BANCO CENTRAL DO BRASIL

VOTO 23/2023–CMN, DE 18 DE MAIO DE 2023

Assuntos de Regulação – Propõe a edição de resolução conjunta dispondo sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Senhores Conselheiros,

A Diretoria Colegiada do Banco Central do Brasil, na 3.490ª sessão, aprovou o incluso Voto 84/2023–BCB, de 10 de maio de 2023, em que se propõe a edição de resolução conjunta dispondo sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

É o que submeto à consideração dos Senhores.

Roberto de Oliveira Campos Neto
Presidente do Banco Central do Brasil

Anexo: 1.

VOTO DO BC 84/2023-BCB/Dinor-Numerado Manualmente

Descrição: Assuntos de Regulação - Propõe a edição de resolução conjunta dispondo sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições ...

Assinado/Autenticado por: - OTAVIO RIBEIRO DAMASO:56368623187 em 11/05/2023;

BANCO CENTRAL DO BRASIL

VOTO 84/2023–BCB, DE 10 DE MAIO DE 2023

Assuntos de Regulação – Propõe a edição de resolução conjunta dispondo sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Senhor Presidente e Senhores Diretores,

Com o avanço do uso de meios de pagamento eletrônicos no País, constata-se nos últimos anos o crescimento das transações financeiras realizadas pela população por meio de canais de atendimento eletrônicos, privilegiando o uso de celulares, seguido do *internet banking*[1]. Esses meios de pagamento e os canais de atendimento eletrônicos contemplam elementos de segurança, seja por iniciativa das próprias instituições, seja por exigência regulatória. Além de seguros, os citados meios de pagamentos eletrônicos permitiram aumentar a eficiência dos sistemas financeiro e de pagamentos, a competitividade e a inclusão financeira.

2. Entretanto o crescimento dessas transações vem sendo acompanhado também pelo aumento de eventos de fraudes e de crimes, incluindo crimes cibernéticos, que, direta ou indiretamente, prejudicam as instituições do Sistema Financeiro Nacional (SFN) e os consumidores de seus produtos e serviços. Os referidos eventos afetam diferentes procedimentos aos cuidados das instituições supervisionadas por este Banco Central do Brasil (BCB), inclusive a prestação de serviços de pagamento, bem como a abertura e a manutenção de contas de depósitos e de pagamento.

3. Visando reduzir a ocorrência de tais eventos, foram editados atos normativos pelo próprio BCB:

I. Resolução BCB nº 142, de 23 de setembro de 2021, dispondo sobre procedimentos e controles para prevenção de fraudes na prestação de serviços de pagamento a serem adotados pelas instituições financeiras, demais instituições autorizadas a funcionar pelo BCB e instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB); e

II. Resoluções BCB nº 103, de 8 de junho de 2021, e nº 147, de 28 de setembro de 2021, que alteraram o Regulamento anexo à Resolução BCB nº 1, de 12 de agosto de 2020, que disciplina o funcionamento do arranjo de pagamentos Pix, para estabelecer novos mecanismos de segurança no âmbito desse arranjo.

[1] Fonte: BCB. Banco Central do Brasil. Estatísticas dos Meios de Pagamento. 2022. Disponível em: https://www.bcb.gov.br/estatisticas/spbadendos. Acesso em 15.9.2022.

4. Nesse contexto, a regulamentação do Conselho Monetário Nacional (CMN) e do BCB disciplinou os requisitos relacionados à segurança cibernética que devem ser observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar por esta Autarquia, por meio da Resolução CMN nº 4.893, de 26 de fevereiro de 2021, e Resolução BCB nº 85, de 8 de abril de 2021, dispondo sobre a política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

5. Cabe ressaltar que este BCB e as instituições reguladas vêm, também, trabalhando no intuito de buscar outras iniciativas para a mitigação da ocorrência de eventos de fraudes que impactam o SFN. Essa busca de soluções, contudo, não tem o intuito de alterar significativamente a experiência e os benefícios no uso de produtos e serviços ofertados pelas instituições supervisionadas.

6. Entre essas iniciativas, destaca-se o compartilhamento de dados e de informações sobre indícios de ocorrências ou de tentativas de fraudes entre as instituições supervisionadas, buscando a redução de assimetrias no acesso a dados e a informações usadas para subsidiar os procedimentos e os controles das instituições para prevenção de fraudes.

7. Uma das causas do aumento das fraudes no SFN está relacionada à assimetria de informação entre as instituições supervisionadas. Nesse sentido, verifica-se que o compartilhamento das informações referentes aos indícios de ocorrências e de tentativas de fraudes entre as diversas instituições teria o potencial de subsidiar a prevenção de novas fraudes relacionadas com a ocorrência compartilhada, bem como interromper as ações que estejam em andamento.

8. Sobre tal compartilhamento de dados e informações, existem experiências internacionais prévias em jurisdições de diferentes continentes, como América do Norte, Europa, Ásia e Oceania. Tais experiências exemplificam a finalidade de tal compartilhamento para: (i) minimizar a ocorrência de ameaças cibernéticas, (ii) prevenir fraudes em transações de pagamento e (iii) prevenir fraudes financeiras de maneira geral.

9. Assim, considerando a relevância do tema e o contínuo processo de aprimoramento da regulamentação, proponho a edição de ato normativo dispondo sobre os requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo BCB. Tais dados e informações devem ser compartilhados com as demais instituições, abrangendo indícios de ocorrências e de tentativas de fraudes identificadas em suas atividades.

10. A finalidade proposta desse compartilhamento é subsidiar procedimentos e controles para prevenção de fraudes, aos cuidados das referidas instituições. Ressalta-se, contudo, a finalidade de compartilhamento como um subsídio, ou seja, a proposta regulatória em pauta preserva as responsabilidades das instituições pelos seus procedimentos e controles para prevenção de fraudes previstos nas normas em vigor. Como exemplo, pode-se citar que o compartilhamento de dados e informações sobre indícios de fraudes poderá subsidiar os procedimentos para abertura e manutenção de contas de depósitos e de contas de pagamento, sem prejudicar a livre tomada de decisões na oferta e prestação de serviços por parte de cada instituição.

11. Quanto à abrangência, propõe-se obrigar o compartilhamento para as instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo BCB. No entanto, considerando as peculiaridades do segmento e o tratamento regulatório específico, a proposta não abrange as administradoras de consórcio.

12. A respeito da forma de compartilhamento, propõe-se que seja implementado por meio de sistema eletrônico com as seguintes funcionalidades mínimas: registro, alteração e exclusão e consulta de dados e informações sobre indícios de ocorrências ou de tentativas de fraude. Propõe-se requisitos mínimos para a implementação desse sistema, como acesso pleno das instituições e padrão único de comunicação que permita a execução de suas funcionalidades. Propõe-se, ainda, sujeitar tal sistema eletrônico a procedimentos e controles para assegurar cumprimento da legislação e regulamentação, inclusive, ao titular dos dados, o livre acesso às informações que lhe digam respeito, bem como a exclusão ou a correção tempestiva de dados e informações registrados, em caso de eventuais erros, inconsistências ou outras demandas, em observância da legislação e da regulamentação vigentes. Propõe-se, também, assegurar a interoperabilidade com outros sistemas implementados, em atendimento a regulamentação, quando existentes.

13. Cabe ressaltar que o referido sistema eletrônico a ser implementado por parte das instituições reguladas para permitir o compartilhamento dos dados e informações sobre indícios de fraudes não exclui a possibilidade de coexistirem outros sistemas ou bases de dados com a finalidade de prevenção a fraudes no âmbito do SFN e do SPB. A respeito, pode-se citar como exemplo o Diretório de Identificadores de Contas Transacionais (DICT), implementado com o propósito específico das transações de pagamento realizadas no âmbito do Pix e ampliado para viabilizar que a consulta a suas informações seja feita com o propósito de alimentar os mecanismos de análise de fraude dos participantes, inclusive em processos que não estejam diretamente relacionados ao Pix. Além disso, nesse caso, por ser um sistema operado pelo Banco Central do Brasil, a proposta normativa em questão não é aplicável ao DICT.

14. Quanto ao conteúdo mínimo a ser compartilhado, cada registro citado no parágrafo 12 deve contemplar, além da descrição dos indícios da ocorrência ou da tentativa de fraude, a identificação (i) de quem, segundo os indícios disponíveis, teria executado ou tentado executar a fraude, quando aplicável; (ii) da instituição responsável pelo registro dos dados e das informações; e (iii) dos dados da conta destinatária ou de seu titular, em caso de transferência ou pagamento de recursos. De notar que esse registro não se aplica a dados sigilosos, nos termos de legislação especial, relacionados a indícios da prática dos crimes de “lavagem” ou ocultação

de bens, direitos e valores, de dinheiro, de que trata a Lei nº 9.613, de 3 de março de 1998[2], e de financiamento do terrorismo, de que trata a Lei nº 13.260, de 16 de março de 2016[3].

15. Adicionalmente, visando proporcionar a devida transparência, a proposta estabelece que as instituições devem obter do cliente com quem possuam relacionamento o consentimento prévio e geral possibilitando o registro no referido sistema eletrônico do conteúdo mínimo referente aos dados e às informações citados no parágrafo 14 deste Voto que digam respeito ao referido cliente. O citado consentimento deve ter como finalidade o tratamento e o compartilhamento de dados e informações sobre indícios de fraudes no âmbito da presente proposta de resolução conjunta e constar de contrato firmado entre o cliente e a instituição, mediante cláusula em destaque no corpo do instrumento contratual ou por outro instrumento jurídico válido, ficando essa documentação à disposição do BCB.

16. Com relação à identificação da pessoa que executou ou tentou executar a fraude, buscando estipular que as instituições não registrem, de forma equivocada, uma eventual vítima da fraude – sem prejuízo da definição de responsabilidade no evento –, a proposta determina que as instituições devem estabelecer e documentar os procedimentos e critérios para identificação da referida pessoa, de forma detalhada e compatível com o perfil de risco da instituição, com a legislação e com a regulamentação em vigor, os quais incluirão, no mínimo, a conferência com dados constantes de sistemas, cadastros e demais bases disponíveis para consulta. Essa documentação deve, ainda, permanecer à disposição deste Banco Central.

17. Quanto aos outros aspectos regulatórios, a proposta de norma estabelece os seguintes:

I. a determinação de responsabilidades às instituições pela confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos dados e informações por elas registrados, pela implementação das funcionalidades e requisitos do sistema eletrônico e pelo cumprimento da legislação e regulamentação em vigor;

II. o estabelecimento de princípios a serem observados pelas instituições para compartilhamento, como segurança e privacidade dos dados e informações; qualidade dos dados e informações; acesso pleno e não discriminatório às funcionalidades do sistema; eficiência no cumprimento dos requisitos do sistema; reciprocidade com outras instituições; e interoperabilidade com outros sistemas, quando existentes;

[2] A Lei nº 9.613, de 3 de março de 1998, dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nessa Lei. O art. 11 dessa Lei estabelece que os entes regulados deverão comunicar ao Conselho de Controle de Atividades Financeiras (Coaf), abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, as operações que apresentem sérios indícios de lavagem de dinheiro, bem como a proposta ou a realização de operações que ultrapassarem determinados limites estabelecidos pela autoridade competente.

[3] A Lei nº 13.260, de 16 de março de 2016, regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis ns. 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013.

III. a faculdade dada às instituições de contratar empresa para a prestação do serviço de compartilhamento efetuado por meio do sistema eletrônico citado nesta proposta, mantendo a responsabilidade pelo serviço prestado nas referidas instituições, inclusive referente ao tratamento de dados compartilhados, realizado em nome da instituição contratante, e observado que esse serviço seja considerado como relevante, nos termos da regulamentação em vigor;

IV. a instituição de mecanismos de acompanhamento e de controle para assegurar a efetividade do cumprimento do disposto na proposta regulatória, inclusive guarda de documentos sobre o sistema eletrônico, com prazos para guarda de dados e informações compartilhados e de dados e registros relativos à aplicação dos citados mecanismos;

V. a possibilidade de o BCB, observados os princípios de que trata o item II, adotar medidas adicionais para cumprimento da citada proposta regulatória, contemplando: as funcionalidades do sistema eletrônico, observado o conteúdo mínimo mencionado no parágrafo 14 deste Voto; o escopo dos dados e das informações; os parâmetros sobre acordos de níveis de serviço; os requisitos técnicos de segurança; a adequação dos mecanismos; outros requisitos técnicos, procedimentos operacionais e outros aspectos para o cumprimento da referida proposta;

VI. as diretrizes gerais que deverão ser observadas pelo BCB na eventualidade de vir a regulamentar o escopo dos dados e das informações a serem registrados, em complemento ao conteúdo mínimo do registro dos dados e das informações de que trata o parágrafo 14 deste Voto, enfatizando que os dados e informações a serem registrados deverão ser aqueles necessários e adequados para subsidiar os procedimentos e controles das instituições para a prevenção de fraudes; e

VII. a determinação de que o acesso aos dados e às informações compartilhados nos termos da proposta de resolução conjunta seja restrito às instituições, ao BCB e às demais autoridades competentes, nos termos da legislação em vigor.

