

GUIA

Open Finance e LGPD

NÚMERO 5/10

A Year in
Privacy

.....

Autores

Ananda Fernandes Garcia

Odélio Porto Júnior

Lucas Oliveira Balsamão Magela

Rafaella Resck Braoios

Clineu Henrique de Andrade

Luiz Felipe Sundfeld Ibrahim

.....

Coordenador e Revisor

Fernando Bousso

Fabiano de Melo Ferreira

.....

Projeto Gráfico

Fernanda Muchon

Laura Klink

Lucas Bittencourt

índice

.....
Introdução p. 04

01

.....
Funcionamento do Open Finance p.05

- 1.1. O que é o Open Finance p.06
- 1.2. Tipos de dados pessoais p.09
- 1.3. Fluxo das informações entre os agentes p.11

02

.....
Open Finance e Proteção de Dados p. 13

- 2.1. Classificação dos agentes e respectivas responsabilidades p.14
- 2.2. Programa de governança em proteção de dados p.15
- 2.3. Incidentes de segurança p.19
- 2.4. Direito dos titulares p. 24

03

.....
Requisitos para o consentimento p. 27

04

.....
Requisitos para a transferência de dados p. 31

.....
Conclusão p. 34

Introdução

Este Guia busca analisar o funcionamento do *Open Finance* sob a perspectiva da Lei Geral de Proteção de Dados Pessoais ('LGPD'), Lei nº 13.709/2018, e demais normas aplicáveis que tratem do tema de privacidade e proteção de dados pessoais, incluindo as normas regulatórias setoriais do sistema financeiro. São avaliados os tipos de dados pessoais usados no *Open Finance*, como os atores se qualificam em relação ao conceito de controlador e operador, as principais obrigações dos agentes de tratamento, com destaque para as relativas à segurança da informação e compartilhamento de dados, e os direitos dos titulares dos dados/clientes.

01

Funcionamento do Open Finance

1.1. O que é o Open Finance

O *Open Finance*¹ é o conjunto de procedimentos e tecnologias que permite a abertura e a integração dos sistemas de instituições que fazem parte do sistema financeiro, para o compartilhamento padronizado de dados sobre produtos e serviços, e de dados cadastrais e transacionais dos usuários. Por meio do consentimento, os usuários permitem que seus dados sejam repassados a instituições terceiras com a finalidade de obter acesso à oferta de novos produtos e serviços, ou melhores condições de contratação².

No Brasil, o *Open Finance* foi regulamentado pelo Banco Central do Brasil (BCB) e pelo Conselho Monetário Nacional (CMN), tendo seus principais pontos sido implementados em quatro fases entre 2021 e 2022.³ Para se ter uma dimensão do projeto, o BCB divulgou comunicado em 2020 listando 1.065 instituições consideradas participantes obrigatórias do *Open Finance*.⁴ Ademais, até a primeira quinzena do mês de maio de 2022, já tinham sido realizadas mais de 233 milhões de chamadas de interações entre as instituições participantes.⁵

Garantir o compartilhamento de dados bancários foi um dos objetivos iniciais do *Open Finance*. Isso porque o mercado de serviços bancários é altamente concentrado, de modo que o acesso a dados constitui uma das barreiras à entrada de concorrentes.⁶ Não por outro motivo, as instituições de maior porte (S1 e S2)⁷ possuem participação obrigatória no *Open Finance* para fins de compartilhamento de dados. Sendo as demais instituições participantes de forma voluntária. São, ainda,

¹ Nova denominação do Open Banking, dada pela Resolução Conjunta nº 4 de 24/3/2022, do Banco Central do Brasil e do Conselho Monetário Nacional.

² A FCA (Financial Conduct Authority) do Reino Unido definiu o Open Banking como a “iniciativa que permite aos clientes consentirem a um terceiro a acessar informações de suas contas, ou fazer pagamentos em seu nome. Disponível em: <https://www.fca.org.uk/publication/call-for-input/call-for-input-open-finance.pdf>. Acesso em: 05/05/2022.

³ Fases de Implementação. Disponível em: <https://openbankingbrasil.org.br/fases-de-implementacao>. Acesso em: 16/05/2022.

⁴ BANCO CENTRAL DO BRASIL. Comunicado nº 36.480 de 4/12/2020. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=36480>. Acesso em: 05/05/2022.

⁵ Vide a série de dados e estatísticas do Open Banking. Dados estatísticos de desempenho e disponibilidade do Open Banking. Disponível em: <https://dashboard.openbankingbrasil.org.br>. Acesso em: 05/05/2022.

⁶ Nota Técnica nº 79/2019, da Superintendência Geral do CADE (Conselho Administrativo de Defesa Econômica), apresentado no âmbito do Processo Administrativo nº 08700.002066/2019-77.

⁷ As instituições (S1) são os bancos múltiplos, comerciais, de investimento, câmbio e caixas econômicas que tenham porte igual ou superior a 10% (dez por cento) do PIB, ou que exerçam atividade internacional relevante. As instituições (S2) são compostas pelos bancos múltiplos comerciais, de investimento, câmbio e caixas econômicas entre 1 e 10% do PIB, e demais instituições autorizadas de porte igual ou superior a 1% do PIB. BANCO CENTRAL DO BRASIL. Panorama da Segmentação e Aplicação Proporcional da Regulação Prudencial. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/regprudencialsegmentacao>. Acesso em: 16/05/2022.

objetivos do projeto: incentivar a inovação; aumentar a eficiência do Sistema Financeiro Nacional e Sistema de Pagamentos Brasileiro; e promover a concorrência e a cidadania financeira.⁸

A concretização do *Open Finance* passa pelo compartilhamento de dados referentes a diversos produtos e serviços nos mercados de pagamentos, crédito, seguros, câmbio e investimentos.

Por isso, o *Open Finance*, por meio do alto investimento das instituições financeiras em tecnologia e inovação e da atuação das fintechs tem potencial de aumentar a competição e a transparência no mercado financeiro, beneficiando e empoderando o consumidor, ao permitir que o titular dos dados tenha o controle destes. Igualmente, a redução de barreiras de acesso a dados fomenta a entrada de novos agentes no mercado. Esse é o caso das novas figuras surgidas nesse mercado, como o iniciador de transação de pagamentos, o agregador de dados e o correspondente digital para o encaminhamento de propostas de crédito.

