessoais"
> **Proteção de dados pessoais: a função e os limites do consentimento** / Bruno Ricardo Bioni – Rio de janeiro: Forense, 2019.)

Portanto, torna-se necessário a reavaliação e a incontestabilidade de que o consentimento configura todo e qualquer cidadão como indivíduo racional, livre e capaz para fazer valer a proteção de seus dados pessoais, uma vez que este protagonismo velado pode ser utilizado no mercado da economia digital como estratégia regulatória para perpetuar seu modelo de negócio sobre limitações técnicas e informacionais, impedindo que os indivíduos ponderem com sensatez sobre os efeitos a curto e longo prazo sobre a concessão de seus dados sensíveis.

### 1.3. Código Civil

O Código Civil de 2002 buscou regular as relações jurídicas privadas e resguardar os direitos das pessoas jurídicas privadas, criando leis acerca da proteção de direitos fundamentais do indivíduo. Dos direitos da personalidade que a Lei 10.406/02 normatizou, encontramos os aspectos como a intransmissibilidade dos direitos, como no artigo 11 "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação

voluntária" e consequências da violação desses direitos no artigo 12 "Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.".

Outra garantia é a proteção à imagem e representações da pessoa enquanto dados pessoais identificáveis, como o nome e a voz. Observa-se a preocupação com estes bens jurídicos ao analisar a redação dos artigos 16, 17, 18 e 20 que vedam a utilização de nome alheio por outrem em publicações ou propagandas comerciais que exponham ou não ao desprezo público, ainda que não haja intenção difamatória e também a divulgação e utilização de escritos e imagem da pessoa. Como se extrai da redação dos artigos supracitados (BRASIL, 2002):

> Art. 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome.
> Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.
> Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial.
> (...)
> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
> (Redação dada pela Lei nº 10.406, de 2002.)

E por fim, o legislador encerra o capítulo versando sobre a proteção à vida privada, assim como já garantida na constituição federal no seu artigo 5, X e XII, complementando ao artigo 21 do Código Civil com o trecho "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.".

Concomitantemente com o avanço tecnológico do século XXI, surgiram novas formas de se comunicar, de se publicizar, de comprar e vender, tudo através da internet,

que possibilitou a aceleração do processo de globalização, e com isso surgiram novas necessidades de o mundo jurídico enxergar e interpretar esta nova realidade com suas novas demandas, conforme defende Ana Frazão, "a coleta e a utilização maciça de dados ensejou a constituição de uma nova forma de capitalismo, fundado na vigilância constante e no controle disperso sobre os cidadãos, a fim de possibilitar uma geração crescente de dados e aplicações".

### 1.4. Projeto de Lei 84/1999 e Lei Carolina Dieckmann

Dessa maneira, a discussão sobre a liberdade exercida na internet tomou pauta, pois começou-se a notar que muitos dos atos tomados na rede de computadores geravam reflexos na realidade social de muitas pessoas no mundo real. A necessidade de leis para regular o ambiente digital gerou muitas controvérsias, enquanto houvesse quem defendia que a intervenção estatal impediria o avanço tecnológico, havia grande parte da internet global reivindicando um caráter de defesa ao anonimato e liberdade quase que absoluta. As preocupações se acirraram devido ao elevado número de casos de violações a direitos fundamentais e transgressões a direitos humanos como apologia ao crime, disseminação de códigos maliciosos, comercialização de produtos e serviços ilegais, invasões a esferas privadas com sequestros de dados, violação a direitos autorais como a pirataria online. Todo esse exercício abusivo da liberdade demonstrou que estas violações a moral, aos bons costumes e aos princípios éticos do direito, precisariam ser contidas por um conjunto de leis reguladoras e limitadoras deste ciberespaço.

> Usando o abalo na credibilidade da rede e nos sistemas de comércio eletrônico, há quem defenda a opinião de que a Internet precisa de maior controle e regulamentação. Alguns sites de hackers chegam a dizer que os verdadeiros responsáveis pela ação são governos e setores conservadores, que buscam um motivo para limitar a liberdade dos usuários na rede. Para os que sustentam tal posição e que defendem insistentemente a chamada liberdade virtual, o direito específico e regulador das questões da criminalidade na rede será sempre encarado como uma "camisa de força" imposta pelos poderes estatais; afinal, segundo os mesmos, o ciberespaço deveria ser regido com base em um sistema que ultrapassa o liberalismo latu sensu e beira o anarquismo, onde toda a forma de interferência dos poderes constituídos revelar-se-ia no mínimo inaceitável e, por isso mesmo, ilegítima.

> (DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. Cybercrimes. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Cood.). **Direito & Internet: Aspectos Jurídicos Relevantes.** Bauru: Edipro, 2000. P. 118)

A proposta de criminalizar atos cometidos dentro da rede informatizada foi levantada no final da década de 90 com o rejeitado Projeto de Lei 84/1999 do ex-deputado federal Luiz Piauhylino (PSDB/PE), que dispunha sobre crimes cibernéticos, suas penalidades e outras providências, caracterizando crime virtual todo aquele praticado por hacker e crackers e sobre utilização indevida de senhas. Posteriormente rejeitado, o tema saiu de pauta, até que em 2012 aprovou-se a Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, que altera o Código Penal para tipificar delitos criminais de invasão de dispositivos informáticos, falsificação de documento ou cartão de crédito e débito e interromper ou dificultar o reestabelecimento de serviços informáticos, garantindo interesses legítimos de proteção aos dados individuais, privacidade e segurança na internet.

## 1. 5. Marco Civil da Internet

Em 2014 aprova-se a lei ordinária federal 12.965/14, mais conhecida como Marco Civil da Internet, que foi encaminhada ao congresso em 2011, pela então presidente da República do Brasil, Dilma Rousseff. Após 3 anos de debates com representantes civis e políticos, foi aprovado o projeto que visava estabelecer princípios, direitos e deveres para o uso da internet no Brasil. Essa lei tem como norte a garantia o protagonismo dos usuários nesse ambiente digital e uma experiência tecnológica digna, resguardados os princípios constitucionais como a liberdade de expressão, a neutralidade da rede e a privacidade, cabendo todas as medidas legais quanto à responsabilização civil dos atos decorrentes nesse ciberespaço.

A respeito do Marco Civil da Internet, Vaz sintetiza:

> São três as principais polêmicas do projeto: anonimato na rede, remoção de conteúdo e registro de internautas. O conceito “neutralidade da rede” significa que todas as informações devem ser tratadas da mesma forma e navegar na mesma velocidade. O Marco Civil tenta garantir a neutralidade para todos os internautas brasileiros, num momento em que a discussão sobre o tema atinge

> o ápice nos EUA - em a autoridade do FCC (Comissão Federal de Comunicações, na sigla em inglês) está sendo questionada. Regular sem censurar, registrar usuários sem invadir a privacidade alheia, proibir o anonimato sem tolher a liberdade de expressão, esses os desafios da regulamentação que se pretende fazer.
> (VAZ, Ana Carolina. Op. Cit., p. 166)

Nesse momento, a redação do MCI optou por preservar sua essência garantindo os direitos à liberdade e privacidade de forma mais abrangente, uma vez que no momento de sua gestação estava sendo discutido nos Estados Unidos o caso de espionagem envolvendo Edward Snowden, reforçando a necessidade de se proteger o direito à proteção dos dados pessoais e privacidade dos indivíduos sem cercear do uso da internet e todo o seu dinamismo. Em seu corpo encontram-se dispositivos que valorizam o usuário como grande protagonista para desempenhar a proteção de seus dados pessoais, enfatizando a expressa necessidade do consentimento do usuário, que deve ser livre, expresso e informado, para a atividades como coleta, uso, armazenamento e tratamento de seus dados pessoais, bem como sua transferência para terceiros.

