



PARECER JURÍDICO – *LEGAL OPINION*

*Análise dos aspectos legais da Resolução Conjunta n.
06/2023 do Banco Central do Brasil e do Conselho
Monetário Nacional*

Parte interessada/solicitante:

Sistema OCB

Acesse a Resolução
pelo QR CODE abaixo
ou [clique aqui](#)



Sumário

1. CONTEXTUALIZAÇÃO DA RESOLUÇÃO	3
1.1 INSTITUIÇÕES SUJEITAS AS REGRAS DA RESOLUÇÃO	3
1.2 SOBRE O COMPARTILHAMENTO	4
1.3 REQUISITOS DOS SISTEMAS ELETRÔNICOS	5
1.4 RELACIONAMENTO COM TERCEIROS	6
1.5 MEDIDAS NECESSÁRIAS PARA O COMPARTILHAMENTO.....	6
1.6 PRAZOS DE RETENÇÃO	7
2. ANÁLISE JURÍDICA DA RESOLUÇÃO CONJUNTA	8
3. CONCLUSÕES	13

1. CONTEXTUALIZAÇÃO DA RESOLUÇÃO

 O Banco Central do Brasil e o Conselho Monetário Nacional, publicaram, no dia 06 de maio de 2023, a **Resolução Conjunta nº 06/2023** com objetivo de estabelecer requisitos para o compartilhamento de dados e informações sobre indícios de fraudes, os quais deverão ser observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

A **Resolução Conjunta** passará a valer a partir de 1º de novembro de 2023 e cria diversas obrigações que devem ser integralmente observadas pelas cooperativas de crédito - algumas delas refletem diretamente nos programas de proteção de dados pessoais e, por consequência, no cumprimento da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Inicialmente, realizamos uma breve contextualização acerca das regras dispostas na **Resolução Conjunta**, objeto deste parecer.

1.1 INSTITUIÇÕES SUJEITAS AS REGRAS DA RESOLUÇÃO

De acordo com o parágrafo segundo do artigo 1º da **Resolução Conjunta**, estão sujeitas aos regramentos definidos no normativo:

- Bancos de qualquer espécie;
- Distribuidoras de valores mobiliários
- Corretoras de câmbio e de valores mobiliários;
- Sociedades de crédito, financiamento e investimentos;
- Sociedades de crédito imobiliário;
- Administradoras de cartões de crédito;
- Sociedades de arrendamento mercantil;
- Administradoras de mercado de balcão organizado;
- Cooperativas de crédito;
- Associações de poupança e empréstimo;
- Bolsas de valores e de mercadorias e futuros;
- Entidades de liquidação e compensação; e
- Outras sociedades que, em razão da natureza de suas operações, assim venham a ser consideradas pelo Conselho Monetário Nacional.

As administradoras de consórcio, por força do disposto no parágrafo primeiro do artigo 1º da **Resolução Conjunta**, não estão sujeitas aos termos do normativo.

1.2 SOBRE O COMPARTILHAMENTO

O compartilhamento instituído pela **Resolução Conjunta** deverá¹ ser operacionalizado pelas instituições através da adoção de sistemas eletrônicos que possuam, no mínimo, as seguintes funcionalidades:

- Registro de dados e de informações sobre indícios de ocorrências ou de tentativas de fraudes identificadas pelas instituições em suas atividades;
- Alteração e exclusão dos dados e das informações registradas; e
- Consulta dos dados e das informações registradas.

Os registros dos dados e informações que serão objeto de compartilhamento, **devem conter**, no mínimo:

- Identificação de quem teria executado ou tentado executar a fraude, quando possível e de acordo com os indícios identificados;
- Descrição dos indícios da ocorrência ou da tentativa de fraude;
- Identificação da instituição responsável pelo registro; e
- Identificação dos dados da conta destinatária e de seu titular, em caso de transferência ou pagamento de recursos.

O normativo prevê expressamente que as informações sigilosas relacionadas com indícios de **crimes de "lavagem" ou ocultação de bens, direitos e valores e de financiamento do terrorismo não devem ser objeto do compartilhamento instituído pela Resolução Conjunta**. Ou seja, caracterizam-se como exceções à regra do compartilhamento impositivo.

¹ Artigo 2º da Resolução Conjunta.