/ Instituições participantes do Open Finance

São participantes do *Open Finance* as instituições financeiras, as instituições de pagamento e as demais instituições autorizadas a funcionar pelo BCB. A regulamentação do *Open Finance* previu, ainda, a interação de entidades não autorizadas, as denominadas “parceiras”. Para isso, tais entidades deverão firmar contrato de parceria com instituições autorizadas pelo BCB para o compartilhamento de dados de clientes em comum.

De acordo com a Resolução Conjunta nº 1/2020 do BCB e do CMN⁹, podemos identificar os seguintes participantes-chave do Open Finance: **(i)** instituição transmissora/receptora de dados; **(ii)** instituição iniciadora de transação de pagamento; **(iii)** instituição detentora de conta; e **(iv)** correspondente de crédito. Além disso, a regulação previu expressamente a atividade de agregação de dados.

⁸ Artigo 3º da Resolução Conjunta nº 01/2020 do Banco Central do Brasil e do Conselho Monetário Nacional. Disponível em: < <https://in.gov.br/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055>>. Acesso em: 16/05/2022.

⁹ Ibid.

¹⁰ OPEN BANKING. Dados estatísticos de desempenho e disponibilidade do Open Banking. Disponível em: <<https://dashboard.openbankingbrasil.org.br>>. Acesso em: 05/05/2022.

¹¹ As instituições (S1) são os bancos múltiplos, comerciais, de investimento, câmbio e caixas econômicas que tenham porte igual ou superior a 10% (dez por cento) do PIB, ou que exerçam atividade internacional relevante. As instituições (S2) são compostas pelos bancos múltiplos comerciais, de investimento, câmbio e caixas econômicas entre 1 e 10% do PIB, e demais instituições autorizadas de porte igual ou superior a 1% do PIB. BANCO CENTRAL DO BRASIL. Panorama da Segmentação e Aplicação Proporcional da Regulação Prudencial. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/regprudencialsegmentacao>>. Acesso em: 16/05/2022.

(i) Instituição transmissora/receptora de dados

Para fins de compartilhamento de dados, atualmente, 158 instituições estão cadastradas no diretório do *Open Finance* como instituições transmissoras e receptoras de dados.¹⁰ A participação nessa modalidade é obrigatória para as instituições enquadradas nos segmentos S1 e S2¹¹, no âmbito da regulação do BCB.

Em breve síntese, a instituição transmissora pode ser definida como aquela onde os dados são originados (onde o cliente possui conta de depósito ou de pagamento pré-paga), sendo responsável por enviar tais dados por meio de chamadas de interfaces (em inglês “Application Programming Interface” – “API”). Enquanto a instituição receptora de dados é aquela que solicita o compartilhamento, por meio de API à instituição transmissora dos respectivos dados.

(ii) Instituição prestadora de serviço de iniciação de transação de pagamentos

O iniciador de transação de pagamento é uma modalidade de instituição de pagamento que foi disciplinada pelo BCB no próprio âmbito da regulação do *Open Finance*. Isso porque a execução de tal atividade depende do compartilhamento padronizado de dados, bem como da integração de sistemas das instituições “detentoras de conta” com as “iniciadoras de transação de pagamento”.

Conforme a definição regulamentar, o serviço de iniciação de transação de pagamento é aquele que possibilita uma instrução de transação de pagamento ordenada pelo cliente, e relacionada a uma conta de depósitos ou de pagamento pré-paga. Com esse objetivo, o iniciador permite que o usuário faça a transação em seu ambiente virtual, sem a necessidade de ser redirecionado para o ambiente da instituição detentora da conta. Dessa forma, a iniciação de pagamentos tem o potencial de reduzir as etapas de pagamento, reduzindo a fricção na jornada do usuário.

(iii) Instituição detentora de conta

Na prática, a instituição detentora de conta é a que mantém conta de depósitos à vista, conta de poupança ou conta de pagamento pré-paga, de livre movimentação pelos consumidores, e autorizadas a funcionar pelo BCB.

A instituição detentora de tais contas, além do compartilhamento de dados, pode se conectar aos sistemas de instituições iniciadoras de transação de pagamento, viabilizando os serviços referentes à iniciação.

(iv) Correspondente de crédito

Trata-se de instituição que tem como atividade o compartilhamento de propostas de crédito e arrendamento mercantil, por meio de canais eletrônicos. A participação no *Open Finance* é obrigatória para instituições financeiras e instituições de pagamento que tenham firmado contrato de correspondente no País, cujas atividades contemplem no mínimo:

1. o recebimento das solicitações de propostas de operação de crédito;
2. o recebimento e envio de dados entre a instituição financeira contratante e o correspondente no País;
3. o envio das propostas de operação de crédito; e
4. o rastreamento das solicitações e das respectivas propostas de operação de crédito.

Em termos concretos, tais atividades têm o potencial de reduzir as barreiras à entrada e aumentar a eficiência no mercado de crédito. Bem como, permitir que os usuários recebam ofertas de crédito mais personalizadas e adequadas às suas necessidades.

1.2. Tipos de Dados Pessoais

O BCB definiu, a partir da Resolução Conjunta nº 1/2020, quais deverão ser os dados mínimos compartilhados entre as instituições participantes. Em relação aos produtos e serviços utilizados pelos titulares, devem ser compartilhadas as seguintes informações:

1. contas de depósito à vista;
2. contas de depósito de poupança;
3. contas de pagamento pré-pagas;
4. contas de pagamento pós-pagas;
5. operações de crédito;
6. operações de câmbio;
7. serviços de credenciamento em arranjos de pagamento;
8. contas de depósito a prazo e outros produtos com natureza de

¹² BANCO CENTRAL DO BRASIL. Resolução Conjunta nº 1, de 4 de maio de 2020. Art. 5º, I, b.

¹³ Ibid, Art. 5º § 4º, I.

investimento;

9. seguros; e

10. previdência complementar aberta;¹²

Por outro lado, no que diz respeito ao cadastro de clientes e de seus representantes, resolveu o BCB que os dados de cadastro devem abranger os dados fornecidos diretamente pelo cliente ou obtidos por meio de consulta a bancos de dados de caráter público ou privado, **exceto**: **(i)** os dados classificados como dado pessoal sensível pela legislação; **(ii)** as notas ou pontuações de crédito; e **(iii)** as credenciais e outras informações utilizadas com o objetivo de efetuar a autenticação do cliente.¹³

Somando-se a isso, outras informações que devem ser levadas em consideração são aquelas diretamente relacionadas com as transações de clientes. Nesse caso, as informações mínimas necessárias são as relacionadas com:

1. contas de depósito à vista;
2. contas de depósito de poupança;
3. contas de pagamento pré-pagas;
4. contas de pagamento pós-pagas;
5. operações de crédito;
6. conta de registro e controle (Resolução nº 3.402, de 6 de setembro de 2006);
7. operações de câmbio;
8. serviços de credenciamento em arranjos de pagamento;
9. contas de depósito a prazo e outros produtos com natureza de investimento;
10. seguros; e
11. previdência complementar aberta.¹⁴

Ademais, vale ressaltar que as informações acima sobre as transações de clientes dizem respeito a duas categorias: (i) produtos e serviços contratados

¹⁴ Ibid, art. 5º, I, d.