18. Considerando o escopo da proposta para instituições financeiras, instituições de pagamento e demais instituições autorizadas, propõe-se que seja normatizada por meio de resolução conjunta do CMN e do BCB, com entrada em vigor em 1º de novembro de 2023. Entende-se que o prazo de vacância resultante dessa previsão será suficiente para o desenvolvimento e a adequação de procedimentos e de sistemas e para eventual celebração de contratos, considerada a faculdade descrita no item III do parágrafo 17 deste Voto.

19. Cumpre destacar, ainda, por força do Decreto nº 10.411, de 30 de junho de 2020, que a edição de atos normativos por órgãos da administração pública federal deve ser precedida de análise de impacto regulatório (AIR). A esse respeito, apresenta-se relatório de AIR anexo a este Voto. Em observância ao art. 15 do Decreto nº 10.411, de 2020, atesta-se que o relatório de AIR observa o art. 5º da Lei nº 13.874, de 20 de setembro de 2019 (Declaração de Direitos de Liberdade Econômica), e preenche os requisitos do Decreto citado, o que revela sua adequação formal. Considera-se que o referido relatório de AIR atingiu seus objetivos, fornecendo subsídios para a tomada de decisão quanto à medida proposta em face das possíveis alternativas.

20. Assim, com base no disposto nos arts. 11, incisos V, alínea "c", e VI, alínea “o”, item 1, e 13, inciso XIII, combinado com o art. 20, inciso IV, alínea "a", todos do Regimento Interno deste Banco Central, trago o assunto à consideração deste Colegiado, na forma da anexa minuta de resolução conjunta, para, após aprovação por esta Diretoria Colegiada, ser submetido ao Conselho Monetário Nacional.

Otávio Ribeiro Damaso
Diretor de Regulação

Anexos: 2.

BANCO CENTRAL DO BRASIL

RESOLUÇÃO CONJUNTA Nº , DE DE DE 2023

Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

O Banco Central do Brasil, na forma do art. 9º da Lei nº 4.595, de 31 de dezembro de 1964, torna público que sua Diretoria Colegiada, em sessão realizada em de de 2023, com base nos arts. 9º-A da Lei nº 4.728, de 14 de julho de 1965, 9º, **caput** e inciso II, da Lei nº 12.865, de 9 de outubro de 2013, e o Conselho Monetário Nacional, em sessão realizada em de de 2023, com base nos arts. 4º, inciso VIII, da Lei nº 4.595, de 1964, 20, § 1º, da Lei nº 4.864, de 29 de novembro de 1965, 1º do Decreto-Lei nº 70, de 21 de novembro de 1966, 7º e 23, alínea "a", da Lei nº 6.099, de 12 de setembro de 1974, 1º, § 1º, inciso XIII, e § 3º, inciso I, da Lei Complementar nº 105, de 10 de janeiro de 2001, 1º, inciso II, da Lei nº 10.194, de 14 de fevereiro de 2001, e 1º, § 1º, da Lei Complementar nº 130, de 17 de abril de 2009,

R E S O L V E R A M :

Art. 1º Esta Resolução Conjunta dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

§ 1º O disposto nesta Resolução Conjunta não se aplica às administradoras de consórcio.

§ 2º Para os fins desta Resolução Conjunta, as instituições de que trata **o caput** são consideradas instituições financeiras para os efeitos da Lei Complementar nº 105, de 10 de janeiro de 2001.

Art. 2º As instituições devem compartilhar dados e informações com as demais instituições referidas no art. 1º com a finalidade de subsidiar seus procedimentos e controles para prevenção de fraudes.

§ 1º O compartilhamento de que trata o **caput** deve ser realizado por meio de sistema eletrônico que contemple, no mínimo, as seguintes funcionalidades:

I - o registro de dados e de informações sobre indícios de ocorrências ou de tentativas de fraudes identificadas pelas instituições em suas atividades;

II - a alteração e a exclusão dos dados e das informações registrados nos termos do § 1º, inciso I, deste artigo, conforme o caso; e

III - a consulta dos dados e das informações registrados de que trata o § 1º, inciso I, deste artigo.

§ 2º O registro dos dados e das informações de que trata o § 1º, inciso I, deste artigo devem contemplar, no mínimo:

I - a identificação de quem, segundo os indícios disponíveis, teria executado ou tentado executar a fraude, quando aplicável;

II - a descrição dos indícios da ocorrência ou da tentativa de fraude;

III - a identificação da instituição responsável pelo registro dos dados e das informações; e

IV - a identificação dos dados da conta destinatária e de seu titular, em caso de transferência ou pagamento de recursos.

§ 3º As instituições de que trata o **caput** devem obter do cliente com quem possuam relacionamento o consentimento prévio e geral, possibilitando o registro dos dados e das informações de que trata o § 2º que digam respeito ao referido cliente.

§ 4º O consentimento de que trata o § 3º deve:

I - ter como finalidade o tratamento e o compartilhamento de dados e informações sobre indícios de fraudes no âmbito desta Resolução Conjunta; e

II - constar de contrato firmado entre o cliente e a instituição, mediante cláusula em destaque no corpo do instrumento contratual ou por outro instrumento jurídico válido.

§ 5º A documentação de que trata o inciso II do § 4º deve ficar à disposição do Banco Central do Brasil.

§ 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.

§ 7º O registro de que trata o § 1º, inciso I, deste artigo não se aplica aos dados e às informações sigilosos, nos termos de legislação especial, relacionados a indícios da prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores e de financiamento do terrorismo.

§ 8º As instituições devem estabelecer e documentar os procedimentos e critérios para identificação de que trata o inciso I do § 2º deste artigo, de forma detalhada e compatível com o perfil de risco da instituição, com a legislação e com a regulamentação em vigor, os quais incluirão, no mínimo, a conferência com dados constantes de sistemas, cadastros e demais bases de dados disponíveis para consulta.

§ 9º Os procedimentos e controles de que trata o **caput** incluem, por exemplo, aqueles previstos para fins de prestação de serviços de pagamento, bem como para a abertura e a manutenção de contas de depósitos e de pagamento, nos termos da regulamentação em vigor.

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:

I - segurança e privacidade de dados e de informações compartilhados no âmbito desta Resolução Conjunta;

II - qualidade dos dados e informações compartilhados;

III - acesso pleno e não discriminatório das instituições às funcionalidades do sistema eletrônico de que trata o art. 2º, § 1º;

IV - eficiência no cumprimento dos requisitos do sistema eletrônico de que trata esta Resolução Conjunta, inclusive no padrão único e comum de comunicação de que trata o art. 4º, inciso II;

V - reciprocidade com outras instituições, no tocante aos dados e às informações compartilhados no âmbito desta Resolução Conjunta; e

VI - interoperabilidade com outros sistemas eletrônicos implementados em atendimento ao disposto nesta Resolução Conjunta, quando existentes, nos termos do art. 4º, inciso IV.

Art. 4º As instituições devem observar, para fins de implementação do sistema eletrônico de que trata o art. 2º, § 1º**,** os seguintes requisitos:

I - permitir o acesso pleno das instituições de que trata o art. 1º às funcionalidades do referido sistema com a respectiva identificação de quem realizou o acesso;

II - adotar um padrão único e comum de comunicação que permita a execução das suas funcionalidades;

III - contemplar procedimentos e controles para assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações nele registrados;

c) a sua aderência a certificações de segurança;

d) a elaboração de relatórios por empresa de auditoria especializada independente relativos aos procedimentos e aos controles utilizados na execução das suas funcionalidades;

e) o provimento de informações e de recursos de gestão adequados ao monitoramento de suas funcionalidades;

f) a identificação e a segregação dos dados e das informações registrados por meio de controles físicos ou lógicos;

g) a qualidade dos controles de acesso voltados à proteção dos dados e das informações registrados por meio do referido sistema; e

h) ao titular dos dados, o livre acesso às informações que lhe digam respeito, bem como a exclusão ou a correção tempestiva dos dados e das informações registrados, em caso de eventuais erros, inconsistências ou outras demandas, em observância da legislação e da regulamentação vigentes; e

IV - assegurar a sua interoperabilidade com outros sistemas eletrônicos implementados em atendimento ao disposto nesta Resolução Conjunta, quando existentes.

Parágrafo único. O atendimento aos requisitos de que trata este artigo deve ser documentado.

Art. 5º É facultada a contratação de empresa para a prestação do serviço de compartilhamento de dados e informações de que trata o art. 2º, com observância do disposto nesta Resolução Conjunta, na legislação e na regulamentação em vigor, especialmente nas regulamentações dispondo sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

§ 1º No caso da contratação de que trata o **caput**, permanecerão com a instituição contratante as responsabilidades para os fins desta Resolução Conjunta, inclusive referentes ao tratamento dos dados compartilhados, realizado em nome da instituição contratante.

§ 2º O serviço prestado de que trata o **caput** é considerado relevante para fins da aplicação da regulamentação vigente sobre a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Art. 6º As instituições de que trata o art. 1º são responsáveis:

I - pela confiabilidade, integridade, disponibilidade, segurança e pelo sigilo em relação aos dados e informações por elas registrados nos termos do art. 2º, § 1º, inciso I;

II - pela implementação das funcionalidades do sistema de que trata o art. 2º, § 1º;

III - pela observância aos requisitos citados no art. 4º;

IV - pela utilização dos dados e das informações por elas obtidos em consulta ao sistema eletrônico de que trata o art. 2º, § 1º, e pela preservação do sigilo de tais dados; e

V - pelo cumprimento da legislação e da regulamentação em vigor.

Art. 7º As instituições de que trata o art. 1º devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a efetividade do cumprimento do disposto nesta Resolução Conjunta, incluindo:

I - a definição de processos, testes e trilhas de auditoria;

II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

Parágrafo único. Os mecanismos de que trata o **caput** devem ser submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos da instituição.

Art. 8º As instituições devem deixar à disposição do Banco Central do Brasil:

I - a documentação sobre o sistema eletrônico de que trata o art. 2º, § 1º, inclusive a respeito dos requisitos de que trata o art. 4º, parágrafo único;

II - por dez anos, os dados e as informações compartilhados, nos termos do art. 2º, § 6º, inciso II, e a documentação com os critérios e procedimentos a que se refere o art. 2º, § 8º; e

III - por cinco anos, os dados, os registros e as informações relativas à aplicação dos mecanismos de acompanhamento e de controle de que trata o art. 7º, contado o prazo referido neste inciso a partir de cada aplicação dos citados mecanismos.

Art. 9º O Banco Central do Brasil poderá adotar, no âmbito de suas atribuições legais, as medidas necessárias à execução do disposto nesta Resolução Conjunta, o que inclui estabelecer, entre outros aspectos:

I - as funcionalidades do sistema eletrônico, observado o conteúdo mínimo do art. 2º, § 1º;

II - o escopo dos dados e das informações a serem registrados de que trata ao art. 2º, § 1º, inciso I, observado o conteúdo mínimo disposto no art. 2º, § 2º;

III - o detalhamento dos parâmetros sobre acordos de níveis de serviço na execução das funcionalidades do sistema de que trata o art. 2º, § 1º;

IV - os requisitos técnicos de segurança para funcionamento do sistema de que trata o art. 2º, § 1º, observado o disposto no art. 4º, conforme o caso;

V - a adequação dos mecanismos de que trata o art. 7º; e

VI - demais requisitos técnicos e procedimentos operacionais para o compartilhamento de dados e informações de que trata o art. 2º.

§ 1º Na regulamentação das medidas de que trata o **caput**, o Banco Central do Brasil deverá observar os princípios referidos no art. 3º.

§ 2º Na regulamentação de que trata o inciso II do **caput**, o Banco Central do Brasil deverá observar, também, as seguintes diretrizes gerais:

I - os dados e as informações sobre indícios de ocorrências ou de tentativas de fraudes a serem registrados deverão ser aqueles necessários e adequados para subsidiar os procedimentos e controles das instituições referidas no art. 1º para prevenção de fraudes; e

II - o conteúdo do registro deverá acompanhar as inovações tecnológicas e procedimentais, a fim de manter sua aptidão para o objetivo de prevenção a fraudes em cenários futuros.

