Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5

PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

RELATÓRIO FINAL E PARECER CONCLUSIVO

11/05/2026

Rony Vainzof (Coordenação)

Annette Pereira

Débora Sirotheau

Leonardo Ferreira

Myreilla Aloia

Rodrigo Pironti

Vitor Moraes

SUMÁRIO

1. CONTEXTUALIZAÇÃO E OBJETIVOS

A proteção ao crédito e a prevenção à fraude tornaram-se pilares importantes e complementares para o desenvolvimento econômico e social. Em um ambiente marcado por transações instantâneas e volume massivo de dados, a solidez das decisões financeiras depende diretamente da qualidade das informações utilizadas para identificar indivíduos, analisar comportamentos e validar operações. Quando esses mecanismos operam de forma integrada, reduzem assimetrias informacionais, fortalecem a segurança, higidez e estabilidade sistêmica e criam uma base confiável para a concessão e gerenciamento de crédito, ampliando liquidez e competitividade no mercado.

Esse alinhamento estratégico se materializa em arquiteturas de dados cada vez mais inteligentes, capazes de cruzar sinais de identidade, padrões de consumo e indicadores de risco em tempo real. Na prática, o que antes eram trilhas paralelas, uma focada na capacidade de pagamento e outra na legitimidade da transação, agora formam um ecossistema unificado de gestão de risco. A convergência entre esses fluxos reduz perdas financeiras, acelera decisões e melhora a experiência dos clientes, equilibrando proteção, eficiência operacional e crescimento sustentável.

Sob a perspectiva regulatória, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) consolida essa aproximação ao oferecer bases legais complementares para o tratamento de dados em ambos os contextos. Os dados pessoais constituem um dos principais insumos para decisões, avaliação de risco, concessão responsável de crédito e prevenção e detecção de comportamentos fraudulentos.

Quando tratados de forma legítima, proporcional e transparente, esses dados pessoais viabilizam um ambiente econômico mais seguro, eficiente e inclusivo, preservando direitos fundamentais e fortalecendo a estabilidade do sistema financeiro.

O equilíbrio entre o uso legítimo de dados pessoais e a salvaguarda da privacidade é eixo estruturante das práticas de mercado. Esse equilíbrio se traduz não apenas em conformidade normativa, mas também em eficiência econômica, mitigação de riscos reputacionais e fortalecimento da confiança entre consumidores, serviços financeiros e o ecossistema digital.

Portanto, o desafio que se coloca ao mercado e aos órgãos reguladores é garantir modelo de governança de dados que harmonize a proteção à privacidade com o interesse público na prevenção de ilícitos e na promoção do crédito responsável.

Além disso, também é relevante avaliar o entendimento do escopo e da amplitude da base legal de proteção do crédito, que não se limita à avaliação de capacidade de pagamento, por envolver uma série de outras atividades de tratamento sob esta base legal.

Em última instância, a diversidade de atividades relacionadas à proteção do crédito, bem como o alinhamento entre proteção de dados pessoais, proteção ao crédito e prevenção à fraude consolida agenda estratégica de confiança digital e inclusão financeira, que são pilares de uma economia moderna, sustentável e orientada à inovação.

Assim, os objetos deste GT são desenvolver diretrizes estratégicas e fornecer subsídios para a Agência Nacional de Proteção de Dados Pessoais (ANPD), com fundamentação técnica, prática e teórica, guiados, de forma não exaustiva, conforme os seguintes quesitos orientativos:

1) A importância socioeconômica do crédito e da prevenção à fraude para o Brasil

1. Qual é a relevância do crédito para o desenvolvimento socioeconômico do Brasil?
2. Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

2) Papel dos dados pessoais no ecossistema de crédito

1. Qual a importância dos dados pessoais para proteção do crédito e demais atividades relacionadas ao tema?
2. Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?

3) Papel dos dados pessoais na prevenção à fraude e outros ilícitos

1. Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?
2. Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos?
3. Quais são os riscos de subutilizar dados pessoais em processos antifraude (ex.: aumento de chargebacks, fraude sintética, falsidade ideológica e riscos sistêmicos)?

4) Convergência entre proteção ao crédito e prevenção à fraude

1. O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?
2. Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?

5) Atividades e bases legais aplicáveis à proteção ao crédito

1. Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?
2. Quais bases legais da LGPD suportam o tratamento de dados para análise e concessão do crédito?

6) Bases legais aplicáveis à prevenção à fraude

1. Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?
2. Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?

7) Princípios da LGPD aplicáveis a ambos os contextos

1. Quais princípios devem orientar a coleta, uso, minimização, retenção e compartilhamento de dados nesses tratamentos?
2. Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?
3. Como operacionalizar transparência sem comprometer a efetividade de sistemas antifraude e de scoring?

8) Governança, controles e segurança

1. Quais frameworks de governança e gestão de riscos são recomendados para operações de crédito e antifraude?
2. Quais controles técnicos e administrativos devem ser implementados para assegurar segurança da informação e mitigação de incidentes?
3. Como estruturar políticas de retenção, registro de logs, auditoria e *accountability*?

9) Decisões automatizadas e Inteligência Artificial

1. Quais são decisões automatizadas mais comuns em crédito e antifraude?
2. Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?
3. Quais diretrizes devem orientar o uso de IA generativa e machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos?
4. Como equilibrar transparência e explicabilidade com segredos de negócio?

2. COMPOSIÇÃO

Nome	Titularidade	Representação
Rony Vainzof	Coordenador Membro Titular	Setor Empresarial

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

Nome	Titularidade	Representação
Annette Pereira	Membro suplente	Setor Empresarial
Débora Sirotheau	Membro titular	Setor Laboral
Leonardo Ferreira	Membro titular	Outros poderes, órgãos ou instituições públicas
Myreilla Aloia	Membro titular	Confederações sindicais representativas do setor produtivo
Rodrigo Pironti	Membro suplente	Instituições Científicas, Tecnológicas e de Inovação
Vitor Morais	Membro titular	Setor Empresarial

Participantes: Tayná Araújo, Kamilla Rodrigues (Ministério da Justiça e Segurança Pública) e Janaina Lopes (Ministério da Justiça e Segurança Pública).

3. ESTUDOS E LEVANTAMENTOS

De início, ressaltamos que o mapeamento de normas aplicáveis e precedentes judiciais não buscou ser exaustivo, tendo caráter descritivo e contextual. O objetivo central foi identificar e sistematizar referências relevantes para a compreensão do tema, sem que isso represente recomendação de adoção de medidas específicas *per se*, ou seja, que desconsiderem o cenário regulatório e econômico brasileiro.

Portanto, optou-se por privilegiar abordagem sintética no corpo do relatório, com detalhamento adicional apresentado em anexo. Ressalta-se, ainda, que qualquer análise ou eventual transposição de tais referências deve considerar de forma cuidadosa o contexto específico brasileiro, com a devida deferência ao arcabouço normativo já existente, especialmente no setor financeiro, que se caracteriza por elevado grau de regulação, maturidade institucional e reconhecida eficiência.

- **Mapeamento de normas aplicáveis – ANEXO I**

O mapeamento normativo aplicável ao tema, presente no ANEXO I, apresenta o arcabouço regulatório aplicável às atividades de proteção ao crédito e prevenção à fraude, reunindo normas nacionais, setoriais e internacionais que disciplinam o tratamento de dados pessoais para tais finalidades. Importante ressaltar que tal mapeamento não é exaustivo, mas busca trazer as principais normas relacionadas ao tema.

No plano central de legalidade e governança de dados pessoais, destaca-se a Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece as bases legais próprias e os limites para o tratamento de dados pessoais de forma geral, aplicável também no contexto de proteção do crédito e prevenção à fraude.

Ao reconhecer expressamente essas bases legais, a LGPD incorpora visão contemporânea sobre o uso de dados pessoais para proteção do crédito e prevenção à fraude, alinhada às dinâmicas do mercado e à necessidade de ambientes modernos mais seguros e eficientes.

Essas atividades de tratamento desempenham papel estrutural na segurança das transações, na liquidez do sistema, na competitividade entre agentes econômicos, na adequada precificação de produtos, no gerenciamento de riscos e na ampliação da inclusão financeira.

Nesse contexto, o uso lícito e responsável de dados pessoais para tais finalidades contribui para reduzir a inadimplência, mitigar riscos de fraude e ilícitos, evitar situações de superendividamento, reduzir custos e aumentar o acesso ao crédito. Reforça-se, assim, a lógica regulatória de que esse tratamento não atende apenas aos interesses do concedente de crédito, mas também produz benefícios concretos ao próprio titular dos dados e ao funcionamento eficiente do mercado.

A respeito do histórico legislativo da LGPD, vale considerar que as bases legais de proteção do crédito e prevenção à fraude, originalmente, não estavam previstas no Projeto de Lei 4.060/2012[1], apresentado pelo então deputado federal Milton Monte, mas foram incluídas na versão consolidada no âmbito do Projeto de Lei da Câmara n° 53, de 2018[2]. As proposições foram mantidas no texto aprovado pelo Congresso que se tornou a Lei nº 13.709/2018, refletindo a escolha normativa deliberada no processo de consolidação do modelo brasileiro, indicando que o legislador reconheceu expressamente a necessidade de conferir base jurídica própria a atividades estruturais do ambiente econômico digital e do sistema financeiro.

Complementando esse eixo, o ordenamento jurídico brasileiro conta com normas específicas voltadas ao ecossistema de crédito e proteção ao consumidor, como a Lei do Cadastro Positivo, que regula a formação e utilização de bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito e impõe limites quanto ao tipo de dados que podem ser utilizados nas bases de dados de cadastro positivo (vedando informações sensíveis e excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor), e o Código de Defesa do Consumidor, que assegura transparência, acesso e

[1] Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL%204060/2012.
[2] Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7738705&ts=1630450891439&disposition=inline.

correção de informações em cadastros de crédito. Importante destacar, nesse ponto, que a legislação do cadastro positivo regula tão somente a formação e consulta de bases de dados de cadastro positivo, os quais são formados e mantidos por bureaus de crédito, e não regulamenta toda a atividade de crédito. Apontamos essa distinção, pois a lei do cadastro positivo tem aplicação limitada ao seu escopo e não se confunde com a proteção do crédito ou com as atividades das instituições financeiras.

Também se destacam a Lei do Superendividamento, que reforça práticas responsáveis de concessão de crédito e a necessidade de consulta e de avaliação da situação financeira do consumidor. Igualmente, são de crucial importância as normas sobre prevenção à lavagem de dinheiro e integridade corporativa, que influenciam diretamente os controles de governança e monitoramento de transações no sistema financeiro.

No âmbito setorial financeiro, diversas normas do Conselho Monetário Nacional, do Banco Central e da Comissão de Valores Mobiliários disciplinam a gestão de riscos, os procedimentos de identificação de clientes e os controles operacionais relacionados à concessão de crédito e à prestação de serviços financeiros, inclusive de pagamento. Essas normas exigem que as instituições adotem procedimentos robustos de verificação de identidade, gestão de dados de clientes, monitoramento de riscos e controles internos, reforçando a integração entre compliance regulatório, gestão de risco e proteção de dados.

Especificamente em relação à prevenção à fraude, há regras setoriais para registro, compartilhamento e monitoramento de indícios de fraude entre instituições financeiras, bem como obrigações de manutenção de registros e implementação de mecanismos de segurança nos serviços de pagamento, com o objetivo de proteger o sistema financeiro e os próprios titulares de dados. Também são incorporadas referências a padrões internacionais e normativos relacionados a controle de fraude, prevenção à lavagem de dinheiro e segurança operacional no sistema financeiro.

O levantamento também considera referências regulatórias internacionais, como o GDPR europeu, a diretiva europeia sobre crédito ao consumidor e normas de prevenção à lavagem de dinheiro e serviços de pagamento. Essas referências indicam a existência, em outros sistemas legislativos distintos, de normas que tratam desses temas e que, em alguma medida, trazem aspectos importantes, como o direito de revisão de decisões automatizadas, a minimização de dados e a transparência no uso de informações financeiras, além de incentivar modelos de governança baseados em segurança e proporcionalidade.

Em conjunto, o mapeamento evidencia que a proteção de dados, a análise responsável de crédito e os mecanismos de prevenção à fraude formam um sistema regulatório integrado, no qual a LGPD

funciona como eixo transversal de governança, permeada por normas financeiras e, quando aplicável, consumeristas.

O material também deixa claro que a proteção de dados pessoais, nesse campo, desloca-se de uma lógica ultrapassada centrada exclusivamente no consentimento para um modelo baseado em *accountability* do controlador. A legitimidade do tratamento decorre menos da manifestação individual do titular e mais da existência de bases legais claras, aplicação de proporcionalidade e demais principais da LGPD, mecanismos de governança, políticas públicas de uso de dados e supervisão regulatória.

O mapeamento demonstra que proteção de dados, proteção ao crédito e prevenção à fraude não são esferas normativas em conflito, e sim dimensões interdependentes de um mesmo arranjo regulatório. Lembramos, também, que o escopo de prevenção a fraudes é bastante amplo, não se limitando ao contexto financeiro. O material oferece base sólida de exemplos de diferentes regras contextualizadas conforme as necessidades e características do Brasil, sendo importante que quaisquer normas que venham a regulamentar o tema mirem sustentar modelos regulatórios que conciliem eficiência econômica, segurança do sistema financeiro e tutela efetiva dos direitos fundamentais, especialmente em um cenário de crescente automação, uso de inteligência artificial e intensificação do compartilhamento de dados.

Mapeamento de precedentes judiciais – ANEXO II

O documento apresenta mapeamento de precedentes judiciais relevantes sobre proteção ao crédito e prevenção à fraude, com foco na interpretação da LGPD, da Lei do Cadastro Positivo (Lei nº 12.414/2011) e de normas correlatas aplicadas pelo Poder Judiciário. O levantamento sistematiza decisões do Superior Tribunal de Justiça e de tribunais de justiça estaduais que tratam do uso, tratamento e compartilhamento de dados pessoais em sistemas de análise de crédito, bem como da responsabilidade por falhas de segurança e fraudes envolvendo dados financeiros. Vejamos alguns deles:

REsp 1.419.697/RS (Tema 710/STJ - 2014) – sistema *"credit scoring"*

- Tribunal / Órgão: STJ, Segunda Seção, recurso repetitivo (Tema 710)
- Tema: Licitude do *score* de crédito e limites de uso dos dados pelo fornecedor/gestor de banco de dados.

Ementa (síntese)

O STJ definiu que o *credit scoring* é método estatístico para avaliação do risco de concessão de crédito, baseado em múltiplas variáveis, com atribuição de pontuação ao consumidor. Ressaltou que o *credit scoring* constitui metodologia de cálculo e não se confunde com banco de dados de crédito em si. A

Corte considerou a prática lícita, à luz da disciplina da proteção ao crédito e da Lei 12.414/2011 (Cadastro Positivo), desde que respeitados: (i) a privacidade, (ii) a transparência nas relações de consumo: o consumidor tem direito de conhecer as informações que influenciaram o seu score, mas o método de cálculo (algoritmo) é segredo comercial; e (iii) os limites de utilização de informações, especialmente evitando dados sensíveis ou excessivos. O consentimento prévio do consumidor é dispensado, mas o titular tem direito de solicitar esclarecimentos sobre as fontes e as informações pessoais utilizadas no cálculo. O uso de dados sensíveis, excessivos, incorretos ou desatualizados, bem como recusa indevida de crédito, pode gerar responsabilidade civil por dano moral.

- O precedente reconhece a licitude do *scoring*, mas o qualifica como metodologia de cálculo, e não como banco de dados em si, o que tem reflexos na aplicação da Lei 12.414/2011.
- A decisão consolidou a ideia de que não há necessidade de consentimento específico para o uso do score, desde que haja direito de informação sobre os dados utilizados e que não se empreguem dados sensíveis ou excessivos.
- Com a edição da LGPD, esse entendimento passou a ser lido em conjunto com o art. 7º, X, LGPD (proteção ao crédito), reforçando a tensão entre a dispensa de consentimento e a exigência de transparência, minimização e finalidade.
- Na prática, o Tema 710 e a Súmula 550/STJ servem como ponto de partida para discussões atuais sobre:
    - deveres de informação dos gestores de *scoring;*
    - fronteira entre dados meramente cadastrais, dados de adimplemento e dados sensíveis; e
    - risco de responsabilização quando o *score* se baseia em dados desatualizados ou incorretos.

REsp 2.133.261/SP (2024) – Diferença de score e histórico

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Compartilhamento, por gestor de banco de dados, de informações cadastrais e de adimplemento com terceiros consulentes.

Ementa (síntese)

O STJ reafirmou a distinção entre *score* de crédito (Tema 710/Súmula 550) e banco de dados regido pela Lei 12.414/2011. Entendeu que o gestor de banco de dados pode registrar e tratar dados de adimplemento sem consentimento, com base na Lei do Cadastro Positivo e na LGPD (art. 7º, X). Contudo, somente o *score* pode ser disponibilizado a terceiros consulentes sem consentimento; o histórico de crédito exige autorização específica do cadastrado, e os dados cadastrais e de adimplemento só podem ser compartilhados com outros bancos de dados, não com terceiros

consulentes. A disponibilização indevida dessas informações a terceiros consulentes configura dano moral presumido *(in re ipsa)* e enseja a responsabilização objetiva do gestor.

- A decisão aproxima a interpretação da Lei do Cadastro Positivo da LGPD, reforçando que a base "proteção ao crédito" não legitima qualquer compartilhamento amplo de dados cadastrais no contexto do cadastro positivo.
- O entendimento consolida que há três níveis de acesso:
    1. *score* (sem consentimento);
    2. histórico de crédito (com autorização específica); e
    3. dados cadastrais e de adimplemento (compartilháveis entre bancos de dados, não a qualquer consulente).
- O julgamento é frequentemente lido como marco na proteção do titular contra o uso expansivo de dados cadastrais em modelos de negócio que extrapolam a finalidade de proteção ao crédito.

REsp 2.115.461/SP – Serasa (2023/2024)

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Compartilhamento de dados cadastrais e de adimplemento; dano moral presumido.

Ementa (síntese)

Em linha com o REsp 2.133.261/SP, o STJ concluiu que o gestor de banco de dados de crédito não pode disponibilizar a terceiros consulentes dados cadastrais e de adimplemento que, por lei, só podem ser compartilhados com outros bancos de dados (art. 4º, III, Lei 12.414/2011). A disponibilização indevida configura violação aos deveres de tratamento de dados, gera dano moral presumido (*in re ipsa*) e acarreta responsabilidade objetiva.

- Este precedente reforça a coerência interna da Terceira Turma em relação à necessidade de consentimento quando o compartilhamento ultrapassa *score* e histórico autorizado.
- O núcleo argumentativo se conecta diretamente à LGPD (arts. 7º, X, 42 e 43) e à Lei 12.414/2011, servindo como referência para políticas internas de governança de dados e limitação de acesso a consulentes.

REsp 2.221.650/SP (2025) – ausência de dano moral presumido (Quarta Turma)

- Tribunal / Órgão: STJ, Quarta Turma
- Tema: Dados pessoais não sensíveis; dano moral não presumido.

Ementa (síntese)

A Quarta Turma, ao tratar da alegada disponibilização de dados pessoais não sensíveis em contexto de proteção ao crédito, reafirmou que o tratamento de dados para proteção do crédito é legítimo, à

luz do art. 7º, X, da LGPD e da Lei nº 12.414/2011 (Cadastro Positivo), e entendeu que não há dano moral presumido. Exige-se (i) prova da disponibilização indevida e (ii) prova de efetivo abalo aos direitos de personalidade. No caso concreto, o recurso foi desprovido por ausência de prova do dano e pela incidência da Súmula 7/STJ.

O caso introduz nuances importantes no debate: enquanto a Terceira Turma admite dano moral presumido em hipóteses de disponibilização indevida de dados cadastrais, a Quarta Turma, em contexto fático específico, enfatiza a necessidade de prova do dano.

- Para fins de política institucional, esse contraste sugere um quadro jurisprudencial ainda em evolução, que pode levar o Conselho a acompanhar a consolidação de entendimentos (eventual afetação a recursos repetitivos ou uniformização futura).
- O precedente também reforça a importância de documentar a origem e o fluxo de dados, uma vez que a própria comprovação da disponibilização indevida se torna elemento central na discussão.

REsp 2.201.694/2201694-SP (2025) – disponibilização indevida de dados em cadastro positivo

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Cadastro Positivo – disponibilização de informações cadastrais e de adimplemento a terceiros consulentes.

Ementa (síntese)

O STJ analisou ação de obrigação de fazer cumulada com indenização por danos morais envolvendo a disponibilização de dados de cadastro positivo a terceiros consulentes. A Terceira Turma afastou a aplicação direta do Tema 710/STJ e da Súmula 550/STJ, que tratam especificamente do *credit scoring*, ressaltando que este não constitui banco de dados, o qual é regulado pela Lei nº 12.414/2011. Com base no art. 4º da Lei do Cadastro Positivo, a Turma reafirmou que o gestor de banco de dados: (i) pode disponibilizar ao consulente o *score* de crédito, sem necessidade de consentimento; (ii) pode disponibilizar o histórico de crédito, desde que haja autorização prévia e específica do cadastrado; e (iii) somente pode compartilhar informações cadastrais e de adimplemento com outros bancos de dados. A disponibilização dessas informações a terceiros consulentes foi qualificada como disponibilização indevida, gerando responsabilidade objetiva do gestor e dano moral presumido (*in re ipsa*), em razão da sensação de insegurança experimentada pelo titular. O recurso especial foi conhecido e provido.

- Reafirma, de forma expressa, a separação entre *"credit scoring"* e banco de dados de crédito, restringindo o alcance do Tema 710/Súmula 550.
- Define um modelo escalonado de acesso:
  - *score* de crédito → disponibilização a consulentes, sem consentimento específico;
  - histórico de crédito → acesso condicionado a autorização específica;

  - dados cadastrais e de adimplemento → compartilhamento restrito a outros bancos de dados.
- Consagra a tese de que a disponibilização indevida de dados cadastrais/adimplemento a consulentes configura, por si só, dano moral presumido, sem necessidade de prova de prejuízo adicional.
- Reforça a leitura de que a base "proteção ao crédito" (art. 7º, X, LGPD) não legitima o uso ampliado de dados cadastrais para finalidades diversas das hipóteses estritas previstas na Lei nº 12.414/2011, em relação ao seu contexto.

Como se percebe, há uma zona de tensão interpretativa dentro do próprio STJ quanto à responsabilização e configuração, ou não, de dano moral presumido em hipóteses de disponibilização indevida de dados de Cadastro Positivo. A decisão no âmbito do REsp 2.201.694/SP é temerária pois, ao reconhecer dano moral presumido pela mera disponibilização de informações pessoais a terceiros sem comunicação prévia e sem consentimento, tem a capacidade de transformar irregularidade formal em indenização automática, sem exigir demonstração de prejuízo concreto ou de efetiva lesão aos direitos da personalidade.

Além disso, o entendimento ignora que o regime jurídico do crédito opera com distinções relevantes entre tipos de informação e níveis de risco, sendo inadequado tratar toda circulação indevida como se tivesse a mesma gravidade. Ao presumir o dano em qualquer hipótese, a decisão enfraquece a previsibilidade do sistema, amplia excessivamente o espaço para litigância oportunista e gera insegurança para atividades legítimas e socialmente relevantes ligadas à avaliação de risco e ao funcionamento do mercado de crédito.

REsp 2.207.172/2207172-SP (2025) – disponibilização indevida de dados e dano moral presumido

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Banco de dados de crédito – limites de compartilhamento e responsabilidade por disponibilização indevida.

Ementa (síntese)

No REsp 2207172/SP, a Terceira Turma voltou a examinar ação de obrigação de fazer cumulada com compensação por danos morais relacionada à disponibilização de dados de cadastro positivo a terceiros consulentes. Assim como em julgados anteriores, o colegiado registrou que o Tema 710/STJ e a Súmula 550/STJ se referem exclusivamente ao *credit scoring*, não se confundindo com bancos de dados regulados pela Lei nº 12.414/2011. Com base nos incisos III e IV do art. 4º da lei, a Turma reiterou que: (i) o gestor de banco de dados pode compartilhar informações cadastrais e de adimplemento apenas com outros bancos de dados; (ii) pode disponibilizar aos consulentes o *score* de crédito, sem consentimento específico; e (iii) pode fornecer o histórico de crédito mediante autorização prévia e específica do titular. A concessão de acesso a dados cadastrais e de

adimplemento diretamente a consulentes foi considerada ilícita, ensejando responsabilidade objetiva e dano moral presumido, diante da violação aos deveres legais de tratamento de dados.