¹⁵ Ibid, art. 5º, § 5º, I.

¹⁶ Ibid, art. 5º, § 5º, II

ou distribuídos por meio da instituição transmissora de dados; e (ii) acessíveis por meio dos seus canais de atendimento eletrônicos, inclusive no tocante aos limites de crédito eventualmente contratados.¹⁵

Além disso, deverão ser abrangidos, no mínimo, os dados e o histórico de transações realizadas nos últimos doze meses com relação aos produtos e serviços com contratos vigentes nesse período¹⁶.

De qualquer forma, ressalta-se que esses são os dados que devem constar na primeira consulta e/ou compartilhamento por parte de uma instituição financeira, de modo que outros dados pessoais, informações bancárias e serviços poderão ser compartilhados pelas partes, desde que exista o consentimento por parte do titular de dados pessoais.

1.3. Fluxo das Informações entre os Agentes

Para que os sistemas das instituições participantes do *Open Finance* possam se integrar são utilizadas APIs (*Application Programming Interface*). Conforme definição do BCB, APIs são um conjunto de regras e procedimentos sobre como um sistema pode acessar dados ou funcionalidades providos por outros sistemas.¹⁷

Por meio de APIs padronizadas, as instituições participantes do *Open Finance* conseguem integrar os seus sistemas e realizar o compartilhamento de dados e a iniciação de pagamentos. Além da padronização, as APIs disponibilizadas pelas instituições participantes do *Open Finance* devem observar condições mínimas de segurança e robustez, estipuladas pelo BCB.

No plano das atividades de compartilhamento de dados, após o consentimento do cliente a instituição receptora envia uma chamada para a API da instituição detentora de conta, que envia os dados, conforme o fluxo abaixo.

¹⁷ BANCO CENTRAL DO BRASIL. Instrução Normativa BCB nº 95, de 14 de abril de 2021. Disponível em: <https://in.gov.br/en/web/dou/-/instrucao-normativa-bcb-n-95-de-14-de-abril-de-2021-314703508>. Acesso em: 17/05/2022.



Nas operações relacionadas à iniciação de transações de pagamento, por sua vez, a integração para o compartilhamento de dados ocorre entre o sistema da instituição iniciadora e o da instituição detentora de conta.



02

Open Finance e Proteção de Dados Pessoais

2.1. Classificação dos agentes e respectivas responsabilidades

O tratamento de dados pessoais pode ser feito por duas figuras básicas, conforme estabelece a LGPD: o controlador e o operador. O controlador (art. 5º, inciso VI) é a quem competem as decisões referentes ao tratamento dos dados pessoais – ou seja, cabe a ele decidir como os dados serão tratados e o motivo/finalidade pelo qual haverá o tratamento desses dados. Já o operador (art. 5º, inciso VII), é a figura responsável por realizar o tratamento dos dados pessoais em nome do controlador. A importância desta definição reside nas responsabilidades que cada parte assumirá perante os titulares e à Autoridade Nacional de Proteção de Dados Pessoais (a 'ANPD').

A estrutura básica do *Open Finance* inclui duas instituições: a instituição transmissora dos dados, que é responsável por transferir os dados, e a instituição receptora, aquela que solicita o compartilhamento e que obtém os dados de outra instituição. Nessa dinâmica, uma interpretação possível é que a instituição transmissora atuará como operadora dos dados pessoais, se considerarmos que a finalidade de uso dos dados transmitidos é definida apenas pela instituição receptora. Nessa interpretação, a transmissora apenas estaria compartilhando os dados devido à obrigação regulatória.

Contudo, pode haver casos em que, por exemplo, o judiciário ou as autoridades reguladoras entendam que determinado compartilhamento atenda finalidades de uso dos dados tanto da receptora como da transmissora. Nesses casos, é possível que o compartilhamento no contexto do *Open Finance* seja entendido como uma controladoria conjunta ou mesmo controladoria singular entre os agentes. Assim, é necessário verificar as características do caso concreto envolvendo o tratamento de dados, e aguardar como as autoridades e agentes reguladores irão interpretar na prática como os agentes se classificam.

Como exemplo prático, temos a situação de um cliente que possui um empréstimo com o banco A, mas deseja melhorar as condições de pagamento e diminuir as taxas de juros. Dessa forma, procura o banco B para averiguar se ele poderá lhe oferecer melhores ofertas, de acordo com o perfil do cliente. Contudo, para que o banco B possa apresentar ofertas ao cliente, é necessário que haja um histórico de seu perfil financeiro, com informações como sua renda, o valor do empréstimo, entre outras. Assim, o cliente consente que o

banco B acesse suas informações, e o banco B solicita então as informações para o banco A, que deve transmiti-las, pois o banco B já garantiu o consentimento do cliente, atuando como controlador dos dados pessoais neste caso. Ressalta-se que em razão do banco B ser controlador dos dados pessoais do cliente, o banco A não deve questionar a entrega dos dados quando requeridos dentro do sistema *Open Finance*.

Em relação aos demais contextos de transferência de dados que podem envolver o *Open Finance* e os respectivos agentes, devem ser analisadas as características do caso concreto para definição dos papéis exercidos pelos agentes (ex.: controlador, operador, co-controlador).

/ Regime de Responsabilidade

O artigo 4º da Resolução Conjunta nº 01/2020 do BCB e CMN dispõe que as instituições participantes do *Open Finance* devem conduzir suas atividades com ética e responsabilidade, observando os princípios da LGPD. Sob o ponto de vista da legislação consumerista, as instituições participantes do *Open Finance* podem ser responsabilizadas pelos danos que causarem aos consumidores, desde que haja responsabilidade objetiva (nexo causal e dano). Importante acrescentar o conteúdo da súmula 489 do Superior Tribunal de Justiça, que estabelece que *“as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias”*.¹⁸

Ademais, a Resolução nº 01/2020 define que para os casos de uso de serviços de autenticação providos por fornecedores terceiros, permanece com a instituição transmissora de dados ou detentora de conta a responsabilidade para os fins da Resolução.