Assim, na concepção dos termos do MCI restaram inequívocos a valorização da autodeterminação e consentimento dos usuários, onde o cidadão goza da liberdade de requerer ainda a exclusão a qualquer momento e definitiva de seus dados pessoais que porventura estivessem armazenados para aplicação na internet e a ênfase no consentimento que se tornou requisito necessário para que qualquer dado fosse coletado e tratado, sendo este consentimento revogável a qualquer hora. E para os operadores fica registrado que devem prestar informações claras, e completas, utilizando-se de cláusulas contratuais destacadas e dando publicidade às suas políticas de uso para o preenchimento dos adjetivos em questão. É com base, justamente, em tais informações, que são especificados os propósitos que justificam a coleta dos dados pessoais para que o seu titular possa fazer as suas escolhas a esse respeito (BIONI, 2019).

## 1. 6. Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709, de 14 de agosto de 2018) foi aprovada em 2018 e entrou em vigor dois anos depois, em 2020, contando com

65 artigos, mais orientações interpretativas (BIONI e MENDES, 2019). Esta lei foi um marco histórico no brasil sobre o tratamento de dados pessoais e sua regulamentação. Este diploma legal dispõe sobre novas diretrizes e como instituições privadas e públicas devem coletar, armazenar e disponibilizar informações sobre usuários de plataformas digitais e meios físicos, além de se aplicar a toda e qualquer operação desde que o tratamento de dados seja realizado no Brasil, independendo do país de onde estejam localizados os dados. Aplica-se também a toda atividade de tratamento que tenha por objetivo a oferta de bens de serviço ou manejo de dados de indivíduos localizados em território nacional, excluindo-se os casos onde essa coleta é feita para fins exclusivamente artísticos, acadêmicos, jornalísticos e nos casos de informações relacionadas à segurança nacional e do Estado, atividades de investigação e repressão de infrações penais.

São fundamentos basilares desta norma o respeito a privacidade, a autodeterminação informativa, a liberdade de informação, a inviolabilidade da intimidade, e os direitos humanos e da personalidade, alinhando-se com a livre concorrência e o desenvolvimento econômico e tecnológico, respeitando a boa-fé, a transparência e a segurança, evidenciando que as soluções de mercado não são suficientes quanto à garantia destes direitos (FRAZÃO, 2019).

No que diz respeito ao tratamento dos dados:

> "ele deverá ocorrer, como regra, de acordo com as hipóteses estabelecidas no artigo 7º da LGPD, sendo certo que no caso de dados sensíveis e de dados de crianças e adolescentes foram positivadas normas mais rígidas, conforme se verá mais adiante. Como restou estabelecido, mesmo nos casos de dispensa da exigência do consentimento, os agentes de tratamento continuarão obrigados com as demais disposições previstas na lei, especialmente com os princípios gerais e os direitos do titular. Ou seja, as proteções conferidas ao titular permanecem e são de observância obrigatória."
> TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 2. ed. São Paulo : Thomson Reuters Brasil, 2020.

Porém, há de se destacar que a transferência da responsabilidade de autotutela para o titular dos dados no tocante ao protagonismo do consentimento levanta discussões importantes. O consentimento dado pelo indivíduo que, ainda que racional, livre e capaz,

não afasta dele a condição de vulnerável. Isso porque o consentimento tem sido visto como o pilar dessa estratégia regulatória, mais como um meio para legitimar os modelos de negócio da economia digital, do que como um meio eficiente para desempenhar a proteção dos dados pessoais, estrangulando a prometida autodeterminação informacional. "Por tal motivo, é de suma importância frisar essa incompatibilidade do desenho normativo de proteção de dados pessoais e, por conseguinte, pensar como isso pode ser absorvido para fins de reflexão e reajustes do ponto de vista de uma (nova) estratégia regulatória." (BIONI, 2019).

Isto se dá porque a proposta central da lei é a valorização do indivíduo como protagonista e fruidor dos princípios e direitos garantidos pelo diploma legal, dentre os quais se destacam a transparência de informações e a vedação à coleta excessiva de dados que seriam desnecessários para a finalidade objetiva do tratamento de dados propostos pelas empresas de tecnologia, que somente poderão ser coletados por meio de cláusulas contratuais de consentimento expresso, tornando nulas todas as autorizações genéricas e fundadas na ausência de transparência ou termos subentendidos.

Ainda em seu período embrionário sofreu importantes alterações, que foram incluídas pela Medida Provisória nº 869, de 27 de novembro de 2018, que posteriormente veio a se tornar a Lei 13.853 de 2019. Das disposições acrescidas, pode-se destacar disposições sobre o compartilhamento de dados e a incidência destas normas às atividades do Poder Público, evidenciando que a obrigatoriedade e observância dos termos da lei fossem respeitados em todos os âmbitos.

Nesse sentido, Guilherme Martins acrescenta:

> De início, a reforma acrescentou ao artigo 1º um parágrafo único, com a seguinte redação: "As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios." Trabalhou-se, conceitualmente, com a concretização da amplitude axiológica do direito fundamental à proteção de dados pessoais4, alinhando-a ao que se discute na Proposta de Emenda à Constituição nº 17/2019, que visa incluir tal direito no texto constitucional, além de definir como de competência exclusiva da União o poder para legislar sobre o assunto. Sem dúvida, o status de direito fundamental confere à proteção de dados

> pessoais um papel imprescindível no tocante à articulação do direito privado frente aos interesses passíveis de tutela no contexto informacional.
> (MARTINS, Guilherme Magalhães; ROZATTILONGHI, João Victor; FALEIROS Jr, José Luiz de Moura. **A consolidação legislativa da proteção de dados no Brasil: comentários às alterações da Lei nº 13.853/2019 à LGPD.** Revista do Ministério Público do Estado do Rio de Janeiro nº 76, abr./jun. 2020)

Sobre o as alterações acerca do compartilhamento de dados, a referida lei delimitou com maior clareza em sua alteração no item VIII do artigo 7º, que tornou "exclusivo" para a tutela da saúde em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária, garantindo uma consonância entre a LGPD e a resoluções do Conselho Federal de Medicina (CFM), dando maior valorização ao sigilo destes dados referentes à saúde. De igual modo, a proibição às operadoras de planos de saúde ao tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários, no §5º do mesmo artigo, ponto importantíssimo no combate à discriminação praticada por estas empresas prestadoras de assistência à saúde.

Tivemos também a criação da Autoridade Nacional de Proteção de Dados no artigo 55-A, um órgão público estatal responsável por fiscalizar e aplicar sanções em casos onde os tratamentos de dados realizados de forma dissonante da LGPD, receber reclamações dos titulares, prestar esclarecimentos e tomar providências, criar diretrizes estratégicas, políticas públicas e ações de cooperação com autoridades de proteção de dados pessoais de outras jurisdições de natureza transnacional ou internacional.