- Reitera, de maneira quase espelhada ao REsp 2201694/SP, a interpretação restritiva do art. 4º da Lei do Cadastro Positivo, consolidando a linha jurisprudencial da Terceira Turma no contexto do cadastro positivo.
- Confirma que, para o STJ, há tratamento diferenciado entre:
  - dados usados para score;
  - dados que compõem o histórico de crédito; e
  - dados cadastrais e de adimplemento, cuja circulação é mais limitada.
- Reforça a ideia de que a mera disponibilização indevida de dados a quem não poderia recebê-los é suficiente para a configuração de dano moral, consolidando o entendimento de dano moral "*in re ipsa*" em hipóteses de violação às regras de compartilhamento do Cadastro Positivo.
- Funciona, na prática, como precedente de confirmação da tese firmada em outros casos da mesma Turma (como REsp 2.133.261/SP e REsp 2.115.461/SP), conferindo estabilidade à interpretação sobre os limites de compartilhamento de dados de crédito.

Apelação Cível nº 1001338-31.2021.8.26.0042 (TJSP) - Divulgação de dados cadastrais – proteção ao crédito – inexistência de dano moral
• Tribunal / Órgão: TJSP, 2ª Câmara de Direito Privado
• Tema: Tratamento e divulgação de dados meramente cadastrais em contexto de proteção ao crédito; limites da base legal do art. 7º, X, da LGPD.

Ementa (síntese)
No julgamento da Apelação Cível nº 1001338-31.2021.8.26.0042, o Tribunal de Justiça de São Paulo analisou controvérsia envolvendo a divulgação, por empresa de proteção ao crédito, de dados pessoais meramente cadastrais do consumidor. O colegiado concluiu que tais informações — não sensíveis, públicas ou obtidas de forma lícita — podem ser utilizadas para fins de proteção ao crédito com base no art. 7º, X, da LGPD, sem necessidade de consentimento prévio ou comunicação específica ao titular.

A Corte afastou a alegação de ilicitude, entendendo que não houve demonstração de compartilhamento indevido para finalidades estranhas à proteção ao crédito, nem evidência de que a divulgação tenha causado prejuízo efetivo aos direitos de personalidade do titular. Consequentemente, rejeitou a pretensão indenizatória por danos morais, por ausência de violação à esfera jurídica do consumidor.

- O acórdão adota interpretação mais flexível da base legal "proteção ao crédito", entendendo legítimo o tratamento de dados cadastrais comuns sem consentimento, quando restrito à finalidade de análise de crédito (proteção ao crédito).
- O TJSP enfatiza a ausência de ilicitude porque:
  - os dados não eram sensíveis;
  - estavam no contexto típico de consultas de proteção ao crédito; e
  - não houve prova de divulgação indevida ou finalidade incompatível.
- O Tribunal faz referência ao Tema 710/STJ *(credit scoring)* como suporte para a regularidade da atuação de *bureaus* de crédito em seu âmbito próprio.
- O entendimento se aproxima da orientação da Quarta Turma do STJ (REsp 2.221.650/SP), ao exigir prova de dano e afastar a tese de dano moral presumido.
- O precedente evidencia que tribunais estaduais ainda aplicam interpretação mais permissiva ao art. 7º, X, LGPD, especialmente quando lidam com dados cadastrais de baixa criticidade.

REsp 2.077.278/SP (2023) – "golpe do boleto" e vazamento de dados bancários

- Tribunal / Órgão: STJ, Terceira Turma (Informativo 791)
- Tema: Vazamento de dados bancários, engenharia social e responsabilidade objetiva da instituição financeira.

Ementa (síntese)

O STJ analisou caso em que dados bancários do consumidor teriam vazado, possibilitando a aplicação do chamado "golpe do boleto". Reconheceu que, se comprovado vazamento de dados sigilosos sob responsabilidade da instituição financeira, há defeito na prestação do serviço, em razão de tratamento irregular e de falha no dever de segurança da informação (art. 14, CDC; arts. 44 e 46 da LGPD). Concluiu que, quando criminosos demonstram possuir informações internas sobre relacionamento bancário e operações do cliente, está caracterizado o fortuito interno, atraindo a responsabilidade objetiva da instituição, nos termos da Súmula 479/STJ[3].

- O caso conecta diretamente LGPD, CDC, sigilo bancário (LC 105/2001) e responsabilidade por falhas de segurança da informação.
- Embora não trate especificamente de *score* ou cadastro positivo, é relevante para o Conselho na medida em que:
  - reforça a exigência de controles técnicos e organizacionais robustos; e
  - vincula vazamento de dados bancários à noção de fortuito interno, afastando excludentes baseadas em "fraude de terceiro".

[3] As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. (SÚMULA 479, SEGUNDA SEÇÃO, julgado em 27/06/2012, DJe 01/08/2012)

- Em diálogo com a Resolução Conjunta 6/2023 do Banco Central (compartilhamento de informações para prevenção a fraudes), o precedente mostra que a base legal ou o dever normativo de compartilhar dados não afastam a responsabilidade quando há falhas de segurança ou uso indevido.

Algumas experiências internacionais recentes no contexto europeu, especialmente sob a aplicação do *General Data Protection Regulation (GDPR),* evidencia o endurecimento do controle regulatório sobre atividades de *credit scoring* e decisões automatizadas no setor financeiro. No caso SCHUFA (CJEU, dezembro de 2023), o Tribunal de Justiça da União Europeia entendeu que a atribuição automatizada de *score* de crédito por *bureau* pode configurar decisão individual automatizada, atraindo a incidência do art. 22 do GDPR, especialmente quando terceiros (como instituições financeiras) se apoiam fortemente nesse valor para estabelecer, executar ou encerrar relação contratual com o titular, com repercussões quanto ao direito à intervenção humana e às informações significativas sobre os critérios gerais aplicados[4]. Em paralelo, autoridades de proteção de dados alemãs aplicaram sanções em contextos de recusa automatizada de crédito sem transparência adequada, retenção excessiva de dados e ausência de base legal após o término da relação jurídica, reforçando os princípios de limitação temporal, necessidade e informação.

Importante ressaltar o GDPR é distinto da LGPD em diversos aspectos, inclusive em relação a decisões automatizadas e proteção do crédito, de modo que não se recomenda importar decisões ou padrões legislativos externos, devendo-se avaliar a pertinência e compatibilidade com o sistema legal e especificidades do cenário brasileiro, ainda mais considerando a existência de precedentes no STJ sobre o tema.

Há registros de atuação sancionatória e de investigações setoriais por autoridade regional alemã *(Hamburg Data Protection Authority – HmbBfDI)* em matéria de retenção/exclusão e governança do tratamento de dados no contexto de cobrança e bases de dados de crédito, reafirmando os princípios de limitação temporal e necessidade[5]. Esses referenciais indicam que, mesmo em ambientes altamente regulados por normas financeiras e de *Open Finance*, autoridades de proteção de dados mantêm escrutínio rigoroso sobre *credit scoring*, decisões automatizadas[6], compartilhamento e retenção de dados.

[4] Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=282187&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=687137
[5] Disponível em: https://datenschutz-hamburg.de/news/branchenweite-schwerpunktpruefung-im-forderungsmanagement
[6] Disponível em: https://www.edpb.europa.eu/news/national-news/2023/berlin-sa-imposes-300-000-euro-fine-against-bank-after-lack-transparency_en

O conjunto de precedentes analisados demonstra que a jurisprudência brasileira reconhece a legitimidade do tratamento de dados pessoais principalmente no contexto da proteção ao crédito, compreendendo essas atividades como parte essencial do funcionamento do mercado de crédito e da gestão de riscos nas relações econômicas. Desde o Tema 710/STJ, consolidou-se o entendimento de que instrumentos como o *credit scoring* são lícitos e podem operar sem necessidade de consentimento do titular, desde que respeitados limites relacionados à transparência, à qualidade das informações e à vedação do uso de dados sensíveis ou excessivos. Os julgados mais recentes reforçam essa lógica ao reconhecer que a base legal da proteção ao crédito (art. 7º, X, da LGPD) legitima o tratamento de dados para análise de risco e compartilhamento dentro das hipóteses legais, ao mesmo tempo em que delimitam os fluxos de acesso entre score, histórico de crédito e dados cadastrais no âmbito do cadastro positivo. Nesse cenário, a responsabilização civil tem sido vinculada principalmente a situações de disponibilização indevida de dados fora das hipóteses legais ou a falhas de segurança, e não ao tratamento regular de dados para fins de proteção ao crédito. Além disso, parte relevante da jurisprudência tem destacado que o dano moral não se presume automaticamente nesses contextos, exigindo demonstração concreta de dano[7], o que reforça a compreensão de que o uso legítimo de dados pessoais em sistemas de proteção ao crédito constitui atividade regular e necessária para a segurança das transações e para a eficiência do mercado.

Como conclusão geral, o levantamento demonstra que o Judiciário brasileiro tem reconhecido a legitimidade do tratamento de dados para crédito e antifraude, mas tem prescrito modelo de legalidade condicionada, no qual a licitude depende de limites de finalidade, minimização, transparência e governança. A base legal de proteção ao crédito é aceita e não funciona como autorização ampla para compartilhamento indiscriminado, especialmente quando envolve dados cadastrais e de adimplemento. A jurisprudência, portanto, sinaliza que a proteção de dados no setor não se resolve pela proibição do tratamento, mas pela delimitação de quem pode acessar o quê, em quais condições e com quais controles.

4. ENTREVISTAS

[7] A Quarta Turma do STJ (REsp 2.221.650/SP) reconheceu que de forma unânime ser indispensável a comprovação de que a conduta de disponibilizar dados pessoais no âmbito do cadastro positivo tenha causado significativo abalo aos direitos de personalidade do titular para fins de responsabilização por dano moral.
Há certa divergência sobre o tema no âmbito do STJ, a exemplo da decisão no âmbito do REsp 2.201.694/SP, na qual a Terceira Turma do Tribunal decidiu, por maioria, que a disponibilização para terceiros de informações pessoais armazenadas em banco de dados, sem a comunicação prévia ao titular e sem o seu consentimento, caracterizaria violação dos direitos de personalidade e justificaria indenização por danos morais. Assim, a disponibilização de informações pessoais armazenadas em banco de dados para terceiros, sem aviso prévio ao titular e sem o seu consentimento, configuraria violação dos direitos da personalidade (como privacidade e intimidade), capaz de gera dano moral presumido, ou seja, a indenização é devida independentemente de comprovação de prejuízo concreto.

- **Jéssica Abreu - Executive Legal Manager at Serasa Experian | Privacy | Positive Data | Regulation – 04/12/25 – ANEXO III**

A entrevista reforçou que proteção do crédito e tratamento de dados pessoais são inseparáveis, pois a estabilidade do mercado, a redução de assimetrias e o combate à fraude dependem diretamente de informações robustas, verificáveis e consistentes. O crédito foi apresentado como ativo estratégico com impacto macro e microeconômico, influenciando consumo, inclusão financeira, políticas públicas e redução de desigualdades regionais.

Destacou-se que economias desenvolvidas operam com elevada relação crédito/PIB, e que o Brasil possui oportunidade estruturante de desenvolvimento caso fortaleça seu ecossistema de crédito com segurança jurídica e governança de dados, alinhando-se a boas práticas internacionais.

Um ponto central foi a crítica à antiga dependência excessiva do consentimento como base legal predominante para o tratamento de dados no crédito. Segundo a entrevistada, modelos baseados exclusivamente em consentimento geram distorções e incentivos à ocultação de informações, favorecendo titulares com maior letramento digital e ampliando riscos sistêmicos. Como evidência, foi citado o impacto positivo da migração do Cadastro Positivo de *opt-in* para *opt-out*, demonstrando que escala e precisão exigem modelos que não dependam apenas da manifestação individual.

Também foi enfatizado que não há concessão segura de crédito sem autenticação robusta de identidade, e que separar juridicamente “proteção do crédito” e “prevenção à fraude” pode não refletir a realidade operacional do mercado. Essa fragmentação regulatória afetaria especialmente micro e pequenos empresários, elevando custos e fragilizando o sistema. A fraude, por sua vez, foi descrita como fenômeno coletivo, que penaliza bons pagadores e encarece o crédito para todos.

No tema biometria, a entrevista apontou risco de banalização em ambientes de baixa governança e alertou para a incoerência regulatória de penalizar instituições com estruturas maduras de compliance, enquanto usos frágeis e pouco controlados permanecem invisíveis. Soma-se a isso o baixo letramento digital da população, que dificulta a compreensão real sobre tecnologias, armazenamento e riscos associados.

Foi relatado ainda o crescimento de percepções equivocadas sobre o alcance dos direitos dos titulares, resultando em pedidos indevidos de exclusão de dados, judicialização em massa e potencial sobrecarga regulatória, sobretudo para empresas menores. Defendeu-se a necessidade de comunicação pública mais clara e ações educativas para evitar interpretações absolutistas.

A entrevistada destacou que proteção ao crédito abrange toda a cadeia, incluindo prospecção e segmentação, concessão, monitoramento, cobrança e recuperação, além de serviços que asseguram

higidez e integridade das bases. Nesse contexto, publicidade desalinhada a políticas reais de crédito gera desperdício econômico e frustração do consumidor.

Quanto aos dados alternativos, defendeu-se que o critério técnico para legitimidade deve ser a relevância estatística, isto é, se determinado dado aumenta a acurácia e reduz risco sistêmico, ele deixa de ser excessivo e passa a ser necessário. Foi sugerida a importância de permitir experimentação regulatória, inclusive para proteger o próprio titular, antecipando sinais de superendividamento.

Por fim, destacou-se que o crédito moderno é intrinsecamente baseado em IA (modelos estatísticos e machine learning), exigindo governança contínua com documentação, auditorias, reavaliações e monitoramento de vieses. A explicabilidade deve equilibrar transparência e direitos do titular com a preservação do segredo de negócio, inclusive respaldada por precedentes judiciais

- **Elias Sfeir - Presidente da ANBC – Associação Nacional dos Bureaus de Crédito & Membro do Conselho Climático da Cidade de São Paulo & Conselheiro Certificado & Membro do ICCR e B Ready Banco Mundial – 08/12/2025 – ANEXO IV**

Em suma, destacou-se como o Brasil é referência global em modelos de crédito e governança de dados. O crédito foi apresentado como instrumento essencial para inclusão e crescimento econômico, sustentado por consumo consciente, crédito responsável e educação financeira.

Apontou-se que a transformação do setor é guiada por velocidade, simplicidade, personalização e segurança, sendo a fraude um fator crítico que encarece o crédito. Na entrevista ressaltou-se que o uso de dados pessoais e dados alternativos é fundamental para reduzir assimetrias de informação, aumentar acurácia dos modelos, prevenir fraudes e ampliar liquidez no mercado. Foi enfatizado que dados alternativos (governamentais, telecom, energia, biometria e metadados comportamentais) são tendência global e essenciais especialmente para inclusão de populações com baixa visibilidade de crédito, como pode ocorrer em regiões do Norte e Nordeste no Brasil.

Quanto ao princípio da necessidade, argumentou-se que a definição de “dado relevante” deve ser baseada em modelagem estatística robusta e validação empírica, e não em percepções abstratas. Dados desnecessários representam risco e responsabilidade para os agentes, sendo evitados pelos birôs. Defendeu-se o uso proporcional de dados pessoais e alternativos para reduzir assimetrias, ampliar acesso ao crédito e prevenir fraudes, especialmente em regiões ainda invisíveis ao sistema.

Sobre IA, destacou-se o uso histórico de modelos avançados pelos birôs, com atenção atual à IA generativa, defendendo transparência responsável e validação estatística para evitar vieses. Por fim,

a LGPD foi avaliada como positiva e equilibrada, especialmente pela base legal específica para proteção ao crédito, mas alertou-se que excesso regulatório pode limitar inovação e excluir cidadãos digitalmente, recomendando regulação equilibrada, governança e estímulo à inclusão via dados alternativos.

- **Diana Loureiro de Moura – Procuradora do Banco Central do Brasil – 11/12/2025 – ANEXO V**

A entrevistada destacou a diferença estrutural entre a lógica de atuação da ANPD, centrada na proteção do indivíduo, e a do BACEN, orientada pela estabilidade sistêmica do mercado de crédito como bem coletivo. Nesse cenário, foi enfatizado que proteção ao crédito e prevenção à fraude são dimensões indissociáveis, pois ambas sustentam a integridade e o funcionamento do sistema financeiro.

Foi reforçado o caráter sistêmico do crédito como mecanismo essencial de circulação de recursos e dinamização econômica, ressaltando que a análise de risco é contínua e não se limita ao momento inicial da concessão. Assim, o uso de dados — inclusive pessoais — é indispensável para monitoramento de comportamento, prevenção de perdas e identificação de operações atípicas.

A entrevistada apontou que eventos aparentemente individuais, como fraudes ou concessões equivocadas, podem gerar efeitos em cadeia e impactar liquidez, cessão de crédito, garantias e confiança do mercado. Por isso, o BACEN considera reclamações individuais como insumos para avaliação estrutural, e não como casos isolados determinantes.

No tocante à Resolução Conjunta nº 6, destacou-se que seu principal avanço não está em alterar modelos internos de gestão de risco, mas em promover interoperabilidade e cooperação entre instituições, permitindo o compartilhamento padronizado de informações sobre suspeitas de fraude. A lógica apresentada é que, diante de fraudadores que atuam de forma colaborativa, o sistema financeiro precisa ter capacidade equivalente de troca de informações.

Foi enfatizado que exigir consentimento para fins de prevenção à fraude é inviável, tanto do ponto de vista operacional quanto jurídico, pois fraudadores não consentiriam, e o titular não possui liberdade real de escolha em serviços financeiros essenciais. Nesse sentido, o consentimento seria apenas informativo, e outras bases legais — como interesse público, proteção ao crédito e prevenção à fraude — seriam suficientes para fundamentar o tratamento de dados previsto.

A entrevista também reforçou que a prevenção à fraude se conecta diretamente ao interesse público, pois contribui para reduzir juros, inadimplência e spreads, ampliando o acesso ao crédito e

promovendo benefícios coletivos. Esse racional foi diferenciado do modelo de consentimento do Open Finance, que opera sob lógica individual e concorrencial.

No tema de inteligência artificial e decisões automatizadas, foi apontado que o BACEN ainda não estabeleceu limites regulatórios específicos, pois não há evidências relevantes que justifiquem intervenção imediata. Entretanto, identificou-se espaço para evolução no debate sobre explicabilidade, buscando equilíbrio entre transparência ao titular, preservação de segredo de negócio e mitigação de riscos de fraude.

Por fim, concluiu-se que o ecossistema de crédito é altamente interdependente e sensível, e que restrições excessivas ao uso ou compartilhamento de dados podem elevar riscos sistêmicos e, paradoxalmente, prejudicar o próprio consumidor. A recomendação central é que a regulação avance de forma calibrada, conciliando proteção de dados, inovação, prevenção à fraude e estabilidade de mercado.

- **Luis Felipe Monteiro – Corporate Affairs – VP da Único – 05/12/2025 - ANEXO VI**

Foi destacado que o uso de dados pessoais e biometria é central para a prevenção de fraudes, descrito como mecanismo que protege o próprio titular ao assegurar autenticidade e legitimidade de transações digitais. Após o uso primário de validação, os dados alimentam modelos de detecção de fraude, fortalecendo continuamente a capacidade do sistema em reconhecer padrões suspeitos. O processo resulta em três respostas essenciais por transação: prova de vida (*liveness*), confirmação de identidade e avaliação de risco.

A biometria foi apontada como a tecnologia que atualmente oferece melhor equilíbrio entre precisão, experiência do usuário e segurança, sobretudo em ambientes integralmente digitais, como bancos digitais, nos quais não há alternativa física para validação de identidade. O entrevistado ressaltou que a sofisticação das fraudes aumentou significativamente, com crescimento de *deepfakes* e ataques de injeção, exigindo investimentos contínuos e tecnologia avançada.

A fraude no Brasil foi caracterizada como fenômeno sistêmico, impulsionado por crime organizado transnacional e atuação em rede, com estimativas de que cerca de 65% dos fraudadores operam colaborativamente. Foi destacado que a fraude na iniciação de crédito, com inadimplência já na primeira parcela, representa cerca de R$ 60 bilhões anuais, associada diretamente à fraude de identidade. A redução desse tipo de fraude foi apontada como condição estrutural para inclusão financeira, fortalecimento da concorrência bancária, redução do custo do crédito e estabilidade de infraestruturas como o Pix.

O entrevistado alertou que restringir ou subutilizar dados pessoais para prevenção à fraude geraria aumento expressivo de perdas sistêmicas, elevação do custo do crédito para toda a população e possível inviabilização de operações totalmente digitais. Foi citada a experiência do México como exemplo de modelo excessivamente dependente de consentimento, associado a maiores níveis de fraude e custo elevado de crédito. Em contraponto, a LGPD foi avaliada como arcabouço equilibrado, oferecendo bases legais adequadas para o setor, como prevenção à fraude, execução de contrato e legítimo interesse (para dados não sensíveis).

No âmbito regulatório, foram apontados riscos em propostas legislativas que imponham consentimento obrigatório para biometria, exijam alternativas físicas obrigatórias para serviços digitais ou tratem biometria de forma genérica, sem diferenciar usos banalizados (como em condomínios) de aplicações críticas com governança robusta (como no sistema financeiro). Essas iniciativas poderiam produzir retrocesso sistêmico, afetando inovação, segurança e inclusão.

Como oportunidades regulatórias, recomendou-se evitar alterações desnecessárias na LGPD e fortalecer políticas públicas que incentivem o uso responsável de biometria em setores de alto risco, como telecomunicações (ativação de chips), hoje apontado como vetor relevante de golpes. Também foi defendida maior aproximação entre ANPD e setores críticos para consolidação de boas práticas, governança e conscientização.

Por fim, enfatizou-se que o Brasil se tornou referência internacional em identificação digital graças ao modelo regulatório vigente e que há mais oportunidades do que riscos no uso seguro da biometria, desde que respeitados proporcionalidade, minimização e governança.

- **Otávio Margonari Russo – Diretor de Combate a Crimes Cibernéticos da Polícia Federal – 09/12/2025 – ANEXO VII**

O entrevistado enfatizou que proteção de dados e persecução penal não são objetivos opostos, mas dimensões que podem se fortalecer mutuamente quando calibradas de forma adequada, alertando que restrições excessivas podem comprometer investigações, aumentar a sensação de impunidade e favorecer o crescimento do crime, enquanto ausência de limites pode gerar exposição desnecessária do cidadão.

No âmbito institucional, destacou-se que a Polícia Federal (PF) possui estrutura interna dedicada à governança de dados, com protocolos de confidencialidade, segurança e uso restrito conforme finalidades legais. A LGPD foi descrita como vetor positivo de aprimoramento, ao impulsionar a PF a adotar padrões ainda mais elevados de proteção e controle. Contudo, foi apontado que o maior desafio prático reside na possibilidade de interpretações excessivamente restritivas por parte de agentes privados, que podem atrasar ou dificultar o fornecimento de informações essenciais para

investigações modernas, as quais dependem de correlação massiva de dados para mapear padrões criminosos, identificar redes e antecipar tendências.

O entrevistado destacou o caráter sistêmico e interligado dos crimes cibernéticos, mencionando que pequenos e médios *e-commerces* são frequentemente invadidos para furto de dados de cartão, os quais alimentam mercados clandestinos e viabilizam fraudes em larga escala. Essa dinâmica conecta múltiplas modalidades criminosas (a exemplo de estelionato, invasões, vazamento e comercialização de bases) e reforça a necessidade de cooperação robusta entre PF, polícias civis e atores privados, sob pena de fragmentação investigativa e perda de eficiência.

Foram apresentados os pilares estruturais da atuação da PF no combate ao crime cibernético: capacitação, com formação contínua de policiais e peritos em delegacias especializadas; repressão por frentes temáticas (como fraude bancária eletrônica, abuso sexual infantil e crimes de ódio); prevenção, com foco em educação digital do usuário e em ações voltadas a jovens para evitar escalada criminosa; e cooperação ampla, incluindo parcerias internas, acordos com o setor privado (ACTs) e articulação internacional com organismos como Europol, Interpol e FBI. Também foi mencionado o uso de bases e plataformas colaborativas, como sistemas de compartilhamento de inteligência (ex.: MISP/capivara), que fortalecem investigações transnacionais.