Art. 10. O Banco Central do Brasil poderá vetar ou impor restrições à contratação de que trata o art. 5º, quando constatar, a qualquer tempo, a inobservância do disposto nesta Resolução Conjunta, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação de processos.

Art. 11. O acesso aos dados e às informações compartilhados nos termos desta Resolução Conjunta será restrito às instituições referidas no art. 1º, ao Banco Central do Brasil e às demais autoridades competentes, nos termos da legislação em vigor.

Art. 12. O disposto nesta Resolução Conjunta não exime a instituição da responsabilidade de:

I - efetuar os procedimentos e os controles para prevenção de fraudes previstos na regulamentação em vigor; e

II - comunicar informações a respeito de fraudes às autoridades competentes, nos termos da legislação em vigor.

Art. 13. Esta Resolução Conjunta entra em vigor em 1º de novembro de 2023.

Roberto de Oliveira Campos Neto
Presidente do Banco Central do Brasil

Análise de Impacto Regulatório

Requisitos para compartilhamento de dados e informações sobre indícios de fraudes

BANCO CENTRAL DO BRASIL

SUMÁRIO

SUMÁRIO EXECUTIVO

Este documento, no formato de relatório, contempla a análise de impacto regulatório (AIR) pertinente aos requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. O relatório contempla cinco seções, descritas na sequência: a identificação do problema regulatório (Seção 1), os objetivos do tratamento regulatório (Seção 2), as alternativas de tratamento regulatório (Seção 3), a proposta regulatória (Seção 4) e as estratégias pós-aprovação da norma (Seção 5). Os responsáveis pela elaboração constam do final do documento.

1. IDENTIFICAÇÃO DO PROBLEMA REGULATÓRIO

Esta seção identifica e descreve o problema regulatório que se pretende solucionar. A este respeito, subdivide-se em quatro subseções. Discorre-se, inicialmente, sobre as evidências do problema regulatório refletido no aumento das fraudes no Sistema Financeiro Nacional (SFN), inclusive sobre a sua extensão (Seção 1.1). Em seguida, apresenta-se a descrição do problema regulatório abrangendo suas causas, suas consequências (Seção 1.2), discorre-se sobre a experiência internacional relativa ao problema descrito (Seção 1.3) e finaliza-se a seção com a descrição dos agentes envolvidos no problema regulatório (Seção 1.4)

1.1 Evidências do Problema Regulatório e de sua Extensão

Num contexto abrangente de evidências do problema relacionado com fraudes observa-se, em princípio, que devido ao avanço do uso de meios digitais houve crescimento das transações financeiras realizadas pelos canais eletrônicos.

A este respeito, inicialmente, o Gráfico 1 expressa a evolução da quantidade de transações no período do 1º trimestre de 2019 ao 4º trimestre de 2021, exibindo o comportamento, em especial, da quantidade de transações por meio do celular, seguida do internet banking.

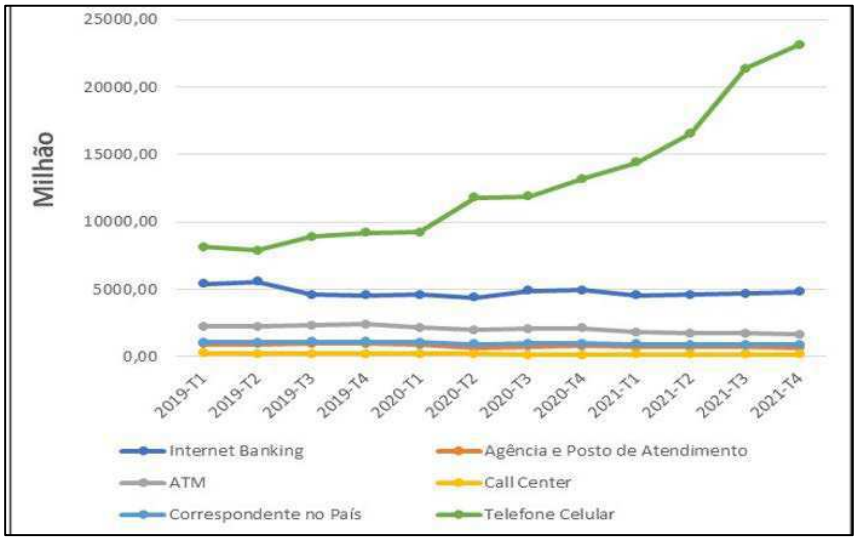

Gráfico 1 - transações por canal de acesso.

Fonte: BCB (2022)[1].

O crescimento do uso dos meios digitais para realização de transações financeiras pela sociedade, evidenciado no **Gráfico 1**, vem sendo acompanhado pela ocorrência de fraudes, golpes e crimes, incluindo crimes cibernéticos, no ambiente digital.

A este respeito, particularizando o problema para a competência de atuação desta Autarquia, estudo realizado pela Federação Brasileira de Bancos – FEBRABAN[2], com base em informações coletadas de 20 instituições que fazem parte do Comitê de Prevenção a Fraudes da referida associação, realizado em fevereiro de 2022, evidenciou crescimento de 165% com relação ao primeiro semestre de 2021 (em comparação com o semestre anterior) nos golpes de engenharia social, que consistem na manipulação psicológica do usuário visando a extorsão de valores, seja por meio de acesso a informações confidenciais dele, tais como senhas e números de cartões, seja pelo convencimento do usuário para que ele próprio realize a operação fraudulenta.

No mesmo período citado no parágrafo anterior, há destaque, também, para o golpe do falso motoboy, que registrou aumento de 271%, para o golpe da falsa central telefônica e do falso funcionário, que aumentou 62%; e para os ataques de *phishing* (golpe eletrônico que visa obter dados

[1] Fonte: BCB. Banco Central do Brasil. Estatísticas dos Meios de Pagamento. 2022. Disponível em: https://www.bcb.gov.br/estatisticas/spbadendos. Acesso em 15.9.2022.
[2] Fonte: Febraban. Federação Brasileira de Bancos. Crescem golpes envolvendo manipulação de vítimas para roubo de informações pessoais. Disponível em: https://febraban.org.br/noticia/3704/pt-br/. Acesso em 7.4.2022.

pessoais do usuário por meio mensagens e e-mails falsos que induzem o usuário a clicar em links suspeitos ou ainda por meio páginas falsas na internet), que cresceu 26%[3].

Desde os meados de 2021, este BCB vem trabalhado no intuito de buscar soluções para a mitigação da ocorrência de fraude/golpes cibernéticos que impactam o Sistema Financeiro Nacional (SFN) por meio do uso de tecnologia e compartilhamento de dados, com base na cooperação dos interessados, levando-se em consideração a Lei Complementar nº 105, de 10 de janeiro de 2001[4] e a Lei nº 13.709, de 14 de agosto de 2018[5].

Observa-se que ações foram implementadas pelas instituições financeiras, verificadas por este BCB em reuniões realizadas com as entidades supervisionadas, das quais destacam-se: investimentos em segurança da informação; aperfeiçoamentos no monitoramento de contas; exigência de autenticação compatível com o nível de risco identificado; implementação de *liveness* - prova de vida - para abertura de contas e para transações fora do padrão; trabalho de conscientização dos clientes; redução de limites para transação por horário e dia da semana; adoção de quantidade, valores e horários e de segurança com base no dispositivo utilizado; utilização de mecanismo de temporização/retardo nas transações suspeitas; regras para contas suspeitas (ex.: limite diário para recebimento de recursos); reforço nas áreas de combate a fraudes e repressão ao crime; e o compartilhamento das informações com delegacias especializadas. Ainda assim, a questão das fraudes no SFN continua sendo objeto de preocupação e tem sido objeto de matérias veiculadas diariamente na mídia.

Os principais problemas trazidos pelas entidades supervisionadas em recentes reuniões junto a este BCB relacionadas às fraudes/ golpes estão destacados a seguir, com explicação resumida de seu mecanismo:

a) aluguel de conta ou empréstimo de conta, por meio do aliciamento de clientes;
b) abertura de conta com dados de terceiros – falsidade ideológica;
c) roubo de celular e acesso ao *app* dos bancos e contas de *e-mail*;
d) *SIM SWAP* - repasse de um número de telefone para um novo chip, que está em posse do criminoso, por vezes com participação de alguém da operadora de telefonia, permitindo o "*reset*" de senha e recebimento de códigos de liberação do dispositivo via *token*;
e) novos entrantes, que em alguns casos não possuem todas a informações e ferramentas de defesa;

[3] Fonte: vide Nota 2.
[4] Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
[5] Lei Geral de Proteção de Dados Pessoais (LGPD).

f) apps que animam fotos, podendo "enganar" o *liveness*;
g) vazamento de dados em geral;
h) fraudes com utilização do Pix combinado com conta ponte: em função da velocidade, há dificuldade de retenção e recuperação de valores;
i) celulares com sistema operacional não atualizado.

Ato contínuo, esta Autarquia expediu os seguintes normativos com o objetivo de minimizar as ocorrências de fraude/ golpes praticados, destacando-se: Resolução BCB nº 142, de 23 de setembro de 2021[6], Resolução BCB nº 147, de 28 de setembro de 2021[7], Resolução CMN nº 4.893, de 26 de fevereiro de 2021 e Resolução BCB nº 85, de 8 de abril de 2021[8]; Resolução CMN nº 4.949, de 30 de setembro de 2021[9]; e a Resolução CMN nº 4.753, de 26 de setembro de 2019, art. 4º, § 2º[10].

Em complemento ao trabalho deste BCB foram encaminhadas a 34 entidades supervisionadas (abrangendo entidades do segmento S1-S2 e entidades dos demais segmentos), no final de fevereiro de 2022, requisições de informações gerenciais sobre operações de transferência, pagamento ou compra, no período entre janeiro/2019 a dezembro/2021, segregadas da seguinte maneira[11]:

a) Fraude/golpe que envolvem os seguintes grupos : **Grupo 1** (golpes)- que envolvem os seguintes tipos de golpes: *phishing*, falsa central de atendimento, falso motoboy, falso leilão, *WhasApp* , extravio de cartão, delivery (maquina adulterada), troca de cartão, falso boleto, crime contra pessoa (sequestro, etc); **Grupo 2** (fraudes) - utilização do dispositivo do cliente (furto, roubo); fraude com utilização de dispositivo novo (não pertencente ao cliente), fraude com invasão do software / app da instituição; e **Grupo 3** (outros) - Abertura de contas com falsidade ideológica; Fraude com a utilização de conta laranja; Fraude na contratação de crédito. Assim, apresenta-se o **Gráfico 2**, com o total de ocorrências;

[6] Dispõe sobre procedimentos e controles para prevenção de fraudes na prestação de serviços de pagamento a serem adotados pelas instituições financeiras, demais instituições autorizadas a funcionar pelo BCB e instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).
[7] Alterou o regulamento do Arranjo Pix e trouxe procedimentos adicionais para prevenção de fraudes no âmbito do referido arranjo de pagamento.
[8] As duas resoluções dispõem sobre a política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, sendo que a Res. BCB nº 85, de 2021, deve ser observada pelas instituições de pagamento e a Res. CMN nº 4.893, de 2021, deve ser observada pelas demais instituições autorizadas pelo BCB.
[9] Dispõe sobre princípios e procedimentos a serem adotados no relacionamento com clientes e usuários de produtos e de serviços.
[10] A Resolução CMN nº 4.753, de 2019, dispõe sobre a abertura, a manutenção e o encerramento de conta de depósitos. O art. 4º, §2º, dessa Resolução estabelece que as instituições devem fornecer ao titular da conta, por meio físico ou eletrônico, prospecto de informações essenciais, explicitando, no mínimo, de forma sintética, informações relativas às regras básicas do funcionamento da conta, os riscos existentes e as medidas de segurança para fins de movimentação da conta, inclusive em caso de perda, furto ou roubo de credenciais do titular.
[11] Fonte: vide Nota 2.

b) Fraude/ golpe que envolvem as seguintes operações[12]: Transferências entre contas na própria instituição; Transferência Eletrônica Disponível (TED); Transação de pagamento instantâneo (Pix); Transferências por meio de Documento de Crédito (DOC); Boletos de pagamento e convênios; Cartão pré-pago; Cartão de débito; Cartão de crédito; Saque em espécie; e

c) Volume de ações judiciais contrárias relativas a fraudes / golpes.