Nesse sentido, Lúcia Maria Teixeira Ferreira expõe:

> Atribuições fundamentais da ANPD, relacionadas aos seus poderes de fiscalização e de enforcement, previstas no art. 31 da LGPD, incluem, ainda, a averiguação de violações em decorrência do tratamento de dados pessoais por órgãos públicos e a adoção de medidas cabíveis para fazer cessar a violação, inclusive as sanções administrativas previstas nos incisos I, IV, V, VI, X, XI e XII do art. 52, que podem ser aplicadas às entidades e aos órgãos públicos, sem prejuízo do disposto no Estatuto do Servidor Público, na Lei de Improbidade

> Administrativa e na Lei de Acesso à Informação (nova redação do §3º do art. 52 da LGPD, após a derrubada, pelo Congresso Nacional, dos vetos presidenciais). É lícito assegurar que competências específicas do Conselho Nacional de Proteção de Dados e da Privacidade contribuirão positivamente para a atuação da ANPD, auxiliando na formulação das diretrizes estratégicas e para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, com especial atenção aos dados pessoais tratados pelo Poder Público.
> (FERREIRA, Lucia Maria Teixeira. **Parecer.** Revista do Ministério Público do Estado do Rio de Janeiro nº 75, jan./mar. 2020.)

Na vigência da Lei 13.853/2019, tivemos a alteração da natureza jurídica da agência, onde a ANPD passou a ser um órgão vinculado diretamente à Presidência da República de natureza jurídica transitória, com o prazo de 2 anos para que se decidisse a natureza jurídica enquanto entidade transitória, conforme parágrafos 1º e 2º do 55-A. Contudo, a Lei 14.460/2022 proveniente da Medida Provisória n. 1.124/2022 que dentre outros dispositivos transformou a Agência Nacional de Proteção de Dados em autarquia de natureza especial para resguardar a garantia de que a mesma goze de maior independência em sua atuação. Importante ressaltar que em todos os países que possuem legislações de proteção de dados existem agências análogas a ANPD, fortes e majoritariamente independentes, sendo que apenas 10% destes países não criaram autoridades específicas ou demoraram demasiadamente para cria-las. (MARTINS et. al, 2020).

Uma das exigências para o ingresso do Brasil na OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e em outras entidades internacionais importantes, como a Eurojustice e a Europol, foi a aprovação e implementação de uma lei geral de proteção de dados, tornando-se necessário o Brasil demonstrar que a LGPD não tenha um caráter meramente decorativo. Todos os países que ingressam na OCDE devem cumprir requisitos técnicos para se adequar aos princípios defendidos pela Organização, incluindo a proteção dos dados pessoais nas transações comerciais nacionais e internacionais, demonstrada assim a importância jurídica e econômica desta lei (FERREIRA, 2020).

# CAPÍTULO 2 - O direito à portabilidade de dados

## 2.1. Noções introdutórias

O direito à portabilidade de dados consiste na possibilidade de transmitir dados pessoais de um controlador para o outro, tendo seu surgimento nos meados de 2012 com a reforma europeia acerca da regulamentação de proteção de dados pessoais enquanto se discutiam direitos referentes a autodeterminação informativa dos indivíduos. Nesse momento emergiram as discussões sobre como transferir ao titular o controle efetivo sobre como seus dados são tratados, dando margem ao surgimento de outros direitos, como o da exclusão, acesso e retificação de dados (PONCE, 2020).

As mudanças tecnológicas advindas da computação e globalização criaram novas necessidades, e sob este espectro, o direito a portabilidade advém da necessidade de respaldar os titulares dos dados em suas privacidades e em relações consumeristas. Este instituto permite que as pessoas tenham um maior controle acerca de seus dados. Dessa maneira, esclarece Daniela Cravo:

> "[...] um instituto de fomento e de estímulo às migrações e ao livre trânsito dos consumidores entre diferentes serviços ou produtos no mercado digital. A portabilidade, dessa forma, apresenta uma dupla essência: além de permitir que os indivíduos exercitem o seu direito à autodeterminação informacional, busca promover a concorrência em um mercado caracterizado por grandes vencedores monopolistas e com efeitos de rede."
>
> CRAVO, Daniela Cravo. **O Direito à Portabilidade na Lei Geral de Proteção de Dados.** In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. São Paulo: Thomson Reuters Brasil, 2020.

Este direito permite que antigas práticas abusivas de mercado não mais se perpetuem em prejuízo dos clientes, como observado nos exemplos de empresas de telefonia que impossibilitavam o cliente trocar de empresa, levando consigo seus dados e seu número de telefone, acarretando em um enorme constrangimento uma vez que o número de telefone carrega consigo um caráter identitário do portador.

Nesse sentido:

> "[...] a portabilidade na área de telefonia, regulamentada pela Resolução nº 460 de 19 de março de 2007 da Agência Nacional de Telecomunicações, corresponde à "facilidade de rede que possibilita ao usuário de serviço de telecomunicações manter o Código de Acesso a ele designado, independentemente de prestadora de serviço de telecomunicações ou de área de prestação do serviço", com isso um usuário pode mudar de uma operadora para a outra mantendo o mesmo número de telefone. Assim, as principais características da portabilidade de serviços ou ativos são: i) Previsão em distintos instrumentos normativos; ii) pressuposição do encerramento do relacionamento com o prestador de serviços anterior; e, iii) Assegura a manutenção dos mesmos direitos ou recursos financeiros já assegurados pelo consumidor em relação ao fornecedor anterior."
>
> VIOLA, Mario; THOMAZELLI, Patrícia. **Portabilidade de Dados, Interoperabilidade e Open Banking.** Instituto de Tecnologia &Sociedade do Rio (ITSRIO), 2021.

Nesta seara, o direito a portabilidade foi recebido como uma medida antitruste de acordo com o direito concorrencial. Além da liberdade de gerenciamento de seus dados entre serviços de empresas concorrentes, o usuário em seu benefício pode escolher qual produto ou fornecedor lhe convém melhor as suas necessidades, fomentando maior concorrência no mercado e estimulando uma maior competitividade dentre as empresas prestadoras de serviços que terão de oferecer melhor vantagens para a captação de novos clientes, que não poderão se obstar quanto ao pedido de transferência de dados quando solicitado (CRAVO, 2020).

Mister ressaltar a diferenciação entre a portabilidade de serviços, onde sujeito titular dos dados escolhe pela troca de controladores que atuam numa mesma área, como exemplo os produtos bancários de previdência privada ou investimentos. Ou seja, nessa modalidade extingue-se o vínculo com a prestadora inicial, implicando na migração de dados para um novo prestador. Dessa maneira, a portabilidade de serviços pode ser enxergada como uma transferência de recursos entre plataformas. Porém, a portabilidade de dados somente se limita à transferência dos dados exigidos, não acarretando o desfazimento do serviço prévio.

Assim, o titular que decide portar apenas seus dados entre empresas controladoras indiretamente se vê numa encruzilhada onde ele tinha um serviço que lhe oferecia alguns

benefícios, em detrimento da nova proposta que pode lhe ser mais conveniente. Só então, que após a portabilidade dos dados, o sujeito pode decidir extinguir seu vínculo com a prestadora de serviços anterior.