No tema de vazamento de dados e *ransomware*, foi apontado um círculo vicioso relevante: empresas atacadas evitam comunicar PF ou ANPD por receio de multas, dano reputacional e complexidades internas, o que enfraquece a inteligência estatal e incentiva o crime. Destacou-se ainda a mudança no *modus operandi* dos grupos de *ransomware*, que vêm migrando de ataques disruptivos com criptografia para roubo silencioso de dados seguido de extorsão, estratégia considerada mais eficaz e menos visível, confirmada em fóruns internacionais.

Há atuação ativa da PF nesse cenário, incluindo monitoramento de credenciais vazadas, alerta preventivo a empresas e participação em operações internacionais, além da repressão a afiliados brasileiros vinculados a modelos de *ransomware-as-a-service*. Sobre o pagamento de resgate, foi reafirmada a orientação global de não pagamento, com possibilidade de exceções em situações extremas (vida ou impacto crítico à sociedade), destacando-se que a PF deve ser acionada previamente para apoiar decisões, monitorar transações e viabilizar investigação. Foi reforçada a premissa institucional de que a empresa atacada deve ser tratada como vítima.

No campo regulatório, o entrevistado sugeriu como prioridade a interpretação da LGPD alinhada ao interesse público, de modo a garantir que a proteção de dados não inviabilize o recebimento de informações em volume, velocidade e formato compatíveis com investigações contemporâneas. Também foi defendida a possibilidade de mecanismos regulatórios que considerem a comunicação

tempestiva à PF como fator relevante na dosimetria de sanções pela ANPD, evitando penalização dupla e incentivando colaboração.

Por fim, foi destacada a necessidade de maior integração institucional entre PF, ANPD e CNPD para fortalecer confiança, fluxo de informações e alinhamento estratégico.

Ao final da entrevista, houve encaminhamento de respostas complementares por escrito, as quais estão registradas no ANEXO VII.

- **Leandro Miranda – Diretor Jurídico da ANBI – 13/01/2026 – ANEXO VIII**

O entrevistado indicou que a base legal autônoma de proteção ao crédito, concebida como elemento essencial e estruturante do marco regulatório brasileiro, não surgiu por mera reprodução do modelo europeu (GDPR), mas sim como resposta às necessidades específicas do mercado nacional, caracterizado por menor maturidade tecnológica, maior incidência de fraudes e particularidades operacionais na concessão de crédito, como o crédito consignado.

Foi exposto que a aplicação estrita da base legal de execução de contrato exigiria solicitação prévia do titular para consulta de dados, o que inviabilizaria o funcionamento do mercado de crédito e poderia gerar colapso operacional, especialmente em modalidades de crédito amplamente utilizadas no Brasil. Também foi apontada dificuldade conceitual em delimitar o que estaria ou não incluído na execução contratual, considerando que toda relação a prazo envolve crédito e que inadimplência não é fenômeno claramente externo ao contrato.

A entrevista reforçou a tese de que o crédito não deve ser tratado como mera relação privada, mas como atividade de inequívoco interesse público, fundamental para inclusão social e equilíbrio macroeconômico. Foram citados dados que demonstram a centralidade do crédito na economia brasileira, com volume superior a seis trilhões de reais e participação expressiva no PIB. Segundo o entrevistado, interpretações excessivamente individualistas da proteção de dados podem desorganizar o sistema econômico e prejudicar o próprio consumidor, ao reduzir acesso ao crédito e elevar custos.

Nesse contexto, a proteção ao crédito foi descrita como política estrutural de país, não limitada à negativação, mas abrangendo todo o ciclo do crédito: oferta e pré-aprovação, execução contratual, monitoramento e recuperação. Assim, a proteção ao crédito deve ser analisada como processo integrado e contínuo, e não como ato isolado vinculado apenas ao momento da concessão.

O entrevistado também apresentou críticas ao uso do legítimo interesse como fundamento central para atividades de crédito, apontando fragilidade jurídica no critério de “legítima expectativa do

titular", pela capacidade de ser excessivamente subjetivo e incompatível com a diversidade individual de percepções de privacidade. Além disso, destacou-se que o direito de oposição do titular, se aplicado amplamente ao crédito e antifraude, poderia fragilizar bancos de dados essenciais e gerar conflito permanente entre interesse coletivo e decisões individuais.

O entrevistado também abordou a relevância ao combate à fraude, apontando que a alta incidência de fraudes financeiras no Brasil exige bancos de dados sólidos, não apenas para proteção do mercado, mas também para proteção direta do titular, com destaque aos mais vulneráveis, que sofrem impactos desproporcionais e têm menor capacidade de reação jurídica. Foi reforçado que mecanismos antifraude evitam danos financeiros, negativação indevida e usurpação de identidade.

Sobre bancos de dados de proteção ao crédito, foi esclarecido que seu papel vai muito além da negativação: inclui validação cadastral, confirmação de identidade e prevenção de fraude na fase pré-contratual. O termo "negativação" foi considerado inadequado, pois os bancos de dados registram apontamentos informados por credores, sem validar o contrato ou o valor.

Em relação ao Cadastro Positivo, apontou-se que o modelo inicial *opt-in* demonstrou baixa adesão e evidenciou a limitada maturidade social brasileira em relação ao uso de dados. Também foram mencionadas fragilidades práticas, como dados desatualizados e ausência de obrigação efetiva de envio correto, além da percepção de lacunas regulatórias, considerando que o Banco Central apenas homologa e não fiscaliza de forma ampla.

No tema de escoragem, o score foi descrito como instrumento estatístico baseado em médias populacionais, incapaz de prever condutas individuais, devendo ser complementado por outras informações. Foi enfatizado que o problema central não é a existência do score em si, mas sim a qualidade, pertinência e proporcionalidade dos dados utilizados.

Quanto a dados excessivos, o entrevistado alertou que o conceito de "excesso" é impreciso e pode gerar insegurança jurídica. Foram citados exemplos como o CEP, considerado estatisticamente relevante por refletir realidade socioeconômica, e argumentou-se que ausência de dados suficientes pode gerar generalizações injustas, prejudicando bons pagadores.

Por fim, a entrevista destacou que maior disponibilidade de dados lícitos pode reduzir discriminações práticas ao permitir análises mais individualizadas. Também foi argumentado que, se a LGPD admite biometria para combate à fraude, não faria sentido restringir dados cadastrais menos invasivos. A visão final reafirmou que a proteção ao crédito é contínua, integrada e de interesse público, protegendo simultaneamente sociedade, credores e titulares, e que restrições excessivas ao uso de dados fragilizam o combate à fraude, aumentam custos e prejudicam a inclusão financeira.

- **Iagê Miola – Diretor da Agência Nacional de Proteção de Dados pessoais – 20/01/2026 – ANEXO IX**

O entrevistado indicou como ponto transversal a necessidade de um diagnóstico aprofundado das práticas efetivamente adotadas pelo mercado, especialmente quanto aos usos concretos de dados pessoais para proteção do crédito e prevenção à fraude. Segundo o entrevistado, o levantamento é essencial para evitar análises excessivamente abstratas, fundamentar discussões regulatórias futuras e permitir a construção de caminhos normativos pela ANPD mais aderentes à realidade operacional.

Foi reconhecida a dificuldade prática de separar, na operação cotidiana, as finalidades de proteção do crédito e prevenção à fraude, apontando convergência entre ambas. Ao mesmo tempo, destacou-se que existem limites jurídicos objetivos impostos pela LGPD, pois o legislador optou por separar expressamente as duas hipóteses legais. Assim, embora a prática de mercado tenda a integrar as finalidades, essa separação normativa não pode ser ignorada no esforço interpretativo.

Nesse contexto, foi salientado que a base legal de proteção do crédito não autoriza, por si só, o tratamento de dados pessoais sensíveis, sendo mais adequado que tais dados se enquadrem na hipótese legal de prevenção à fraude. A reflexão central proposta foi a necessidade de conciliar a realidade operacional do mercado com os limites jurídicos da legislação vigente.

No tema de decisões automatizadas e aprendizado de máquina, destacou-se que as questões levantadas pelo GT são centrais e refletem dilemas enfrentados pela ANPD na agenda regulatória sobre decisões automatizadas. A experiência do setor de crédito foi apontada como potencial fonte de exemplos concretos para subsidiar orientações regulatórias mais amplas, especialmente quanto ao equilíbrio entre necessidade de dados, prevenção de discriminação e governança de modelos.

Por fim, a entrevista reforçou que o combate a fraudes é um desafio sistêmico que exige cooperação institucional, envolvendo ANPD, Senacon, Banco Central e eventualmente Anatel. Foi destacado que respostas fragmentadas são insuficientes diante da sofisticação das práticas criminosas e que existe expectativa de fortalecimento de arranjos cooperativos já existentes.

- **Livia Vieira – Febraban – 29/01/2026 – ANEXO X**

A entrevistada ressaltou que a proteção do crédito deve ser compreendida como eixo estratégico do Sistema Financeiro Nacional, com impacto que ultrapassa a relação entre instituição e cliente. Trata-se de mecanismo estrutural para a estabilidade econômica e para a higidez do sistema financeiro, cujas restrições indevidas podem gerar efeitos sistêmicos, inclusive transnacionais. Ao mesmo tempo, destacou sua dimensão social, pois o uso adequado de dados permite crédito mais acessível, análises mais precisas, prevenção ao superendividamento e tratamento mais justo entre consumidores.

A entrevistada também destaca o conceito do ciclo de vida do crédito, enfatizando que a proteção não se limita à concessão inicial, mas abrange desde a oferta e pré-aprovação até o monitoramento, gestão de risco, renegociação e recuperação. Essa abordagem reforça a ideia de processo contínuo, e não de evento isolado, e integrando-se à prevenção a fraudes, à autenticação e à segurança cibernética, especialmente em um contexto de alta incidência de golpes no Brasil.

Outro ponto relevante diz respeito à necessidade de alinhamento entre proteção do crédito e regulação financeira prudencial. A entrevistada defende que eventuais orientações normativas da ANPD devem considerar a interdependência com o Banco Central e a CVM, sob pena de gerar impactos adversos à estabilidade do sistema.

Ademais, o papel dos dados alternativos na inclusão financeira também é destacado, ao permitir maior precisão estatística e análises individualizadas, especialmente para públicos com histórico bancário limitado, como jovens ou pessoas recém-inseridas no sistema financeiro, com observância dos princípios da LGPD, com ênfase em minimização, ética e prevenção de discriminação ilícita.

Como principal conclusão, defende-se que o tema deve ser tratado de forma sistêmica e equilibrada, evitando interpretações excessivamente restritivas que desconsiderem a complexidade operacional do setor e seus reflexos econômicos e sociais.

5. INSUMOS DAS ENTIDADES

O envio do ofício às entidades decorreu diretamente da necessidade de construção de diagnóstico técnico e regulatório consistente, de modo a garantir que o relatório final do GT5 fosse construído com base em evidências, experiências práticas e visões plurais[8] sobre o uso de dados pessoais no ecossistema de crédito e antifraude.

A amplitude das perguntas e o detalhamento dos tópicos reforçam que o propósito do ofício não se limitava à obtenção de opiniões genéricas, mas sim à consolidação de material técnico capaz de refletir a complexidade do setor e suas interseções com inovação tecnológica, risco sistêmico e direitos fundamentais.

As sínteses das demais respostas recebidas estão indicadas abaixo.

- **Associação Nacional dos Bureaus de Crédito (ANBC) – ANEXO XII**

[8] Foram contatadas 14 entidades: FEBRABAN, ANBIMA, ABBC, ABECS, Zetta, ANBC, Conexis Brasil Digital, ABIACOM, Brasscom, ABES, ABFintechs, ABRID, ANBI e o SERPRO.

Em suma, o posicionamento conclui que crédito e prevenção à fraude são pilares complementares do desenvolvimento socioeconômico, pois o crédito impulsiona inclusão financeira e crescimento econômico, enquanto a prevenção à fraude garante estabilidade, confiança e redução de custos sistêmicos.

Defende-se que dados pessoais são insumos indispensáveis tanto para análise e concessão responsável de crédito quanto para identificação de riscos e combate a fraudes, especialmente no contexto de digitalização massiva do sistema bancário.

Sustenta-se ainda que separar crédito e antifraude como finalidades distintas gera ineficiência e maior vulnerabilidade, sendo necessária abordagem integrada, com bases legais adequadas na LGPD, aplicação rigorosa de princípios (proporcionalidade, segurança e transparência) e governança robusta, inclusive para decisões automatizadas e uso de IA. Nesse sentido, a ANBC indica que "para obter esse equilíbrio seguem algumas diretrizes: (a) adoção da transparência por camadas; (b) implementação da intervenção humana ("human in the loop); (c) documentação interna robusta e governança algorítmica; (d) educação e conscientização interna."

- **Associação Brasileira das Empresas de Tecnologia em Identificação Digital (ABRID) – ANEXO XIII**

O documento sustenta, como conclusão central, que crédito e prevenção à fraude são dimensões indissociáveis da economia digital e da inclusão financeira no Brasil, pois ambos operam sobre os mesmos fluxos de risco e dependem de confiança e segurança para funcionarem de modo eficiente.

Também afirma que o tratamento de dados pessoais é estrutural e indispensável tanto para a concessão responsável de crédito quanto para a prevenção de fraudes, uma vez que apenas com dados completos (cadastrais, financeiros, comportamentais, biométricos e contextuais) é possível reduzir assimetrias informacionais, melhorar a precificação do risco e ampliar a oferta de crédito com menor inadimplência.

De acordo com a Associação, para assegurar governança robusta na concessão de crédito, o tratamento de dados deve ser analisado conforme cada etapa do fluxo, definindo-se a base legal adequada em cada momento:

a. Prospecção e pré-análise: fundamenta-se no legítimo interesse (art. 7º, IX, LGPD), permitindo uso de dados de prospectos e de fontes externas para ofertas e análises preliminares.
b. Processamento e formalização: aplica-se a base de procedimentos preliminares/execução de contrato (art. 7º, V) e, quando necessário, cumprimento de obrigação legal/regulatória (art. 7º, II), especialmente para atender exigências do Bacen e normas de PLD.

c. Análise de risco: utiliza-se a base de proteção ao crédito (art. 7º, X) para *scoring* e consultas a *bureaus*, além da hipótese do art. 11, II, "g", para tratamento de dados sensíveis (biometria) voltado à autenticação, prevenção à fraude e segurança do titular.

Com relação às atividades que podem ser tratadas conforme as bases legais, destaca-se para a proteção do crédito: "(a) Análise de risco/score de crédito, incluindo a modelagem de *credit scoring* que visa atribuir uma pontuação de risco a um titular com base em dados históricos de pagamentos e comportamento financeiro, e a avaliação de capacidade de pagamento, considerando a renda e os compromissos financeiros assumidos. (b) Gestão da Inadimplência, contando com a negativação de titulares devedores e consultas a bases de dados de terceiros para verificar débitos pendentes de um prospecto. (c) Prevenção ao superendividamento, mediante análise contínua de comportamento financeiro do cliente para identificar sinais de insolvência e evitar concessão de novos créditos que possam comprometer a subsistência do titular analisado. (d) Gestão do Cadastro Positivo, com o processamento das obrigações financeiras liquidadas ou em andamento para formar o histórico de bom pagador. (e) Localização de devedores e atividades de cobrança (fase pré-judicial): considerando que crédito não se resume ao momento da concessão, mas sim compreende a concessão, a manutenção e a recuperação, localizar um titular devedor é uma etapa intrínseca à proteção da operação de crédito efetuada. Além disso, a localização do devedor permite a notificação do titular antes de uma negativação formal, conforme o CDC." (p. 9)

E para a prevenção à fraude, indica-se que: "(a) Legítimo Interesse (art. 7º, IX, LGPD), para proteção do patrimônio e segurança da plataforma do Controlador. (b) Cumprimento de Obrigação Legal ou Regulatória (art. 7º, II, LGPD), para cumprir as exigências legais e regulatórias definidas pelo BACEN, CVM ou COAF. (c) Execução de Contrato ou procedimentos preliminares relacionados a contrato (art. 7º, V, LGPD), para garantir que a transação solicitada pelo titular seja legítima. (d) Garantia da Prevenção à Fraude e Segurança do Titular (art. 11, II, "g", LGPD), para proteger o titular de ter seus dados utilizados por terceiros. (e) Exercício regular de direitos, inclusive em contrato e em processos judiciais, administrativos e arbitrais (art. 7º, VI e art. 11, II, "d", LGPD), na proteção jurídica do Controlador" (p.10).

O texto também conclui que a subutilização de dados pessoais fragiliza o sistema, pois impede análises contextuais, aumenta *chargebacks*, favorece fraudes sofisticadas (como fraude sintética) e eleva custos operacionais, levando a maior restrição de crédito e risco sistêmico. No plano regulatório, o posicionamento defende que a LGPD não impede, mas legitima o tratamento de dados para essas finalidades, desde que amparado em bases legais adequadas (proteção do crédito, obrigação legal/regulatória, execução de contrato, legítimo interesse e hipóteses para dados sensíveis como biometria), com ênfase no interesse público, na estabilidade financeira e na segurança do titular

Por fim, expõe-se que o avanço do crédito digital e do antifraude exige governança robusta, controles técnicos e *accountability*, com transparência proporcional (sem comprometer segurança e segredos de negócio), políticas de retenção e auditoria, além de critérios de explicabilidade e mitigação de vieses em decisões automatizadas e uso de IA.

- **Associação Nacional dos Bureaus de Informação (ANBI) – Anexo XIV**

A Associação defende uma interpretação sistêmica, teleológica e economicamente informada da LGPD sobre proteção ao crédito e prevenção à fraude, sustentando que ambas são atividades contínuas, integradas e de interesse público. A Associação afirma que o crédito é instrumento estruturante do desenvolvimento socioeconômico, essencial para consumo, investimento, empreendedorismo e inclusão financeira, especialmente para as classes mais vulneráveis. Além disso, também sustenta que restringir o uso de dados pessoais nesse contexto tende a gerar efeitos regressivos: encarecimento do crédito, retração da oferta e ampliação da exclusão financeira

Em seu posicionamento, a ANBI também enfatiza que a prevenção à fraude é indissociável da proteção ao crédito, pois fraudes elevam custos sistêmicos, aumentam juros, reduzem liquidez e prejudicam diretamente os titulares (endividamento indevido, negativação injusta e perda de identidade). Assim, limitar dados e ferramentas antifraude não protege o consumidor, mas amplia sua vulnerabilidade.

A ANBI defende que dados pessoais são o insumo central do ecossistema de crédito, necessários para reduzir assimetrias informacionais, melhorar modelos de risco, evitar concessões irresponsáveis e prevenir superendividamento, destacando o papel do Cadastro Positivo como mecanismo de eficiência e inclusão. No campo antifraude, argumenta que dados comportamentais, metadados e biometria são essenciais para combater fraudes modernas e validar identidade em ambientes digitais, e que sua subutilização gera aumento de fraudes sintéticas, *chargebacks* e decisões erradas (bloqueios indevidos ou permissividade excessiva).

Com relação ao cenário internacional, afirma-se que regimes do GDPR e da CCPA “também reconhecem a prevenção à fraude e a segurança como finalidades legítimas e essenciais, justamente porque a restrição desproporcional a esses mecanismos tende a aumentar danos reais ao consumidor e instabilidade econômica. A conclusão é objetiva: a prevenção à fraude não é um “uso tolerado” de dados pessoais, mas atividade essencial de interesse público e econômico, indispensável para a proteção da identidade do titular, para a segurança jurídica das contratações e para a sustentabilidade do ecossistema de crédito ao longo de todo o seu ciclo”.

Defende-se que a base legal da proteção ao crédito (art. 7º, X) deve ser interpretada de forma ampla para cobrir todo o ciclo do crédito (pré-contratação, concessão, monitoramento, renegociação e

cobrança), com bases complementares como obrigação legal/regulatória e legítimo interesse. Para prevenção à fraude, invoca também hipóteses do art. 11 para dados sensíveis, especialmente biometria.

Por fim, afirma que transparência e explicabilidade devem ser funcionais e proporcionais, preservando o segredo empresarial, citando jurisprudência do STJ sobre *scoring*, e recomenda governança robusta com frameworks como ISO e NIST, políticas de retenção, logs, auditoria, *accountability* e revisão humana em decisões automatizadas e IA.

- **Federação Brasileira de Bancos (Febraban) e Associação Brasileira das Empresas de Cartões de Crédito e Serviços (ABECS) – ANEXO XV**

Ambas as instituições sustentam que a discussão sobre proteção ao crédito e prevenção à fraude deve partir de uma compreensão estrutural do funcionamento do ecossistema financeiro e comercial, especialmente diante da intensificação das operações digitais. O tratamento de dados pessoais é elemento indispensável para a sustentabilidade desse sistema, sendo necessário que a aplicação da LGPD considere as especificidades do setor e os impactos econômicos e sociais decorrentes de interpretações excessivamente restritivas.

No campo socioeconômico, o posicionamento conjunto defende que o crédito representa um dos principais instrumentos de desenvolvimento nacional, pois viabiliza investimentos, expansão de empresas, geração de empregos e acesso das famílias a bens e serviços essenciais, como moradia e educação. Além disso, o crédito é descrito como ferramenta de inclusão financeira, com papel relevante na formalização econômica e na ampliação de oportunidades em regiões e grupos historicamente excluídos do sistema bancário, contribuindo diretamente para liquidez e estabilidade do mercado.

Paralelamente, enfatiza-se que a prevenção à fraude não constitui atividade secundária, mas sim um vetor estratégico de preservação da confiança e da segurança no ambiente digital. Em um cenário de crescente digitalização, fraudes são tratadas como riscos sistêmicos capazes de afetar consumidores, instituições e a economia como um todo, razão pela qual a atuação preventiva, apoiada em tecnologia e monitoramento comportamental, é considerada essencial para assegurar a sustentabilidade do sistema financeiro e incentivar a continuidade da inovação.

Sob a perspectiva da governança de dados, defende-se que dados pessoais são insumos centrais para a proteção ao crédito, pois permitem avaliações mais precisas de perfil e capacidade de pagamento,

além de viabilizarem a precificação adequada do risco e a prevenção à inadimplência. Ressalta-se que a coleta e o tratamento responsável de informações como histórico de pagamentos, renda, CPF, restrições cadastrais e score de crédito reduzem assimetrias informacionais e aumentam a eficiência do mercado, favorecendo decisões mais justas, personalizadas e alinhadas à inclusão financeira.

No âmbito da prevenção à fraude, o posicionamento destaca que o tratamento de dados como biometria, metadados e dados comportamentais é indispensável para autenticação, validação de identidade e detecção de padrões suspeitos em tempo real. Sustenta-se que a integração dessas camadas informacionais fortalece mecanismos antifraude e reduz vulnerabilidades associadas a engenharia social e fraude sintética. Nesse sentido, a restrição indevida desses dados seria prejudicial não apenas às instituições, mas também aos próprios titulares, que ficam mais expostos a ilícitos e prejuízos financeiros.

Também é afirmado que subutilizar dados pessoais em processos antifraude tende a produzir consequências práticas relevantes, como aumento de *chargebacks*, elevação de custos operacionais, perda de liquidez e expansão de golpes baseados em falsidade ideológica. Além disso, tais limitações podem gerar riscos sistêmicos, incluindo perda de confiança no sistema financeiro, maior inadimplência e danos reputacionais, o que reforça a necessidade de uso eficiente e proporcional de dados em conformidade com a LGPD e com normas setoriais.

Argumenta-se que ambas as atividades (proteção ao crédito e prevenção à fraude) compartilham os mesmos fluxos, dados e tecnologias, pois os mecanismos utilizados para avaliação de risco e concessão de crédito são os mesmos que subsidiam processos de validação e detecção de ilícitos. Dessa forma, separar essas finalidades como trilhas independentes produziria inconsistências, redundâncias, aumento de burocracia e enfraquecimento da resposta institucional a ameaças emergentes, prejudicando a experiência do consumidor e a eficiência do mercado. E, de maneira exemplificativa, são citadas algumas atividades como: análise de crédito; concessão de crédito; gestão do risco de crédito; bancos de dados de proteção ao crédito; modelagem estatística e score de crédito; concessão e gestão de financiamentos, empréstimos e cartões; recuperação de crédito; e cessão de crédito.