Neste trabalho citado no parágrafo anterior foram considerados como golpes as situações em que o criminoso conta com a colaboração/ participação do próprio cliente, que está sendo enganado, para realizar a transação financeira; e, foram consideradas como fraudes as situações em que o criminoso não necessita da participação direta do cliente para realizar a transação financeira. Os dados recebidos foram analisados e as principais conclusões estão citadas a seguir.

Verifica-se no **Gráfico 2**, que o volume de ocorrências de fraudes/golpes aumentou significativamente no período de tempo analisado, apresentando um crescimento de cerca de 230% de janeiro/2019 a dezembro/2021.

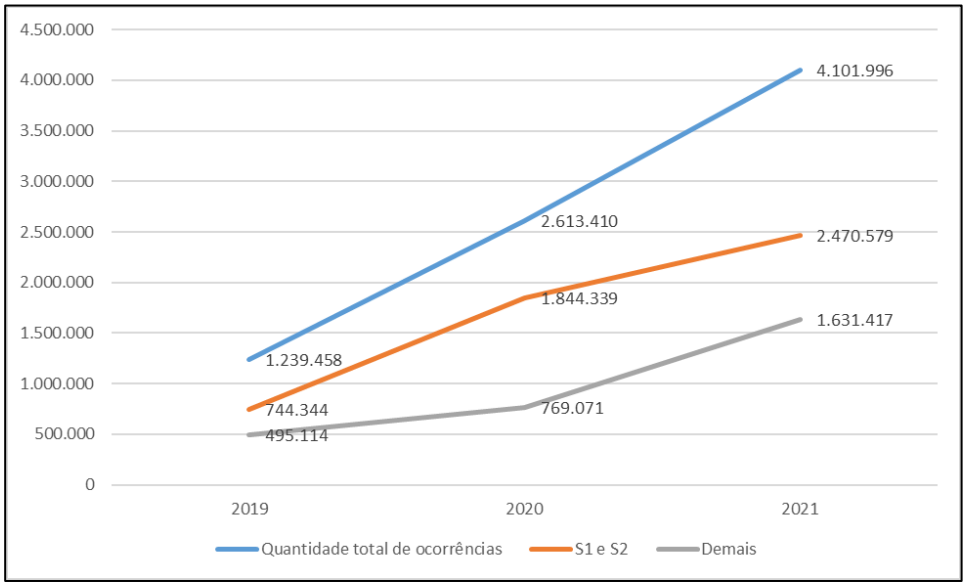

Gráfico 2 – Quantidade de ocorrências (Grupos 01, 02 e 03 – Fraudes, Golpes, Outros)
Fonte: elaborado a partir de informações recebidas das instituições.

Quanto ao **Gráfico 3**, descrito na sequência, há destaque para os golpes da central de atendimento falsa e de *phishing*.

[12] Foram considerados os instrumentos utilizados pelos criminosos citados nas reuniões realizadas durante os trabalhos para recebimento dos dados.

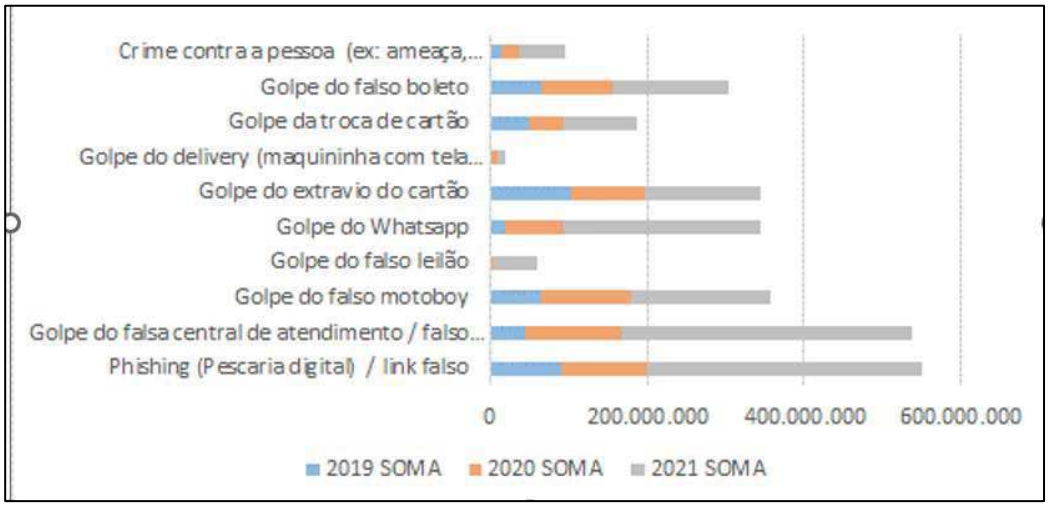

Gráfico 3 – Valores envolvidos – 2019 a 2021 – Golpes
Fonte: elaborado a partir de informações recebidas das instituições.

O **Gráfico 4** apresenta destaque para invasão do software / app da entidade, fato que evidencia atenção para a necessidade de se observar o processo de desenvolvimento de software seguro (*security by design*)[13]. Ressalte-se, entretanto, que essa fragilidade foi evidenciada em cerca de 90% por uma única entidade supervisionada.

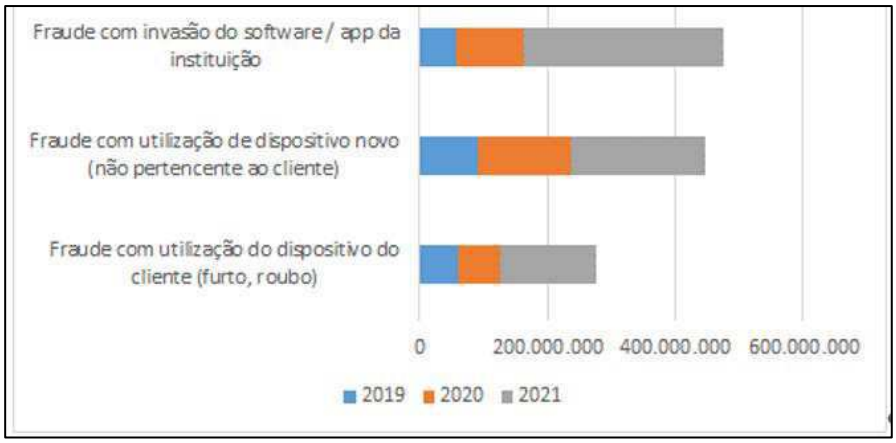

Gráfico 4 – Valores Envolvidos – 2019 a 2021 – Fraudes
Fonte: elaborado a partir de informações recebidas das instituições.

O **Gráfico 5** refere-se às fraudes do 'Grupo 3'[14] onde há destaque significativo para os casos de fraudes com utilização de contas laranja, que somam cerca de R$ 1,8 bilhão nos três anos analisados.

[13] A este respeito, a Resolução nº. 4.893, de 2021, art. 3º inciso II, combinado com §3º do mesmo artigo, determina que os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição.
[14] Conforme previamente citado neste relatório, o Grupo 3 (outros) contempla 'Abertura de contas com falsidade ideológica'; 'Fraude com a utilização de conta laranja'; 'Fraude na contratação de crédito'.

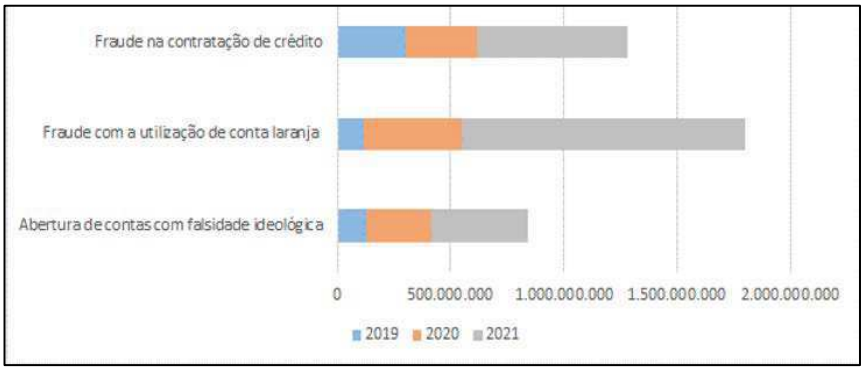

Gráfico 5 - Valores envolvidos – 2019 a 2021 – Grupo 3 – Outros
Fonte: elaborado a partir de informações recebidas das instituições.

O **Gráfico 6** apresenta o valor recuperado pelas entidades por tipo (golpe, fraudes e outros). Verifica-se um total recuperado de R$ 1,5 bilhão no período analisado (3 anos), que representa cerca de 19,5% do valor total envolvido. Nos casos de golpes, as instituições têm feito campanhas de conscientização por meios dos vários canais de atendimento existentes e, também, por meio da mídia e redes sociais.

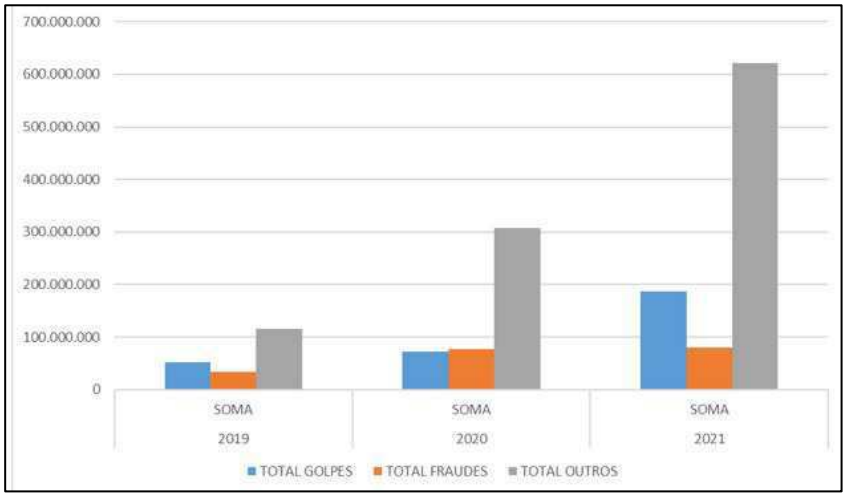

Gráfico 6 - Valores recuperados por tipo – 2019 a 2021
Fonte: elaborado a partir de informações recebidas das instituições

Uma descrição do prejuízo sofrido pelas entidades supervisionadas está apresentada no **Gráfico 7**. Conforme esperado, com base nos dados já apresentados, o prejuízo tem sido crescente no período analisado, tendo evoluído de R$630 milhões, em 2019, para R$983 milhões, em 2020, alcançando R$1,9 bilhão, em 2021.

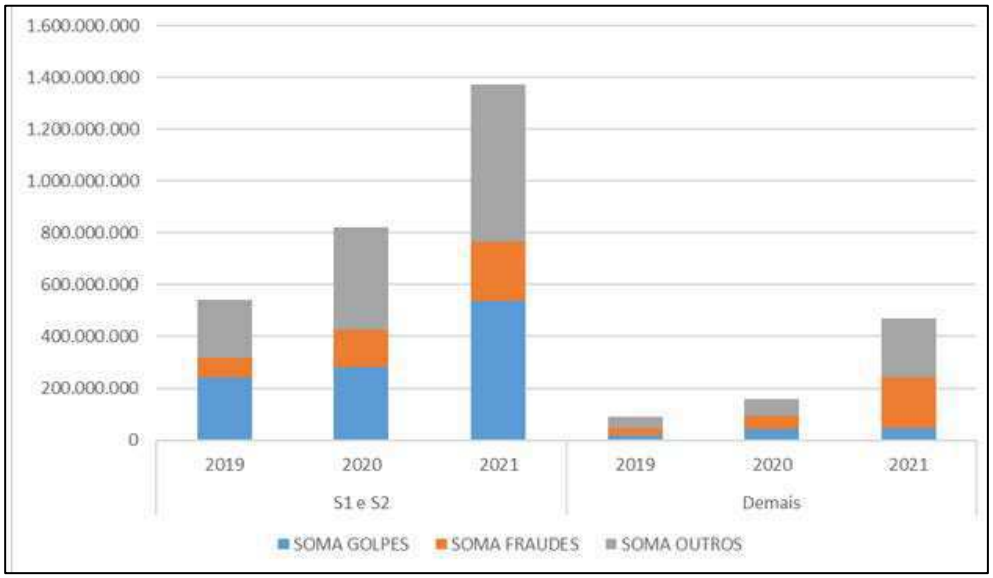

Gráfico 7 – Prejuízos por segmento -2019 a 2021
Fonte: elaborado a partir de informações recebidas das instituições

O **Gráfico 8** mostra as ocorrências com base nos sistemas de transferência, exceto cartão de crédito, utilizados na prática delituosa, havendo preferência pelo Pix, a partir do momento em que é disponibilizado à população em geral, em 16 de novembro de 2020 e, em contrapartida, queda na preferência por boletos de pagamento/convênios, desaceleração no crescimento das ocorrências relacionadas a cartão de débito e também manutenção do ritmo de crescimento nas transferências pela TED.