2.2. Programa de Governança em Proteção de Dados

Por ser caracterizado pelo amplo compartilhamento de dados, o *Open Finance*, para funcionar adequadamente, precisa contar com estrutura de governança em relação à proteção de dados pessoais e à privacidade. É necessário, portanto, um programa de governança que atenda adequadamente às necessidades do setor financeiro e dos seus usuários – afinal, a boa qualidade dos dados utilizados interessa a ambas as partes.

¹⁸ Disponível em: < https://www.coad.com.br/busca/detalhe_16/2409/Sumulas_e_enunciados >

O processo de governança passa por estabelecer metas, torná-las coerentes, implementá-las e avaliar os resultados alcançados, o que inclui a responsabilização.¹⁹

Conforme se verá, não existe apenas uma estrutura de governança que irá reger as instituições que atuam no *Open Finance*. Além de uma estrutura interna, individual, que cada agente deverá adotar, uma estrutura macro de governança também deverá operar. E, como não poderia deixar de ser, para além da regulamentação trazida pelo BCB, a Lei Geral de Proteção de Dados terá um importante papel.

Isso porque a LGPD, por si só, já traz a governança como um elemento importante para o tratamento de dados pessoais. O seu art. 49 afirma que o tratamento de dados pessoais deve atender, dentre outros requisitos, aos padrões de boas práticas e de governança. Nesse sentido, o art. 50 afirma que os controladores e operadores *“poderão formular regras de boas práticas e de governança que estabeleçam [...] mecanismos internos de supervisão e de mitigação de riscos [...]”*. O artigo também estabelece, em seu § 1º, que o controlador e o operador deverão levar em consideração, *“a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular”*.

Para a implementação do programa de governança, deverá se observar, ainda, a estrutura, a escala e o volume das operações do controlador; bem como a sensibilidade dos dados tratados, e a probabilidade e gravidade de eventuais danos sofridos pelos titulares dos dados (art. 50, § 2º, da LGPD):

- (I) **demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;**
- (II) **ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;**
- (III) **ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados trata-**

¹⁹ PETERS, B. “O que é governança?”. Revista do TCU, pp. 28-33, Maio/Ago. 2013.

dos;

- (IV) **estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;**
- (V) **ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;**
- (VI) **estar integrado a sua estrutura geral de governança estabelecendo mecanismos de supervisão internos e externos;**
- (VII) **contar com planos de resposta a incidentes e remediação; e**
- (VIII) **ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.**

Adicionalmente, considerando as características específicas do setor financeiro, é possível que tanto o BCB como as próprias entidades representativas do mercado busquem criar requisitos de governança específicos para o setor.

Importante ressaltar, ademais, que, se implementado o programa de governança em privacidade, ele deverá ser publicado e atualizado periodicamente, bem como será necessário demonstrar a sua efetividade quando apropriado e, em especial, a pedido da ANPD (art. 50, § 2º, II, e § 3º, da LGPD).

A LGPD, ainda, ao tratar das sanções aplicáveis pela autoridade nacional, consigna que deverá ser levada em consideração, quando da aplicação das sanções, a adoção de política de boas práticas e governança (art. 52, § 1º, IX).

Porém, no âmbito do *Open Finance*, a estrutura de governança não será apenas interna. Isso porque a Resolução Conjunta nº 1/2020 do BCB define, em seu art. 44, § 1º, que as instituições participantes do sistema devem estabelecer estrutura responsável pela governança do processo de celebração de convenção, que deverá ser representativa da pluralidade de instituições e segmentos participantes, garantido o acesso não discriminatório.

A Circular nº 4.032, de 23 de junho de 2020, do BCB, dispõe sobre a estru-

tura inicial responsável pela governança do processo de implementação desse novo sistema, trazendo três níveis de implementação: estratégico, técnico e administrativo. De fato, a anteriormente citada Resolução Conjunta nº 1/2020 prevê, agora para o âmbito interno dos agentes regulados, em seu art. 37, I, que, quando da contratação de parceria por parte das instituições autorizadas que busquem implementar o *Open Finance* com entidades não autorizadas a funcionar pelo BCB, será obrigatória a adoção de práticas de governança corporativa e de gestão proporcionais aos riscos a que estejam expostas.

Ou seja, além da estrutura externa de governança para a implementação do *Open Finance*, que será integrada pela pluralidade de instituições e segmentos participantes, também deverá existir uma estrutura interna de governança, em linha do já recomendado pela LGPD.

Na verdade, essa necessidade já era prevista pela Resolução CMN nº 4.658, de 26 de abril de 2018, em seu art. 12, I. A resolução em questão dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo BCB. Dessa forma, o artigo supracitado determina que as instituições em questão, quando do processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas.

A todo esse quadro normativo se soma a Resolução BCB nº 32, de 29 de outubro de 2020, a qual estabelece os requisitos técnicos e procedimentos operacionais para a implementação do *Open Finance* no Brasil. Os seus artigos de 12 a 17, por sua vez, seguem de forma a trazer uma série de requisitos e disposições concernentes à estrutura responsável pela governança do *Open Finance*. Destacam-se itens como a sua atribuição para *“gerenciamento da identidade e da autorização das aplicações das instituições participantes, que abrange a identificação, a autorização e a revogação de certificados utilizados no compartilhamento de dados e serviços do escopo do Open Finance”* (art. 13, II);

e a sua obrigação de “*disponibilizar canal de atendimento gratuito e disponível, ininterruptamente, durante vinte e quatro horas por dia e sete dias por semana*” (art. 14, caput).

Conclui-se que a preocupação com a proteção de dados pessoais no âmbito do Open Finance está devidamente amparada em sua regulamentação pelo BCB, de forma que as estruturas de governança tenham especial relevância. Como na LGPD, nota-se, da regulamentação do BCB, que o risco surge como principal régua para definição de quais medidas devem ser implementadas.