Nesse sentido, defende-se a interpretação ampla da base legal de proteção ao crédito, ressaltando que ela não se restringe a cadastros negativos ou positivos, mas abrange todas as atividades necessárias ao ciclo de vida do crédito, incluindo análise, concessão, monitoramento, score, recuperação, cessão e gestão de risco. Além disso, reconhece que outras bases legais podem ser aplicadas de forma complementar, como execução de contrato, cumprimento de obrigação legal/regulatória, legítimo interesse e consentimento, a depender do contexto e da finalidade concreta do tratamento.

Quanto à prevenção à fraude, aponta-se que a LGPD autoriza o tratamento de dados pessoais e sensíveis com fundamento em múltiplas hipóteses legais, destacando-se a obrigação legal/regulatória, o legítimo interesse e a hipótese específica do art. 11, II, "g", para uso de biometria e autenticação em sistemas eletrônicos. Nesse enquadramento, a prevenção à fraude é tratada como finalidade que atende ao interesse público, pois preserva a confiança no mercado e protege o patrimônio de cidadãos e instituições, desde que observados princípios de proporcionalidade, transparência e respeito aos direitos fundamentais.

Por fim, expõe-se que a efetividade desse modelo depende de governança e segurança robustas, recomendando a adoção de frameworks reconhecidos (como ISO e NIST), controles técnicos e administrativos, auditorias periódicas, gestão de logs e políticas de retenção alinhadas à legislação. No campo de decisões automatizadas e inteligência artificial, sustenta-se que o setor já opera com scores e modelos de machine learning para crédito e antifraude, sendo importante manter explicabilidade, rastreabilidade e mitigação de vieses, sem que a transparência comprometa segredos comerciais ou a eficácia dos sistemas de proteção.

- **Zetta – ANEXO XVI**

Em síntese, a Zetta parte da premissa de que crédito, prevenção à fraude e tratamento de dados pessoais são dimensões estruturalmente interligadas, e que a governança regulatória deve reconhecer essa interdependência para garantir eficiência econômica, segurança jurídica e proteção efetiva dos titulares.

No plano socioeconômico, sustenta-se que o crédito é pilar essencial do desenvolvimento brasileiro, pois impulsiona consumo, investimento, inovação e inclusão financeira, além de contribuir para redução de desigualdades regionais. A Zetta enfatiza que a transformação digital do sistema financeiro ampliou drasticamente o acesso a serviços financeiros e permitiu incorporar novos grupos ao mercado, inclusive aqueles historicamente excluídos por ausência de histórico bancário. Nesse cenário, a oferta de crédito eficiente e inclusiva depende diretamente do uso proporcional de dados pessoais ao longo de todo o ciclo da relação creditícia.

Também se defende que a prevenção à fraude é componente estrutural da gestão do risco de crédito, uma vez que fraudes elevam inadimplência, distorcem a precificação, aumentam custos operacionais e pressionam spreads bancários, afetando inclusive bons pagadores. Fraude, portanto, não é tratada como uma finalidade isolada, mas como variável diretamente ligada à solvência das operações e à estabilidade do sistema. A Zetta argumenta que fragilizar mecanismos antifraude por insegurança jurídica ou limitação indevida de dados tende a gerar efeitos adversos relevantes, como exclusão financeira e encarecimento generalizado do crédito.

Assim, os dados pessoais são insumo indispensável para reduzir assimetrias informacionais, calibrar modelos de risco e promover maior liquidez no mercado. A associação diferencia dados tradicionais (histórico de crédito, birôs e SCR) de "informações relevantes" (dados cadastrais, comportamentais e digitais), defendendo que ambos são necessários para decisões mais justas e eficientes. A proteção ao crédito é descrita como um fluxo contínuo, que vai muito além do score, abrangendo prospecção responsável, verificação de identidade (KYC), avaliação e monitoramento do risco, prevenção ao superendividamento, cobrança e recuperação. Neste sentido, compartilha a seguinte tabela:

Fluxo da proteção ao crédito					
Pré-aplicação	**Cadastro e autenticação (KYC/AML)**	**Avaliação do risco de inadimplência**	**Monitoramento do desempenho do crédito**	**Prevenção ao superendividamento**	**Cobrança e recuperação de crédito**
Direcionamento de ofertas adequadas ao perfil do consumidor Evita concessão irresponsável e garante cumprimento de regras de suitability	Verificação de identidade Prevenção de fraudes, uso de documentos falsos, e identidade de terceiros	Modelagem de risco mais ampla que o score Análise de renda, comportamento, contexto e exposição total	Identificação da deterioração da qualidade creditícia Revisões periódicas exigidas pelas normas prudenciais do BCB	Avaliação contínua do comprometimento de renda Cumprimento da Lei do Superendividamento e do CDC	Planejamento de estratégias de cobrança Estimativa de perdas esperadas Recuperação de ativos problemáticos

Fonte: Zetta, 2026, p. 7.

No eixo da prevenção à fraude, a Zetta destaca que o tratamento de dados comportamentais, metadados e biometria tornou-se essencial diante da sofisticação do crime digital, com uso de *deepfakes*, identidades sintéticas e automação criminosa. Defende-se que o combate eficaz exige múltiplas camadas de validação e análise em tempo real, com apoio de inteligência artificial e machine learning. O documento argumenta que restringir tais dados aumenta riscos como *chargebacks*, falsidade ideológica e ataques coordenados, comprometendo não apenas as instituições financeiras, mas também a proteção direta do titular contra roubo de identidade e danos patrimoniais.

Ademais, a Zetta entende que proteção ao crédito e prevenção à fraude compartilham fluxos, dados e objetivos, pois ambas operam sobre o mesmo evento econômico: a solvência da obrigação financeira. A separação rígida dessas finalidades seria artificial e contraproducente, pois aumentaria

fricção, inconsistência decisória, duplicação de custos e vulnerabilidades sistêmicas. Em contraste, a integração permitiria governança mais eficiente, modelos mais robustos e decisões mais coerentes, em linha com padrões prudenciais como Basileia e exigências do Banco Central.

Do ponto de vista jurídico, a Zetta sustenta que a base legal da proteção ao crédito (art. 7º, X, LGPD) deve ser interpretada de modo amplo, abrangendo todo o ciclo de vida do crédito e não apenas a análise pontual de inadimplência no momento da contratação. Defende-se que essa base legal legitima atividades como prospecção responsável, *onboarding*, monitoramento contínuo, cobrança, recuperação e tratamentos indissociáveis como autenticação e validação de identidade. O documento ainda aponta a aplicação complementar de outras bases legais, como execução de contrato, obrigação legal/regulatória, legítimo interesse e o art. 11, II, "g" para dados sensíveis em autenticação e antifraude.

No campo principiológico, argumenta-se que proporcionalidade e necessidade não podem ser definidas por listas rígidas *ex ante*, mas devem ser avaliadas conforme a finalidade concreta e a evidência empírica da utilidade do dado. A Zetta defende uma regulação orientada a resultados e impactos, com governança, documentação e auditoria, evitando soluções prescritivas que cristalizem ineficiências e reduzam a capacidade do setor de responder à evolução tecnológica e ao dinamismo das fraudes. Quanto à transparência, propõe-se uma noção de transparência funcional, centrada na compreensão do impacto pelo titular e na garantia de contestação, sem exigir a exposição integral de modelos ou parâmetros internos. Portanto, sustenta-se que a abertura excessiva favorece engenharia reversa e aumenta o risco de manipulação ("gaming"), prejudicando a segurança e a competitividade. Assim, a explicabilidade deve focar no que é significativo ao titular, preservando segredos comerciais e a efetividade dos sistemas antifraude e de *scoring*.

Por fim, a Zetta recomenda governança robusta baseada em frameworks internacionais e prudenciais, destacando Basileia, COSO ERM, ISO 31000, ISO 27001/27701, NIST AI RMF e o modelo de "três linhas de defesa". No âmbito de decisões automatizadas e IA, defende-se supervisão humana contínua ("human-on-the-loop"), validação independente, monitoramento de vieses e auditorias recorrentes, argumentando que exigir revisão humana caso a caso é inviável e pode reduzir eficiência e inclusão financeira. O documento conclui que uma interpretação sistemática da LGPD, aliada à governança técnica adequada, fortalece a segurança do ecossistema digital, reduz custos, aumenta concorrência e contribui para um mercado de crédito mais justo e inclusivo no Brasil.

6. REUNIÕES

Foram realizadas diversas reuniões ordinárias e extraordinárias do GT5. As atas de todas as reuniões foram encaminhadas à Secretaria-Geral para fins de transparência e arquivo.

7. PARECER CONCLUSIVO

Diante de todo o trabalho exposto e consignado neste Relatório Final e respectivos anexos, **o GT 5 do CNPD aprova os seguintes subsídios**, na temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD).

Respostas aos quesitos:

1) A importância socioeconômica do crédito e da prevenção à fraude para o Brasil

1. **Qual é a relevância do crédito para o desenvolvimento socioeconômico do Brasil?**

O crédito constitui instrumento estruturante do desenvolvimento econômico e social. Ele viabiliza consumo, investimento, financiamento da produção, expansão empresarial e geração de empregos, além de permitir a gestão de liquidez por famílias e empresas ao longo de seu ciclo de vida financeiro. Na prática, possibilita a aquisição de moradia, acesso à educação e saúde, compra de bens duráveis, capital de giro, inovação e expansão produtiva.

Nesse contexto, interpretações que inviabilizem análises técnicas adequadas na concessão e na precificação do crédito tendem a produzir efeitos macroeconômicos relevantes, como retração do crédito produtivo, aumento das taxas, redução de investimentos e ampliação da exclusão financeira, comprometendo o funcionamento eficiente da atividade econômica.

O crédito também possui dimensão distributiva e inclusiva. Em um país marcado por desigualdades regionais e sociais, a ampliação do acesso a produtos financeiros formais reduz a dependência de mecanismos informais mais caros e menos seguros, favorece a bancarização e fortalece a cidadania econômica.

Nesse cenário, o tratamento de dados pessoais para finalidades relacionadas à concessão e proteção do crédito contribui para reduzir assimetrias de informação, como evidenciado por iniciativas como o Cadastro Positivo e o Open Finance, ampliando a competitividade, aprimorando a avaliação de risco e possibilitando condições mais eficientes de financiamento, com potencial redução de juros e estímulo ao crescimento sustentável do mercado.

Por essas razões, a proteção ao crédito não deve ser compreendida apenas como interesse privado de credores, mas como componente de interesse público ligado à estabilidade do sistema financeiro, à estabilidade econômica, à mobilidade social, à eficiência econômica e à própria proteção do

consumidor, na medida em que um mercado de crédito saudável tende a oferecer condições mais compatíveis com o risco real, maior concorrência e menor custo agregado.

2. Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

A prevenção à fraude deve ser compreendida como atividade essencial de inequívoco interesse público, indispensável à estabilidade financeira, à proteção dos consumidores e ao desenvolvimento socioeconômico. Trata-se de componente estrutural da gestão de riscos no sistema financeiro. Em sentido amplo, abrangendo os setores bancário, de capitais, securitário e previdenciário, mas também em diversos outros setores da economia, como varejo, saúde e serviços públicos.

Sob a perspectiva econômica, a fraude não constitui evento isolado. Quando ocorre em escala, gera perdas sistêmicas que elevam custos operacionais e de produtos, ampliam provisões, aumentam spreads e tarifas e restringem a oferta de crédito. Tais efeitos acabam sendo absorvidos e redistribuídos no mercado, impactando especialmente consumidores e empresas que atuam de forma regular.

Ao proteger patrimônio, identidade e reputação dos cidadãos, evitando golpes, roubo de identidade e endividamento indevido, contribui para a preservação da confiança nas relações econômicas e para a proteção material do indivíduo e consumidor.

Esse papel torna-se ainda mais relevante em um contexto de intensa digitalização dos serviços financeiros e das relações de consumo. A integridade e a segurança das transações constituem condição para a adoção segura de soluções como *onboarding* digital, Pix, Open Finance e contratação remota, que ampliam acesso a serviços financeiros e digitais e favorecem a inclusão econômica.

Nesse cenário, o tratamento de dados pessoais para fins de prevenção à fraude representa instrumento técnico essencial para reduzir assimetrias de informação, detectar comportamentos suspeitos e mitigar riscos operacionais e financeiros. O enfraquecimento desses mecanismos, por interpretações excessivamente restritivas sobre o uso de dados, não elimina os riscos existentes; ao contrário, tende a ampliá-los e a redistribuí-los de forma regressiva, com aumento de custos, restrição de acesso ao crédito e maior exposição dos próprios consumidores a práticas fraudulentas.

Por essas razões, a prevenção à fraude deve ser reconhecida como vetor estratégico para o desenvolvimento socioeconômico do Brasil, na medida em que fortalece a confiança nas relações econômicas, protege direitos, reduz perdas sistêmicas e contribui para a estabilidade, eficiência e sustentabilidade do sistema financeiro e do mercado como um todo.

2) Papel dos dados pessoais no ecossistema de crédito

1. **Qual a importância dos dados pessoais para proteção do crédito e demais atividades relacionadas ao tema?**

Os dados pessoais são essenciais para a proteção do crédito uma vez que viabilizam a gestão adequada, responsável e contínua do risco de crédito ao longo de todo o ciclo de vida da relação creditícia. São, portanto, insumo técnico central e condicionante do ecossistema de crédito: sem tratamento diversificado e estruturado de dados pessoais, a concessão e proteção do crédito tende a se aproximar de exercício de especulação, incompatível com almejada previsibilidade e proteção efetiva do cidadão.

Dados pessoais bem tratados viabilizam identificar corretamente o titular, estimar capacidade de pagamento, mensurar inadimplência esperada, definir limites, taxas, garantias e acompanhar a evolução do risco ao longo de toda a relação. Sem dados cadastrais, financeiros, históricos e comportamentais, a concessão e proteção de crédito seria pouco robusta e precisa.

Isto reflete-se no estudo do Banco Central do Brasil (BCB) sobre os efeitos do Cadastro Positivo, no qual demonstra que quando o mercado dispõe de dados pessoais completos, como cadastrais e comportamentais, o crédito cresce, o *spread* cai e, consequentemente, bilhões de reais adicionais podem ser injetados na economia brasileira de forma assertiva e sustentável[9]. Birôs de crédito e cadastros positivos, ao consolidar históricos de pagamento, ampliam a base de informação e permitem inclusão de consumidores antes “invisíveis”, o que aumenta a taxa de bancarização e o acesso a financiamentos para consumo, habitação e capital de giro[10].

Vejamos alguns exemplos:

[9] Análise dos efeitos do Cadastro Positivo. [s.l: s.n.]. Disponível em: Análise dos efeitos do Cadastro Positivo. Acesso em: 6 jan. 2026.
[10] CNN Brasil. Mais de 13 milhões de pessoas entraram no cadastro positivo desde 2020, aponta Serasa. Disponível em: . Acesso em: 5 jan. 2026.

- Avaliação de risco e capacidade de pagamento: dados cadastrais e histórico financeiro suportam decisões de concessão, limites, preço e garantias.
- Oferta responsável e prevenção ao superendividamento: calibragem de produto/limite à realidade do cliente, com adequação.
- Gestão do ciclo de vida: monitoramento, renegociação, cobrança e recuperação de crédito dependem de sinais de risco e consistência cadastral.
- Integridade cadastral (KYC): validações reduzem concessões indevidas e suportam prevenção a ilícitos correlatos.

Ou seja, o tratamento de dados pessoais não se limita ao momento da concessão, pois também sustentam etapas de pré-análise, elegibilidade, modelagem estatística, monitoramento, revisão de limites, renegociação, cobrança e recuperação. O tratamento adequado dos dados pessoais reduz assimetrias informacionais, favorece inclusão de consumidores antes invisíveis ao sistema, melhora a precificação e reduz o risco de concessões incompatíveis com a realidade financeira do titular dos dados. Por isso, a interpretação da LGPD no contexto creditício deve preservar essa funcionalidade sistêmica, sempre com observância aos princípios da LGPD.

Eventual restrição ao uso de dados pessoais no contexto do crédito não aumenta a proteção do titular. Ao contrário, produz efeitos opostos: elevação do custo do crédito, endurecimento de políticas de concessão, aumento da exclusão financeira e fortalecimento de alternativas informais mais onerosas e menos seguras.

Por essa razão, os dados pessoais devem ser compreendidos como alicerce técnico da proteção ao crédito. Seu tratamento, quando realizado de forma proporcional, transparente, segura e aderente às finalidades legítimas, protege simultaneamente o sistema financeiro, o mercado e o próprio titular, promovendo crédito mais justo, inclusivo e sustentável. A interpretação da LGPD, nesse contexto deve preservar essa funcionalidade, conciliando proteção de dados, segurança jurídica e desenvolvimento socioeconômico.

2. **Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?**

O uso qualificado de dados pessoais reduz assimetrias informacionais ao permitir que o mercado diferencie, com maior precisão, perfis de risco heterogêneos que, sem informação suficiente, tenderiam a ser tratados de forma uniforme. Quando há melhor visibilidade sobre histórico de pagamento, consistência cadastral, renda, comprometimento financeiro e comportamento de adimplemento, há maior capacidade de distinguir bons e maus riscos, reduzindo riscos.

A redução de assimetrias informacionais decorre da capacidade de estimar risco de modo mais granular, com três efeitos econômicos principais. Primeiro, aumenta a liquidez, pois mais pessoas e empresas se tornam elegíveis a operações antes inviabilizadas pela incerteza. Segundo, reduz inadimplência, na medida em que a concessão se torna mais aderente à capacidade de pagamento e à exposição efetiva ao risco. Terceiro, eleva a eficiência do mercado, porque reduz perdas esperadas, melhora a alocação de capital, favorece concorrência e pode contribuir para spreads mais compatíveis com o risco real. Em sentido oposto, restringir o tratamento de dados amplia a opacidade informacional, encarece o crédito e reforça a exclusão financeira. Essa eficiência, contudo, exige contrapesos de governança e privacidade, com qualidade, segurança e mecanismos de transparência.

3) Papel dos dados pessoais na prevenção à fraude e outros ilícitos

1. **Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?**

A utilização de dados pessoais constitui elemento estrutural e indispensável das estratégias de prevenção à fraude, repressão a ilícitos e gestão de risco no sistema financeiro digital e na economia contemporânea. Em um ambiente marcado pela digitalização intensiva dos serviços financeiros, do comércio e de tantas atividades (inclusive a utilização de serviços governamentais), a capacidade de verificar identidades, monitorar comportamentos e identificar anomalias em tempo real depende do tratamento qualificado de um conjunto amplo de dados, que não se limita a informações cadastrais básicas.

As fraudes modernas são, em grande medida, de identidade, de comportamento e de engenharia social. Assim, dados pessoais são indispensáveis para identificação e validação do titular, detecção de inconsistências cadastrais e transacionais, indícios de falsidade ideológica, uso indevido de dados de terceiros e simulação/manipulação de perfis. Sem isso, não há contratação segura, crédito legítimo, tão pouco proteção jurídica mínima do mercado. A subutilização desses dados “cega” o sistema para o risco e amplia perdas e danos aos próprios titulares.

Essa importância é ainda mais evidente em setores regulados, nos quais o tratamento de dados pessoais é essencial para o cumprimento das obrigações regulatórias de *Know your client* (KYC) e de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/CFT).

Dados cadastrais, documentais e biométricos são fundamentais para mitigar riscos de falsidade ideológica, enquanto o uso de informações complementares e metadados, como endereço de IP, geolocalização, características dos dispositivos e padrões comportamentais, permitem identificar

inconsistências e sinais de fraude, com mudanças abruptas de localização ou uso de dispositivos atípicos.

A incorporação de técnicas de inteligência artificial e machine learning potencializa esse processo ao viabilizar a análise de volume relevante de dados transacionais e comportamentais, permitindo a detecção de anomalias e padrões ilícitos que seriam imperceptíveis à análise humana. Esses mecanismos são fundamentais para a identificação de fraudes em pagamentos, lavagem de dinheiro, financiamento ao terrorismo e ataques cibernéticos estruturados, inclusive aqueles baseados em engenharia social e cooptação de colaboradores.

Neste sentido, verifica-se iniciativas do Ministério da Justiça e Segurança Pública, como o programa "Celular Seguro" e os acordos firmados no âmbito da Aliança de Combate a Fraudes Bancárias Digitais, reconhecem expressamente o tratamento de dados pessoais para fins de segurança e prevenção a fraudes como matéria de ordem e interesse públicos, orientado à proteção do cidadão e do interesse coletivo. Tais iniciativas se estruturam sobre pilares com o aprimoramento contínuo dos mecanismos de prevenção, o compartilhamento responsável de dados entre agentes públicos e privados, o suporte às investigações, a capacitação institucional, e a promoção do letramento digital.

Em convergência, o Banco Central do Brasil, por meio da Resolução Conjunta nº 6/23, avançou na implementação, pelas instituições do Sistema Financeiro Nacional, de outros mecanismos estruturados de prevenção, detecção e mitigação de fraudes, incorporando essas medidas à governança corporativa, à gestão de riscos e à segurança operacional.

Diante disso, os dados pessoais são a base para identificar quem é o titular, distinguir comportamentos legítimos de ilícitos e responsabilização; sem esse uso, a prevenção à fraude se torna ineficaz, aumentando riscos, custos e impactos negativos para todo o sistema e para os próprios titulares.

2. **Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos?**

Dados comportamentais, biométricos e metadados contribuem justamente para distinguir operações legítimas de tentativas de fraude por meio de comparação, correlação e validação, incluindo o uso estritamente necessário de dados sensíveis (como biometria) para prevenção à fraude e segurança do titular, com salvaguardas reforçadas. Dados comportamentais, biométricos e metadados permitem avaliar não apenas "quem" é o titular, mas "como", "de onde" e "em que contexto" ele interage com o sistema. Os dados comportamentais ajudam a identificar desvios de padrão, automação indevida, coerção e sinais de engenharia social; os biométricos fortalecem autenticação, prova de vida e verificação de identidade; e os metadados (como IP, dispositivo, geolocalização,

horário, rede e características da sessão) fornecem contexto essencial para detectar inconsistências, fraudes sintéticas e uso indevido de credenciais.

A integração dessas camadas amplia substancialmente a capacidade preditiva dos sistemas antifraude, reduz falsos negativos e melhora o controle de falsos positivos, permitindo respostas mais proporcionais, como *step-up authentication*, bloqueio preventivo, revisão manual ou monitoramento reforçado. Em ambiente digital complexo e dinâmico, esses dados são essenciais para atuação em tempo real e para a construção de trilhas auditáveis que apoiem investigação, contestação e responsabilização posterior.

Nesse contexto, é importante reconhecer que o legítimo interesse pode servir de fundamento jurídico para atividades de prevenção à fraude quando envolver dados pessoais não sensíveis[11], especialmente em hipóteses de monitoramento de padrões, detecção de anomalias e verificação de inconsistências cadastrais, desde que observados os requisitos de necessidade, proporcionalidade e transparência. Contudo, quando a prevenção à fraude demanda o uso de dados sensíveis, como biometria para autenticação reforçada, o sistema jurídico exige base legal específica e salvaguardas adicionais, justamente porque o grau de risco aos direitos do titular pode ser superior. Por isso, a existência de base legal própria voltada à segurança do titular e à prevenção de ilícitos revela-se fundamental para conferir maior estabilidade e segurança jurídica ao tratamento, evitando que atividades estruturais e recorrentes fiquem dependentes exclusivamente de uma hipótese aberta e sujeita a testes casuísticos de balanceamento, como ocorre no legítimo interesse.

No direito comparado, essa compreensão é amplamente consolidada, como trazido na *General Data Protection Regulation* (GDPR) o qual admite-se o uso de dados biométricos para fins de segurança e prevenção à fraude quando necessário e proporcional, sendo prática corrente em sistemas financeiros europeus o uso de biometria facial para onboarding digital e validação de identidade, inclusive sob supervisão das autoridades de proteção de dados. Países como Reino Unido, Espanha e Alemanha utilizam biometria facial em processos de verificação remota de identidade no setor financeiro, com base em orientações da *European Banking Authority* (EBA) e autoridades nacionais de proteção de dados.