No tocante, Viola e Thomazelli esclarecem:

> "[...] a portabilidade do direito acumulado por participante de determinado plano de previdência privada para outro plano de previdência está prevista no inciso II do art. 14 da Lei Complementar nº 109, de 29 de maio de 2001. Nesse caso a "portabilidade" importará a transferência dos recursos do participante de um prestador de serviços para outro. Na mesma linha é a portabilidade de operações de crédito, regulada pela Resolução nº 4.292 do Banco Central. Aqui, assim como no caso da portabilidade da previdência privada, o foco é a transferência dos recursos financeiros do cliente de um prestador de serviços para outro.
>
> [...] a portabilidade na área de telefonia, regulamentada pela Resolução nº 460 de 19 de março de 2007 da Agência Nacional de Telecomunicações, corresponde à "facilidade de rede que possibilita ao usuário de serviço de telecomunicações manter o Código de Acesso a ele designado, independentemente de prestadora de serviço de telecomunicações ou de área de prestação do serviço", com isso um usuário pode mudar de uma operadora para a outra mantendo o mesmo número de telefone. Assim, as principais características da portabilidade de serviços ou ativos são: i) Previsão em distintos instrumentos normativos; ii) pressuposição do encerramento do relacionamento com o prestador de serviços anterior; e, iii) Assegura a manutenção dos mesmos direitos ou recursos financeiros já assegurados pelo consumidor em relação ao fornecedor anterior."
>
> VIOLA, Mario; THOMAZELLI, Patrícia. **Portabilidade de Dados, Interoperabilidade e Open Banking.** Instituto de Tecnologia &Sociedade do Rio (ITSRIO), 2021.

Portanto, a evolução temporal deu ao direito novas necessidades e aplicações práticas ao seu uso uma vez que novas ferramentas tecnológicas surgiram para que a simplicidade e produtividade das tarefas sociais fossem aumentadas. Com a LGPD, estas aplicações moldaram-se sob novas características e regulamentações, conforme a redação expressa no texto da lei, como se observa no artigo 18 e incisos II e V da supracitada:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> [...]
> II - acesso aos dados;
> [...]
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> (Redação dada pela Lei nº 13.709, de 2018.)

Para isso, fora suscitadas no presente dispositivo legal maneiras e limites de como garantir que essa portabilidade fosse feita, para que passasse por um crivo criterioso, de modo a garantir que existissem padrões a serem seguidos pelas empresas participantes. Um deles pode-se destacar é que a portabilidade de dados não incluiria dados já anonimizados pelo controlador (artigo 18, §7º), uma vez que o artigo 12 da lei indica expressamente que dados anonimizados não seriam considerados dados pessoais, impossibilitados de serem associados ao titular. Outro limite seria o segredo comercial e industrial, que estes deixam de ter status de dados pessoais e são transformados em ferramentas de funcionamento operacional de uma empresa por meio de algoritmos e *softwares* próprios destas corporações, se tornando objeto de *expertise* negocial. Estes limites devem garantir que estes processamentos assegurem que os dados deixem de tornar uma pessoa identificável ou identificada, caso contrário não estão anonimizados e, portanto, dados pessoais passíveis de portabilidade.

Diante desta realidade, o direito a portabilidade seria considerado como um remédio para negativa de acesso aos dados em determinadas hipóteses uma vez que se caracterizaria atitude anticompetitiva, enquanto alguns autores defendem padronização de formatos necessária para a portabilidade plena seria um fator que limitaria os sistemas e auxiliaria negócios rivais, de maneira que estes argumentos seriam suficientemente válidos para a restrição da padronização. Dessa maneira, existe o risco de aprisionamento de dados por estas empresas, que dificultaria ainda mais a portabilidade de dados.

Nesse sentido, Daniela Cravo:

> "Para agravar ainda mais a situação, relata-se que o risco de aprisionamento é a regra, e não a exceção no que toca a plataformas online. Há incentivos e interesse das empresas em manter seu sistema fechado, o que gera problemas de acesso a outras empresas que necessitem dos dados dos usuários para competir ou oferecer serviços e produtos complementares[45]. No serviço de busca, que é aquele em que o consumidor procura informações, sendo exemplos o Google, o Yahoo, o Bing, os custos de troca entre os mecanismos são altos. Cabe ressaltar que o aprisionamento é desejado por essas empresas, já que quanto mais usuários um serviço de busca possui, mais atrativo ele é para publicidade.
>
> [...] Para os consumidores, apesar de existir baixos custos de troca, como regra, nos marketplaces online, esses podem ser impostos por meio da cobrança de taxa para deixar o serviço. Ademais, a familiarização com as regras da plataforma e sua forma de utilização podem gerar o efeito de aprisionamento." CRAVO, Daniela Copetti. **O direito à portabilidade na Lei de Proteção de Dados.** In: Ana Frazão; Gustavo Tepedino; Milena Donato Oliva. (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1ed.São Paulo: Revista dos Tribunais, 2019.

Por mais que se reconheça a enorme importância deste instituto, o direito à portabilidade somente restará efetivo para se tornar um direito viável no que tange às questões complexas para seu efetivo funcionamento através do tempo, não somente para os titulares como para os controladores que se preocupam com os custos operacionais e as limitações técnicas (FRAZÃO, 2018).

Porém, tais dúvidas somente poderão ser enfrentadas com o próprio início da aplicação do direito à portabilidade, bem como com a sua eventual regulamentação, o que permitirá uma investigação real e simultânea do fenômeno, devendo ser implementado ao lado de políticas de segurança. (CRAVO, 2020).

# CAPÍTULO 3 - O que é Open Finance?

## 3. 1 No Reino Unido e EUA

O Sistema Aberto Financeiro, ou Open Finance, foi uma iniciativa do Banco Central da Inglaterra que criou um ecossistema de compartilhamento de dados, de pessoas

físicas ou jurídicas, entre instituições financeiras, por meio de uma plataforma digital integrada. A ideia deste sistema surgiu através da tentativa do governo de estabelecer um método onde um grande número de empresas do ramo financeiro pudesse aumentar a competitividade entre elas. Por meio de APIs se tornou possível a transferência e a comunicação dos dados dos consumidores como histórico de transações e score financeiro entre plataformas, e assim as empresas puderam propor novos serviços e produtos mais específicos, onde o consumidor pode obter taxas e juros mais vantajosos para sua realidade, ao invés de ficar engessado nos termos de uma única instituição.

As APIs são interfaces que interligam os diferentes sistemas das instituições, que quando disponibilizadas pelos participantes podem realizar esta comunicação para que ocorra o compartilhamento de dados nesse ambiente unificado, permite que toda uma rede seja criada para sustentar o fornecimento desse serviço, onde os provedores terceirizados, desde Fintechs até provedores de serviços técnicos, integram esse sistema por meio da adequação e regulação de seus serviços em observação ao *compliance* dos órgãos reguladores estatais.