2.3. Incidentes de Segurança

Tanto a LGPD como as normas setoriais do BCB estabelecem obrigações relacionadas à segurança da informação. Vale esclarecer brevemente que um incidente de segurança pode ser definido como a violação de um ou mais dos seguintes atributos da informação: **(i) confidencialidade**, quando uma informação é acessada ou disponibilizada a pessoas não autorizadas; **(ii) integridade**, quando uma informação é alterada de forma não autorizada; e **(iii) disponibilidade**, quando uma informação não pode ser utilizada quando necessário.²⁰



Voltando à análise sobre as obrigações normativas de segurança, elas podem ser divididas em duas categorias básicas: um dever geral de adoção de medidas adequadas de segurança da informação, e, após a ocorrência de um incidente, obrigações de notificação aos afetados e autoridades competentes.

²⁰ BANCO CENTRAL DO BRASIL. Resolução BCB nº 85, de 8 de abril de 2021, art. 3, II e III.

/ Obrigações de Segurança da Informação

A LGPD estabelece ser obrigação dos agentes de tratamento, controladores e operadores, “adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais” (art. 46), sendo eles obrigados a garantir a segurança da informação. Ou seja, os agentes devem adotar tanto medidas técnicas (p. ex. medidas básicas como uso de antivírus, realização de testes para avaliação dos sistemas, testes de penetração/pen testing, etc) quanto medidas administrativas, por meio da implementação de estruturas de governança (p. ex. definição de políticas de segurança da informação, atribuição de responsabilidade aos colaboradores, etc).

A LGPD não impõe padrões de segurança específicos, mas esclarece que a ANPD pode vir a regular sobre o tema (art. 46, §1º). Ademais, a LGPD estabelece ser obrigação dos agentes de tratamento adotarem medidas desde a fase de desenvolvimento de produto/serviços até a sua execução/lançamento no mercado (art. 46, §2º).

Em relação às regras setoriais do Open Finance, importante destacar duas normativas. A Resolução Conjunta do BCB e CMN – Resolução Conjunta do BCB e CMN nº 1/2020, que estabelece, resumidamente, obrigação geral de garantia da segurança da informação no compartilhamento de dados do Open Finance (arts 4, 31, 39, 40 e 48); adoção de mecanismos de autenticação para o compartilhamento de dados (arts 16 e 17); e a necessidade de uso cláusulas de segurança da informação na contratação de parceria com entidades não autorizadas a funcionar pelo BCB, incluindo o dever de o parceiro contratado informar sobre a ocorrência de incidentes (art. 38).²¹

Já a Resolução nº 32 do BCB estabelece que será criado um “Manual de Segurança do Open Finance” cujo objetivo é detalhar padrões de segurança e requisitos técnicos (art. 16),²² diferentemente da LGPD, vale notar, que estabelece apenas obrigações gerais de segurança. A elaboração do Manual é feita pelo BCB e implementada através de instrução normativa.²³

²¹ BANCO CENTRAL DO BRASIL; CONSELHO MONETÁRIO NACIONAL. Resolução Conjunta nº 1 de 4/5/2020. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1>>. Acesso em: 19/05/2022.

²² BANCO CENTRAL DO BRASIL. Resolução BCB nº 32 de 29/10/2020. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=32>>. Acesso em: 19/05/2022.

²³ BANCO CENTRAL DO BRASIL. Instrução Normativa BCB nº 134 de 22/7/2021. Disponível em: <<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=134>>. Acesso em: 19/05/2022.

Por fim, relativo ao tema de políticas de segurança e computação em nuvem, deve-se mencionar a Resolução do BCB nº 85/2021 que define a obrigação das instituições de pagamento de adotarem políticas internas de segurança da informação, e procedimentos para contratação de serviços de computação em nuvem (arts 11 a 18). Apesar de não ser uma regulação elaborada especificamente para o Open Finance, essa Resolução estabelece obrigações importantes sobre segurança da informação. Dentre as políticas exigidas pela Resolução estão uma “Política de Segurança Cibernética” e um “Plano de Ação e de Resposta a Incidentes”.

A “Política de Segurança Cibernética” deve definir os objetivos de segurança, procedimentos internos de avaliação e mitigação de risco, registro dos incidentes, capacitação de pessoal, e procedimentos para orientação de usuários finais em relação à segurança (arts 2 a 6). Já o “Plano de Ação e de Resposta a Incidentes” deve definir as ações a serem tomadas para implementação da Política de Segurança Cibernética, procedimentos e tecnologias a serem utilizadas para prevenir e responder a incidentes de segurança, e definição da **área responsável pelo registro e controle de incidentes** (arts 6 a 10).

/ Obrigações Após a Ocorrência de um Incidente

Em relação às obrigações de notificação, a LGPD estabelece que, caso ocorra um incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados, é obrigação do controlador dos dados notificar a ANPD e os titulares (art. 48). Desse modo, em caso de incidente envolvendo dados pessoais, a instituição afetada deve avaliar os riscos e danos gerados aos titulares para verificar se há necessidade de notificá-los.

A ANPD já disponibilizou modelo parcial de notificação de incidente à Autoridade, devendo o incidente ser notificado à ANPD pelo seu website por meio da plataforma do governo federal para “Petição Eletrônica”, o SEI.²⁴

Em relação ao Open Finance, a Resolução Conjunta nº 1/2020 do BCB e do CMN define que as instituições participantes devem registrar semestralmente a ocorrência de incidentes de segurança da informação e as medidas to-

²⁴ AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS. Comunicação de incidentes de segurança. Disponível em: < <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca> >. Acesso em: 18/05/2022.

²⁵ CONSELHO MONETÁRIO NACIONAL. Resolução nº 4.893 de 26/02/2021. Disponível em: < <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893> >. Acesso em: 19/05/2022.

madras (art. 33).

As Resoluções do BCB nº 85/2021 e do CMN nº 4.893/2021²⁵ estabelecem o dever das instituições de pagamento e instituições autorizadas a funcionar pelo BCB de comunicarem tempestivamente o BCB sobre “ocorrências de incidentes relevantes e das interrupções dos serviços relevantes [...] que configurem uma situação de crise pela instituição financeira” (ambas, art. 20, III). Interessante notar que os critérios para caracterização de uma “situação de crise” são deixados para serem definidos e documentado pelas próprias instituições reguladas (ambas, art. 20, Parágrafo Único). Vale lembrar que as Resoluções não regulam diretamente o Open Finance, mas sim questões de segurança da informação e uso de computação em nuvem.

Adicionalmente, as Resoluções do BCB nº 85/2021 e do CMN nº 4.893/2021 estabelecem que as políticas de segurança da informação das instituições de pagamento e instituições autorizadas a funcionar pelo BCB devem conter iniciativas para compartilhamento de informações sobre incidentes de segurança entre si para fins de aprendizado (ambas, art. 22) e com o BCB (ambas, art. 22, §2º). Contudo, as Resoluções não entram em detalhe sobre como devem ser elaboradas essas iniciativas de compartilhamento.