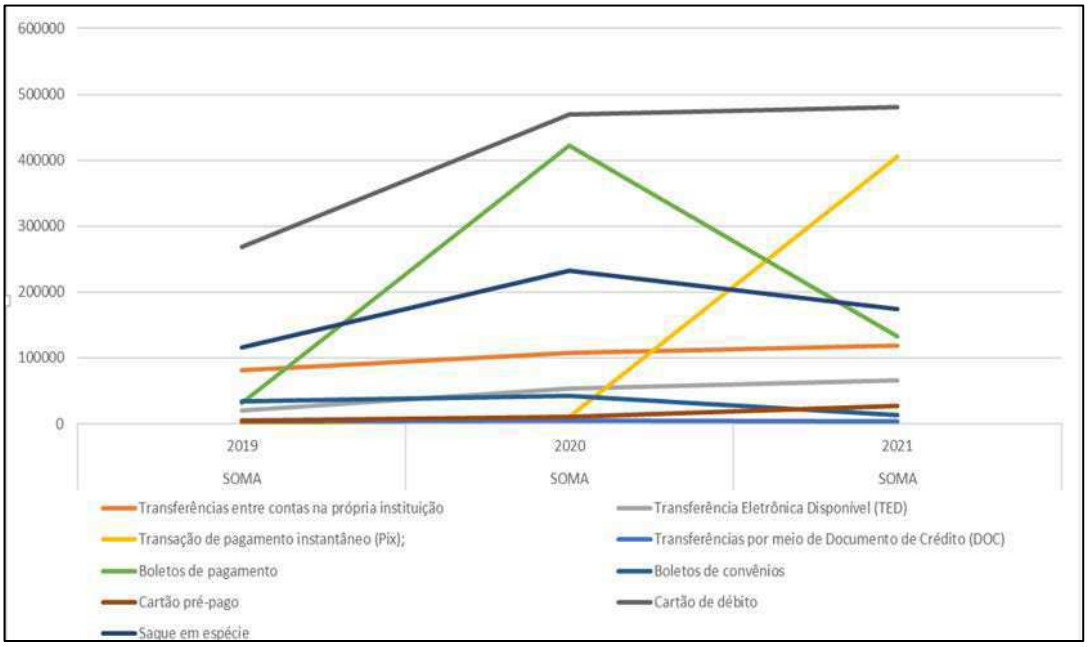

Gráfico 8 – Ocorrências por instrumento utilizados, exceto cartão de crédito – 2019 a 2021- valores anuais.
Fonte: elaborado a partir de informações recebidas das instituições

O **Gráfico 9**, a seguir, mostra as ocorrências com utilização do cartão de crédito. Essa análise foi apartada do Gráfico 8, devido ao volume de ocorrências e por se tratar de um meio de pagamento possuidor de processos específicos para tratamento de práticas criminosas. No caso de cartões de crédito, há destaque para as entidades do segmento S1 e S2 que são as maiores emissoras desse tipo de meio de pagamento.

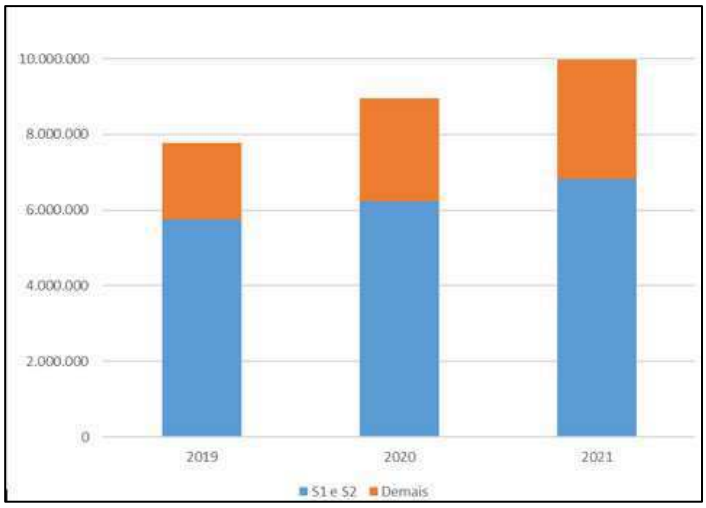

Gráfico 9 – Ocorrências Cartões de Crédito – 2019 a 2021
Fonte: elaborado a partir de informações recebidas das instituições

O **Gráfico 10** traz a quantidade total de ocorrências por instrumento utilizado, exceto cartão de crédito, onde se observa as ocorrências envolvendo cartão de débito, boletos de pagamento, saques, Pix e transferência dentro da própria instituição.

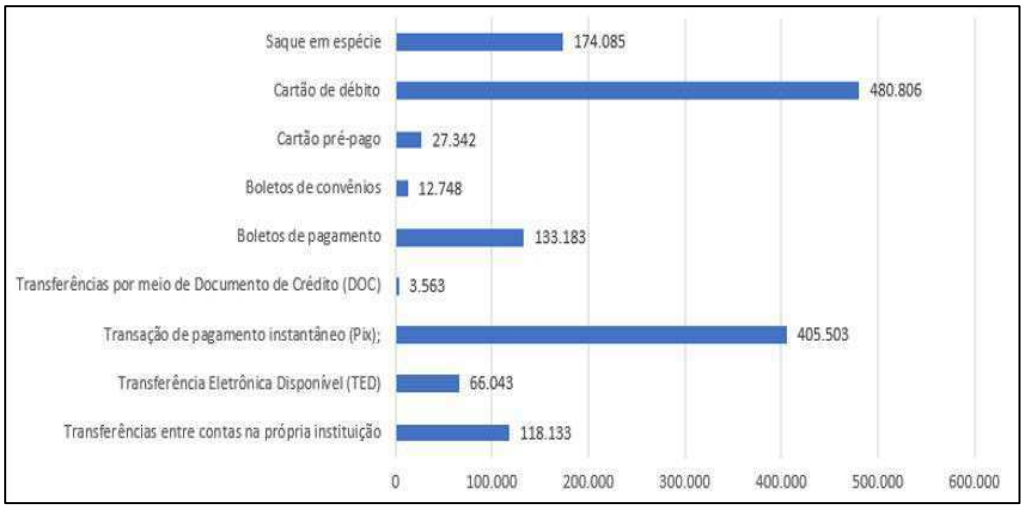

Gráfico 10 – Ocorrências por instrumento (exceto cartão de crédito) – 2021
Fonte: elaborado a partir de informações recebidas das instituições

Com base no que foi exposto, especialmente nos gráficos 2 a 9, pode-se inferir, com os gráficos apresentados, no geral constatou-se o aumento de ocorrências de fraude/golpes em transações financeiras ao longo do tempo. Também se percebeu o aumento dos valores envolvidos em proporção maior do que as ocorrências. Observa-se também que as instituições mais afetadas pertencerem aos segmentos S1 e S2, justamente por terem maior clientela, porém também é perceptível o aumento de fraudes junto a instituições de menor porte. Cabe acrescentar que, a partir da análise do Gráfico 10, excluindo-se as transações com cartão de crédito, pois esses possuem processos específicos para o tratamento de fraudes/golpes, o cartão de débito e o Pix foram citados em destaque nas ocorrências de fraudes/golpes.

Nesse contexto, as instituições supervisionadas devem estar em aprimoramento contínuo dos mecanismos que visam a reduzir a ocorrência desses eventos e ampliar a segurança para os clientes, visto que ações criminosas no ambiente financeiro vêm evoluindo, com os surgimentos de diversos serviços financeiros oferecidos no ambiente digital, seja na abertura de contas digitais ou nos mais diversos tipos de transações financeiras realizadas. De notar que, os aprimoramentos que se fizerem necessários devem evitar a alteração substancial da experiência e os benefícios no uso de produtos e serviços ofertados por essas instituições.

Faz-se necessário que este Banco Central se mantenha vigilante em suas competências fiscalizatórias e regulatórias para atuar promovendo e incentivando a mitigação dos riscos por parte das instituições por ele autorizadas integrantes do SFN e do Sistema de Pagamentos Brasileiro (SPB).

1.2 Descrição do Problema Regulatório

Esta subseção descreve o problema regulatório apresentando suas principais causas e consequências. Inicialmente, a Figura 1 descreve o Diagrama da Árvore de Problema.

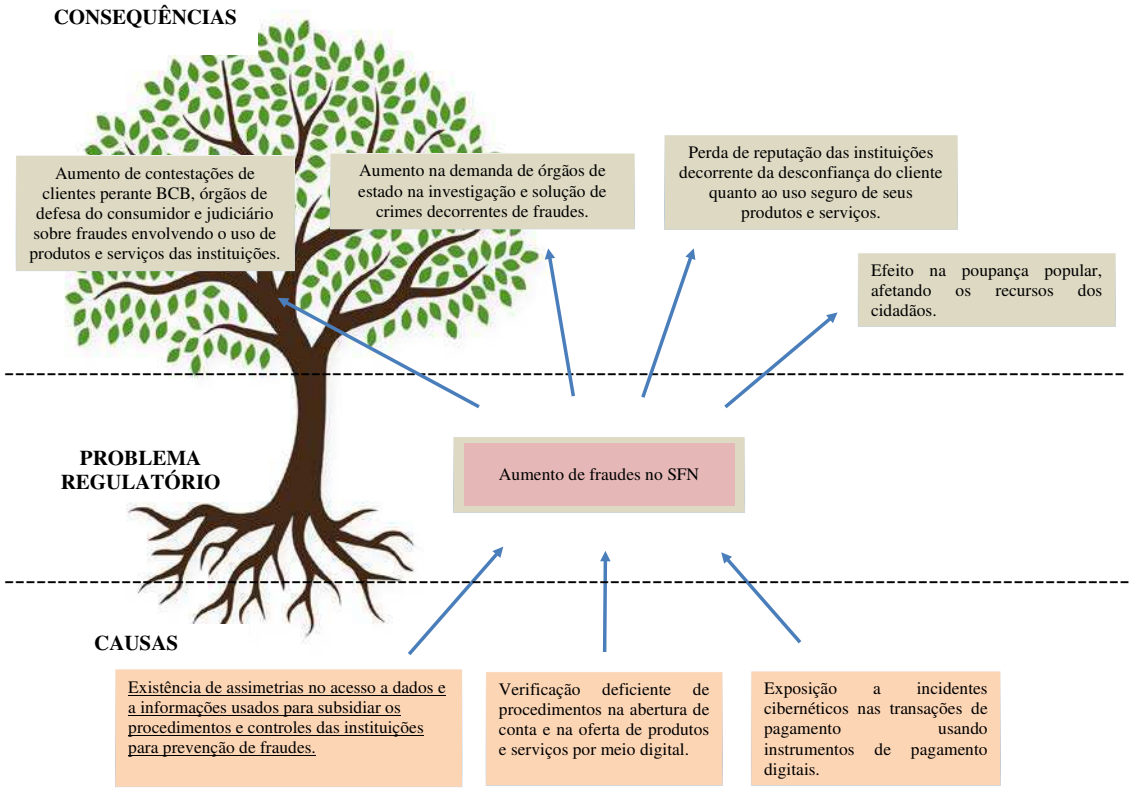

Figura 1 – Diagrama da Árvore do Problema.

Legenda: SFN significa 'Sistema Financeiro Nacional'.

Conforme apresentado na **Figura 1**, as causas do aumento das fraudes contemplam, entre outras, a assimetria de informação entre as instituições autorizadas, a verificação deficiente na abertura de contas e na oferta de produtos e serviços por meio digital, e a exposição a incidentes cibernéticos nas transações de pagamento usando instrumentos de pagamento digitais.

Ainda com base na **Figura 1**, as consequências abrangem perda de reputação das instituições decorrente da desconfiança de clientes quanto ao uso seguro de produtos e serviços, aumento das contestações de clientes perante o BCB, órgãos de defesa do consumidor e Poder Judiciário sobre fraudes envolvendo o uso de produtos e serviços das instituições, aumento das demandas de órgãos de estado na investigação e solução de crimes decorrentes de fraudes e efeito na poupança popular, afetando os recursos do cidadão.