O Reino Unido regulou padrões e normas a serem seguidos pelos os bancos e provedores terceirizados para o compartilhamento de dados a partir de APIs por meio do PSD2 (*Revised Payment Service Directive*). A partir do modelo bem sucedido de implementação do Open Banking no Reino Unido, diversas jurisdições começaram a adotar tal iniciativa em seus Estados, adaptando às suas realidades políticas e socioeconômicas distintas, como observamos nos casos dos Estados Unidos e do Brasil, direcionados pelo mercado e pelo Estado, respectivamente.

Nos Estados Unidos, o governo federal tem tentado implementar políticas reguladoras e iniciativas que pudessem colaborar com a implementação desse sistema. Porém, devido o enorme número de instituições bancárias que beira os 10.000, e a natureza fragmentada das muitas agências reguladoras do sistema financeiro norte americanas, como a OCC (Office of the Comptroller of the Currency), a FDIC (Federal Deposit Insurance Corporation), NCUA (The National Credit Union Administration), a implementação do Open Banking ainda se encontra à sabor do mercado. Esse grande número de entidades envolvidas, com interesses distintos, dificulta o alinhamento político para que a Agência de Proteção Financeira ao Consumidor americana, a CFPB, consiga

passar o projeto de reforma na Seção 1033 da Lei Pública 111-203 – 21 de julho de 2010 (Dodd-Frank Wall Street Reform and Consumer Protection Act) acerca do direito dos consumidores de ter acesso aos seus dados financeiro, que abrirá caminhos para o futuro do sistema financeiro aberto no futuro. Em nível de jurisdição estadual, a Califórnia inovou com as leis CCPA (California Consumer Privacy Act) de 2018, posteriormente complementada pela CPRA (California Privacy Rights and Enforcement Act) de 2020 que regulamentaram e tutelaram os direitos de privacidade dos consumidores, também em esferas digitais, muito pela necessidade da corte californiana de solucionar conflitos devido ao alto número de judicializações oriundos de empresas gigantescas localizadas no Vale do Silício, como Facebook, Apple, entre outras.

### 3.2. No Brasil

No Brasil o cenário é de segurança jurídica para que tais políticas sejam implementadas, uma vez que o Banco Central tomou uma série de medidas como a Resolução nº 4658, de 26 de abril de 2018, para que se tratasse da segurança cibernética e contratação de serviços de processamento e armazenamento de dados em nuvens pelas instituições financeiras, preparando o terreno para a implementação do Open Banking. De igual maneira, posteriormente foi sancionada em agosto a Lei 13.709 de 2018, ou Lei Geral de Proteção de Dados Pessoais, que se assemelha a legislação europeia, a GDPR (General Data Protection Regulation). O Banco Central decidiu então por começar o processo de implementação do Open Banking em 2020 por meio da Resolução Conjunta nº 1/2020 do Banco Central do Brasil, que posteriormente foi atualizada pela Resolução Conjunta nº 4 24/03/2022 e alterou a norma anterior para dispor sobre o Open Finance, com o objetivo de regulamentar o planejamento e as diretrizes do projeto por meio de uma autorregulação assistida, delegando as instituições participantes a capacidade de estipular regras para o funcionamento sob controle e orientação mediante aprovação e veto das diretrizes que divergissem do projeto do BCB.

Sua implementação consiste em 4 fases que devem evoluir de forma escalonada até o total funcionamento deste serviço. Na 1ª etapa teve início em 01/02/2021 como o objetivo reunir as instituições financeiras interessadas para que fornecessem e coletassem informações relacionados a serviços e produtos oferecidos no mercado a fim de promover

o alinhamento de perfil dos consumidores com os serviços existentes no mercado, ainda sem qualquer compartilhamento de dados.

A 2ª fase possibilitou que os clientes já pudessem solicitar, de forma escalonada, o compartilhamento de seus dados cadastrais e transacionais, entre as instituições participantes. Essa etapa teve início em 13/08/2021 com a limitação de 0,1% dos clientes das instituições de origem e o compartilhamento limitado apenas a dados cadastrais, e ao fim desta etapa no dia 24/10/2021, os pedidos podiam ser feitos por 10% dos clientes destas instituições, podendo ser solicitado o compartilhamento de dados cadastrais, históricos de transações relacionadas a cartões de crédito e operações de crédito, como financiamentos e empréstimos.

Na 3ª fase surgem novas possibilidades de transações de pagamentos e de encaminhamentos de propostas de crédito, como a implementação gradual e restrita do Pix e QR Codes, dentro dos regimes e restrição de funcionamento. Essa modernização é primordial para o desenvolvimento de um ambiente com acesso a serviços financeiros mais céleres e descomplicados para o cliente. Foi fundamental que fossem observados os prazos para que as instituições participantes disponibilizassem e implementassem suas APIs e recursos técnicos eficientes para que tais fases estivessem em vigor de acordo com as diretrizes do planejamento do Banco Central.

Por fim, no último estágio torna-se possível que os clientes da base de dados deste sistema possam compartilhar suas informações de investimentos, seguros, previdências privadas e operações de câmbio com as empresas participantes e acessar todas as possibilidades de contratações de novos produtos e serviços que lhes ofereçam novas soluções e ofertas personalizadas e mais acessíveis para suas realidades. Assim, ficou estipulado que a 4ª fase teria início em 15/12/2021, com a previsão de um lançamento escalonado das APIs até 25/05/2022.

Observou-se, portanto, que com o lançamento escalonado destas APIs houve uma aceitação muito positiva dos parâmetros estatísticos avaliados na pesquisa feita pelo monitoramento oficial do Open Banking Brasil, onde foram estudadas as chamadas de APIs bem sucedidas, as rejeitadas, as disponibilidades, a disponibilidade média entre

outros dados. Estes resultados demonstram um comportamento de ampla aceitação e sucesso técnico deste serviço.

O presente gráfico mostra a evolução temporal Open Banking, correlacionando as quatro fases da implementação e a demonstração de chamadas de APIs bem sucedidas das instituições participantes.