Por fim, as Resolução do BCB nº 85/2021 e a Resolução do CMN nº 4.893/2021 impõe a elaboração de relatório anual sobre a implementação do plano de resposta a incidentes que contenha os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período (art. 8, III).

Quadro Resumo

Norma	Obrigações
LGPD	Adoção de medidas adequadas de segurança da informação (técnicas e administrativas); Adoção desde a concepção de medidas de segurança da informação desde o desenvolvimento de produtos/serviços; e Notificação dos titulares e autoridades após ocorrência de incidente.

BCB – Resolução nº 85/2021	<p>Exigência de estruturas de governança em segurança da informação;</p> <p>Incentivo de compartilhamento de informações sobre incidentes entre instituições, para fins de aprendizado conjunto.</p>
CMN – Resolução nº 4.893/2021	<p>Adoção de “Política de Segurança Cibernética”;</p> <p>Adoção de “Plano de Ação e de Resposta a Incidentes”; e</p> <p>Requisitos para contratação de serviços de computação em nuvem.</p>
BCB e CMN – Resolução Conjunta nº 1/2020	<p>Dever geral de garantia da segurança da informação no compartilhamento de dados do Open Finance;</p> <p>Mecanismos de autenticação para o compartilhamento de dados;</p> <p>Dever de utilizar cláusulas com obrigações de segurança da informação na contratação de parceria com entidades não autorizadas a funcionar pelo BCB, para implementação do Open Finance;</p> <p>Dever de registro semestral de incidentes de segurança ocorridos e das medidas de prevenção e solução adotadas.</p>
BCB – Resolução nº 32/2020	<p>Define que o BCB deve elaborar o Manual de Segurança para as instituições participantes do Open Finance.</p>
BCB - Instrução Normativa nº 134/2021	<p>Divulga a versão 3.0 do Manual de Segurança do Open Finance, com medidas específicas a serem adotadas.</p>

2.4. Direitos dos Titulares

Considerando o grande volume de compartilhamento de dados pessoais que envolve o Open Finance, é evidente a importância da garantia dos direitos dos titulares dos dados, principalmente os previstos na (i) LGPD, e (ii) na Resolução Conjunta nº 1/2020.

/ Portabilidade

A LGPD reconhece, em seu art. 18, V, o direito do titular de requisitar a portabilidade dos dados a outro fornecedor de serviço ou produto, de acordo com regulamentação da ANPD, observados os segredos comercial e industrial. O direito à portabilidade de dados que o agente de tratamento, a pedido de um indivíduo, transfira as informações pessoais coletadas para um terceiro selecionado.

Porém, o direito de portabilidade suscita controvérsias na medida em que pode envolver direitos de propriedade intelectual, de forma que:

“ainda que não definido pelo sistema, entende-se que provavelmente não deverão estar no escopo da portabilidade, como também não integram os compartilhamentos que serão realizados pelo Open Finance (art. 5º, §4º, I, “b”), os dados considerados inferidos e derivados – que são aqueles gerados ou complementados a partir de tratamentos realizados pela instituição controladora e constituem o seu know-how (inteligência artificial, algoritmos etc).”²⁶

No mais, por ser outro ponto de polêmica, deve-se destacar que o titular pode realizar a portabilidade dos registros de suas atividades bancárias mesmo que contenham dados pessoais de terceiro com quem eventualmente tenha realizado alguma transação financeira, desde que a informação do terceiro esteja inevitavelmente associada ao dado pessoal do titular, e, ainda, que sejam adotadas medidas que restrinjam os tratamentos que poderão ser feitos pelo novo controlador com os dados pessoais do terceiro²⁷.

/ Demais Direitos Previstos na LGPD

Ainda, além dos já descritos, os outros direitos listados na LGPD (art. 18) tam-

²⁶ ITS – Instituto de Tecnologia & Sociedade do Rio. Open Banking e Proteção de Dados, p. 14, nov. 2020. Disponível em: <https://itsrio.org/wp-content/uploads/2020/11/Relatorio-Open-Banking-e-Protecao-de-Dados.pdf>

²⁷ Ibid.

bém são aplicáveis às pessoas naturais no contexto do Open Finance, a qualquer momento e mediante requisição, sendo eles:

- (IX) confirmação da existência de tratamento dos dados;
- (X) acesso aos dados;
- (XI) correção de dados incompletos, inexatos ou desatualizados;
- (XII) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- (XIII) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em situações específicas delimitadas na Lei;
- (XIV) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; e

Tais direitos são benéficos não apenas aos titulares, pois:

“além de resguardar o controle do titular em relação a seus dados, grande parte dos direitos dos titulares estabelecidos na LGPD possibilitam a adequação e melhoria do oferecimento de produtos e prestação de serviços aos indivíduos, uma vez que, como exemplo, o tratamento de dados completos, exatos e atualizados é fundamental para o funcionamento otimizado e orgânico do mercado de crédito, impactando diretamente o mercado financeiro e demais setores da economia”²⁸

Ressalta-se, ademais, que um importante ponto a se considerar, quando da análise do assunto, é que a Resolução do BCB também se aplica aos clientes que são pessoas jurídicas (art. 2º, II), enquanto a LGPD se aplica apenas aos titulares pessoas naturais (art. 1º, caput).

Pode-se concluir que *“há um paralelismo importante entre os direitos presentes na LGPD e o que é garantido na regulamentação de Open Finance”*.²⁹ Assim, ambas as legislações devem necessariamente ser consultadas quando da análise dos direitos do titular dos dados pessoais, quando for pessoa natural.

Pode-se concluir que o titular dos dados está amparado por uma série de direitos em sua posição de usuário do sistema de Open Finance no Brasil,

²⁸ LAPIN – Laboratório de Políticas Públicas e Internet. Open Banking & LGPD: Entraves e Eficiências, p. 17, nov. 2020. Disponível em: https://lapin.org.br/wp-content/uploads/2020/11/Relatorio-Open-Banking-LGPD_LAPIN.pdf

²⁹ ITS – Instituto de Tecnologia & Sociedade do Rio. Open Banking e Proteção de Dados, p. 13, nov. 2020. Disponível em: <https://itsrio.org/wp-content/uploads/2020/11/Relatorio-Open-Banking-e-Protecao-de-Dados.pdf>

os quais estão previstos em uma série de normativas distintas, mas semelhantes em seu conteúdo. Importante destacar que tais direitos, além de resguardarem o controle do titular de dados, são importantes para a manutenção da qualidade do sistema, pois:

“possibilitam a adequação e melhoria do oferecimento de produtos e prestação de serviços aos indivíduos, uma vez que, como exemplo, o tratamento de dados completos, exatos e atualizados é fundamental para o funcionamento otimizado e orgânico do mercado de crédito, impactando diretamente o mercado financeiro e demais setores da economia”³⁰.