Embora procedimentos e controles possam ser recomendados por meio de política de segurança cibernética, cabe a cada instituição a sua implementação. Em adição, crimes cibernéticos não são matéria regulada pelo CMN e pelo BCB, estando a investigação desses assuntos aos cuidados de autoridades policiais.

Contudo, o problema regulatório existe e o seu tratamento pode ser incentivado buscando endereçar esforços para tratar a Causa da **Figura 1** que denota existência de assimetrias no acesso a dados e a informações usadas para subsidiar os procedimentos e os controles das instituições para prevenção de fraudes.

Por fim, a redução das referidas assimetrias de informações pode ser buscada por meio do compartilhamento de dados e de informações. Sobre tal compartilhamento existe experiência internacional prévia, conforme detalhado no item 1.3, a seguir.

1.3 Experiência Internacional

Com relação à experiência internacional, este item apresenta exemplos não exaustivos relativos ao compartilhamento de dados e informações. Os exemplos abrangem o compartilhamento para: 1. minimizar a ocorrência de ameaças cibernéticas, 2. prevenir fraudes especificamente em transações de pagamento, 3. prevenir fraudes financeiras de maneira geral (com conexão ou não com a prevenção à lavagem de dinheiro e do financiamento do terrorismo – PLD/FT). É adequado citar que, para os fins deste trabalho, certa ênfase será dada para as iniciativas de compartilhamento de dados sobre fraudes financeiras em geral.

O primeiro exemplo de compartilhamento citado no primeiro parágrafo enaltece o combate às ameaças cibernéticas. Nos Estados Unidos - EUA, uma das iniciativas adotadas é o compartilhamento de informações baseado na Seção 314 (b) *do USA Patriotic Act*[15]. A este respeito, a literatura indica que há desafios a serem superados sobre essa forma de compartilhamento: mentalidade de 'silos' por parte das instituições (dificultando/evitando o compartilhamento de dados com outras instituições), a velocidade e a agilidade com que os crimes cibernéticos ocorrem, e a participação voluntária (não se verificando compulsoriedade na troca de informações)[16].

O segundo exemplo internacional de compartilhamento refere-se à prevenção de fraudes em transações de pagamento. Ele se baseia em iniciativa do *European Banking Authority* - EBA, sinali-

[15] A respeito desse assunto, ver 'FINCEN.Financial Crimes Enforcement Network. Section 314(b). Disponível em: https://www.fincen.gov/section-314b. Acesso em 9.9.2022'.
[16] Sobre tais desafios, vide 'CHAMBERLAIN, K. CAFP, november, 5th, 2018. Disponível em: https//bankingjournal.aba.com/2018/11/cyber-threats-how-banks-can-share-information-effectively/. Acesso em 4.2.2022'.

zando que as instituições forneçam dados sobre fraudes relacionadas com diferentes meios de pagamento às suas autoridades competentes e que estas, por sua vez, forneçam esses dados de forma agregada a EBA e ao *European Central Bank* - ECB[17].

O terceiro exemplo de compartilhamento baseia-se em iniciativas sobre o compartilhamento de dados e informações para prevenção de fraudes financeiras, com conexão ou não com PLD/FT. A este respeito, pode ser lembrado, o estudo no escopo do programa *Future of Financial Intelligence Sharing* (FFIS) em parceria com o *Royal United Services Institute* (RUSI)[18]. Em essência, o estudo extrai informações de referência e detalhadas sobre exemplos de 15 plataformas para compartilhamento de informações financeiras do setor privado para o setor privado do Reino Unido, Holanda, EUA, Cingapura, Estônia, Suíça e Austrália. Para realizar tal estudo, efetuou-se levantamento e processo de *workshop* entre meados de 2021 e junho de 2022. O escopo abrangeu a segmentação de plataformas em três domínios: aquelas centradas em fraudes, aquelas focadas em PLD/FT, e aquelas abrangendo ambos domínios (**Figura 2**).

[17] Maiores esclarecimentos sobre tal iniciativa, ver 'European Banking Authority. *Final Report on Fraud Reporting Guidelines under PSD2, July, 6th,* 2018. Disponível em: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2281937/5653b876-90c9-476f-9f44-507f5f3e0a1e/Final%20report%20on%20Guidelines%20on%20fraud%20reporting%20under%20Article%2096%286%29%20PSD2%20%28EBA-GL-2018-05%29.pdf?retry=1 Acesso em: 9.9.2022'.

[18] Maxwell, N. A Survey and Policy Discussion Paper: 'Lessons in private-private financial information sharing to detect and disrupt crime'. Future of Financial Intelligence Sharing (FFIS) research programme. 2022. Disponível em: https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf. Acesso em 9.9.2022.

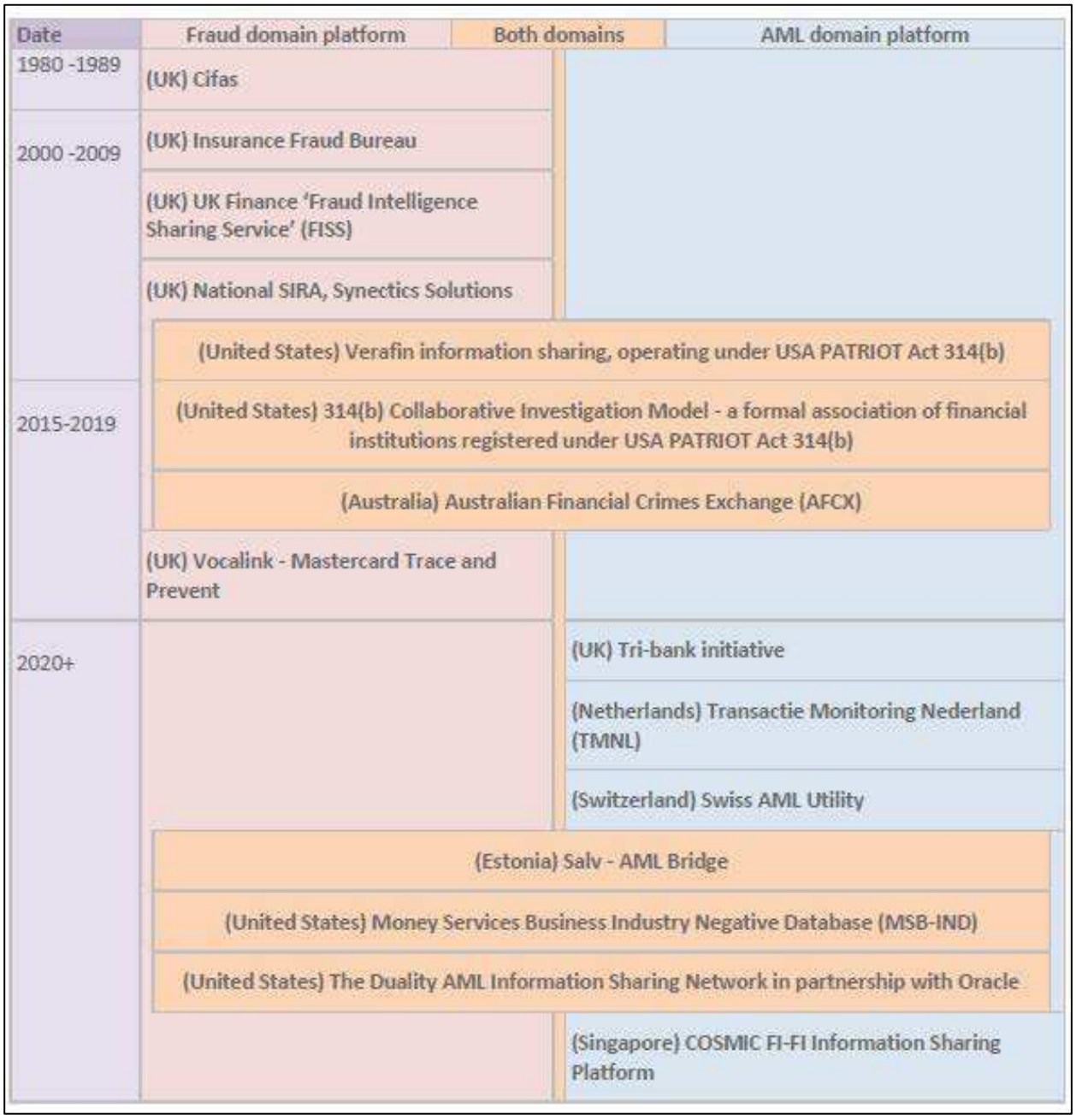

Figura 2: Evolução da implantação de plataformas e respectivos domínios de aplicação.

Fonte: Maxwell (2022)[19].

A **Figura 2**, além de ilustrar as quinze plataformas e os domínios a que se referem, permite ilustrar as jurisdições dessas plataformas e exibe um conjunto de datas relativas à implementação delas com o passar do tempo. É possível constatar que o compartilhamento de fraudes é abordado há décadas (a partir dos anos 80) e em anos recentes (de 2020 em diante) existe um aumento de

[19] Vide Nota 18.

plataformas. Importante citar que essas iniciativas de plataformas devem procurar em suas jurisdições guardar compatibilidade com normas e leis, as quais dão base legal buscando viabilizar o compartilhamento de dados e informações[20].

Por fim, os resultados do estudo que dá base à **Figura 2** evidenciam um cenário de diferentes recursos e de abordagens para as principais questões de design sendo implantadas em plataformas de compartilhamento de informações. Observa-se um cenário de políticas nascentes e ainda em desenvolvimento para apoio ao compartilhamento de informações privado-privado. Os resultados do referido estudo apresentam *insights* para desenvolvedores de políticas em 3 temas-chave: 1. visão estratégica compartilhada entre os agentes envolvidos do setor público e privado; 2. um ambiente legislativo e regulatório claro e favorável; 3. governança robusta, ética de dados e responsabilidade.

1.4 Agentes Envolvidos no Problema Regulatório

Esta subseção descreve os agentes envolvidos e afetados pelo problema regulatório:

(i) as instituições supervisionadas pelo BCB: incluem as instituições financeiras, demais instituições autorizadas a funcionar pelo BCB que atuam no Sistema Financeiro Nacional (SFN), instituições de pagamento integrantes do SPB, no papel de prestadoras dos serviços e das atividades envolvidas nas tentativas e ocorrências de fraudes no setor financeiro;

(ii) o BCB: como órgão público regulador (conjuntamente com o Conselho Monetário Nacional, conforme suas competências legais) e supervisor das instituições referidas no item ‘i’;

[20] A este respeito ver, inclusive, o texto de Oliveira, I. S. *Challenges to Information Sharing – Perceptions and Realities. Royal United Services Institute*. Occasional Paper, July 2016. Disponível em: https://static.rusi.org/20160708_ines_challenges_to_info_sharing_final1.pdf, acesso em 9/9/2022.

(iii) os órgãos públicos de segurança e demais entidades do setor público: nessa categoria incluem os mais diversos órgãos públicos no âmbito federal, estadual, distrital e municipal, como, por exemplo, aqueles responsáveis por garantir a segurança pública, à proteção do consumidor, à proteção de dados pessoais etc.;

(iv) a sociedade: as pessoas naturais e jurídicas, incluindo os clientes das instituições supervisionadas, vítimas das fraudes e dos fraudadores; e

(v) demais entidades do setor privado: pessoas jurídicas que prestem serviços contratados pelas instituições do SFN.

2. OBJETIVOS DO TRATAMENTO REGULATÓRIO

O objetivo do tratamento do problema regulatório, de forma ampla, é reduzir a quantidade de ocorrências de fraudes no âmbito do SFN e Sistema de Pagamentos. Como descrito na Seção 1, há mais de uma causa que ocasiona esse problema. A presente análise foca no tratamento de uma das causas identificadas, relacionada a assimetria de informações no acesso a dados e a informações usadas para subsidiar os procedimentos e controles das instituições para prevenção de fraudes.

Especificamente no caso descrito neste relatório, o objetivo do tratamento regulatório é 'reduzir assimetrias no acesso a dados e a informações usadas para subsidiar os procedimentos e controles das instituições para prevenção de fraudes'. Espera-se com o alcance desse objetivo contribuir para aprimorar a prevenção de fraudes aos cuidados dessas instituições e, consequentemente, reduzir a ocorrência de fraudes.

3. ALTERNATIVAS DE TRATAMENTO REGULATÓRIO

Esta Seção apresenta as alternativas propostas para o tratamento regulatório visando contribuir para corrigir o problema descrito na Seção 2, com o objetivo de reduzir as assimetrias no acesso a dados e a informações usadas para subsidiar os procedimentos e controles das instituições para prevenção de fraudes.