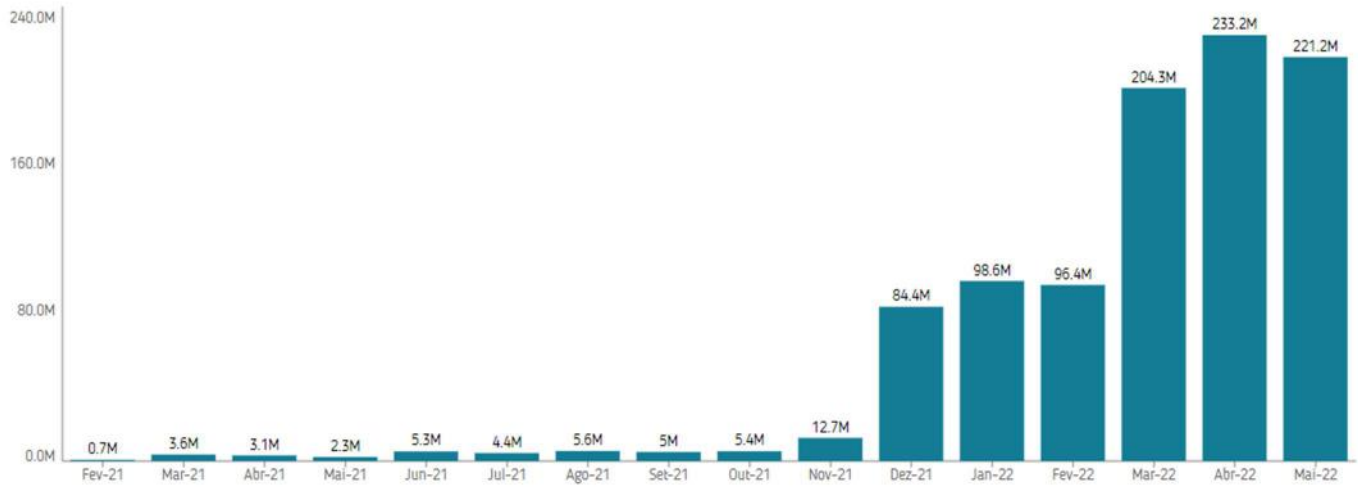


Gráfico 1 – Demonstração de APIs Bem Sucedidas
Fonte: Open Banking Brasil

O gráfico 1 nos apresenta dados de um recorte amostral do período recente da operacionalização das ofertas de APIs, de fevereiro de 2021 até maio de 2022, onde podemos enxergar muito definida a proposta de lançamento gradual do sistema, da primeira fase até a quarta fase da instauração do Open Banking. Esta demonstração é apenas das ofertas bem sucedidas de APIs, ou seja, demonstra todas as vezes que um usuário, seja pessoa física ou pessoa jurídica, logrou êxito em sua chamada de portabilidade de dados entre as instituições participantes.

No primeiro ciclo, início da amostragem, tivemos a implementação da 1ª fase que durou de fevereiro até julho de 2021. Nesse período se o alinhamento das instituições financeiras interessadas em participar com as normativas do sistema, ainda sem compartilhamento de dados, onde observa-se que o lançamento de APIs estavam em teste e o número de chamadas por mês ficou abaixo dos 4.4 milhões.

O lançamento escalonado da segunda fase ocorreu de agosto a outubro de 2021, que foi também dividido em 4 ciclos. No primeiro e segundo ciclo as diretrizes eram para que de agosto a setembro fossem liberados gradualmente de 0,1% a 0,5% dos usuários, com a implementação de APIs restringidas à dados cadastrais, consentimento, criação, consulta, revogação, contas de depósito a vista, poupança e contas pré-pagas.

Do terceiro ao quarto ciclo da segunda fase foram adicionados os serviços de cartões de crédito e operações de crédito para assim solidificar todas as APIs da segunda fase, aumentando o limite de consentimento de 1% para 10%, proporcionando uma maior estabilidade para testes e eventuais expansões nas ofertas de novos serviços, totalizando até então uma quantidade média de 5 milhões de chamadas bem sucedidas nestes meses.

Ao início dos primeiros ciclos da terceira fase, do fim de outubro a novembro de 2021, tivemos a iniciação do fornecimento de APIs para pagamentos via PIX, o pagamento eletrônico instantâneo a uma base de clientes limitada a até 1% das contas de pessoas físicas e pessoas jurídicas das instituições bancárias. Com o aumento da base de clientes e ofertas de serviço pudemos observar o salto de chamadas de APIs bem sucedidas onde este número mais que duplicou quando comparado ao mês anterior, saltando de 5.4 milhões de chamadas para 12.7 milhões de chamadas em novembro.

Com um sistema já quase completo em seu fornecimento de serviço, restou para o terceiro e quarto ciclo da 3ª fase de implementação do Open Banking a inserção do uso de QR Codes e o agendamento de PIX. Do período de 1 de dezembro de 2021 a 17 de fevereiro de 2022 as instituições financeiras participantes já estavam estruturadas o suficiente para poder abrir seus serviços e APIs a toda a base de clientes, onde registrou-se no gráfico um aumento gigantesco na demanda, registrando números médios de 90 milhões de chamadas bem sucedidas nestes três meses. Isso se deu pela disponibilidade

do serviço se dar no horário integral de funcionamento em todos os dias da semana, durante 24 horas por dia, e sua possibilidade de acesso ser tanto em desktops quanto via mobile.

Por fim, em março de 2022 a 4ª e última fase de lançamento escalonado foram implementados quatro grupos de serviços financeiros, conforme Instrução Normativa nº 171 de 11 de outubro de 2021 do Bacen. O primeiro grupo contou com APIs de seguros, previdência complementar aberta e capitalização a partir de 4 de março de 2022, o segundo com APIs de serviços de credenciamento em arranjos de pagamentos, o terceiro com APIs de operações de câmbio e o quarto com APIs de contas de depósito à prazo e outros produtos de investimento, totalizando assim uma gama de opções de operações financeiras destes bancos, instituições de pagamentos, fintechs, cooperativas de créditos e outras organizações autorizadas que trabalham juntos nesse ecossistema.

De março até mês de maio contabilizou-se uma média total de 220 milhões de chamadas bem sucedidas de APIs. Estes números são muito positivos do ponto de vista técnico quando comparados com as estatísticas que demonstram o número total de chamadas rejeitadas das APIs disponíveis.


Gráfico 2 – Demonstração de chamadas rejeitadas de APIs

Fonte: Open Banking Brasil

Do início da primeira fase da implementação gradual do Open Banking em fevereiro de 2021 até maio de 2022 foi feito o levantamento estatístico de dados para que pudesse ser acompanhado de perto o desempenho do sistema em questão. Percebeu-se que 85 instituições somaram um total de menos de 100 casos onde as chamadas de APIs apresentaram falhas de comunicação entre os players participantes.

Posteriormente demonstrou-se que apenas duas instituições participantes apresentaram um número maior que 100 e menor que 1000 casos de chamadas fracassadas, e 5 outras empresas vieram a apresentar um número maior que 10.000 de chamadas incompletas. Neste recorte amostral temos que o total percentual de falhas representa apenas 4,60% do total de chamadas, como demonstra o gráfico 3.