Nos Estados Unidos, sob a *California Consumer Privacy Act* (CCPA) e normas setoriais financeiras, o uso de biometria e dados comportamentais para prevenção à fraude e segurança é amplamente admitido, sendo prática comum em bancos, fintechs e bureaus de crédito, desde que observados limites claros de finalidade, retenção e segurança. Em todos esses ordenamentos, parte-se do

[11] A respeito, ver: Data Privacy Brasil. O legítimo interesse na LGPD: quadro geral e exemplos de aplicação Texto de Discussão 01/2021. 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/10/O-legitimo-interesse-na-LGPD.pdf.

reconhecimento de que fraudes financeiras não podem ser combatidas com instrumentos analógicos em um ambiente digital.

3. **Quais são os riscos de subutilizar dados pessoais em processos antifraude (ex.: aumento de chargebacks, fraude sintética, falsidade ideológica e riscos sistêmicos)?**

A subutilização de dados pessoais fragiliza a capacidade de prevenção, detecção e resposta a eventos fraudulentos. Entre os riscos mais evidentes estão o aumento de *chargebacks* e de outros tipos de perdas financeiras, maior incidência de fraude sintética e golpes, abertura de contas com identidade falsa, concessão de crédito indevida, compra de produtos indevida, falsidade ideológica, *spoofing* biométrico e crescimento de perdas operacionais e reputacionais.

Além disso, o enfraquecimento dos controles antifraude gera efeitos sistêmicos: eleva custos de conformidade e de recuperação, encarece produtos e serviços, reduz a confiança em canais digitais e induz maior seletividade na concessão de crédito. Em termos práticos, os prejuízos decorrentes da subutilização de dados não recaem apenas sobre as instituições, mas sobre todo o mercado e, em especial, sobre titulares legítimos, que passam a enfrentar mais fricção, maior custo e menor acesso.

4) Convergência entre proteção ao crédito e prevenção à fraude

1. **O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?**

Os tratamentos envolvendo crédito e fraude compartilham dados, sistemas e decisões, uma vez que ambos avaliam o mesmo risco econômico, a solvabilidade da operação, de modo que separar essas análises fragmenta a gestão de risco e reduz a eficácia do modelo.

- Eventos e dados comuns: *onboarding*, alterações cadastrais, comportamento transacional e relacionamento alimentam crédito e antifraude.
- Objetivo convergente: mensurar e mitigar risco (inadimplência vs. perda por ilícito), preservando solvência, confiança e precificação correta.
- Infraestrutura compartilhada: KYC, cadastros, motores de decisão, trilhas de auditoria e governança de modelos tendem a ser comuns.

Há, portanto, forte convergência funcional entre essas atividades. Separá-las desconsidera a realidade operacional do mercado e reduz a eficiência dos controles.

No plano internacional, essa convergência é amplamente reconhecida. Tanto o GDPR quanto a CCPA partem da premissa de que avaliação de risco, segurança, integridade de transações financeiras e

prevenção à fraude integram um mesmo contexto funcional, legitimando o uso proporcional de dados pessoais para essas finalidades.

A LGPD, por ter uma base legal específica para a proteção ao crédito, adotou solução ainda mais clara e adequada à realidade nacional, reconhecendo expressamente a natureza sistêmica e contínua dessas atividades.

2. **Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?**

Tratar as finalidades como trilhas separadas pode: fragmentar fluxos decisórios que avaliam o mesmo evento econômico (solvabilidade); gerar decisões inconsistentes e sequenciais não coordenadas; aumentar fricção/latência/custo por transação; e gerar, de um lado, aprovação de crédito sem validação antifraude robusta (inadimplência "certa"), e, de outro, bloqueios antifraude excessivos (queda na taxa de aprovação e na inclusão).

Por isso, tratar crédito e fraude como trilhas estanques gera duplicidade de processos, inconsistência de dados, aumento de custo e decisões fragmentadas sobre o mesmo titular e a mesma operação. Isso pode resultar, por um lado, em concessões aprovadas sem validação antifraude robusta e, por outro, em bloqueios excessivos ou recusas indevidas de clientes legítimos, comprometendo inclusão, experiência do usuário e eficiência operacional.

A fragmentação também dificulta *accountability*, rastreabilidade e governança, pois distribui responsabilidades em fluxos paralelos, reduzindo visão integrada do risco. No agregado, esse modelo aumenta fricção, latência, custo por transação, perdas esperadas e consumo de capital, pressionando spreads, reduzindo taxa de aprovação e enfraquecendo a estabilidade do sistema.

5) Atividades e bases legais aplicáveis à proteção ao crédito

1. **Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?**

A base legal de proteção do crédito (art. 7º, X) deve ser interpretada de forma funcional e abrangente, alcançando o conjunto integrado de atividades necessárias para viabilizar todo o ciclo de vida do crédito, e não apenas a "fotografia" do momento contratual, além das diversas outras atividades que envolvem crédito, porque a proteção ao crédito é base legal pensada para abranger o funcionamento real do mercado, que opera em cadeia e exige decisões sucessivas antes, durante e após a contratação.

Nesse sentido, o ciclo do crédito normalmente se inicia na fase pré-contratual, em que são realizadas atividades como prospecção de clientes, análise preliminar de elegibilidade, segmentação de ofertas, simulações de capacidade de pagamento e pré-aprovação. Nessa etapa, é comum o uso de dados cadastrais e históricos para identificar perfil de risco e viabilidade de oferta, inclusive com consultas a *bureaus* e cruzamentos informacionais. Essas operações não configuram ainda formalização contratual, mas integram o próprio mecanismo de gerenciamento do risco e proteção ao crédito, pois visam evitar concessão temerária e reduzir inadimplência futura.

Em seguida, durante a fase de solicitação e concessão, podem ser realizadas atividades como *onboarding*, validação de identidade (KYC), verificação de documentos, confirmação de renda, avaliação e constituição de garantias, análise de score, cálculo de limites e definição de taxa e condições. Aqui, além do uso típico de *bureaus*, de outras informações e modelos de risco, podem ocorrer também checagens antifraude integradas (ex.: validação de consistência cadastral e comportamento transacional), evidenciando que a proteção ao crédito depende da correta identificação do titular e da mitigação de risco associado à fraude de identidade.

Após a contratação, o ciclo se mantém ativo por meio do monitoramento e gestão contínua do risco, não apenas individual, mas também institucional e sistêmico, inclusive em relação. São comuns práticas como atualização cadastral, reavaliação periódica de score, revisão de limites, análise de comportamento financeiro e de pagamento, detecção de deterioração do perfil de risco, alertas de exposição excessiva e acompanhamento de indicadores de inadimplência. Trata-se de fase essencial, pois o risco de crédito não se encerra no momento da assinatura do contrato e não envolve apenas essa atividade: ele se desenvolve ao longo do tempo e exige acompanhamento contínuo para preservar a estabilidade da operação e evitar superendividamento.

Também integra o ciclo a fase de gestão de inadimplência e renegociação, que inclui, por exemplo, cobrança, envio de notificações, protesto, ofertas de renegociação, reestruturação contratual, acordos, recuperação extrajudicial e judicial, excussão de garantias, cessão de crédito e registro de informações de inadimplemento. Essas atividades não apenas decorrem da relação contratual, mas são essenciais para assegurar o funcionamento saudável do mercado, reduzindo perdas sistêmicas e permitindo que o crédito continue circulando de forma sustentável.

Por fim, deve-se reconhecer que a proteção ao crédito inclui ainda outras atividades, como a realização de transações envolvendo crédito, tais como cessão e aquisição de carteiras e recebíveis de crédito, além de outras atividades indispensáveis, como o desenvolvimento, treinamento, teste, calibração e uso de modelos de credit scoring e políticas de crédito, prevenção a ilícitos correlatos, auditorias internas, compliance regulatório e compartilhamento de dados em situações justificadas (ex.: SCR e outras obrigações impostas pelo Bacen), pois o crédito depende de confiança sistêmica e integridade do ambiente financeiro.

Destacamos que descrição de atividades que podem estar incluídas na base legal de proteção do crédito ou de etapas do ciclo de crédito não é exaustiva. A lógica do art. 7º, X, portanto, não se limita à "avaliação da capacidade de pagamento" ou ao "momento da concessão", mas abrange todas as etapas necessárias para que o crédito seja concedido, mantido, monitorado e recuperado de forma responsável.

2. **Quais bases legais da LGPD suportam o tratamento de dados para análise e concessão do crédito?**

O art. 7º, X (proteção do crédito) ocupa posição central justamente por conferir coerência e segurança jurídica ao ecossistema, permitindo sustentar conjunto amplo de atividades, conforme descrito de forma não exaustiva no item anterior. Contudo, essa base convive com hipóteses complementares, como:

- **Execução de contrato ou procedimentos preliminares (art. 7º, V, LGPD):** permite o tratamento de dados para a execução de contrato do qual o titular seja parte, inclusive de procedimentos preliminares relacionados ao contrato, como avaliações prévias, propostas e contratos de financiamento, empréstimos ou cartões de crédito.
- **Cumprimento de obrigação legal ou regulatória (art. 7º, II, LGPD):** autoriza o tratamento de dados para atender obrigações legais e/ou regulatórias, inclusive as decorrentes de normas e requisições de órgãos como Bacen, Conselho Monetário Nacional (CMN), Comissão de Valores Mobiliários (CVM), Agência Nacional de Proteção de Dados (ANPD) e demais autoridades.
- **Legítimo interesse (art. 7º, IX, LGPD):** permite o tratamento de dados pessoais para finalidades legítimas atreladas ao apoio e promoção de atividades do controlador e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, como por exemplo, para o direcionamento de ofertas adequadas ao titular, observando riscos de crédito e/ou de superendividamento.
- **Consentimento (art. 7º, I, LGPD):** pode ser empregado em situações específicas, como no Open Finance ou quando o titular voluntariamente autoriza tratamentos adicionais.
- **Exercício regular de direitos em processo judicial, administrativo ou arbitral** (art. 7º, II, da LGPD): no caso de medidas necessárias, inclusive anteriores, a processos que envolvam crédito.
- **Prevenção à fraude e segurança do titular** (art.11, II, "g", LGPD): em contextos que envolvem dados biométricos utilizados para validação de identidade, autenticação e prevenção de fraudes, cuja finalidade é assegurar a integridade do cadastro, a proteção do titular e a sustentabilidade da operação de crédito.

6) Bases legais aplicáveis à prevenção à fraude

1. Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?

A prevenção à fraude, no ambiente digital, não se apresenta como atividade eventual, meramente acessória ou estática, mas como componente estrutural da operação financeira e comercial moderna. Isso significa que a escolha da base legal deve refletir a realidade de que a fraude se manifesta em múltiplas etapas do relacionamento com o titular, exigindo tratamentos contínuos, dinâmicos e proporcionais e, em particular, reconhecer o cenário brasileiro, em que há altos índices de fraude.

Para prevenção à fraude, as bases legais possíveis são conforme o caso concreto. O legítimo interesse (art. 7º, IX) é frequentemente invocado como fundamento para atividades preventivas permanentes, especialmente aquelas voltadas à proteção da segurança do titular e à preservação da integridade do sistema, como monitoramento de padrões de transação, identificação de anomalias e criação de mecanismos de detecção de risco. Quando bem documentado e submetido a teste de balanceamento, o legítimo interesse é compatível com o combate à fraude, pois atende não apenas ao interesse empresarial, mas ao interesse coletivo e individual de proteção do ambiente digital e analógico, prevenindo danos que atingiriam diretamente consumidores e a confiança do mercado.

O cumprimento à obrigação legal ou regulatória (art. 7º, II) tem grande relevância no setor financeiro, pois diversas normas prudenciais e regulatórias exigem controles antifraude, prevenção à lavagem de dinheiro e mecanismos de identificação e monitoramento de transações suspeitas. A prevenção à fraude, portanto, não se limita à esfera privada da empresa: em muitos casos, integra deveres normativos impostos por autoridades setoriais (como Bacen e CVM), sendo componente de compliance obrigatório. Isso reforça o caráter público e sistêmico da prevenção à fraude.

Além disso, a execução de contrato e procedimentos preliminares (art. 7º, V) fundamenta o tratamento de dados em contextos em que o titular solicita um serviço ou transação, sendo necessário validar identidade, autenticar acesso e confirmar legitimidade da operação para viabilizar a contratação. Isso inclui, por exemplo, a verificação de identidade para abrir uma conta, antes de liberar crédito, autorizar um Pix, aprovar compra com cartão, permitir alteração cadastral ou validar renegociação digital. Nesse ponto, vale destacar que sem autenticação e análise antifraude, a execução contratual pode não se concretizar de forma segura, o que torna a prevenção à fraude um pressuposto operacional do próprio contrato.

O exercício regular de direitos (art. 7º, VI) também é hipótese legal importante porque, diante de um cenário de fraude recorrente e litígios em massa, as instituições precisam tratar dados para prevenir prejuízos, constituir evidências, registrar ocorrências, sustentar defesa em disputas administrativas

e judiciais e viabilizar recuperação de perdas. Como já mencionado, a prevenção à fraude não se encerra na detecção: inclui também investigação interna, auditoria, produção de prova e preservação de logs para eventual responsabilização civil e criminal, o que se conecta diretamente ao exercício regular de direitos.

Quando o tratamento envolve dados sensíveis, com destaque à biometria, o art. 11, II, "g", da LGPD, autoriza o uso desses dados quando estritamente necessário para prevenção à fraude e garantia da segurança do titular. Deve-se reconhecer que a biometria é um dos meios mais eficazes para impedir fraudes de identidade, *deepfakes*, uso de documentos falsos e contratações indevidas. Por isso, a interpretação normativa deve evitar classificações genéricas e considerar o contexto, porque para fins de antifraude, a biometria atua como mecanismo de proteção do próprio titular e do sistema.

Vale considerar que em mercados altamente digitalizados, como ocorre no cenário brasileiro, a prevenção à fraude integra a própria infraestrutura de confiança: sem ela, não há escalabilidade do crédito, não há expansão sustentável do Pix, não há contratação remota segura, e o risco sistêmico se intensifica.

Assim, eventuais leituras excessivamente restritivas da LGPD não fortalecem os direitos dos titulares. Ao contrário, fragilizam a segurança e ampliam o risco de danos patrimoniais, reputacionais e sociais.

2. **Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?**

A interpretação deve ser teleológica e sistêmica. A base legal de prevenção à fraude, interpretada à luz do interesse público, da segurança dos titulares e da estabilidade financeira, deve ser vista como instrumento que equilibra a proteção dos direitos individuais com a necessidade coletiva de manter ambiente econômico seguro e confiável, o qual beneficia o titular e toda a sociedade.

O interesse público está diretamente relacionado à redução de crimes financeiros e outros ilícitos, à proteção do patrimônio dos cidadãos e das instituições, bem como à preservação da confiança no sistema bancário, comercial e em atividades governamentais. Ao permitir o tratamento de dados pessoais para prevenir fraudes, a legislação busca evitar prejuízos que afetam não apenas indivíduos, mas também empresas e o próprio funcionamento do mercado, uma vez que a fraude digital contemporânea gera externalidades negativas relevantes: elevação de custos, exclusão financeira, deterioração da confiança e risco sistêmico.

Neste sentido, o tratamento de dados pessoais fundado na finalidade de prevenção a fraudes é essencial para garantir a estabilidade financeira e a segurança dos titulares, evitando prejuízos financeiros e que reflitam no interesse público.

A fraude digital produz externalidades negativas relevantes: aumenta custos, reduz confiança, restringe acesso a serviços, compromete meios de pagamento e intensifica risco sistêmico. Por isso, o tratamento de dados para prevenção à fraude não atende apenas a um interesse empresarial, mas protege o próprio titular, preserva a segurança das transações e favorece a estabilidade financeira.

Sob esse enfoque, a prevenção à fraude deve ser lida como atividade funcionalmente vinculada à resiliência do sistema econômico. A segurança do titular não se opõe à proteção de dados; ao contrário, depende de mecanismos adequados de verificação, autenticação e monitoramento. Leituras excessivamente restritivas tendem a comprometer essa finalidade, aumentar a incidência de danos patrimoniais e reputacionais e fragilizar a confiança coletiva em infraestruturas digitais essenciais.

7) Princípios da LGPD aplicáveis a ambos os contextos

1. **Quais princípios devem orientar a coleta, uso, minimização, retenção e compartilhamento de dados nesses tratamentos?**

Os tratamentos voltados a crédito e antifraude devem ser orientados pelos princípios do art. 6º da LGPD, aplicados de forma funcional e contextualizada. Destacam-se a finalidade, para delimitar propósitos legítimos e específicos; a adequação, para alinhar o uso de dados ao contexto informado; a necessidade, para restringir o tratamento ao mínimo necessário; a qualidade dos dados, para assegurar acurácia e atualização; a transparência, para informar categorias de dados, finalidades e compartilhamentos de modo inteligível; a segurança e a prevenção, para mitigar acessos indevidos, vazamentos, fraudes e incidentes; a não discriminação, para evitar tratamentos abusivos ou ilícitos; e a responsabilização e prestação de contas, para demonstrar conformidade e governança.

A minimização se concretiza, ainda, quando possível, por meio de: (i) limitação de escopo, evitando a coleta de dados excessivos ou periféricos ao risco avaliado; (ii) segmentação de acessos, assegurando que apenas perfis autorizados tratem dados sensíveis ou de maior impacto; (iii) revisões periódicas de necessidade, especialmente em modelos, regras e bases históricas reutilizadas; dentre outras práticas correlatas.

Em operações de risco, esses princípios não devem ser tratados como exigências meramente formais, mas como critérios operacionais concretos que estruturam a coleta, a retenção, o compartilhamento e o descarte de dados ao longo de toda a jornada, observando-se a situação concreta.

2. **Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?**

A proporcionalidade, necessidade e adequação em modelos de risco integrados se concretizam por processos: mapeamento completo dos fluxos e das categorias de dados, documentação das finalidades, políticas de minimização/retenção/descarte e, quando aplicável, análises de impacto; a necessidade deve ser calibrada de acordo com o caso concreto e ao risco (p.ex., concessão remota e fraude de identidade podem justificar dados mais robustos), e modelos devem ser continuamente revisados para reduzir excessos, evitar vieses e manter aderência à finalidade.

Adicionalmente:

- Arquitetura por níveis de risco: *step-up authentication* e coleta adicional apenas quando o risco aumentar;
- Controle de acesso e segregação: *need-to-know*, trilhas e revisão periódica de perfis;
- Avaliação de impacto e testes: medir ganho de performance vs. intrusão; reduzir dados com baixo ganho marginal; e
- Pseudonimização/anonimização quando possível: especialmente em desenvolvimento e validação de modelos.

Esses princípios se concretizam por meio de governança. É recomendável mapear fluxos e finalidades, catalogar categorias de dados, justificar a pertinência de variáveis, calibrar a coleta ao risco concreto e revisar continuamente a utilidade da informação. Em modelos integrados, a necessidade deve ser aferida em função da jornada, do tipo de operação e do nível de risco, admitindo reforço de controles quando a operação assim o justificar.

3. **Como operacionalizar transparência sem comprometer a efetividade de sistemas antifraude e de scoring?**

A transparência deve ser operacionalizada de modo funcional e proporcional: informar finalidades gerais, categorias de dados utilizadas, existência de modelos e direitos/canais de atendimento, sem exigir divulgação de fórmulas, pesos, limiares ou mecanismos sensíveis que comprometam segredo empresarial e eficácia antifraude (inclusive por risco de "*gaming*"). Esse equilíbrio também é amparado por entendimento jurisprudencial sobre licitude do *credit scoring* com direito à informação/correção e resguardo do segredo empresarial.

Ou seja:

- Transparência em camadas: explicar finalidades, categorias de dados, fontes e efeitos, sem revelar regras operacionais que facilitem fraude.
- Explicação por fatores: fornecer motivos gerais (ex.: inconsistência cadastral, padrão atípico) sem expor pesos/limiares.
- Canal de contestação e revisão: permitir reavaliação quando cabível e registrar decisões.
- Proteção de segredos de negócio e segurança: limitar detalhamento externo, mantendo *accountability* e auditabilidade interna.

O equilíbrio adequado consiste em fornecer explicações suficientes para assegurar compreensão e pode ser operacionalizada por meio de políticas de privacidade, exercício de direitos e contestação, preservando, ao mesmo tempo, a integridade dos modelos e evitando risco de manipulação do sistema. Isso é especialmente importante em antifraude e *scoring*, nos quais abertura excessiva pode reduzir a efetividade dos mecanismos de proteção.

8) Governança, controles e segurança

1. **Quais frameworks de governança e gestão de riscos são recomendados para operações de crédito e antifraude?**

Não há framework único e isolado, mas sim a necessidade de arquitetura de governança integrada, capaz de articular risco, dados, tecnologia e conformidade, com foco em efetividade, proporcionalidade e interesse público. Crédito e antifraude exigem governança baseada em três pilares complementares: frameworks estruturantes de gestão de risco, para organizar e justificar decisões; controles técnicos e administrativos, para prevenir e reagir a incidentes; rastreabilidade e accountability, para demonstrar conformidade, reduzir danos e permitir auditoria contínua. Isso significa construir um sistema confiável, resiliente e auditável.

Como frameworks de governança e gestão de riscos, recomenda-se combinação de padrões prudenciais e boas práticas, como por exemplo: Basileia (gestão integrada e supervisão), COSO ERM e ISO 31000 (gestão transversal de riscos), Model Risk Management (p.ex., SR 11-7) e NIST AI RMF (governança de IA), além de normas ISO para segurança e privacidade (27001/27002/27005/27701 etc.), com ênfase em resiliência e *accountability*.

Além disso, para empresas atuantes no mercado financeiro, por ex. instituições de pagamento, há regulamentações específicas a serem observadas pelo programa de governança das operações de crédito e antifraude, como:

- BACEN, Resolução Conjunta 6/2023, que estabelece o compartilhamento obrigatório de informações de fraude entre instituições, visando a construção de inteligência coletiva do sistema financeiro.
- BACEN, Resolução BCB nº 142/2021, disciplina controles para prevenção de fraudes em serviços de pagamento; e
- BACEN, Resolução BCB nº 265/2022, atualizada pela Resolução BCB nº 447/2024, que define a estrutura de gerenciamento de riscos para instituições de pagamento.

2. Quais controles técnicos e administrativos devem ser implementados para assegurar segurança da informação e mitigação de incidentes?

Devem ser combinados controles técnicos, administrativos e operacionais proporcionais ao risco. Entre os técnicos, destacam-se criptografia, gestão de chaves, autenticação multifator, *step-up authentication*, monitoramento contínuo, detecção de anomalias, WAF, EDR, DLP, pseudonimização, segregação de ambientes, *backup*, *disaster recovery* e mecanismos de resposta rápida. Entre os administrativos, são importantes políticas internas, treinamento, gestão de acessos, classificação da informação, *secure* SDLC, gestão de mudanças, *due diligence* e governança contratual de terceiros.

No plano operacional antifraude, também são recomendáveis *playbooks* de resposta, gestão de exceções, revisão de alertas, cadeia decisória clara, monitoramento em tempo real e preservação de evidências. O objetivo é assegurar prevenção, detecção, contenção, recuperação e capacidade de auditoria.

Adicionalmente, seguindo padrões nacionais e internacionais, exemplifica-se os seguintes controles:

- Modelo de Três Linhas de Defesa: segregação entre gestão operacional, funções independentes de risco/compliance e auditoria interna (Res. CMN nº 4.557/2017), garantindo *accountability* e supervisão contínua.
- Ética e Mitigação de Vieses: validações periódicas para identificar e corrigir discriminações ilícitas ou abusivas, para que decisões automatizadas ou semi-automatizadas sejam válidas, inclusivas e éticas.
- Responsabilização e Governança de Terceiros: políticas formais de *accountability* para tecnologias internas e fornecedores, exigindo padrões de segurança e controles equivalentes.
- Monitoramento Contínuo e Resposta em Tempo Real: uso de tecnologias para detecção proativa de anomalias, fraudes e ataques cibernéticos, com capacidade de resposta automatizada para reduzir perdas e riscos sistêmicos.