Destaca-se que o Decreto nº 10.411, de 30 de junho de 2020, que regulamenta a análise de impacto regulatório, estabelece um rol de metodologias que podem ser utilizadas, mas permite que o órgão

escolha outra metodologia, desde que justifique tratar-se da metodologia mais adequada para a resolução do caso concreto.

Nesse caso específico, considerando que a decisão do melhor modelo a ser implementado não está baseada apenas no custo financeiro, bem como a dificuldade de quantificar os demais aspectos do problema regulatório envolvido, a metodologia utilizada para comparação das alternativas consideradas foi uma análise qualitativa das vantagens e desvantagens para os principais agentes envolvidos descritos no Item 1.3 – o Banco Central do Brasil e as instituições do SFN e instituições de pagamento integrantes do SPB.

A propósito do tratamento regulatório, cabe mencionar, inicialmente, que as instituições financeiras e demais instituições autorizadas pelo BCB já devem observar e implementar uma série de requisitos de procedimentos e controles relacionados ao gerenciamento de riscos estabelecidos pela regulamentação vigente.

Como exemplo, a Resolução CMN nº 4.753, de 26 de setembro de 2019, e a Resolução BCB nº 96, de 19 de maio de2021, estabelecem que as instituições, para fins da abertura de conta de depósitos e contas de pagamento, devem adotar procedimentos e controles que permitam verificar e validar a identidade e a qualificação dos titulares da conta e, quando for o caso, de seus representantes, bem como a autenticidade das informações fornecidas pelo cliente, inclusive mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público ou privado. Ademais, as instituições, por meio dos procedimentos e tecnologias utilizados na abertura, na manutenção e no encerramento dessas contas, devem assegurar, a integridade, a autenticidade e a confidencialidade das informações e dos documentos eletrônicos utilizados, bem como a proteção contra o acesso, o uso, a alteração, a reprodução e a destruição não autorizados das informações e de documentos eletrônicos.

De forma complementar, a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, e a Resolução BCB nº 85, de 8 de abril de 2021, estabelecem procedimentos e controles que as instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo BCB devem observar referente à política de segurança cibernética e aos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Além disso, com relação aos meios de pagamentos digitais, a Resolução BCB nº 142, de 23 de setembro de 2021, que dispõe sobre procedimentos e controles para prevenção de fraudes na prestação de serviços de pagamento, estabelece limites máximos de valores para a realização de transações de pagamento, prazos mínimos para alteração de limites solicitados pelo cliente, necessidade de registros diários detalhando as ocorrências de fraudes ou de tentativas de fraude na prestação de serviços de pagamento por parte das instituições, entre outros.

No entanto, apesar dos diversos procedimentos e controles para o gerenciamento de riscos que cada instituição deve observar, considera-se que grande parte das fraudes pode afetar diferentes instituições, com ações dos fraudadores em mais de uma instituição do SFN. Como exemplo dessa situação, podemos citar as iniciativas de abertura de contas, com falsidade ideológica ou não, utilizando-se as mesmas informações cadastrais em diferentes instituições, bem como as ocorrências de fraudes relacionadas às transações de pagamento interbancárias, que utilizam, ao menos, duas instituições na cadeia de movimentação dos recursos fraudados.

Nesse sentido, verifica-se que o compartilhamento dos dados e das informações referentes aos indícios de ocorrências e de tentativas de fraudes entre as diversas instituições autorizadas teria o potencial de subsidiar a prevenção de novas fraudes relacionadas com a ocorrência compartilhada, bem como subsidiar a interrupção das ações fraudulentas que estejam em andamento.

Cabe apontar que iniciativa semelhante, relativa ao compartilhamento de dados e informações sobre incidentes cibernéticos, já foi regulada no País. Conforme determinado pelas regulamentações do CMN e do BCB vigentes[21], as instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo BCB devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes cibernéticos relevantes, abrangendo as informações recebidas de empresas prestadoras de serviços a terceiros, mantendo as informações compartilhadas à disposição do BCB. Esse compartilhamento, também, está especificado no âmbito do Open Finance, abrangendo incidentes que ocorrerem especificamente no escopo desse ambiente.

Dessa forma, a proposta para o tratamento regulatório envolve requisitos para determinar o compartilhamento de dados e informações sobre indícios de fraudes entre as instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar por este Banco Central, de

[21] Essas regulamentações abrangem a Res. CMN nº 4.893, de 2021, e a Res. BCB nº 85, de 2021, ambas já descritas nesta Seção e na Nota 8

forma a aprimorar os procedimentos e controles que cada instituição, de forma individual, já deve implementar e gerenciar.

Considerando o objetivo de proporcionar amplo acesso às informações sobre indícios de fraudes entre as instituições, esse compartilhamento pode ser efetuado por meio de diferentes alternativas. Nesse estudo, analisam-se duas alternativas.

A primeira alternativa (Proposta I) apresenta um sistema eletrônico de bases de dados gerenciada pelo Banco Central do Brasil. A segunda (Proposta II) descreve um sistema eletrônico de base de dados sob a responsabilidade das instituições supervisionadas.

ALTERNATIVA I – SISTEMA ELETRÔNICO IMPLEMENTADO PELO BANCO CENTRAL DO BRASIL

A centralização das informações sobre indícios de fraudes em um sistema de base de dados implementado e gerenciado pelo Banco Central do Brasil é uma das alternativas. Nesse caso, a Autarquia ficaria responsável pela gestão técnica do sistema eletrônico, bem como de sua governança, disciplinando as regras de funcionamento operacional em todos os seus aspectos.

No entanto, a responsabilidade pelos dados e informações registrados na referida base permaneceria com as instituições supervisionadas, atuando como fonte das informações durante as atividades prestadas. Nesse sentido, o BCB, atuando como operador desse sistema, não se responsabilizaria por eventuais dados e informações incorretos que fossem disponibilizados na base.

Nessa alternativa podem ser destacadas as seguintes vantagens:

(i) Menor custo de participação para as instituições – por ser um sistema gerido pelo poder público, que não visa ao lucro em sua operação, as eventuais cobranças a serem efetuadas das instituições participantes teriam como propósito apenas ressarcir os custos referentes à prestação de serviços das infraestruturas e dos sistemas mantidos pelo BCB;

(ii) Menor complexidade com relação a questões de governança do sistema – a disponibilização do acesso à base de dados pelo BCB, cumprindo adicionalmente a função de instituidor das regras operacionais, facilitaria na convergência aos mesmos padrões e procedimentos entre todas as instituições supervisionadas, considerando a heterogeneidade do SFN; e

(iii) Centralização de informações em uma única base de dados – a oferta do sistema pelo BCB permitiria que os dados fossem concentrados em uma mesma plataforma, gerando ganhos de eficiência no acesso e na disponibilização das informações.

Por outro lado, nessa alternativa destacam-se as seguintes desvantagens:

(i) Maior limitação de recursos – o poder público, relativamente ao setor privado, apresenta maior restrição orçamentária e de recursos materiais e humanos para a implementação e gestão do sistema pretendido, que poderia requerer aprimoramentos, bem como manutenções de segurança, para o seu pleno funcionamento;

(ii) Possibilidade de restrição a mudanças – a base de dados gerenciada pelo poder público poderia limitar a flexibilidade a mudanças eventualmente propostas pelo próprio mercado, restringindo o surgimento de novas soluções de maneira ágil; e

(iii) Assunção de responsabilidade inerente das próprias instituições – a gestão de uma base de dados por parte do próprio órgão regulador e supervisor pode acarretar na assunção de responsabilidades pelo gerenciamento de riscos de fraudes atribuídas a cada instituição supervisionada, a qual deve observar a legislação e a regulamentação vigentes quanto à implementação de procedimentos e controles para prevenção de fraudes e assegurar a confiabilidade e segurança de suas operações, incluindo aspectos relacionados à proteção dos dados e informações cadastrais de seus clientes.

ALTERNATIVA II – SISTEMA ELETRÔNICO IMPLEMENTADO POR INSTITUIÇÕES AUTORIZADAS

A segunda alternativa a ser analisada é a implementação do sistema eletrônico que contemple base de dados sobre indícios de fraudes, gerenciado por instituições autorizadas. Considera-se, nessa proposta, que as instituições poderiam realizar essa atividade empregando meios próprios ou contratando um terceiro para a prestação desse serviço.

Além disso, para atender ao objetivo de constituição de um sistema eletrônico que seja implementado por instituições, seriam necessárias determinadas condições de governança, na qual seriam estabelecidas, no que for compatível e não estiver disciplinado em regulamentação do CMN e do BCB, as regras operacionais necessárias para o funcionamento do sistema.

A gestão técnica do sistema eletrônico a ser implementado e as regras operacionais ficariam na responsabilidade das instituições supervisionadas; no entanto, as regras referentes à obrigatoriedade de participação das instituições, bem como quais informações seriam disponibilizadas ao sistema, entre outros aspectos regulatórios, ficariam à cargo da ação regulatória do Banco Central do Brasil e do Conselho Monetário Nacional.

Nessa alternativa podem ser destacadas as seguintes vantagens:

(i) Maior agilidade e adaptabilidade do sistema – um sistema eletrônico que gerencie base de dados e que for implementado por instituições autorizadas pode possuir maior agilidade para a sua implementação, bem como para adaptações, considerando a maior flexibilidade e disponibilidade para investimentos e aplicações de recursos;

(ii) Maior incentivo à inovação – maior liberdade e experiência das instituições para agregarem novas funcionalidades ao sistema, como serviços customizados e complementares, visando atender às necessidades das próprias instituições e do setor; e

(iii) Maior autonomia para a implementação – as instituições teriam maior autonomia para decidir a forma e o modelo de sistema que melhor se encaixe para atender as exigências regulatórias, convencionando regras, padrões e procedimentos e, se for o caso, decidindo pelo prestador do serviço a ser contratado na forma da regulamentação vigente.

Por outro lado, nessa alternativa destacam-se as seguintes desvantagens:

(i) Maior complexidade para definições de governança – a heterogeneidade das instituições autorizadas, com características e perfis de negócios distintos, poderia ser uma barreira à convergência de decisões necessárias para a implementação e gestão de um sistema eletrônico implementado por instituições autorizadas; e

(ii) Possibilidade de existência de múltiplos sistemas implementados por instituições autorizadas – tendo em vista a eventual dificuldade apontada no item (i), múltiplos sistemas poderiam ser criados por grupos de instituições para fins de atendimento da medida regulatória, demandando uma interoperabilidade entre as bases de dados para que o objetivo de redução de assimetria informacional seja atingido.

4. PROPOSTA REGULATÓRIA

Após análise das alternativas para tratamento regulatório, considerando as vantagens e desvantagens de ambos os modelos propostos, sugere-se a adoção da Alternativa II descrita na Seção 3, que estabelece requisitos para compartilhamento de dados e informações sobre indícios de fraudes, considerando a implementação de sistema eletrônico, com acesso a base de dados, aos cuidados das próprias instituições autorizadas.

Quanto a identificação e a definição dos efeitos e riscos decorrentes da edição do ato normativo[22], espera-se que a proposta regulatória sugerida contribua para reduzir a exposição a fraudes/golpes no SFN identificadas conforme a Seção 1.1. Como exemplo, o Gráfico 2 da referida seção apresenta que mais de 4 milhões de ocorrências, segregadas conforme os grupos fraudes, golpes e outros, foram registradas pelas instituições selecionadas em 2021.

Além disso, a implementação da proposta regulatória conforme Alternativa II, tendo em vista a complexidade para definições de governança citada como desvantagem ao modelo, pode eventualmente acarretar ao CMN e ao BCB a necessidade de disciplinar, futuramente, os aspectos de governança do sistema eletrônico a ser implementado pelas instituições.

Com relação a exposição dos possíveis impactos das alternativas identificadas, inclusive quanto aos seus custos regulatórios[23], a possibilidade de serem desenvolvidos múltiplos sistemas pelas instituições pode acarretar custos para assegurar a interoperabilidade entre tais sistemas. Adicionalmente, os custos para a implementação do referido sistema eletrônico pelas instituições autorizadas ainda não são plenamente conhecidos. No entanto, cabe destacar que os referidos custos de implementação poderão ser compensados pela redução do prejuízo financeiro decorrente das fraudes a serem evitadas.

A propósito dos impactos sobre as microempresas e as empresas de pequeno porte [24], cabe destacar que a proposta regulatória será aplicada às instituições autorizadas a funcionar pelo BCB, excluindo as administradoras de consórcio. Dessa forma, entende-se que o escopo já abrange instituições que, em sua maioria, não se enquadram como microempresas e empresas de pequeno porte.