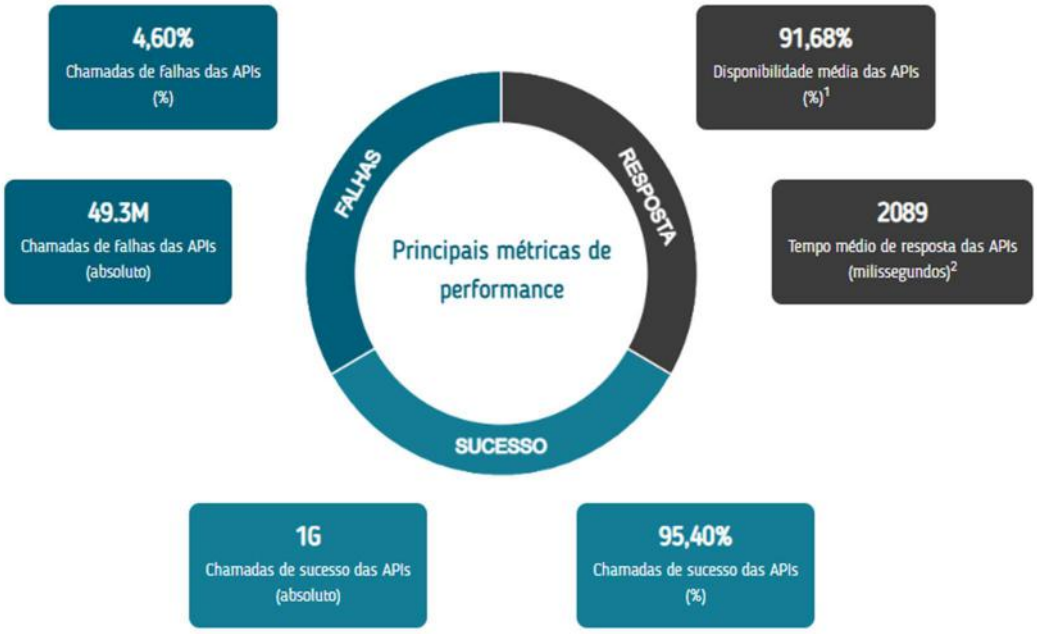


Gráfico 3 - Panorama de 02/2021 à 04/2022

Fonte: Open Banking Brasil

Estes dados em especifico são muito positivos devido baixo número de falhas técnicas apresentadas quando comparadas ao número total de chamadas bem sucedidas que chegou ao limite de 220 milhões, o que permite concluir que este ecossistema técnico está preparado e estabilizado para funcionar de forma que opere um grande número de solicitações sem que venha apresentar grandes problemas, demonstrando que o trabalho

da implementação escalonada em fases foi fundamental para respeitar o processo de desenvolvimento e não comprometer a experiencia positiva do público participante.

### 3. 1. Inclusão Financeira

Até o presente ano o Brasil não participa da OCDE (Organização para Cooperação e Desenvolvimento Econômico) pois não dispõe do reconhecimento do nível de proteção adequado pela comunidade europeia nos termos da GDPR. Isso significa dizer que, para qualquer transferência internacional de dados, as empresas que realizam este fluxo internacional de informações com o Brasil demandarão maior tempo e custo em operações de *compliance,* enquanto países da América do Sul como Argentina e Uruguai, que são homologados pela União Europeia gozam de status privilegiado no comércio internacional.

Na dura realidade enfrentada pelo empresariado local, a ausência de reconhecimento de elevado nível de proteção de dados no Brasil gera enormes custos para as empresas brasileiras e também para as empresas estrangeiras que querem estabelecer negociações com as nossas empresas, na medida em que esta situação implica aumento de exigências e burocracias para a comprovação das garantias de cumprimento dos princípios de proteção de dados, dos direitos do titular e do regime geral de proteção de dados previstos na LGPD e na GDPR, encarecendo bastante os produtos e serviços brasileiros (FERREIRA, 2020).

A aposta em novas formas de acessar seu banco, novas formas de pagamento (“maquininhas”, Pix, QR Code) e novos arranjos regulatórios têm ajudado a difundir o acesso a novas tecnologias, junto com o contexto da Lei Geral de Proteção de Dados, contribui para que o campo de ação esteja propício para o surgimento de novas *fintechs*. Estas buscam aperfeiçoar e automatizar a utilização desses serviços financeiros, explorando mais o novo mercado consumidor que se digitaliza mais a cada dia que passa, tornando possível que essa cultura da inovação esteja acessível para toda a população e trazendo oportunidades a todos que queiram utilizá-las por meio de termos claros e interfaces que não sejam enganosas para seus consumidores, valorizando sempre a autodeterminação dos consumidores sobre seus dados e direitos.

Portanto, em consonância com a análise dos dados estatísticos previamente observados não restam dúvidas de que o Sistema Financeiro Aberto atingiu com êxito seus objetivos em cada fase de implementação, demonstrados pela ampla porcentagem de chamadas de sucesso de APIs, como se observa no gráfico 3. Esses dados demonstram a funcionabilidade do sistema e a grande aceitação do público alvo, que trará um impacto positivo a longo prazo, na forma como a sociedade utiliza os serviços financeiros e bancários, e na realidade concorrencial das empresas envolvidas neste universo.

Por intermédio deste sistema, o consumidor pode definir quais instituições terão acesso a seus dados, ganhando poder de gestão sobre eles. Como resposta, bancos, corretoras e *fintechs* acirrarão a disputa a fim de aumentar a captação de clientes com a ampliação de produtos e serviços que antes estavam disponíveis de forma padronizada, mas com o Sistema Financeiro Aberto estas empresas terão a sua disposição o acesso ao histórico financeiro do consumidor, o que possibilitaria para elas uma análise mais precisa de como fornecer produtos mais personalizado para estes consumidores de acordo com suas respectivas realidades financeiras.

Essa concorrência acarretaria por incluir a parcela de pessoas que antes estavam subservidas e à margem desse sistema, de forma que esses consumidores agora pudessem escolher o que melhor lhe conviesse, ao contrário de ter que se adaptar a produtos engessados que não lhes eram úteis em suas respectivas realidades. “A expectativa é de que haja a expansão da concessão de crédito e a possibilidade de redução de taxas de juros para quem compartilha os dados” (LEITE e CAMARGO, 2022).

Para Carlos Zanvettor, CEO do Banco Afinz:

> “O Brasil dará esse salto criando mais bancos altamente competitivos, especializados no mercado endereçável de sua escolha e alavancados não só no balanço, mas também pelo domínio e emprego de tecnologias contemporâneas. Verdadeiros “neobancos”, não porque independem de agências físicas, mas, sim, capazes de suprir as necessidades dos investidores e dos tomadores de forma primorosa, multiplicando o uso da moeda, aplicando preços justos e surpreendendo com formas inovadoras de servir com crédito, investimentos e pagamentos.”

Zanvettor, Carlos. Fintechs e Open banking são próximos passos para inclusão financeira.
**Exame invest**. São Paulo, 01 de maio de 2022. Disponível em: https://exame.com/invest/opina/fintechs-e-open-banking-sao-proximos-passos-para-inclusao-financeira/. Acesso em: 29 de out. de 2022.

## CONCLUSÃO

Todo o exposto no presente trabalho explicitou que existe uma urgente e real necessidade do emprego de um olhar mais cauteloso para como são utilizados os dados pessoais, uma vez que a economia se adaptou para mover-se através destas informações, utilizando-as como recursos para suas operações (TEPEDINO, FRAZÃO E OLIVA, 2019). Pôde-se observar que as corporações tecnológicas investem em *evercookies* que consistem em diversas formas e ferramentas que as permitam colher informações de seus clientes e usuários, utilizando-se da inovação como forma de driblar um eventual bloqueio de acesso dos próprios usuários (BIONI, 2018) e como os termos de adesão, em forma de contrato de adesão, são ineficazes como instrumento de conscientização e informação para os contratantes, uma vez que estes são feitos de forma propositalmente extensa e técnica, desmotivando os usuários a lerem os termos do contrato.

Com isso, conclui-se que a aprovação da Lei Geral de Proteção de Dados trouxe um maior poder de tutela e gerenciamento dos dados por meio dos próprios titulares, uma vez que a proteção de dados se encontra prevista como direito autônomo no inciso LXXIX do artigo 5º da Constituição Federal, a partir da Emenda 115/22. Estas alterações legislativas organizaram o ambiente econômico e trouxeram mais segurança jurídica para o sistema brasileiro, que passou a considerar que os dados pessoais são de propriedade dos usuários, e não mais um elemento etéreo que está à disposição das empresas como insumo para suas atividades econômicas.