- Verificação em Múltiplas Camadas e *Privacy by Design*: combinação de biometria e análise comportamental integrada a técnicas de preservação de privacidade (como criptografia e anonimização), prevenindo identidades sintéticas.
- Explicabilidade e Transparência: implementação de técnicas que permitam interpretar as decisões dos modelos, garantindo o direito do titular à revisão e explicação de decisões automatizadas.
- Testes de Estresse e Robustez: avaliação periódica com dados sintéticos para validar a resiliência frente a cenários adversos e mudanças de padrão de fraude, assegurando estabilidade operacional.
- Gestão de Risco Cibernético: adoção de frameworks (ISO/IEC 27001/27002) e conformidade com as políticas de segurança cibernética do CMN/BCB, garantindo a tríade CID (Confidencialidade, Integridade e Disponibilidade).

3. Como estruturar políticas de retenção, registro de logs, auditoria e accountability?

As políticas de retenção devem ser definidas por finalidade, considerando duração da relação contratual, obrigações legais e regulatórias, prazos prescricionais, necessidade de investigação e defesa, riscos residuais legítimos e existência de outras finalidades e contexto do tratamento. O registro de logs deve garantir rastreabilidade de acessos, consultas, alterações, eventos críticos, inputs relevantes, decisões tomadas e versão de modelos ou regras utilizadas, com integridade, cadeia de custódia e acesso restrito.

A auditoria deve ser periódica e documentada, abrangendo aderência a políticas, revisão de controles, análise de incidentes, validação de modelos, monitoramento de *drift* e verificação de vieses. Já a *accountability* exige definição clara de papéis e responsabilidades entre negócio, risco, segurança, jurídico, privacidade e auditoria, além de documentação suficiente para demonstrar conformidade.

No contexto brasileiro, essa abordagem também dialoga com regulações setoriais do Banco Central do Brasil, que exigem registros, rastreabilidade, controles internos e capacidade de auditoria em operações financeiras e de crédito, reconhecendo que esses elementos são essenciais para a estabilidade do sistema financeiro e para a proteção do consumidor.

9) Decisões automatizadas e Inteligência Artificial

1. Quais são decisões automatizadas mais comuns em crédito e antifraude?

As decisões automatizadas/semi-automatizadas mais comuns cobrem todo o ciclo, da prospecção à recuperação, e incluem, por exemplo, onboarding/validação de identidade e autenticidade

(cruzamento de dados cadastrais, biometria e informações do dispositivo), além de decisões de concessão/limite e bloqueio/aprovação em antifraude. Essas decisões são sustentadas por modelos estatísticos, *Machine Learning* (ML) e, mais recentemente, modelos fundacionais e/ou Inteligência Artificial Generativa (GenAI).

Portanto:

- No crédito: aprovação/recusa, limite, análise de perfil, exigência de garantia, bloqueios preventivos, revisão de limite, estratégias de cobrança;
- Para antifraude: validação de identidade, *step-up*, bloqueio/declínio de transação, congelamento temporário, encaminhamento para revisão manual, classificação/priorização de alertas.

2. **Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?**

A governança algorítmica deve incluir documentação do objetivo do modelo, base legal, dados de entrada, features relevantes, processo de treinamento, validação, testes, métricas de desempenho, critérios de *override* e monitoramento contínuo. A explicabilidade não deve ter como foco revelar código-fonte ou fórmula integral, mas em permitir compreensão dos fatores mais relevantes, justificativas gerais da decisão e meios efetivos de contestação.

Quanto à mitigação de vieses, são recomendáveis testes periódicos de *fairness*, revisão de proxies indevidos, análise de impactos desproporcionais por subgrupos, controle de qualidade e representatividade dos dados e governança de exceções. O objetivo é equilibrar eficiência, segurança, inclusão e proteção de direitos, sem inviabilizar modelos que, quando bem governados, podem reduzir fraude, ampliar acesso e melhorar a qualidade da decisão.

Por isso, explicabilidade, governança algorítmica e mitigação de vieses devem ser tratadas como elementos estruturantes de gestão de risco, com documentação, responsabilidades claras, validação periódica e supervisão humana efetiva. A explicabilidade com critérios gerais, fatores relevantes e consequências para o titular, sem exigir abertura de código-fonte, pesos ou algoritmos, o que comprometeria segredo empresarial e a própria eficácia de *scoring*/antifraude.

Revisão humana individualizada para cada decisão automatizada tende a ser contraproducente e inviável, uma vez que pode inviabilizar o uso de tecnologias que, na prática, demonstram ganhos relevantes de eficiência, redução de fraudes e ampliação do acesso ao crédito, ainda mais considerando o volume de transações e operações. O desafio regulatório e operacional reside, portanto, em construir mecanismos proporcionais de explicabilidade, supervisão e controle, baseados em governança, testes de vieses, validações periódicas e monitoramento de

impactos, que preservem os direitos dos titulares sem comprometer os benefícios sociais e econômicos associados à inovação e à inclusão financeira.

3. **Quais diretrizes devem orientar o uso de IA generativa e machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos?**

O uso de ML e IA generativa deve ser orientado por finalidade legítima, proporcionalidade, segurança, supervisão adequada, rastreabilidade e controle de risco. Em geral, modelos tradicionais de ML são mais aderentes a decisões de risco, score e detecção de fraude, enquanto IA generativa tende a ser mais apropriada para apoio operacional, triagem, sumarização, apoio analítico e atendimento assistido, e não para decisão final autônoma em contextos de maior impacto.

Também são essenciais validação contínua, testes de robustez, monitoramento de erro, proteção contra vazamento, *prompt injection* e usos indevidos, segregação de dados, versionamento, *logging* e *fallback* para regras ou revisão humana quando necessário. A governança deve ser calibrada ao porte, à complexidade e ao potencial impacto do sistema.

Além disso, vale ressaltar que, quando aplicável, no início do desenvolvimento, pode haver um fluxo de supervisão humana do resultado desses modelos para a construção de conjuntos de dados verdadeiros e verificados (*ground truth*) para incrementar a robustez dessas técnicas e ferramentas empregadas. Entretanto, é essencial reconhecer que exigências excessivas de transparência absoluta ou revisão humana individualizada para cada decisão automatizada podem inviabilizar soluções tecnológicas que demonstram, na prática, ganhos reais em eficiência, segurança e inclusão financeira.

Desta forma, tais ferramentas exigem atenção as diretrizes já existentes, aos princípios de ética, transparência, segurança, privacidade e conformidade legal. Assim, quando possível, faz-se necessária a validação dos modelos, com a realização de testes de desempenho, robustez, vieses e estabilidade, além de assegurar aderência às normas aplicáveis, como a LGPD e a regulação setorial.

4. **Como equilibrar transparência e explicabilidade com segredos de negócio?**

Esse equilíbrio pode ser alcançado por transparência significativa e por camadas. A disponibilização de informações, considerando o contexto, deve considerar explicações mais gerais sobre o que pode ser analisado e decisões que podem ser tomadas em termos gerais, quais categorias de dados foram relevantes e quais canais existem para revisão ou contestação, quando aplicável. Ao mesmo tempo, devem ser preservados pesos, limiares, fórmulas, regras antifraude detalhadas, listas operacionais e demais elementos sensíveis cuja divulgação comprometeria segurança, concorrência e eficácia do

sistema. Além disso, são válidas respostas fundamentadas na possibilidade de recusa do crédito por desinteresse comercial da instituição.

Ademais, também é recomendável a priorização de supervisão humana do sistema (monitoramento contínuo, auditorias, testes e revisão de premissas) em vez de revisão humana caso a caso, que seria impraticável em escala e potencialmente menos precisa.

Em outras palavras, a transparência deve ser suficiente para garantir direitos, mas não a ponto de expor o funcionamento íntimo do mecanismo decisório e permitir *gaming*, evasão ou comprometimento do segredo comercial. Esse modelo é especialmente adequado para *scoring* e antifraude, nos quais a efetividade depende, em grande parte, da preservação da lógica operacional interna.

Assim, pode-se explicar o "o quê" e "por quê" em alto nível ao titular, restringindo o "como" (sinais/limiares) por segurança e segredo de negócio. Ainda, informar fatores determinantes sem expor pesos/limiares ou listas operacionais.

De São Paulo para Brasília, 01 de maio de 2026.

Atenciosamente,

GT5 – Proteção ao Crédito e Prevenção à Fraude

ANEXO I – Normas aplicáveis

1) Nacionais Gerais

Norma	Artigos relevantes
Lei Geral de Proteção de Dados (Lei 13.709/28)	Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) **X - para a proteção do crédito**, inclusive quanto ao disposto na legislação pertinente. Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...) II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...) g) garantia da **prevenção à fraude** e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Art. 20. O titular dos dados tem **direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado** de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu **perfil** pessoal, profissional, de consumo e **de crédito** ou os aspectos de sua personalidade. Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: (...) V - na hipótese de a transferência dos dados **objetivar exclusivamente a prevenção de fraudes e irregularidades**, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.
Lei do Cadastro Positivo (Lei nº 12.414/2011)	Art. 1º Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, **para formação de histórico de crédito**, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor. Art. 2º Para os efeitos desta Lei, considera-se: I - **banco de dados**: conjunto de dados relativo a pessoa natural ou jurídica armazenados

	com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro; (...) VII - **histórico de crédito**: conjunto de dados financeiros e de pagamentos, relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica. Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a **formação do histórico de crédito**, nas condições estabelecidas nesta Lei. (...) § 3º Ficam proibidas as anotações de: I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. Art. 5º São direitos do cadastrado: (...) II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, **inclusive seu histórico e sua nota ou pontuação de crédito**, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado; (...) § 8º O cancelamento de cadastro implica a impossibilidade de uso das informações do histórico de crédito pelos gestores, para os fins previstos nesta Lei, inclusive para a composição de nota ou pontuação de crédito de terceiros cadastrados, na forma do art. 7º-A desta Lei. Art. 7º **As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para: I - realização de análise de risco de crédito do cadastrado; ou II - subsidiar a concessão ou extensão de crédito** e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente. Parágrafo único. Cabe ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar aos consulentes as informações de adimplemento do cadastrado. Art. 7º-A **Nos elementos e critérios considerados para composição da nota ou pontuação de crédito de pessoa cadastrada em banco de dados de que trata esta Lei, não podem ser utilizadas informações: I - que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas**; (...) § 1º O **gestor de banco de dados deve disponibilizar em seu sítio eletrônico, de forma clara, acessível e de fácil compreensão, a sua política de coleta e utilização de dados pessoais para fins de elaboração de análise de risco de crédito**.

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

Código de Defesa do Consumidor (Lei nº 8.078/1990)	Art. 54-D. **Na oferta de crédito**, previamente à contratação, o fornecedor ou o intermediário deverá, entre outras condutas: (Incluído pela Lei nº 14.181, de 2021) I - informar e esclarecer adequadamente o consumidor, considerada sua idade, sobre a natureza e a modalidade do crédito oferecido, sobre todos os custos incidentes, observado o disposto nos arts. 52 e 54-B deste Código, e sobre as consequências genéricas e específicas do inadimplemento; (Incluído pela Lei nº 14.181, de 2021) **II - avaliar, de forma responsável, as condições de crédito do consumidor, mediante análise das informações disponíveis em bancos de dados de proteção ao crédito**, observado o disposto neste Código e na legislação sobre proteção de dados; (Incluído pela Lei nº 14.181, de 2021) III - informar a identidade do agente financiador e entregar ao consumidor, ao garante e a outros coobrigados cópia do contrato de crédito. (Incluído pela Lei nº 14.181, de 2021) Art. 43. O consumidor, sem prejuízo do disposto no art. 86, **terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele**, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

	§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (Vigência)
Lei do Superendividamento (Lei n° 14.181/2021 e Decreto nº11.567/23)	Aperfeiçoa a disciplina do crédito ao consumidor e dispõe sobre a prevenção e o tratamento do superendividamento.
Lei do Sigilo Bancário (Lei Complementar nº 105/2001)	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Lei sobre crimes de lavagem de dinheiro (Lei nº 9.613/98)	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.
Lei Anticorrupção (Lei nº 12.846/2013)	Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.
Lei sobre crimes contra o sistema financeiro nacional (Lei nº 7.492/1986)	Define os crimes contra o sistema financeiro nacional, e dá outras providências.

2) Nacionais Setoriais

2.1) Normas de Crédito

Norma	Artigos relevantes
Resolução CMN n° 4.557/2017 (aqui)	Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.
Resolução BCB n° 265/2022 (aqui)	Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de instituição classificada como Tipo 3 enquadrada no Segmento 2 – S2, Segmento 3 – S3 ou Segmento 4 – S4.
Resolução BCB n° 96/2021 (aqui)	Dispõe sobre a abertura, a manutenção e o encerramento de contas de pagamento. Art. 4º As instituições referidas no art. 1º, para fins da abertura de conta de pagamento, devem adotar procedimentos e controles que permitam verificar e validar a identidade e a qualificação do titular da conta e, quando for o caso, de seus representantes, bem como a autenticidade das informações por eles fornecidas, inclusive mediante confrontação

	dessas informações com as disponíveis em bancos de dados de caráter público ou privado.
Resolução BCB n° 155/2021 (aqui)	Dispõe sobre princípios e procedimentos a serem adotados no relacionamento com clientes e usuários de produtos e de serviços pelas administradoras de consórcio, pelas instituições de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil. Art. 7º As instituições mencionadas no art. 1º devem assegurar a consistência de rotinas e de procedimentos operacionais afetos ao relacionamento com clientes e usuários, bem como sua adequação à política institucional de relacionamento de que trata o art. 6º, inclusive quanto aos seguintes aspectos: (...)VII - coleta, tratamento e manutenção de informações dos clientes e usuários em bases de dados;
Resolução BCB n° 368/2024 (aqui)	Altera as Resoluções BCB ns. 28, de 23 de outubro de 2020; 65, de 26 de janeiro de 2021; 85, de 8 de abril de 2021; 93, de 6 de maio de 2021; 155, de 14 de outubro de 2021; e 260, de 22 de novembro de 2022, para incluir em seus escopos de aplicação as sociedades corretoras de títulos e valores mobiliários, as sociedades distribuidoras de títulos e valores mobiliários e as sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.
Resolução CMN n° 4.949/2021 (aqui)	Dispõe sobre princípios e procedimentos a serem adotados no relacionamento com clientes e usuários de produtos e de serviços.
Resolução BCB nº 303/2023 (aqui)	Estabelece os procedimentos para o cálculo da parcela dos ativos ponderados pelo risco (RWA) referente às exposições ao risco de crédito sujeitas ao cálculo do requerimento de capital mediante sistemas internos de classificação do risco de crédito (abordagens IRB) autorizados pelo Banco Central do Brasil (RWA_{CIRB}), de que tratam a Resolução CMN nº 4.958, de 21 de outubro de 2021, e a Resolução BCB nº 200, de 11 de março de 2022.
Circular BCB nº 3.876/2018 (aqui)	Dispõe sobre metodologias e procedimentos para a avaliação da suficiência do valor de Patrimônio de Referência (PR) mantido para a cobertura do risco de variação das taxas de juros em instrumentos classificados na carteira bancária (IRRBB), a identificação, mensuração e controle do IRRBB e a remessa ao Banco Central do Brasil de informações relativas ao IRRBB.
Instrução Normativa BCB nº 609/2025 (aqui)	Dispõe sobre as informações que devem constar no relatório de que trata o art. 123, § 3º, inciso III da Resolução BCB nº 303, de 16 de março de 2023, faculta a etapa de análise preliminar e esclarece sobre a avaliação da candidatura.

2.2) Normas de Prevenção à Fraude

Norma	Artigos relevantes
Resolução Conjunta nº 6/2023 (aqui)	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.

	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. 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. (...)
Resolução BCB nº 142/2021 (aqui) **e atualização pela Resolução BCB nº 501/2025** (aqui)	Resolução BCB nº 142/2021: 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 Banco Central do Brasil e instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB). Art. 1º Esta Resolução 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 Banco Central do Brasil e instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB). Art. 4º As instituições mencionadas no art. 1º devem manter registros diários detalhando as ocorrências de fraudes ou de tentativas de fraude na prestação de serviços de pagamento, discriminando inclusive as medidas corretivas adotadas. Resolução BCB nº 501/2025: Altera 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 a serem adotados pelas instituições financeiras, demais instituições autorizadas a funcionar pelo Banco Central do Brasil e instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro – SPB.
Carta Circular BCB nº 4.001/2020 (aqui)	Divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento ao terrorismo, previstos na Lei nº

	13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf).
Circular n° 3.978/2020 (aqui)	Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.
Resolução BCB n° 475/2025 (aqui)	Dispõe sobre sistema de comunicação de restrição a contratações no Sistema Financeiro Nacional.
Resolução BCB n° 491/2024 (aqui)	Estabelece as diretrizes para cadastramento de dispositivo de acesso para a iniciação de transações Pix e para o gerenciamento de chaves Pix e define o valor máximo permitido para iniciar transações Pix em dispositivo de acesso não cadastrado.
Resolução BCB n° 493/2025 (aqui)	Altera a Resolução BCB nº 1, de 12 de agosto de 2020, que institui o arranjo de pagamentos Pix e aprova o seu regulamento, para ajustar dispositivos relacionados ao funcionamento do Fórum Pix, e altera o regulamento anexo à Resolução BCB nº 1, de 12 de agosto de 2020, para aprimorar o Mecanismo Especial de Devolução e os procedimentos de alteração de informações vinculadas às chaves Pix.
Resolução BCB nº 506/2025 (aqui)	Altera a Resolução BCB nº 1, de 12 de agosto de 2020, que institui o arranjo de pagamentos Pix e aprova o seu regulamento, para ajustar dispositivos relacionados ao critério de autorização das instituições de pagamento não autorizadas a funcionar pelo Banco Central do Brasil e que sejam participantes do Pix; e altera o regulamento anexo à Resolução BCB nº 1, de 12 de agosto de 2020, que disciplina o funcionamento do arranjo de pagamentos Pix, para aprimorar os mecanismos de segurança do arranjo e para ajustar dispositivos relativos às penalidades aplicáveis aos participantes do Pix.
Resolução BCB n° 669/2025 (aqui)	Altera a Instrução Normativa BCB nº 512, de 30 de agosto de 2024, que dispõe sobre os limites de valor para as transações no âmbito do Pix, para ajustar os critérios que devem ser observados pelos participantes para estabelecer limites máximos de valor para as transações.
Resolução Conjunta nº 6/2023 (aqui)	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. 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. 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. (...)

3) Internacionais

Norma	Artigos relevantes
União Europeia: Diretiva da UE sobre crédito ao consumidor 2023/2225 (aqui)	A Diretiva faz referência explícita ao GDPR, sublinhando sua aplicabilidade ao tratamento de dados pessoais tanto por credores quanto por intermediários de crédito. - Proibição do Uso de Dados Sensíveis (Considerando 48): Credores e intermediários estão proibidos de usar categorias especiais de dados pessoais, como dados de saúde, incluindo informações sobre diagnósticos de câncer. - Requisitos para Avaliação de Crédito (Considerando 55): A avaliação de crédito deve basear-se em dados necessários, proporcionais, relevantes, precisos e completos, incluindo renda, despesas e obrigações financeiras, mas sem incluir dados sensíveis (ex.: saúde). - Direito de Revisão em Decisões Automatizadas (Art. 18(8)): Consumidores têm direito a solicitar intervenção humana para obter explicações claras sobre decisões automatizadas, expressar suas opiniões e pedir revisão das decisões relacionadas à avaliação de crédito. - Bases de Dados e Acesso Não Discriminatório (Art. 19): credores de outros Estados-Membros devem ter acesso igualitário às bases de dados de crédito, desde que em conformidade com o Regulamento (UE) 2016/679. Essas bases devem ser atualizadas e precisas, excluindo dados sensíveis. Consumidores têm direito de contestar informações e devem ser informados sobre mudanças em seus registros.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

União Europeia: Proposta de Regulamento Europeu relativo a Framework para acesso a dados financeiros (Framework for Financial Data Access) - Parecer do EDPS (European Data Protection Supervisor) - Opinion n. 38/2023 (aqui)	O objetivo do Framework é promover o desenvolvimento de serviços financeiros baseados em dados, permitindo que consumidores e empresas controlem o acesso a seus dados financeiros. Isso facilita o acesso a produtos e serviços personalizados, ao mesmo tempo que mitiga os riscos do compartilhamento de dados. O EDPS analisou a proposta e destacou a importância que o Framework dá aos seguintes aspectos relacionados à proteção de dados pessoais: (i) ao controle do cliente sobre os dados; (ii) aos limites de uso de dados seguindo princípios da proporcionalidade e minimização, para evitar discriminação ou exclusão financeira; (iii) necessidade de exclusão de dados sensíveis, como informações de saúde ou perfilamento, reduzindo riscos à privacidade; (iv) obrigações dos usuários e Detentores de Dados : usuários devem justificar a solicitação de dados com base legal clara, enquanto detentores de dados garantem precisão, segurança e atualização das informações; (v) cooperação entre autoridades: reguladores financeiros e autoridades de proteção de dados devem trabalhar juntos para evitar conflitos e garantir aplicação coerente das leis; (vi) Diretrizes sobre Uso de dados: Reguladores como EBA e EIOPA devem estabelecer diretrizes para o uso de dados financeiros em conformidade com leis de proteção de dados, evitando combinações excessivas ou inadequadas.[1]
União Europeia: GDPR Regulamento UE 2016/679 - (aqui)	Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para o EEE) Considerando (47) | Os interesses legítimos de um responsável pelo tratamento, incluindo os de um responsável pelo tratamento a quem os dados pessoais possam ser divulgados, ou de um terceiro, podem constituir uma base jurídica para o tratamento, desde que os interesses ou os direitos e liberdades fundamentais do titular dos dados não se sobreponham, tendo em conta as expectativas razoáveis dos titulares dos dados com base na sua relação com o responsável pelo tratamento. Tal interesse legítimo pode existir, por exemplo, quando existe uma relação relevante e adequada entre o titular dos dados

	e o responsável pelo tratamento em situações em que o titular dos dados é um cliente ou está ao serviço do responsável pelo tratamento. Em qualquer caso, a existência de um interesse legítimo exigiria uma avaliação cuidadosa, incluindo se o titular dos dados pode razoavelmente esperar, no momento e no contexto da recolha dos dados pessoais, que o tratamento para esse fim possa ocorrer. Os interesses e direitos fundamentais do titular dos dados podem, em particular, prevalecer sobre o interesse do responsável pelo tratamento dos dados quando os dados pessoais são tratados em circunstâncias em que os titulares dos dados não esperam razoavelmente que haja um tratamento posterior. Dado que cabe ao legislador estabelecer por lei a base jurídica para o tratamento de dados pessoais pelas autoridades públicas, essa base jurídica não deve aplicar-se ao tratamento por parte das autoridades públicas no exercício das suas funções. O tratamento de dados pessoais estritamente necessário para efeitos de prevenção da fraude constitui igualmente um interesse legítimo do responsável pelo tratamento em causa. O tratamento de dados pessoais para fins de marketing direto pode ser considerado como sendo realizado para um interesse legítimo. Considerando (71) | O titular dos dados deve ter o direito de não ser sujeito a uma decisão, que pode incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, baseada exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou que o afetem significativamente de forma semelhante, como a recusa automática de um pedido de crédito online ou práticas de recrutamento eletrônico sem qualquer intervenção humana. Esse tratamento inclui a “criação de perfis”, que consiste em qualquer forma de tratamento automatizado de dados pessoais que avalie os aspectos pessoais relativos a uma pessoa singular, em particular para analisar ou prever aspetos relativos ao desempenho profissional, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou ao comportamento, à localização ou aos movimentos da pessoa em causa, quando produz efeitos jurídicos que lhe digam respeito ou a afetem de forma significativa. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição

	de perfis, deve ser permitida quando expressamente autorizada pela legislação da União ou dos Estados-Membros a que o responsável pelo tratamento está sujeito, incluindo para efeitos de monitorização e prevenção da fraude e da evasão fiscal, realizada em conformidade com os regulamentos, normas e recomendações das instituições da União ou dos órgãos de supervisão nacionais e para garantir a segurança e a fiabilidade de um serviço prestado pelo responsável pelo tratamento, ou necessária para a celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento, ou quando o titular dos dados tiver dado o seu consentimento explícito. Em qualquer caso, esse tratamento deve estar sujeito a garantias adequadas, que devem incluir informações específicas ao titular dos dados e o direito de obter intervenção humana, de expressar o seu ponto de vista, de obter uma explicação sobre a decisão tomada após essa avaliação e de contestar a decisão. Essa medida não deve dizer respeito a crianças. A fim de garantir um tratamento justo e transparente em relação ao titular dos dados, tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais são tratados, o responsável pelo tratamento deve utilizar procedimentos matemáticos ou estatísticos adequados para a definição de perfis, implementar medidas técnicas e organizativas adequadas para garantir, em particular, que os fatores que resultam em imprecisões nos dados pessoais sejam corrigidos e que o risco de erros seja minimizado, proteger os dados pessoais de forma a ter em conta os riscos potenciais para os interesses e direitos do titular dos dados e a evitar, nomeadamente, efeitos discriminatórios sobre as pessoas singulares com base na origem racial ou étnica, opiniões políticas, religião ou crenças, filiação sindical, estado genético ou de saúde ou orientação sexual, ou que resultem em medidas com tais efeitos. A tomada de decisões automatizada e a definição de perfis com base em categorias especiais de dados pessoais só devem ser permitidas em condições específicas. Artigo 6. (...) f) | o tratamento for necessário para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por um terceiro, exceto quando sobre esses interesses se sobreponham os interesses ou os direitos e

	liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais, em especial quando o titular dos dados for uma criança.
União Europeia: Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão (aqui)	Capítulo V – Proteção de dados, conservação de registos e dados estatísticos. Artigo 40.º (...) b) (...) Após o termo dos períodos de conservação referidos no primeiro parágrafo, os Estados-Membros devem assegurar que as entidades obrigadas apaguem os dados pessoais, salvo disposição em contrário da legislação nacional, que determinará em que circunstâncias as entidades obrigadas podem ou devem continuar a conservar os dados. Os Estados-Membros podem autorizar ou exigir a conservação dos dados após terem procedido a uma avaliação exaustiva da necessidade e da proporcionalidade dessa conservação e considerarem que esta se justifica como necessária para a prevenção, deteção ou investigação de branqueamento de capitais ou de financiamento do terrorismo. Esse período de conservação adicional não pode exceder cinco anos. Artigo 41.º 1. O tratamento de dados pessoais ao abrigo da presente diretiva está sujeito aos Regulamentos (UE) 2016/679 (22) e (UE) 2018/1725 (23) do Parlamento Europeu e do Conselho. 2. Os dados pessoais devem ser tratados pelas entidades obrigadas com base na presente diretiva apenas para efeitos de prevenção do branqueamento de capitais e do financiamento do terrorismo, tal como referido no artigo 1.º, e não devem ser tratados posteriormente de forma incompatível com esses fins. É proibido o tratamento de dados pessoais com base na presente diretiva para quaisquer outros fins, tais como fins comerciais. (...) Artigo 43.º O tratamento de dados pessoais com base na presente diretiva para efeitos de prevenção do branqueamento de capitais e do financiamento do terrorismo, tal como referido no artigo 1.º, é considerado uma questão de interesse público nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (24). Artigo 56.º (...) 2. Os Estados-Membros devem assegurar que, a fim de cumprir as suas funções previstas na presente

	diretiva, as suas UIF cooperem na aplicação de tecnologias de ponta, em conformidade com a sua legislação nacional. Essas tecnologias devem permitir às UIF comparar os seus dados com os de outras UIF de forma anônima, garantindo a proteção total dos dados pessoais, com o objetivo de detectar pessoas de interesse para a UIF noutros Estados-Membros e identificar os seus rendimentos e fundos.
União Europeia: Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010 e revoga a Diretiva 2007/64/CE (aqui)	Definições (...) (32) «Dados de pagamento sensíveis»: dados, incluindo credenciais de segurança personalizadas, que podem ser utilizados para cometer fraudes. No que diz respeito às atividades dos prestadores de serviços de iniciação de pagamentos e dos prestadores de serviços de informação sobre contas, o nome do titular da conta e o número da conta não constituem dados de pagamento sensíveis; CAPÍTULO 4 - Proteção de dados. Artigo 94. Proteção de dados. Os Estados-Membros devem permitir o tratamento de dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços de pagamento, quando necessário para salvaguardar a prevenção, investigação e deteção de fraudes nos pagamentos. A prestação de informações às pessoas singulares sobre o tratamento de dados pessoais e o tratamento desses dados pessoais e qualquer outro tratamento de dados pessoais para efeitos da presente diretiva deve ser efetuada em conformidade com a Diretiva 95/46/CE, as regras nacionais que transpõem a Diretiva 95/46/CE e o Regulamento (CE) n.º 45/2001. 2. Os prestadores de serviços de pagamento só podem aceder, tratar e conservar os dados pessoais necessários para a prestação dos seus serviços de pagamento, com o consentimento explícito do utilizador dos serviços de pagamento.
União Europeia: Diretiva (UE) 2023/2225 do Parlamento Europeu e do Conselho, de 18 de outubro de 2023, relativa aos contratos de crédito aos consumidores e que revoga a Diretiva 2008/48/CE (aqui)	Considerando (13) | É necessária uma harmonização total para garantir que todos os consumidores da União beneficiem de um nível elevado e equivalente de proteção dos seus interesses e para criar um mercado interno que funcione bem. Por conseguinte, os Estados-Membros não devem ser autorizados a manter ou introduzir disposições nacionais que divergem das estabelecidas na presente diretiva, salvo disposição em contrário na presente diretiva. No entanto, essa restrição só deve aplicar-se quando existam disposições harmonizadas na presente diretiva. Na

	ausência de disposições harmonizadas, os Estados-Membros devem continuar a ter a liberdade de manter ou introduzir legislação nacional. Por conseguinte, os Estados-Membros devem ter a possibilidade de manter ou introduzir disposições nacionais relativas à responsabilidade solidária do fornecedor de bens ou do prestador de serviços e do credor. Os Estados-Membros devem também ter a possibilidade de manter ou introduzir disposições nacionais relativas à rescisão de um contrato de venda de bens ou de prestação de serviços quando o consumidor exercer o seu direito de rescisão do contrato de crédito. A este respeito, no caso dos contratos de crédito a prazo indeterminado, os Estados-Membros devem poder fixar um prazo mínimo que deve decorrer entre o momento em que o credor solicita o reembolso e o dia em que o crédito deve ser reembolsado. Considerando (29) | A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos, em especial, pela Carta. Em particular, a presente diretiva respeita plenamente os direitos à proteção dos dados pessoais, à propriedade, à não discriminação, à proteção da vida familiar e profissional e à proteção dos consumidores, nos termos da Carta. Considerando (30) | A presente diretiva não prejudica o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (7), que se aplica a qualquer tratamento de dados pessoais efetuado por credores e intermediários de crédito abrangidos pelo âmbito de aplicação da presente diretiva, e, em particular, não prejudica os princípios relativos ao tratamento de dados pessoais estabelecidos no artigo 5.º desse regulamento, incluindo a minimização dos dados, a exatidão e a limitação da finalidade. Considerando (46) | Tal como salientado na proposta da Comissão de um regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Lei da Inteligência Artificial), publicada em 21 de abril de 2021, os sistemas de inteligência artificial (IA) podem ser facilmente implementados em vários setores da economia e da sociedade, incluindo a nível transfronteiriço, e podem circular em toda a União. Neste contexto, os credores e os intermediários de crédito, ao personalizarem o preço das

	suas ofertas para consumidores específicos ou categorias específicas de consumidores com base em decisões automatizadas, devem informar claramente os consumidores de que o preço que lhes é apresentado é personalizado com base no tratamento automatizado de dados pessoais, incluindo dados inferidos, para que possam ter em conta os riscos potenciais na sua decisão de compra. Nos termos do artigo 14.º, n.º 2, alínea f), do Regulamento (UE) 2016/679, os credores e os intermediários de crédito são igualmente obrigados a informar os consumidores que recebem a oferta sobre as fontes de dados utilizadas para a personalização da oferta. Considerando (48) | Devido ao seu historial médico, muitos sobreviventes de cancro em remissão prolongada são frequentemente vítimas de um tratamento injusto no acesso aos serviços financeiros. Muitas vezes, enfrentam prémios proibitivamente elevados, apesar de estarem curados há muitos anos, ou mesmo décadas. A fim de proporcionar aos consumidores que sobreviveram ao cancro igualdade de acesso aos seguros relacionados com contratos de crédito, os Estados-Membros devem exigir que as apólices de seguro não se baseiem em dados pessoais relativos ao diagnóstico de doenças oncológicas dos consumidores após um período de tempo relevante após o fim do tratamento médico desses consumidores. Esse período de tempo, determinado pelos Estados-Membros, não deve exceder 15 anos a contar do fim do tratamento médico do consumidor. Considerando (55) | A avaliação da solvabilidade deve basear-se em informações sobre a situação financeira e económica. Essas informações devem ser necessárias e proporcionadas à natureza, duração, valor e riscos do crédito para o consumidor, em conformidade com o princípio da minimização de dados estabelecido no Regulamento (UE) 2016/679, e devem ser relevantes, completas e precisas. Essas informações devem incluir, pelo menos, os rendimentos e as despesas do consumidor, tendo devidamente em conta as obrigações atuais do consumidor, nomeadamente as despesas de subsistência do consumidor e do seu agregado familiar, bem como as responsabilidades financeiras do consumidor. Essas informações não devem

	incluir categorias especiais de dados pessoais referidas no artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, tais como dados relativos à saúde, incluindo dados sobre o cancro, nem informações obtidas a partir de redes sociais. As Orientações da Autoridade Bancária Europeia, de 29 de maio de 2020, sobre a concessão e o acompanhamento de empréstimos fornecem orientações sobre as categorias de dados que podem ser utilizadas para o tratamento de dados pessoais para efeitos de avaliação da solvabilidade, que incluem provas de rendimentos ou outras fontes de reembolso e informações sobre ativos e passivos financeiros ou sobre outros compromissos financeiros. Os consumidores devem fornecer informações sobre a sua situação financeira e económica, a fim de facilitar a avaliação da sua solvabilidade. O crédito só deve ser concedido ao consumidor se o resultado da avaliação da sua solvabilidade indicar que as obrigações decorrentes do contrato de crédito serão provavelmente cumpridas nos termos previstos nesse contrato. Ao avaliar a capacidade do consumidor para cumprir as suas obrigações decorrentes do contrato de crédito, o credor deve ter em conta fatores relevantes e circunstâncias específicas, por exemplo, mas não se limitando a, no caso de crédito concedido em conformidade com a presente diretiva para financiar estudos ou cobrir despesas de saúde excecionais, a existência de provas suficientes de que esse crédito proporcionará rendimentos futuros ao consumidor, ou a existência de garantias reais ou outras formas de garantias que o consumidor possa fornecer para garantir o crédito. Considerando (68) | As partes contratantes devem ter o direito de rescindir um contrato de crédito renovável. Além disso, quando assim acordado no contrato de crédito, o credor deve ter o direito de suspender o direito do consumidor de utilizar um contrato de crédito renovável por motivos objetivamente justificados. Essas razões podem incluir, por exemplo, a suspeita de utilização não autorizada ou fraudulenta do crédito ou um aumento significativo do risco de o consumidor não conseguir cumprir a sua obrigação de reembolsar o crédito. A presente diretiva não deve afetar o direito contratual nacional que regula os direitos das partes contratantes de rescindir o contrato de crédito com base numa violação do contrato.

	Artigo 13.º – Ofertas personalizadas com base no tratamento automatizado. Sem prejuízo do Regulamento (UE) 2016/679, os Estados-Membros devem exigir que os credores e os intermediários de crédito informem os consumidores de forma clara e compreensível quando lhes for apresentada uma oferta personalizada baseada no tratamento automatizado de dados pessoais. Artigo 18.º – Obrigação de avaliar a solvabilidade do consumidor (...) 8. Quando a avaliação da solvabilidade envolver o uso de tratamento automatizado de dados pessoais, os Estados-Membros devem garantir que o consumidor tenha o direito de solicitar e obter do credor a intervenção humana, consistindo no direito de: (a) solicitar e obter do credor uma explicação clara e compreensível da avaliação da solvabilidade, incluindo sobre a lógica e os riscos envolvidos no tratamento automatizado de dados pessoais, bem como o seu significado e efeitos na decisão; (b) expressar o seu próprio ponto de vista ao credor; e (c) solicitar uma revisão da avaliação da solvabilidade e da decisão sobre a concessão do crédito pelo credor. Artigo 19.º – Bases de dados (...) 5. Os credores e os intermediários de crédito não devem tratar categorias especiais de dados, tal como referido no artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, nem dados pessoais tratados a partir de redes sociais que possam estar contidos nas bases de dados referidas no n.º 1 do presente artigo.
União Europeia: **Digital Operational Resilience Act (DORA** - aqui**)**	Regulamento para reforçar a resiliência digital das entidades financeiras.
EUA: FCRA - Fair Credit Reporting Act (EUA) (aqui e aqui)	A lei regula como as agências de crédito coletam, acessam e compartilham as informações contidas nos seus relatórios de crédito.
EUA: Equal Credit Opportunity Act (aqui)	A lei proíbe credores de discriminar solicitantes de crédito.
Reino Unido: Regulamentos dos Serviços de Pagamento de 2017 (PSRs) (aqui)	2. Dados de pagamento sensíveis: informações, incluindo credenciais de segurança personalizadas, que podem ser utilizadas para cometer fraudes; mas, no que diz respeito aos serviços de informação sobre contas e aos serviços de iniciação de pagamentos, não incluem o nome do titular da conta nem o número da conta;

	97. Um prestador de serviços de pagamento não deve aceder, tratar ou conservar quaisquer dados pessoais para a prestação de serviços de pagamento por si, a menos que tenha o consentimento explícito do utilizador dos serviços de pagamento para o fazer.
Reino Unido: Lei de Dados (Uso e Acesso) de 2025 (aqui)	Acrescenta como interesse público a prevenção e detecção à fraude: Para efeitos do presente parágrafo, o armazenamento técnico ou o acesso técnico a informações é estritamente necessário para a prestação de um serviço da sociedade da informação solicitado pelo assinante ou utilizador se, por exemplo, o armazenamento ou o acesso for estritamente necessário (...) (c) para prevenir ou detectar fraudes relacionadas com a prestação do serviço solicitado.
Reino Unido: Regulamentos de 2017 relativos à lavagem de dinheiro, financiamento do terrorismo e transferência de fundos (aqui)	41. (1) Quaisquer dados pessoais obtidos pelas pessoas relevantes para os fins do presente regulamento só podem ser tratados para efeitos de prevenção do branqueamento de capitais, do financiamento do terrorismo ou do financiamento da proliferação. (...) (6) Antes de estabelecer uma relação comercial ou realizar uma transação ocasional com um novo cliente, bem como de fornecer ao cliente as informações exigidas nos termos do artigo 13.º das informações a fornecer quando os dados pessoais são recolhidos junto do titular dos dados, as pessoas relevantes devem fornecer ao cliente uma declaração de que quaisquer dados pessoais recebidos do cliente serão tratados apenas — (a) para efeitos de prevenção do branqueamento de capitais, do financiamento do terrorismo ou do financiamento da proliferação, ou (b) conforme permitido nos termos do n.º (3).
Argentina: Lei 25.326/2000 (aqui)	Artigo 26.º (Prestação de serviços de informação de crédito). 1. Na prestação de serviços de informação de crédito, só podem ser tratados dados pessoais de natureza patrimonial relativos à solvência económica e ao crédito, obtidos de fontes acessíveis ao público ou provenientes de informações fornecidas pelo interessado ou com o seu consentimento. 2. Também podem ser tratados dados pessoais relativos ao cumprimento ou incumprimento de obrigações de conteúdo patrimonial, fornecidos pelo credor ou por quem agir por sua conta ou interesse. 3. A pedido do titular dos dados, o responsável ou usuário do banco de

	dados comunicará as informações, avaliações e apreciações que tenham sido comunicadas sobre o mesmo durante os últimos seis meses e o nome e endereço do cessionário, no caso de se tratar de dados obtidos por cessão. 4. Só poderão ser arquivados, registrados ou cedidos os dados pessoais que sejam significativos para avaliar a solvência econômico-financeira dos afetados durante os últimos cinco anos. Esse prazo será reduzido para dois anos quando o devedor cancelar ou extinguir de outra forma a obrigação, devendo esse fato ser registrado. 5. A prestação de serviços de informação de crédito não exigirá o consentimento prévio do titular dos dados para efeitos de sua cessão, nem a posterior comunicação da mesma, quando estiverem relacionados com o exercício das atividades comerciais ou de crédito dos cessionários.
Paraguai: Lei nº 7.593/2025 (aqui)	Artigo 21. Tratamento de dados de informação creditícia. A proteção de dados creditícios, a regulamentação da atividade de coleta e acesso a dados de informação creditícia, bem como a constituição, organização, funcionamento, direitos, obrigações e extinção das pessoas jurídicas que se dedicam à obtenção e fornecimento de informação creditícia serão regidos pela lei específica vigente a esse respeito. Exceto as funções e atribuições expressamente atribuídas ao Banco Central do Paraguai, as demais concedidas para a implementação da lei que regula os dados de crédito serão exercidas pela autoridade de controle e supervisão da presente lei. A presente lei será de aplicação supletiva para as questões não previstas na lei que regula os dados de crédito, desde que sejam compatíveis com a natureza dessas informações. Artigo 33. Direitos perante decisões individuais automatizadas ou semiautomatizadas. O titular dos dados tem o direito de solicitar a revisão das decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem negativamente os seus interesses ou produzam efeitos jurídicos, incluindo as decisões destinadas a definir os seus aspectos pessoais, profissionais, de consumo, de crédito e de personalidade. Tem também o direito de expressar o seu ponto de vista e de contestar a decisão. O responsável pelo tratamento deve fornecer, sempre que solicitado, informações claras, completas e adequadas sobre os critérios e procedimentos utilizados para a decisão

	automatizada, respeitando os segredos comerciais e industriais do titular ou que o titular seja obrigado por lei ou por contrato a guardar. Deve adotar as medidas adequadas para salvaguardar os direitos do titular dos dados. Este direito não suprime nem substitui o exercício de outros direitos que possam ocorrer.
Uruguai: Lei nº 18.331/2008 (aqui)	Artigo 16.º (Direito de impugnar avaliações pessoais). As pessoas têm o direito de não serem submetidas a uma decisão com efeitos jurídicos que as afete significativamente, baseada no tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, tais como o seu desempenho profissional, crédito, fiabilidade, conduta, entre outros. O interessado poderá contestar os atos administrativos ou decisões privadas que impliquem uma avaliação do seu comportamento, cujo único fundamento seja um tratamento de dados pessoais que ofereça uma definição das suas características ou personalidade. Neste caso, o interessado terá o direito de obter informações do responsável pela base de dados tanto sobre os critérios de avaliação como sobre o programa utilizado no tratamento que serviu para adotar a decisão manifestada no ato. Artigo 22.º (Dados relativos à atividade comercial ou de crédito). É expressamente autorizado o tratamento de dados destinados a informar sobre a solvência patrimonial ou de crédito, incluindo aqueles relativos ao cumprimento ou incumprimento de obrigações de natureza comercial ou de crédito que permitam avaliar a celebração de negócios em geral, a conduta comercial ou a capacidade de pagamento do titular dos dados, nos casos em que os mesmos sejam obtidos de fontes de acesso público ou provenientes de informações fornecidas pelo credor ou nas circunstâncias previstas na presente lei. No caso das pessoas jurídicas, além das circunstâncias previstas na presente lei, é permitido o tratamento de todas as informações autorizadas pela normativa vigente. Os dados pessoais relativos a obrigações de natureza comercial de pessoas físicas só poderão ser registrados por um prazo de cinco anos a partir de sua incorporação. Caso, ao término desse prazo, a obrigação permaneça inadimplente, o credor poderá solicitar ao responsável pela base de dados, por uma única vez, seu novo registro por mais cinco anos. Esse novo

	registro deverá ser solicitado no prazo de trinta dias anteriores ao vencimento original. As obrigações canceladas ou extintas por qualquer meio permanecerão registradas, com menção expressa desse fato, por um prazo máximo de cinco anos, não renovável, a partir da data do cancelamento ou extinção. Os responsáveis pelas bases de dados limitar-se-ão a realizar o tratamento objetivo das informações registradas tal como lhes foram fornecidas, devendo abster-se de fazer avaliações subjetivas sobre as mesmas. Quando a cancelamento de qualquer obrigação não cumprida registrada em uma base de dados se tornar efetivo, o credor deverá, no prazo máximo de cinco dias úteis após o fato, comunicá-lo ao responsável pela base de dados ou pelo tratamento correspondente. Uma vez recebida a comunicação pelo responsável pela base de dados ou pelo tratamento, este disporá de um prazo máximo de três dias úteis para proceder à atualização dos dados, registando a sua nova situação.

Adoção Voluntária:

Norma	Temática
ISO 37003	Sistemas de Gestão de Controle de Fraude
ISA 240	Norma Internacional de Auditoria sobre Fraude (IAASB)

Conselheiros responsáveis: Rony Vainzof, Myreilla Aloia e Annette Pereira.

ANEXO II – Precedentes judiciais

Levantamento apresenta precedentes judiciais relevantes sobre proteção ao crédito e prevenção à fraude, com foco em:

- legalidade e limites do *score* de crédito;
- interação entre LGPD e Lei do Cadastro Positivo (Lei 12.414/2011);
- tratamento e compartilhamento de dados pessoais em bancos de dados de crédito; e
- responsabilidade por fraudes e vazamento de dados em operações financeiras.

Conforme alinhado em reunião do GT5, para cada precedente selecionado, são indicados ementa (em síntese), link de referência do julgado e comentários sobre fundamentos e impactos práticos, em linguagem técnica, porém descritiva, voltada ao apoio dos debates do CNPD.

1. Precedentes selecionados
Quadro-resumo

Julgado	Tema central	Tese sobre compartilhamento / consentimento	Posição sobre da no moral	Impacto prático r esumido
REsp 1.419.697/ RS (Tema 710/STJ)	Licitude do *credit scoring* e limites de uso de dados	*Score* pode ser utilizado sem consentimento específico, desde que respeitados privacidade, transparência e vedação a dados sensíveis/excessivos.	Admite dano moral em caso de uso abusivo, com dados incorretos, sensíveis ou excessivos.	Paradigma sobre *score*; base para leitura conjunta com a LGPD e para deveres de transparência e qualidade dos dados.
REsp 1.344.352/ SP (Tema 793/STJ)	Reprodução de dados cartorários por órgãos de proteção ao crédito	Reprodução fiel, objetiva e atualizada de dados públicos cartorários dispensa consentimento e comunicação prévia ao consumidor.	Afasta dever de indenizar em caso de reprodução fiel de dados cartorários públicos.	Fundamenta o cadastro negativo pré-LGPD; hoje precisa ser lido à luz de finalidade, necessidade e transparência.
REsp 2.133.261/ SP (Boa Vista)	Cadastro Positivo – compartilhamento de dados cadastrais/adi mplemento	Tratamento pode ocorrer sem consentimento, mas dados cadastrais/adimplemento só podem ser compartilhados entre bancos de dados; histórico requer autorização específica.	Dano moral presumido pela disponibilização indevida de dados cadastrais/adimpl emento.	Marco de contenção do uso expansivo de dados cadastrais; reforç a limites da Lei 12.414/2011 e da LGPD.