Com objetivo de limitar o acesso às informações registradas no sistema de compartilhamento, a **Resolução Conjunta** destaca que somente terão acesso:

- As instituições sujeitas aos regramentos da resolução;
- O Banco Central do Brasil; e
- Autoridades competentes.

1.3 REQUISITOS DOS SISTEMAS ELETRÔNICOS

O normativo indica no artigo 4º, que o sistema eletrônico utilizado para compartilhamento das informações e dados deverá:

- Permitir o acesso pleno às funcionalidades com a respectiva identificação de quem realizou o acesso ao ambiente;
- Adotar um padrão único e comum de comunicação que permita a execução das suas funcionalidades;
- Assegurar a interoperabilidade com outros sistemas eletrônicos implementados para atendimento da resolução, quando existentes;
- Contemplar procedimentos e controles para assegurar:
 - cumprimento da legislação e da regulamentação em vigor;
 - confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações nele registrados;
 - aderência a certificações de segurança;
 - elaboração de relatórios por empresa de auditoria especializada e independente relativos aos procedimentos e aos controles utilizados na execução das suas funcionalidades;
 - provimento de informações e de recursos de gestão adequados ao monitoramento de suas funcionalidades;
 - identificação e segregação dos dados e das informações registrados por meio de controles físicos ou lógicos;
 - qualidade dos controles de acesso voltados à proteção dos dados e das informações registrados por meio do sistema; e
 - possibilitar aos titulares dos dados o livre acesso, exclusão ou correção das informações registradas, em caso de eventuais erros, inconsistências ou outras demandas.

1.4 RELACIONAMENTO COM TERCEIROS

A **Resolução Conjunta** traz regras claras acerca da possibilidade² de contratação de terceiros para o fornecimento dos sistemas eletrônicos utilizados para o compartilhamento dos dados e informações. Todavia, as instituições deverão assegurar que os termos da Resolução, as legislações e os regulamentos vigentes sejam integralmente observados pelos terceiros contratados.

De acordo com o texto, os terceiros deverão observar as regras contidas na **Resolução CMN nº 4.893/2021**, que regulamenta a política de segurança cibernética e requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.



Vale referir que as responsabilidades decorrentes das obrigações previstas na **Resolução Conjunta** permanecem com as instituições, ainda que elas realizem a contratação de terceiros para o fornecimento ou gerenciamento do sistema eletrônico.

Inclusive, importante destacar que o Banco Central do Brasil³ pode vetar ou impor restrições à contratação dos terceiros que fornecerem os sistemas eletrônicos, quando constatar, a qualquer tempo, a inobservância das disposições previstas na **Resolução Conjunta**.

1.5 MEDIDAS NECESSÁRIAS PARA O COMPARTILHAMENTO

As cooperativas deverão obter o consentimento prévio e geral do associado ou cliente para a realização do registro e compartilhamento das informações e dados. O consentimento deverá, obrigatoriamente, contemplar os seguintes requisitos:

- **Finalidade:** tratamento e compartilhamento de dados e informações sobre os indícios de fraudes;

² Artigo 5º da Resolução Conjunta.

³ Artigo 10 da Resolução Conjunta.

- **Forma:** cláusula em destaque;
- **Local:** em destaque no corpo do instrumento contratual ou outro instrumento jurídico válido.

Além da obtenção do consentimento, durante as atividades de registro e compartilhamento das informações, as cooperativas deverão respeitar os seguintes princípios:

- Segurança e privacidade de dados e informações compartilhados;
- Qualidade dos dados e informações compartilhados;
- Acesso pleno e não discriminatório às funcionalidades do sistema eletrônico utilizado;
- Eficiência no cumprimento dos requisitos do sistema eletrônico exigidos na Resolução Conjunta, inclusive no padrão único e comum de comunicação entre sistemas;
- Reciprocidade com outras instituições; e
- Interoperabilidade com outros sistemas eletrônicos implementados em atendimento ao disposto na Resolução Conjunta.

1.6 PRAZOS DE RETENÇÃO

Por fim, a **Resolução Conjunta** estabelece alguns prazos de retenção para informações e documentos, que, igualmente, deverão ser observados pelas cooperativas.