Através destas inovações legais vieram o amadurecimento dos institutos legais como o da portabilidade e o da interoperabilidade, que tomaram forma conforme a necessidade de utilização deles aumentava, por conta do exponencial surgimento de novas

tecnologias, comércio virtual e comunicação *online*. A globalização criou a necessidade de estar-se sempre em contato direto, através do *networking*, e esta troca de informações é vital para alimentar e perpetuar o sistema capitalista atual. Dessa maneira, a ligação e interdependência da portabilidade de dados e da interoperabilidade se tornaram fundamentais para a existência da competitividade de plataformas digitais e do mercado financeiro.

Neste cenário surge no Brasil o *Open Finance*, através da Resolução Conjunta nº 1/2020 do Banco Central, que buscou regulamentar e implementar este sistema que permite o compartilhamento de dados entre plataformas através da abertura e integração de sistemas de bancos, instituições de pagamento, cooperativas de crédito, *fintechs* e outras organizações. Esta ferramenta é a máxima da utilização bem sucedida da portabilidade de dados, mostrando-se em completa conformidade com a LGPD e demonstrando a importância da regulação desta lei para o ordenamento jurídico do país.

Conclui-se, portanto, que todo o esforço que possibilitou a criação deste sistema aberto restou constatado através impactos positivos demonstrados no presente trabalho, como o estímulo à competitividade e ascensão de novos *players* no mercado. Esta concorrência acarreta em novas tecnologias, e na oferta de produtos e serviços com taxas de juros adequadas para cada pessoa em sua realidade, através da utilização do histórico de dados fornecidos pelos titulares.

Desta maneira, resta demonstrada que a implementação do Sistema Financeiro Aberto no Brasil estimula em muito a inclusão financeira de uma parcela da população que antes se encontrava subservida com produtos bancários e financeiros, concluindo-se dessa maneira que tanto o titular dos dados será diretamente e positivamente beneficiado, quanto os as empresas também, de forma que estas poderão atentar-se ao histórico financeiro das pessoas, calculando melhor os riscos para ofertar seus produtos personalizados para seus clientes.

**REFERÊNCIAS BIBLIOGRÁFICAS**

BAKOS, YANNIS; MAROTTA-WURGLER, FLORENCIA; AND TROSSEN, DAVID R., "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts" (2014). New York University Law and Economics Working Papers. Paper 195.

BIONI, BRUNO RICARDO. **Proteção de dados pessoais: a função e os limites do consentimento**. – Rio de janeiro: Forense, 2019.

BRASIL. Banco Central e Conselho Monetário Nacional. **Resolução Conjunta nº 1** (2020). Disponível em: http://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v4_P.pdf. Acesso em: 17 set. 2022

BRASIL. Banco Central e Conselho Monetário Nacional. **Resolução Conjunta nº 4** (2020). Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3% A3o%20Conjunta&numero=4. Acesso em: 17 set. 2022

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, Senado Federal: Centro Geográfico, 1988.

BRASIL. Federação Brasileira de Bancos (FEBRABAN). **Pesquisa FEBRABAN de Tecnologia Bancária 2019.** Realização Deloitte. Disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf. Acesso em: 17 ago. 2022

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Dísponivel em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 ago. 2022

BELLI, L. & VENTURINI, J. (2016). **Private ordering and the rise of terms of service as cyber-regulation.** *Internet Policy Review*, *5*(4). https://doi.org/10.14763/2016.4.44

CORRÊA, David Pedroso. **O Open Banking como política concorrencial: no Brasil e no mundo.** Revista do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (IBRAC), nº 1, p. 465-489, 2021. Disponível em: https://ibrac.org.br/UPLOADS/PDF/RevistadoIBRAC/Revista_do_IBRAC_n_1_2021.pdf. Acesso em: 05 out. 2022.

CRAVO, Daniela Copetti. **Portabilidade de dados como um remédio antitruste.** Revista do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (IBRAC), nº 1, p. 145-164, 2020. Disponível em: https://ibrac.org.br/UPLOADS/PDF/RevistadoIBRAC/Revista_do_IBRAC_n_1_2020.pdf. Acesso em: 04 ago. 2022.

CRAVO, Daniela Cravo. **O Direito à Portabilidade na Lei Geral de Proteção de Dados.** In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2020, p. 343–362.

CRAVO, Daniela Copetti. **Direito à portabilidade de dados: interface entre defesa da concorrência, do consumidor e proteção de dados.** Rio de Janeiro: Lumen Juris, 2018

CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. **A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais.** Revista de Direito Privado. vol. 98, p. 161-186. mar/abr 2019.

DE FILIPPI, P, Belli, L, **'Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation'**, European Journal for Law and Technology, Vol. 3, No. 2, 2012

FERREIRA, Lucia Maria Teixeira. **Parecer.** Revista do Ministério Público do Estado do Rio de Janeiro nº 75, jan./mar. 2020. Disponível em: https://www.mprj.mp.br/documents/20184/1606722/Lucia_Maria_Teixeira_Ferreira.pdf Acesso em: 20 de nov. 2022.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. **Portabilidade de dados pessoais e o recrudescimento do controle do titular de dados nas relações de consumo.** Revista de Direito do Consumidor. vol. 135. ano 30. p. 203-227. São Paulo: Ed. RT, maio/jun. 2021. Disponível em: . Acesso em: 04 out. 2022.

MELO, Lígia Tomás de; NASARET, Matheus Mendes. **Open Banking e direito da concorrência: uma análise dos impactos da implementação do Sistema Financeiro Aberto sobre as preocupações do CADE em relação ao setor financeiro brasileiro.** Revista do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional (IBRAC), nº 1, p. 491-520, 2021. Disponível em: https://ibrac.org.br/UPLOADS/PDF/RevistadoIBRAC/Revista_do_IBRAC_n_1_2021.pdf. Acesso em: 05 out. 2022.

PONCE, Paula Pedigoni. **Direito à portabilidade de dados: entre a proteção de dados e a concorrência.** Revista de Defesa da Concorrência, Brasília, v. 8, n. 1, p. 134-176, 2020. Disponível em: https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/521. Acesso em: 07 ago. 2022.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 2. ed. São Paulo : Thomson Reuters Brasil, 2020. Proview. Livro eletrônico sem paginação. ISBN 978-85-5614-007-0.

VENTURINI, J. et al. (2016). **Terms of service and human rights: an analysis of online platform contracts**. Editora Revan. Rio de Janeiro, Brazil.

VIOLA, Mario; THOMAZELLI, Patrícia. **Portabilidade de Dados, Interoperabilidade e Open Banking.** Instituto de Tecnologia &Sociedade do Rio (ITSRIO), 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/02/Portabilidade-InteroperabilidadeOpenBanking.pdf. Acesso em: 05 ago. 2022.

ZANVETTOR, Carlos. Fintechs e Open banking são próximos passos para inclusão financeira. **Exame invest**. São Paulo, 01 de maio de 2022. Disponível em: https://exame.com/invest/opina/fintechs-e-open-banking-sao-proximos-passos-para-inclusao-financeira/. Acesso em: 29 de out. de 2022.

ZUBOFF, Shoshana (2019). **A era do capitalismo de vigilância.** Editora Intrínseca. Rio de Janeiro, Brasil.