³⁰ LAPIN – Laboratório de Políticas Públicas e Internet. Open Banking & LGPD: Entraves e eficiências, p. 17, nov. 2020. Disponível em: <https://lapin.org.br/wp-content/uploads/2020/11/Relatorio-Open-Banking-LGPD_LAPIN.pdf>. Acesso em: 18/05/2022.

03

Requisitos para o consentimento

Primeiramente, deve-se destacar o **direito de transparência em relação ao consentimento**. O consentimento do titular de dados é tido como requisito essencial para os serviços do Open Finance, (art. 10 da Resolução nº 1/2020). Porém, em consonância com a LGPD, uma série de requisitos devem ser cumpridos para que o consentimento seja válido, sendo o seu cumprimento um direito do titular e uma obrigação das instituições receptoras dos dados

A LGPD afirma, em seu art. 5º, XII, que o consentimento deve ser livre, informado, inequívoco, e que deve ter finalidade determinada. O consentimento, ainda, deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular; e, se fornecido por escrito, deverá constar de cláusula destacada das demais (art. 8º, caput e § 1º). Ainda, é vedado o tratamento de dados pessoais mediante vício de consentimento (art. 8º, § 3º). Por fim, o titular tem o direito de receber informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (todos direitos listados no art. 18 da LGPD).

Já a Resolução nº 1/2020 do BCB e da CMN traz requisitos na mesma linha dos elencados na LGPD. Nesse sentido, a instituição receptora de dados deverá identificar o cliente e obter o seu consentimento previamente ao compartilhamento dos seus dados. Para esse consentimento ser considerado válido, ele deverá (art. 10):

- (xv) ser solicitado por meio de uma linguagem clara, objetiva e adequada;
- (xvi) ter finalidades claras;
- (xvii) prazo de validade adequado a finalidade apresentada, sendo esse prazo limitado a 12 meses;
- (xviii) indicar qual é a instituição transmissora de dados;
- (xix) apresentar de forma clara quais dados ou serviços serão objeto de compartilhamento;
- (xx) identificar o cliente; e

³¹ Art. 2º da LGPD: “consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

³² European Data Protection Supervisor. Guidelines on data protection in EU financial services regulation, p. 14, nov. 2014. Disponível em: https://edps.europa.eu/sites/default/files/publication/14-11-25_financial_guidelines_en.pdf.

(xxi) ser obtido apenas posteriormente à data de vigência do regulamento.

O consentimento não será considerado válido se for obtido:

(xxii) por meio de contrato de adesão,

(xxiii) via formulário com opção de aceite previamente preenchida ou

(xxiv) de forma presumida.

Conforme pode ser observado, as condições definidas pela Resolução nº 1/2020 tiveram o cuidado de levar em consideração os requisitos para obtenção do consentimento e os fundamentos³¹ da LGPD, entre eles, o princípio da autodeterminação informativa.

No entanto, apesar da Resolução nº 1/2020 ter um grande enfoque na necessidade de obtenção do consentimento para transferência dos dados, **isso não implica que todo tratamento de dados deve ser baseado exclusivamente no consentimento**. Em alguns casos, especificamente quando relacionado a tratamentos que vão além ou são subsequentes ao escopo do Open Finance, eles podem ser baseados no legítimo interesse da instituição, na execução de contrato ou mesmo na proteção de crédito da instituição financeira receptora. Tal entendimento, inclusive segue linha similar ao adotado pela European Data Protection Supervisor ao preparar um guia específico sobre a regulamentação de serviços financeiros³². Além do mais, no caso da instituição transmissora, o compartilhamento dos dados não decorre do consentimento do cliente ou titular, mas sim da obrigação regulatória imposta pela própria Resolução Conjunta.

Cabe ressaltar que, para os casos em que o consentimento não é necessário ou aplicável devido à utilização de outras bases legais, ainda devem ser observadas em conjunto e de forma harmônica as demais regras determinadas nas normas regulatórias do Open Finance.

A **opção da revogação do consentimento** deve ser disponibilizada, ao menos, pelo mesmo canal de atendimento pelo qual o consumidor consentiu previamente, caso o canal ainda exista (art. 15 § 1º, da Resolução do nº 1/2020). Adicionalmente, é vedado à instituição financeira propor ao cliente a

³³ ITS – Instituto de Tecnologia & Sociedade do Rio. Open Banking e Proteção de Dados. p. 13-14, nov. 2020. Disponível em: <https://itsrio.org/wp-content/uploads/2020/11/Relatorio-Open-Banking-e-Protecao-de-Dados.pdf>

³⁴ LAPIN – Laboratório de Políticas Públicas e Internet. Open Banking & LGPD: Entraves e eficiências, p. 25, nov. 2020. Disponível em: https://lapin.org.br/wp-content/uploads/2020/11/Relatorio-Open-Banking-LGPD_LAPIN.pdf

³⁵ Ibid.

revogação do consentimento, com exceção de haver suspeita de fraude (art. 15, § 2º, da Resolução). No mais, a revogação deverá ser realizada em até um dia, contado a partir da solicitação do cliente, para serviços de transação de pagamento, e de forma imediata para os demais casos (art. 15, §3º, da Resolução do nº 1/2020). Na realidade, deve-se considerar que a mesma facilidade para fornecer o consentimento também deve existir para retirá-lo, o que é decorrência da lógica da LGPD de que o exercício dos direitos seja acessível e fácil para os titulares dos dados³³.

Por fim, vale notar que alguns autores criticam na Resolução nº 1/2020 o que chamam de *“fadiga do consentimento”*, situação causada pelo *“extenso conteúdo e complexidade na avaliação das consequências da autorização para o tratamento de seus dados pessoais”*³⁴. Ou seja, a crítica à base legal do consentimento está relacionada à complexidade do fluxo informacional e a real capacidade de os titulares compreenderem como seus dados serão utilizados antes de consentirem³⁵.