Segundo a norma, os dados e informações objeto de compartilhamento devem ser mantidos pelo prazo de **10 (dez) anos**, assim como a documentação relacionada aos critérios adotados pela instituição para a identificação das fraudes.

Além disso, os dados e informações relacionadas aos mecanismos de acompanhamento e controle deverão ser mantidos pelo prazo de **05 (cinco) anos**, os quais serão contados a partir da aplicação dos respectivos mecanismos pela instituição.

2. ANÁLISE JURÍDICA DA RESOLUÇÃO CONJUNTA

Conforme identificado no tópico anterior, a **Resolução Conjunta nº 06/2023** estabeleceu rol de obrigações que deverão ser observadas pelas cooperativas do ramo crédito, especialmente nas circunstâncias envolvendo indícios de ocorrências ou de tentativas de fraudes, hipótese em que os dados pessoais e informações relativas a associados e outras pessoas físicas poderão ser compartilhados, nos termos do regramento.

Com efeito, dispõe a norma que dados pessoais como a “identificação das partes” e “dados bancários dos envolvidos” devem ser compartilhados pelas cooperativas com as demais instituições para possibilitar e qualificar o combate a fraudes no sistema financeiro.

Considerando que para atendimento da resolução as cooperativas realizarão tratamento de dados pessoais dos seus clientes, associados e de outras pessoas físicas, aplicável ao caso as disposições previstas na Lei Geral de Proteção de Dados Pessoais (LGPD). Não por acaso, o dever de cumprimento da referida legislação está indicado expressamente no artigo 2º, § 6º⁴ e no artigo 3º⁵, ambos da **Resolução Conjunta**.

Desta forma, caberá às cooperativas observarem as disposições da LGPD e harmonizá-las com as regras estabelecidas na resolução ora analisada, uma vez que são complementares.

O primeiro ponto de destaque e complementação entre a LGPD e a resolução em análise vincula-se ao consentimento para compartilhamento de informações e dados pessoais. Segundo a resolução, o referido consentimento deverá:

⁴ §6º - Os dados e as informações a serem compartilhados, conforme o disposto no caput deste artigo, devem ser disponibilizados em conformidade com a legislação e a regulamentação em vigor, observado o dever de sigilo, a proteção dos dados pessoais e a livre concorrência.

⁵ Art. 3º As instituições de que trata o art. 1º, para atingir a finalidade do compartilhamento de que trata o art. 2º, devem conduzir suas atividades em observância da legislação e da regulamentação em vigor, observados o dever de sigilo, a proteção de dados pessoais e a livre concorrência, bem como os seguintes princípios:

- Ter como finalidade o tratamento e o compartilhamento dos dados e informações pelas cooperativas; e
- Constar de contrato firmado entre o associado/cliente e a cooperativa.

O consentimento deverá estar em cláusula destacada e no corpo do próprio contrato firmado com o associado ou cliente ou em outro instrumento jurídico válido adotado pela cooperativa, o qual deverá estar à disposição do Banco Central do Brasil, conforme Art. 2º, §5º, da **Resolução Conjunta**.

Entretanto, importante ressaltar que as cooperativas devem adotar cautela na identificação da hipótese legal para o tratamento dos dados pessoais decorrentes do cumprimento da **Resolução Conjunta**, uma vez que, embora a própria resolução indique que deverá haver consentimento prévio para o tratamento e compartilhamento dos dados e informações, este "consentimento" não se confunde com a hipótese de tratamento de dados pessoais prevista no artigo 7º, inciso I, da LGPD.

Isso porque, há inúmeras diferenças práticas entre o "consentimento" da LGPD (enquanto hipótese de tratamento de dados pessoais) e o "consentimento" previsto em outras bases do direito privado, como no Código Civil ou nas regulamentações setoriais, como é o caso da Resolução Conjunta objeto desta análise jurídica. De acordo com a LGPD, por exemplo, o consentimento deve ser uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Art. 5º, XII) e ser "fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (Art. 8º).

Assim, considerando que o tratamento de dados pessoais para cumprimento da resolução em comento não será facultativo, mas sim um dever decorrente de normativo emitido por órgãos reguladores do sistema financeiro, para efeitos de LGPD, **os dados serão tratados para cumprimento de obrigação regulatória, cujo cumprimento é impositivo para as cooperativas.**

Desta forma, muito embora ocorra a coleta de consentimento dos associados e clientes para possibilitar a execução da atividade, este não será o que legitimará o tratamento dos dados pessoais, uma vez que a hipótese legal aplicável e que deverá ser registrada no Registro das Operações de Tratamento de Dados Pessoais, é aquela contida no Art. 7º, inciso II, da LGPD, qual seja:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
[...]
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
[...]