[22] Alinhado ao disposto no art. 6º, inciso X, do Decreto nº 10.411, de 2020.
[23] Alinhado ao disposto no art. 6º, inciso VII, do Decreto nº 10.411, de 2020.
[24] Alinhado ao disposto no art. 6º, inciso VII-A, do Decreto nº 10.411, de 2020.

Considerando o que foi exposto, esta seção aborda o detalhamento da proposta regulatória sugerida, contemplando: 1. a base normativa usada para a proposta, 2. a formalização do objeto proposto a ser regulado, ligado ao compartilhamento de dados e informações, 3. as instituições que estariam obrigadas a efetuar tal compartilhamento, 4. a forma que tal compartilhamento ocorrerá, 5. quais informações mínimas seriam compartilhadas, 6. outros aspectos regulatórios, a serem disciplinadas por meio de ato normativo proposto.

Sobre a **base normativa** para propor essa proposta, entende-se que está abrangida nas competências do BCB e do CMN. Para o BCB, essa competência está amparada no art. 9º-A da Lei nº 4.728, de 14 de julho de 1965, e no art. 9º, caput e inciso II, da Lei nº 12.865, de 9 de outubro de 2013, e para o CMN ela está amparada nos arts. 4º, inciso VIII, da Lei nº 4.595, de 1964, 20, § 1º, da Lei nº 4.864, de 29 de novembro de 1965, 1º do Decreto-Lei nº 70, de 21 de novembro de 1966, 7º e 23, alínea "a", da Lei nº 6.099, de 12 de setembro de 1974, 1º, § 1º, inciso XIII, e § 3º, inciso I, da Lei Complementar nº 105, de 10 de janeiro de 2001, 1º, inciso II, da Lei nº 10.194, de 14 de fevereiro de 2001, e 1º, § 1º, da Lei Complementar nº 130, de 17 de abril de 2009, sem prejuízo da observância de outras legislações aplicáveis a segmentos específicos de instituições autorizadas pelo BCB.

Quanto à formalização do **objeto**, esta proposta regulatória dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes. Tais informações abrangeriam indícios de ocorrências e de tentativas de fraudes identificadas nas atividades das instituições. A finalidade desse compartilhamento é subsidiar procedimentos e controles para prevenção de fraudes, aos cuidados das referidas instituições[25].

A respeito da **abrangência**, propõe-se obrigar o compartilhamento para as instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo BCB. O único segmento que não seria contemplado nessa obrigatoriedade seriam as Administradoras de Consórcio[26].

[25] Importa ressaltar a finalidade de compartilhamento como um subsídio, ou seja, a proposta regulatória preserva as responsabilidades das instituições pelos seus procedimentos e controles para prevenção de fraudes previstos nas normas em vigor, cabendo a cada instituição a decisão sobre como vai empregar os dados e as informações a serem compartilhados para subsidiar tais procedimentos e controles.

[26] A exceção do segmento das Administradoras de consórcio considera as peculiaridades do segmento e o tratamento regulatório sob a égide de normas específicas editadas pelo BCB. Adicionalmente, para tais entidades não se aplicam normas editadas para a contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem (as quais são aplicáveis a demais instituições autorizadas, com base na Res. CMN nº 4.893, de 2021 e Res. BCB nº 85, de 2021).

Quanto à **forma de compartilhamento**, propõe-se que seja implementada por meio de sistema eletrônico com as seguintes funcionalidades mínimas: registro, alteração e exclusão e consulta de dados e informações sobre indícios de ocorrências ou de tentativas de fraude[27]. Propõe-se que tal sistema observe requisitos mínimos para sua implementação, como acesso pleno das instituições e padrão único de comunicação que permita a execução de suas funcionalidades. Propõe-se, ainda, sujeitar tal sistema eletrônico a procedimentos e controles para assegurar cumprimento da legislação e regulamentação, inclusive, ao titular dos dados, o livre acesso às das informações que lhe digam respeito, bem como a exclusão e correção tempestiva de dados e informações registrados, em caso de eventuais erros, inconsistências ou outras demandas, em observância da legislação e da regulamentação vigentes. Propõe-se, também, que seja assegurada a interoperabilidade com outros sistemas implementados em atendimento a regulamentação, quando existentes.

Quanto ao **conteúdo mínimo a ser compartilhado**, cada registro citado no parágrafo anterior deve contemplar, além da descrição dos indícios da ocorrência ou da tentativa de fraude, a identificação (i) de quem, segundo os indícios disponíveis, teria executado ou tentado executar a fraude, quando aplicável[28]; (ii) da instituição responsável pelo registro dos dados e das informações; e (iii) dos dados da conta destinatária ou de seu titular, em caso de transferência ou pagamento de recursos. De notar que esse registro não se aplica a dados sigilosos, nos termos de legislação especial,

[27] Cabe ressaltar que o requerido sistema eletrônico, a ser implementado por parte das instituições reguladas para permitir o compartilhamento dos dados e informações sobre indícios de fraudes, não exclui a possibilidade de coexistirem outros sistemas ou bases de dados que contribuam para a prevenção a fraudes no âmbito do SFN e do SPB. A este respeito, pode-se citar como exemplo o Diretório de Identificadores de Contas Transacionais (DICT), implementado com o propósito específico das transações de pagamento realizadas no âmbito do Pix e ampliado para viabilizar que a consulta a suas informações seja feita com o propósito de alimentar os mecanismos de análise de fraude dos participantes, inclusive em processos que não estejam diretamente relacionados ao Pix. Além disso, nesse caso, por ser um sistema operado pelo BCB, a proposta normativa em questão não é aplicável ao DICT.

[28] Com relação à identificação da pessoa que executou ou tentou executar a fraude, buscando estipular que as instituições não registrem, de forma equivocada, uma eventual vítima da fraude – sem prejuízo da definição de responsabilidade no evento –, a proposta determina que as instituições devem estabelecer e documentar os procedimentos e critérios para identificação da referida pessoa, de forma detalhada e compatível com o perfil de risco da instituição, com a legislação e com a regulamentação em vigor, os quais incluirão, no mínimo, a conferência com dados constantes de sistemas, cadastros e demais bases disponíveis para consulta. Essa documentação deve, ainda, permanecer à disposição do Banco Central.

relacionados a indícios da prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores[29] e de financiamento do terrorismo[30].

Adicionalmente, visando proporcionar a devida transparência, a proposta estabelece que as instituições devem obter do cliente com quem possuam relacionamento o consentimento prévio e geral possibilitando o registro no referido sistema eletrônico do conteúdo mínimo referente aos dados e às informações citados no parágrafo anterior que digam respeito ao referido cliente. O citado consentimento deve ter como finalidade o tratamento e o compartilhamento de dados e informações sobre indícios de fraudes no âmbito da presente proposta de Resolução Conjunta e constar de contrato firmado entre o cliente e a instituição, mediante cláusula em destaque no corpo do instrumento contratual ou por outro instrumento jurídico válido, ficando essa documentação à disposição do BCB.

Em complemento, quanto a **outros aspectos regulatórios**, a proposta estabelece o seguinte:

(i) A determinação de responsabilidades às instituições pela confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos dados e informações por elas registrados, pela implementação das funcionalidades e requisitos do sistema eletrônico e pelo cumprimento da legislação e regulamentação em vigor[31];

(ii) O estabelecimento de princípios a serem observados pelas instituições para compartilhamento, como segurança e privacidade dos dados e informações; qualidade dos dados e informações; acesso pleno e não discriminatório às funcionalidades do sistema; eficiência no cumprimento dos requisitos do sistema; reciprocidade com outras instituições; e interoperabilidade com outros sistemas, quando existentes;

[29] Essa legislação específica contempla a Lei nº 9.613, de 3 de março de 1998. Essa lei dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - Coaf, e dá outras providências. O art. 11, inciso II da referida lei, dispõe sobre a Comunicação ao Coaf: "(...) as pessoas referidas no art. 9º: (...) II - deverão comunicar ao Coaf, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização: (...)"

[30] A Lei nº 13.260, de 16 de março de 2016, regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013.

[31] As normas referentes a essa legislação e regulamentação em vigor foram previamente exemplificadas na Subseção 1.1 deste documento. Como exemplos delas, podem ser citadas: Lei nº 13.709, de 2018; Lei Complementar nº 105, de 2001; Res. CMN nº 4753, de 2019; Res. BCB nºs 85, 142 e 147, todas de 2021; Res CMN nºs 4.893 e 4949, ambas de 2021; e Res. CMN nº 4.983, de 2022.

(iii) A faculdade dada às instituições de contratar empresa para a prestação do serviço de compartilhamento efetuado por meio do sistema eletrônico citado nesta proposta, mantendo-se a responsabilidade pelo serviço prestado nas referidas instituições, inclusive referente ao tratamento de dados compartilhados, realizado em nome da instituição contratante, e observado que esse serviço seja considerado como relevante[32], nos termos da regulamentação em vigor;

(iv) A instituição de mecanismos de acompanhamento e de controle para assegurar a efetividade do cumprimento do disposto na proposta regulatória, inclusive guarda de documentos sobre o sistema eletrônico, com prazos para guarda dados e informações compartilhados, e dados e registros relativos à aplicação dos citados mecanismos; e

(v) A possibilidade de o BCB, observados os princípios previamente citados no item (ii) deste parágrafo, adotar medidas adicionais para cumprimento da citada proposta regulatória, contemplando: as funcionalidades do sistema eletrônico, observado o conteúdo mínimo previamente citado nesta Seção, o escopo dos dados e das informações; os parâmetros sobre acordos de níveis de serviço; os requisitos técnicos de segurança; a adequação dos mecanismos; outros requisitos técnicos, procedimentos operacionais e outros aspectos para o cumprimento da referida proposta;

(vi) As diretrizes gerais que deverão ser observadas pelo BCB na eventualidade de vir a regulamentar o escopo dos dados e das informações a serem registrados, em complemento ao conteúdo mínimo do registro dos dados e das informações previamente citado nesta Seção, enfatizando que os dados e informações a serem registrados deverão ser aqueles necessários e adequados para subsidiar os procedimentos e controles das instituições para a prevenção de fraudes; e

(vii) A determinação de que o acesso aos dados e às informações compartilhados nos termos da proposta de Resolução Conjunta seja restrito às instituições, ao BCB e às demais autoridades competentes, nos termos da legislação em vigor.

[32] Em outras palavras, seriam aplicáveis a este contrato as regras previstas para a contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem previstas na Res. nº 4.893, de 2021 (para o caso de instituições autorizadas) e na Res. BCB nº 85, de 2021 (para o caso de instituições de pagamento).

5. ESTRATÉGIAS PÓS-APROVAÇÃO DA NORMA

Esta seção apresenta uma descrição de estratégias a serem implementadas após a aprovação da proposta de norma. Inicialmente, espera-se que o prazo de vacância (considerada a previsão de entrada em vigor em 1º de novembro de 2023) seja suficiente para o desenvolvimento e a adequação de procedimentos, sistemas e para eventual celebração de contratos, considerada a faculdade de que trata o item (iii) do penúltimo parágrafo da Seção 4 deste documento.

Após a entrada em vigor da regulação proposta, eventuais ajustes nos dispositivos regulatórios sugeridos serão avaliados, conforme retorno a ser obtido por meio dos Departamentos da Área de Fiscalização e do Departamento de Atendimento Institucional - Deati, bem como das instituições autorizadas afetadas, inclusive por meio de suas associações de classe.

Entre adaptações possíveis de serem efetuadas no âmbito da regulação, o BCB poderá editar normas, no âmbito de suas competências legais, para detalhar procedimentos previstos na referida proposta regulatória, alinhado às medidas adicionais no âmbito da competência desta Autarquia citadas no penúltimo parágrafo da Seção 4 deste documento.

Por fim, registra-se que o ato normativo em questão deverá ser verificado quanto à necessidade de atualização do estoque regulatório até o fim do período de que trata o art. 19, inciso II, do Decreto nº 10.139, de 28 de novembro de 2019, qual seja, até o fim do segundo ano do mandato presidencial.

RESPONSÁVEIS PELA ELABORAÇÃO

(Assinado digitalmente)

Antonio Marcos Fonte Guimarães

Consultor

Departamento de Regulação do Sistema Financeiro (Denor)

(Assinado digitalmente)

João André Calvino Marques Pereira

Chefe

Departamento de Regulação do Sistema Financeiro (Denor)