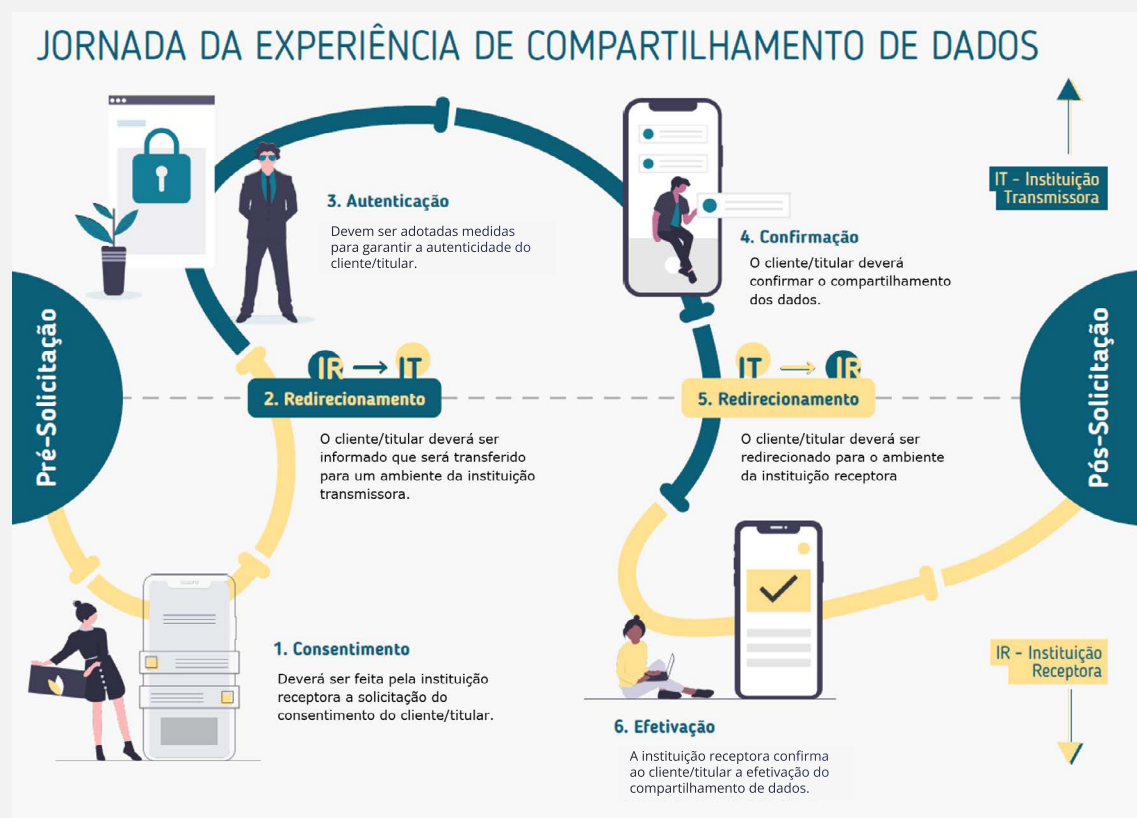
04

Requisitos para a transferência de dados

Após a obtenção do consentimento pelo titular de acordo com as obrigações aplicáveis, a Resolução nº 1/2020 e a Resolução BCB nº 32 de 29/10/2020, tiveram o cuidado de estabelecer requisitos técnicos e procedimentos operacionais para implementação adequada do Open Finance pelas **instituições financeiras envolvidas**.

Esse procedimento leva em consideração a experiência do cliente, padrões para o desenvolvimento de APIs, medidas de segurança e mecanismos para resolução de conflitos e podem ser encontrados de forma detalhada no Guia da Experiência do Usuário³⁶ e no Portal do Open Finance Brasil dedicado aos desenvolvedores³⁷.

Segue abaixo um breve resumo sobre a jornada da experiência de compartilhamento de dados:



Fluxograma elaborado pelo BCB para descrever a jornada do usuário no Open Finance.

³⁶ BCB – Banco Central do Brasil. Guia do Usuário: requisitos mínimos e recomendações das jornadas, mai. 2021. Disponível em: <<https://openbanking-brasil.github.io/areadesenvolvedor/versions/v1.0.0-rc6.8/documents/GuiaDeExperienciaDoUsuarioCompartilhamentoDeDadosElNiciacaoDePagamento.pdf>>. Acesso em: 18/05/2022.

³⁷ BCB – Banco Central do Brasil. Área do Desenvolvedor do Portal do Open Banking Brasil. Disponível em: <<https://openbanking-brasil.github.io/areadesenvolvedor/?javascript#introducao>>. Acesso em: 18/05/2022.

³⁸ BCB – Banco Central do Brasil. Guia do Usuário: requisitos mínimos e recomendações das jornadas, p.34, mai. 2021. Disponível em: <<https://openbanking-brasil.github.io/areadesenvolvedor/versions/v1.0.0-rc6.8/documents/GuiaDeExperienciaDoUsuarioCompartilhamentoDeDadosElNiciacaoDePagamento.pdf>>. Acesso em: 18/05/2022.

Como é possível observar, todo o sistema de Open Finance foi estruturado de forma a garantir a segurança e transparência, adotando no processo de compartilhamento etapas de autenticação do titular da conta, confirmação das escolhas feita e a notificação de que processo foi concluído com sucesso.

Conclusão

Conforme exposto, o Open Finance surge para estimular uma oferta mais competitiva de serviços financeiros por meio do compartilhamento de dados pessoais dos clientes entre instituições financeiras. Contudo, para que esse compartilhamento possa ser realizado, uma série de requisitos devem ser cumpridos para proteção dos dados pessoais e privacidade dos clientes. Dentre eles, destacam-se os requisitos para a obtenção de um consentimento adequado do titular dos dados para autorizar o compartilhamento (conforme a LGPD e a Resolução nº 1/2020 do BCB e CMN); os deveres de segurança da informação, principalmente em relação às regras específicas definidas pela regulação setorial do BCB, (*“Manual de Segurança do Open Finance”*); e a definição de quais dados devem ser compartilhados e as regras para o compartilhamento. Verificou-se que os requisitos regulatórios do setor elaborados pelo BCB buscaram estar, no geral, em sintonia com os requisitos da LGPD, o que deve ser considerado pelos agentes nas suas iniciativas de adequação às normas de proteção de dados.

b/luz
deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.



baptistaluz.com.br