Portanto, relativamente ao “consentimento” imposto pela **Resolução Conjunta**, tem-se que as cooperativas deverão observar os requisitos contidos na norma (Art. 2º, §4º) e não aqueles estabelecidos na LGPD (Art. 8º), uma vez que o consentimento que deverá ser coletado diz respeito a uma regra de operacionalização da atividade de combate à fraude e não para justificar, de acordo com as hipóteses previsto no art. 7º da LGPD, o tratamento dos dados pessoais em si.

➤ A respeito disso, recomenda-se que as cooperativas envolvam seus Encarregados pelo tratamento de dados pessoais (DPOs) na implementação das regras previstas na **Resolução Conjunta**, considerando que a atividade de compartilhamento precisará ser devidamente mapeada e inserida no Registro de Operações de Tratamento de Dados Pessoais (RoPA/ROT) da cooperativa, uma vez que envolve o tratamento (coleta, processamento, compartilhamento e armazenamento) de dados pessoais.

Além deste aspecto legal relacionado ao “consentimento”, insta referir que as cooperativas deverão observar também 1) os requisitos do sistema eletrônico (Art. 2º e 4º); 2) as regras para a contratação de terceiros para fornecimento do sistema eletrônico (Art. 5º); e 3) a documentação obrigatória e respectivos prazos de conservação (Art. 8º).

Dentre os pontos destacados acima, importante tecer algumas considerações sobre a possibilidade das cooperativas contratarem prestadores de serviços para fornecimento do sistema eletrônico. Conforme autorização expressa extraída do artigo

5º da resolução, as cooperativas poderão contratar prestadores de serviço para fornecerem o sistema eletrônico que operacionalizará o tratamento e compartilhamento de dados e informações, desde que os contratados observem integralmente as regras contidas na **Resolução Conjunta** e na **Resolução CMN nº 4.893/2021**⁶.

Em razão disso, é imprescindível que as cooperativas estabeleçam cláusulas robustas nos contratos de prestação de serviços com os terceiros que venham a ser contratados, as quais devem estabelecer, além das regras jurídicas decorrentes da prestação do serviço propriamente dito, aspectos específicos como:

- Compromisso de agir em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD;
- Obrigação de implementar e manter medidas técnicas e organizacionais necessárias para a proteção dos dados pessoais tratados por conta do serviço prestado, contra destruição acidental ou ilegal, acesso não autorizado, alterações, perdas, divulgação ou qualquer outra medida de violação;
- Possibilidade de submeter a empresa contratada a rotinas de auditoria para verificação acerca do cumprimento das disposições previstas no contrato e nas normas aplicáveis;
- Dever de auxílio no atendimento aos direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais - LGPD;
- Dever de comunicação de incidentes de segurança da informação de forma imediata ou no prazo máximo de 01 (um) dia útil, descrevendo, no mínimo, quais foram os titulares afetados, os dados pessoais violados e as medidas de tratamento/mitigação adotadas;
- Proibição expressa de utilização dos dados para finalidades distintas ao objeto da **Resolução Conjunta**;
- Compromisso de eliminação dos dados e informações compartilhadas, quando formalmente solicitado ou em caso de eventual rescisão contratual, término do prazo de vigência ou qualquer outra modalidade de extinção contratual, ressalvadas as hipóteses de manutenção obrigatória das informações para cumprimento de leis e regulamentos;
- Dever de adoção das medidas previstas na LGPD para autorizar a transferência internacional de dados, quando aplicável;
- Compromisso de estabelecer com os subcontratados instrumentos jurídicos que incorporem todas as obrigações previstas no contrato firmado e imponha o cumprimento

⁶ Resolução que estabelece regras sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições financeiras.

das medidas técnicas e/ou administrativas indicadas no instrumento e nas legislações aplicáveis;

- Dever de observância da **Resolução Conjunta** e **Resolução CMN nº 4.893/2021**;
- Dever de implementar os requisitos estabelecidos nos artigos 2º e 4º da **Resolução Conjunta**;
- Compromisso de atualização do sistema para adequá-lo com às atualizações da **Resolução Conjunta** ou de regramentos complementares que venham a ser estabelecidos pelo Banco Central do Brasil (Art. 9º da **Resolução Conjunta**);
- Dever de indenização pelo descumprimento das regras da **Resolução Conjunta**, bem como daquelas contidas no contrato e legislações aplicáveis; e
- Dever de fornecer a documentação sobre o sistema eletrônico e atender aos requisitos indicados no artigo 4º, parágrafo único da **Resolução Conjunta**.

Em relação às cláusulas de proteção de dados pessoais constantes nos contratos formalizados com os terceiros, além dos itens especificados acima, devem ser estabelecidas obrigações robustas, considerando o objeto do contrato, seus respectivos riscos, as características e o volume dos dados que serão tratados pelos terceiros em nome da cooperativa.

Por fim, considerando que a atividade de tratamento de dados estabelecida pela **Resolução Conjunta** pode gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais, é recomendável que as cooperativas confeccionem Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

Acerca do tema, importante destacar as orientações⁷ divulgadas recentemente pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), segundo as quais, como regra geral, é recomendado elaborar o RIPD em todo contexto em que as operações de tratamento de dados pessoais possam gerar **alto risco** à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD, às liberdades civis e

⁷ Perguntas e respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais

aos direitos fundamentais dos titulares de dados pessoais, conforme art. 5º, inciso XVII, e art. 55-J, inciso XIII, da LGPD.

De acordo com a ANPD, o tratamento será de **alto risco** se verificado, no caso concreto, a presença de, ao menos, um critério geral (“larga escala” ou “afetar significativamente interesses e direitos fundamentais dos titulares”) e de um critério específico (“uso de tecnologias emergentes ou inovadoras”, “vigilância ou controle de zonas acessíveis ao público”, “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais” ou “utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos”).

Assim, considerando que na atividade instituída pela **Resolução Conjunta**, verifica-se a presença do critério geral “larga escala” e parcialmente, em primeira análise, dos critérios específicos “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais” e “utilização de dados pessoais de crianças, de adolescentes e de idosos”, é **recomendável que as cooperativas procedam com a confecção do RIPD** antes do início da atividade, como medida de boa prática em proteção de dados pessoais.

Vale destacar que o próprio RIPD auxiliará as cooperativas no atendimento aos requisitos de segurança estabelecidos pela **Resolução Conjunta**, uma vez que possibilitará uma avaliação prévia dos possíveis riscos associados ao tratamento e auxiliará na identificação das medidas, salvaguardas e mecanismos de mitigação dos riscos identificados.

3. CONCLUSÕES

A partir da análise jurídica da **Resolução Conjunta**, solicitada pelo Sistema OCB, identificou-se que caberá às cooperativas do ramo crédito:

-  Observar as funcionalidades (Art. 2º, §1º) e os requisitos mínimos de implementação (Art. 4º) aplicáveis aos sistemas eletrônicos;
-  Documentar a coleta do consentimento para tratamento e compartilhamento dos dados e informações em contratos ou documentos equivalentes, em cláusula destacada;
-  Disponibilizar a documentação relacionada aos procedimentos e critérios para identificação dos indícios de fraude, de forma detalhada e compatível com o perfil de risco da cooperativa;
-  Instituir mecanismos de acompanhamento e de controle (Art. 7º) para assegurar a efetividade das regras contidas na resolução;
-  Estabelecer contratos específicos com terceiros para fornecimento do sistema eletrônico, inclusive contemplando cláusulas de proteção de dados pessoais adequadas aos seus respectivos programas de conformidade com a LGPD;
-  Manter os dados e informações pelos prazos estabelecidos na resolução;
-  Confeccionar o respectivo Relatório de Impacto à Proteção de Dados Pessoais, considerando as características da atividade realizada; e
-  Envolver o Encarregado pelo Tratamento de Dados Pessoais (DPO) para auxiliar na implementação da atividade regrada pela resolução e para mapeá-la e incluí-la no Registro de Operações de Tratamento de Dados Pessoais (RoPA/ROT), justificando-se com a hipótese prevista no art. 7º, II da LGPD.