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

REsp 2.115.461/ SP (Serasa)	Cadastro Positivo – disponibilização indevida a consulentes	Consulentes podem receber *score* sem consentimento e histórico com autorização; dados cadastrais/adimplemento só podem circular entre bancos de dados.	Dano moral presumido em razão da sensação de insegurança do titular.	Consolida a linha da Terceira Turma sobre ilicitude de compartilhamento indevido de dados cadastrais/adimplemento.
REsp 2.221.650/ SP (Quarta Turma)	Dados pessoais não sensíveis – necessidade de prova do dano	Tratamento para proteção do crédito é legítimo; mera alegação de disponibilização, sem prova concreta, não basta para responsabilização.	Não admite dano moral presumido; exige prova de abalo aos direitos de personalidade.	Introduz nuance e possível tensão com a Terceira Turma; reforça importância da prova da disponibilização indevida.
REsp 2.077.278/ SP	"Golpe do boleto" e vazamento de dados bancários	Vazamento de dados bancários sigilosos caracteriza defeito do serviço; tratamento inadequado que facilita golpes gera responsabilidade da instituição.	Reconhece dever de indenizar quando demonstrado nexo entre vazamento e fraude; alinhado à Súmula 479/STJ.	Aproxima LGPD, CDC e sigilo bancário; relevante para modelos de antifraude e segurança da informação.
REsp 2.201.694 / 2201694-SP	Cadastro Positivo – disponibilização indevida a consulentes	*Score* pode ser fornecido a consulentes; histórico depende de autorização; dados cadastrais/adimplemento só podem circular entre bancos de dados.	Dano moral presumido pela disponibilização indevida.	Reforça limites da Lei 12.414/2011 e consolida leitura restritiva sobre circulação de dados de crédito.
REsp 2.207.172 / 2207172-SP	Cadastro Positivo – confirmação da linha sobre dano presumido	Reitera distinção entre score, histórico e dados cadastrais/adimplemento; considera ilícito o acesso de consulentes a dados que só circulariam entre bancos de dados.	Dano moral presumido em caso de disponibilização indevida.	Precedente de confirmação, conferindo estabilidade à jurisprudência da Terceira Turma.
Apelação Cível 1 001338-	Divulgação de dados meramente cadastrais	Admite uso de dados meramente cadastrais para proteção ao crédito sem	Afasta dano moral na hipótese concreta;	Exemplo de interpretação mais flexível em

31.2021.8.26.0042 (TJSP)		comunicação prévia na hipótese concreta, com base no art. 7º, X, LGPD.	entende inexistente ilicitude.	instância ordinária, contrastando com a linha mais protetiva do STJ.

1.1. *Score* de crédito – paradigma do STJ

RECURSO ESPECIAL Nº 1.419.697 - RS (2013/0386285-0)

REsp 1.419.697/RS (Tema 710/STJ) – sistema *"credit scoring"*

- Tribunal / Órgão: STJ, Segunda Seção, recurso repetitivo (Tema 710)
- Tema: Licitude do *score* de crédito e limites de uso dos dados pelo fornecedor/gestor de banco de dados.

Ementa (síntese)

O STJ definiu que o *credit scoring* é método estatístico para avaliação do risco de concessão de crédito, baseado em múltiplas variáveis, com atribuição de pontuação ao consumidor. Ressaltou que o *credit scoring* constitui metodologia de cálculo e não se confunde com banco de dados de crédito em si. A Corte considerou a prática lícita, à luz da disciplina da proteção ao crédito e da Lei 12.414/2011 (Cadastro Positivo), desde que respeitados: (i) a privacidade, (ii) a transparência nas relações de consumo e (iii) os limites de utilização de informações, especialmente evitando dados sensíveis ou excessivos. O consentimento prévio do consumidor é dispensado, mas o titular tem direito de solicitar esclarecimentos sobre as fontes e as informações pessoais utilizadas no cálculo. O uso de dados sensíveis, excessivos, incorretos ou desatualizados, bem como recusa indevida de crédito, pode gerar responsabilidade civil por dano moral.

Comentários – fundamentos e impactos

- O precedente reconhece a licitude do *scoring*, mas o qualifica como metodologia de cálculo, e não como banco de dados em si, o que tem reflexos na aplicação da Lei 12.414/2011.
- A decisão consolidou a ideia de que não há necessidade de consentimento específico para o uso do score, desde que haja direito de informação sobre os dados utilizados e que não se empreguem dados sensíveis ou excessivos.
- Com a edição da LGPD, esse entendimento passou a ser lido em conjunto com o art. 7º, X, LGPD (proteção ao crédito), reforçando a tensão entre a dispensa de consentimento e a exigência de transparência, minimização e finalidade.
- Na prática, o Tema 710 e a Súmula 550/STJ servem como ponto de partida para discussões atuais sobre:
  - deveres de informação dos gestores de *scoring;*
  - fronteira entre dados meramente cadastrais, dados de adimplemento e dados sensíveis; e
  - risco de responsabilização quando o *score* se baseia em dados desatualizados ou incorretos.

RECURSO ESPECIAL Nº 1.344.352 - SP (2012/0194674-7)
REsp 1.344.352/SP – reprodução fiel de dados cartorários em banco de dados • Tribunal / Órgão: STJ, Segunda Seção, recurso repetitivo (Tema 793) • Tema: Reprodução, por órgão de proteção ao crédito, de registros de cartório de distribuição judicial. **Ementa (síntese)** O STJ fixou a tese de que, diante da presunção de veracidade e publicidade dos registros do cartório de distribuição judicial, a reprodução objetiva, fiel, atualizada e clara desses dados por órgão de proteção ao crédito, ainda que sem ciência do consumidor, não gera dever de indenizar. Trata-se de exercício regular de direito, dispensando notificação prévia ao consumidor. **Comentários – fundamentos e impactos** • Este repetitivo consolida, no "pré-LGPD", uma orientação de ampla legitimação da reprodução de dados públicos (cartórios) por órgãos de proteção ao crédito. • Após a LGPD, a leitura desse precedente convive com princípios de necessidade, finalidade e transparência, sem que a publicidade da fonte elimine, por si só, os deveres de limitação e governança do tratamento. • Para a governança de dados, o caso é frequentemente citado como fundamento histórico da legitimidade do cadastro negativo, mas hoje precisa ser contextualizado à luz do novo regime de proteção de dados.

1.2. Consentimento, LGPD e Cadastro Positivo

RECURSO ESPECIAL Nº 2133261 - SP (2024/0109609-9)
REsp 2.133.261/SP – Boa Vista (2024) • Tribunal / Órgão: STJ, Terceira Turma • Tema: Compartilhamento, por gestor de banco de dados, de informações cadastrais e de adimplemento com terceiros consulentes. **Ementa (síntese)** O STJ reafirmou a distinção entre *score* de crédito (Tema 710/Súmula 550) e banco de dados regido pela Lei 12.414/2011. Entendeu que o gestor de banco de dados pode registrar e tratar dados de adimplemento sem consentimento, com base na Lei do Cadastro Positivo e na LGPD (art. 7º, X). Contudo, somente o *score* pode ser disponibilizado a terceiros consulentes sem consentimento; o histórico de crédito exige autorização específica do cadastrado, e os dados cadastrais e de adimplemento só podem ser compartilhados com outros bancos de dados, não com terceiros consulentes. A disponibilização indevida dessas informações a terceiros

consulentes configura dano moral presumido *(in re ipsa)* e enseja a responsabilização objetiva do gestor.

Comentários – fundamentos e impactos

- A decisão aproxima a interpretação da Lei do Cadastro Positivo da LGPD, reforçando que a base "proteção ao crédito" não legitima qualquer compartilhamento amplo de dados cadastrais.
- O entendimento consolida que há três níveis de acesso:
  1. *score* (sem consentimento);
  2. histórico de crédito (com autorização específica); e
  3. dados cadastrais e de adimplemento (compartilháveis entre bancos de dados, não a qualquer consulente).
- O julgamento é frequentemente lido como marco na proteção do titular contra o uso expansivo de dados cadastrais em modelos de negócio que extrapolam a finalidade de proteção ao crédito.

RECURSO ESPECIAL Nº 2221650 - SP (2025/0242836-6)

REsp 2.221.650/SP (2025) – ausência de dano moral presumido (Quarta Turma)

- Tribunal / Órgão: STJ, Quarta Turma
- Tema: Dados pessoais não sensíveis; dano moral não presumido.

Ementa (síntese)

A Quarta Turma, ao tratar da alegada disponibilização de dados pessoais não sensíveis em contexto de proteção ao crédito, reafirmou que o tratamento de dados para proteção do crédito é legítimo, à luz do art. 7º, X, da LGPD e da Lei nº 12.414/2011 (Cadastro Positivo), mas entendeu que não há dano moral presumido. Exige-se (i) prova da disponibilização indevida e (ii) prova de efetivo abalo aos direitos de personalidade. No caso concreto, o recurso foi desprovido por ausência de prova do dano e pela incidência da Súmula 7/STJ.

Comentários – fundamentos e impactos

O caso introduz nuances importantes no debate: enquanto a Terceira Turma admite dano moral presumido em hipóteses de disponibilização indevida de dados cadastrais, a Quarta Turma, em contexto fático específico, enfatiza a necessidade de prova do dano.

- Para fins de política institucional, esse contraste sugere um quadro jurisprudencial ainda em evolução, que pode levar o Conselho a acompanhar a consolidação de entendimentos (eventual afetação a recursos repetitivos ou uniformização futura).
- O precedente também reforça a importância de documentar a origem e o fluxo de dados, uma vez que a própria comprovação da disponibilização indevida se torna elemento central na discussão.

Apelação Cível nº 1001338-31.2021.8.26.0042

Apelação Cível nº 1001338-31.2021.8.26.0042 (TJSP) - Divulgação de dados cadastrais – proteção ao crédito – inexistência de dano moral

- Tribunal / Órgão: TJSP, 2ª Câmara de Direito Privado
- Tema: Tratamento e divulgação de dados meramente cadastrais em contexto de proteção ao crédito; limites da base legal do art. 7º, X, da LGPD.

Ementa (síntese)

No julgamento da Apelação Cível nº 1001338-31.2021.8.26.0042, o Tribunal de Justiça de São Paulo analisou controvérsia envolvendo a divulgação, por empresa de proteção ao crédito, de dados pessoais meramente cadastrais do consumidor. O colegiado concluiu que tais informações — não sensíveis, públicas ou obtidas de forma lícita — podem ser utilizadas para fins de proteção ao crédito com base no art. 7º, X, da LGPD, sem necessidade de consentimento prévio ou comunicação específica ao titular.

A Corte afastou a alegação de ilicitude, entendendo que não houve demonstração de compartilhamento indevido para finalidades estranhas à proteção ao crédito, nem evidência de que a divulgação tenha causado prejuízo efetivo aos direitos de personalidade do titular. Consequentemente, rejeitou a pretensão indenizatória por danos morais, por ausência de violação à esfera jurídica do consumidor.

Comentários – fundamentos e impactos

- O acórdão adota interpretação mais flexível da base legal "proteção ao crédito", entendendo legítimo o tratamento de dados cadastrais comuns sem consentimento, quando restrito à finalidade de análise de crédito (proteção ao crédito).
- O TJSP enfatiza a ausência de ilicitude porque:
  - os dados não eram sensíveis;
  - estavam no contexto típico de consultas de proteção ao crédito; e
  - não houve prova de divulgação indevida ou finalidade incompatível.
- O Tribunal faz referência ao Tema 710/STJ *(credit scoring)* como suporte para a regularidade da atuação de *bureaus* de crédito em seu âmbito próprio.
- O entendimento se aproxima da orientação da Quarta Turma do STJ (REsp 2.221.650/SP), ao exigir prova de dano e afastar a tese de dano moral presumido.
- O precedente evidencia que tribunais estaduais ainda aplicam interpretação mais permissiva ao art. 7º, X, LGPD, especialmente quando lidam com dados cadastrais de baixa criticidade.

RECURSO ESPECIAL Nº 2115461 - SP (2023/0453798-4)

REsp 2.115.461/SP – Serasa (2023/2024)

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Compartilhamento de dados cadastrais e de adimplemento; dano moral presumido.

Ementa (síntese)

Em linha com o REsp 2.133.261/SP, o STJ concluiu que o gestor de banco de dados de crédito não pode disponibilizar a terceiros consulentes dados cadastrais e de adimplemento que, por lei, só podem ser compartilhados com outros bancos de dados (art. 4º, III, Lei 12.414/2011). A disponibilização indevida configura violação aos deveres de tratamento de dados, gera dano moral presumido (*in re ipsa*) e acarreta responsabilidade objetiva.

Comentários – fundamentos e impactos (descritivo)

- Este precedente reforça a coerência interna da Terceira Turma em relação à necessidade de consentimento quando o compartilhamento ultrapassa *score* e histórico autorizado.
- Na perspectiva de risco, as decisões 2.133.261 e 2.115.461 são utilizadas como base para ações de massa sobre disponibilização de dados cadastrais, pois dispensam prova de dano concreto para configurar dano moral.
- O núcleo argumentativo se conecta diretamente à LGPD (arts. 7º, X, 42 e 43) e à Lei 12.414/2011, servindo como referência para políticas internas de governança de dados e limitação de acesso a consulentes.

-

1.3. Proteção do crédito, LGPD e fraudes

RECURSO ESPECIAL Nº 2.077.278 - SP (2023/0190979-8)

REsp 2.077.278/SP (2023) – "golpe do boleto" e vazamento de dados bancários

- Tribunal / Órgão: STJ, Terceira Turma (Informativo 791)
- Tema: Vazamento de dados bancários, engenharia social e responsabilidade objetiva da instituição financeira.

Ementa (síntese)

O STJ analisou caso em que dados bancários do consumidor teriam vazado, possibilitando a aplicação do chamado "golpe do boleto". Reconheceu que, se comprovado vazamento de dados sigilosos sob responsabilidade da instituição financeira, há defeito na prestação do serviço, em razão de tratamento irregular e de falha no dever de segurança da informação (art. 14, CDC; arts. 44 e 46 da LGPD). Concluiu que, quando criminosos demonstram possuir informações internas sobre relacionamento bancário e operações do cliente, está caracterizado o fortuito interno, atraindo a responsabilidade objetiva da instituição, nos termos da Súmula 479/STJ[1].

Súmula 479/STJ
As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. (SÚMULA 479, SEGUNDA SEÇÃO, julgado em 27/06/2012, DJe 01/08/2012)

Comentários – fundamentos e impactos

- O caso conecta diretamente LGPD, CDC, sigilo bancário (LC 105/2001) e responsabilidade por falhas de segurança da informação.
- Embora não trate especificamente de *score* ou cadastro positivo, é relevante para o Conselho na medida em que:
  - reforça a exigência de controles técnicos e organizacionais robustos; e
  - vincula vazamento de dados bancários à noção de fortuito interno, afastando excludentes baseadas em "fraude de terceiro".
- Em diálogo com a Resolução Conjunta 6/2023 do Banco Central (compartilhamento de informações para prevenção a fraudes), o precedente mostra que a base legal ou o dever normativo de compartilhar dados não afastam a responsabilidade quando há falhas de segurança ou uso indevido.

RECURSO ESPECIAL Nº 2201694 - SP (2025/0081134-2)

REsp 2.201.694/2201694-SP (2025) – disponibilização indevida de dados em cadastro positivo

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Cadastro Positivo – disponibilização de informações cadastrais e de adimplemento a terceiros consulentes.

Ementa (síntese)

O STJ analisou ação de obrigação de fazer cumulada com indenização por danos morais envolvendo a disponibilização de dados de cadastro positivo a terceiros consulentes. A Terceira Turma afastou a aplicação direta do Tema 710/STJ e da Súmula 550/STJ, que tratam especificamente do *credit scoring*, ressaltando que este não constitui banco de dados, o qual é regulado pela Lei nº 12.414/2011. Com base no art. 4º da Lei do Cadastro Positivo, a Turma reafirmou que o gestor de banco de dados: (i) pode disponibilizar ao consulente o *score* de crédito, sem necessidade de consentimento; (ii) pode disponibilizar o histórico de crédito, desde que haja autorização prévia e específica do cadastrado; e (iii) somente pode compartilhar informações cadastrais e de adimplemento com outros bancos de dados. A disponibilização dessas informações a terceiros consulentes foi qualificada como disponibilização indevida, gerando responsabilidade objetiva do gestor e dano moral presumido (*in re ipsa*), em razão da sensação de insegurança experimentada pelo titular. O recurso especial foi conhecido e provido.

Comentários – fundamentos e impactos

- Reafirma, de forma expressa, a separação entre *"credit scoring"* e banco de dados de crédito, restringindo o alcance do Tema 710/Súmula 550.
- Define um modelo escalonado de acesso:
  - *score* de crédito → disponibilização a consulentes, sem consentimento específico;
  - histórico de crédito → acesso condicionado a autorização específica;
  - dados cadastrais e de adimplemento → compartilhamento restrito a outros bancos de dados.
- Consagra a tese de que a disponibilização indevida de dados cadastrais/adimplemento a consulentes configura, por si só, dano moral presumido, sem necessidade de prova de prejuízo adicional.
- Reforça a leitura de que a base "proteção ao crédito" (art. 7º, X, LGPD) não legitima o uso ampliado de dados cadastrais para finalidades diversas das hipóteses estritas previstas na Lei nº 12.414/2011.

RECURSO ESPECIAL Nº 2207172 - SP (2025/0119413-2)

REsp 2.207.172/2207172-SP (2025) – disponibilização indevida de dados e dano moral presumido

- Tribunal / Órgão: STJ, Terceira Turma
- Tema: Banco de dados de crédito – limites de compartilhamento e responsabilidade por disponibilização indevida.

Ementa (síntese)

No REsp 2207172/SP, a Terceira Turma voltou a examinar ação de obrigação de fazer cumulada com compensação por danos morais relacionada à disponibilização de dados de cadastro positivo a terceiros consulentes. Assim como em julgados anteriores, o colegiado registrou que o Tema 710/STJ e a Súmula 550/STJ se referem exclusivamente ao *credit scoring*, não se confundindo com bancos de dados regulados pela Lei nº 12.414/2011. Com base nos incisos III e IV do art. 4º da lei, a Turma reiterou que: (i) o gestor de banco de dados pode compartilhar informações cadastrais e de adimplemento apenas com outros bancos de dados; (ii) pode disponibilizar aos consulentes o *score* de crédito, sem consentimento específico; e (iii) pode fornecer o histórico de crédito mediante autorização prévia e específica do titular. A concessão de acesso a dados cadastrais e de adimplemento diretamente a consulentes foi considerada ilícita, ensejando responsabilidade objetiva e dano moral presumido, diante da violação aos deveres legais de tratamento de dados.

Comentários – fundamentos e impactos

- Reitera, de maneira quase espelhada ao REsp 2201694/SP, a interpretação restritiva do art. 4º da Lei do Cadastro Positivo, consolidando a linha jurisprudencial da Terceira Turma.

- Confirma que, para o STJ, há tratamento diferenciado entre:
  - dados usados para score;
  - dados que compõem o histórico de crédito; e
  - dados cadastrais e de adimplemento, cuja circulação é mais limitada.
- Reforça a ideia de que a mera disponibilização indevida de dados a quem não poderia recebê-los é suficiente para a configuração de dano moral, consolidando o entendimento de dano moral "*in re ipsa*" em hipóteses de violação às regras de compartilhamento do Cadastro Positivo.
- Funciona, na prática, como precedente de confirmação da tese firmada em outros casos da mesma Turma (como REsp 2.133.261/SP e REsp 2.115.461/SP), conferindo estabilidade à interpretação sobre os limites de compartilhamento de dados de crédito.

-

2. Aspectos transversais identificados na pesquisa

2.1. Aplicação do regime de proteção de dados na prevenção e detecção de fraudes

A legislação brasileira, especialmente a LGPD, combinada com normas setoriais do Banco Central (como a Resolução Conjunta nº 6, de 23/5/2023), admite o tratamento de dados pessoais para segurança e prevenção a fraudes, desde que observados os princípios de finalidade, adequação, necessidade, segurança e responsabilização.

Esse tratamento se distingue do processamento voltado exclusivamente à concessão de crédito:

- na prevenção a fraudes, o foco é a identificação de comportamentos ou operações atípicas;
- exige seleção de dados estritamente relevantes para essa finalidade; e
- demanda mecanismos de rastreabilidade e auditoria, em especial diante da possibilidade de responsabilização civil por vazamentos ou uso indevido.

A Resolução Conjunta nº 6/2023 estabelece, entre outros pontos:

- que o compartilhamento de informações sobre indícios de fraude ocorra por meio de sistema eletrônico capaz de registrar, alterar, excluir e consultar informações, garantindo integridade e rastreabilidade;
- conteúdo mínimo dos registros (identificação do suposto autor, descrição dos indícios, instituição responsável, conta destinatária, quando aplicável);
- previsão de hipóteses específicas de consentimento e de requisitos reforçados de governança, conforme o tipo de registro e o fluxo de compartilhamento; e
- controles técnicos e administrativos para assegurar confidencialidade, integridade, disponibilidade e segregação de dados, com mecanismos de auditoria e interoperabilidade entre sistemas.

No recorte específico de crédito e prevenção a fraudes, ganham destaque os limites ao uso de dados pessoais sensíveis e a proteção adicional de grupos vulneráveis. A base legal de "proteção ao crédito" (art. 7º, X, da LGPD) não legitima, por si só, o tratamento de dados pessoais sensíveis (como dados de saúde, biometria,

filiação sindical ou convicções religiosas) e tende a ser pertinente apenas quando a prevenção a fraudes estiver funcionalmente integrada à decisão ou à gestão de crédito; em outros fluxos antifraude (p. ex., monitoramento transacional, segurança do canal, prevenção a ataques e engenharia social), é comum também o enquadramento por obrigação legal/regulatória (art. 7º, II) e/ou legítimo interesse (art. 7º, IX), conforme o caso, com documentação e medidas de governança.

Além disso, tratamentos que envolvam crianças e adolescentes, por exemplo, dados de dependentes vinculados a contas de responsáveis, demandam cuidado reforçado, em consonância com o art. 14 da LGPD, o que indica um campo relevante para futura análise e eventual produção de orientações específicas pelo CNPD e pela ANPD.

2.2. Transparência e direitos dos titulares

Os precedentes sobre *score* de crédito (Tema 710/STJ) e Cadastro Positivo apontam para um núcleo comum:

- o *credit scoring* é prática lícita, mas sujeita a deveres de transparência e respeito à privacidade;
- o titular tem direito a esclarecimentos sobre fontes e categorias de dados utilizados, bem como sobre critérios relevantes que afetem sua pontuação; e
- subsistem plenamente os direitos previstos na LGPD, como acesso, correção, exclusão, anonimização e oposição, especialmente quando o tratamento impacta a concessão de crédito ou o compartilhamento de dados.

A jurisprudência recente do STJ (como no REsp 2.133.261/SP) reconhece que a inobservância de deveres de tratamento, incluindo o dever de informar e de manter dados corretos e atualizados, pode gerar:

- pretensão de cessar a ilicitude (como ordens de não compartilhamento indevido); e
- indenização por danos morais, sobretudo quando há negativa indevida de crédito ou disponibilização irregular de dados.

Há decisões de instâncias ordinárias, como a Apelação Cível nº 1001338-31.2021.8.26.0042 (TJSP), que entendem que, em certas hipóteses envolvendo dados meramente cadastrais utilizados estritamente para proteção do crédito, o art. 7º, X, da LGPD poderia afastar a necessidade de comunicação específica ao titular. Esse entendimento, contudo, não reflete a linha majoritária do STJ, que tende a preservar a centralidade da transparência tanto no *scoring* quanto na gestão de bancos de dados.

De forma sintética, o panorama atual se organiza em torno de três premissas:

1. direito à informação sobre variáveis e fontes no *scoring*;
2. direito de acesso, correção, exclusão e oposição no contexto de bancos de dados; e
3. responsabilização objetiva quando o tratamento contrariar limites da LGPD, do CDC ou da Lei nº 12.414/2011.

No contexto de proteção ao crédito e prevenção a fraudes, é relevante observar que diversos modelos utilizados pelas instituições – como sistemas de *credit scoring*, motores de decisão de crédito e ferramentas automatizadas de detecção de transações suspeitas – podem configurar decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, com efeitos relevantes para o titular (por exemplo, concessão ou recusa de crédito, bloqueio de operações ou aumento de monitoramento).

Nesses casos, ganham relevo as garantias previstas no art. 20 da LGPD, que assegura ao titular o direito de solicitar revisão de decisões automatizadas, bem como informações claras e acessíveis sobre os critérios gerais utilizados. Embora ainda não haja consolidação jurisprudencial específica sobre a aplicação desse dispositivo em matéria de crédito e antifraude, o tema tende a se tornar objeto de futura atuação normativa e interpretativa da ANPD e do próprio CNPD, especialmente quanto à definição de parâmetros mínimos de transparência e salvaguardas em modelos estatísticos e algorítmicos.

2.3. Atuação da ANPD no contexto de proteção ao crédito e prevenção a fraudes

O tratamento de dados pessoais para proteção ao crédito e prevenção a fraudes, ainda que apoiado em bases legais específicas (art. 7º, X, II e IX, LGPD), está sujeito à fiscalização administrativa da ANPD e às sanções dos arts. 52 a 54 da LGPD, tais como:

- advertência;
- multa simples ou diária;
- publicização da infração;
- bloqueio ou eliminação de dados pessoais; e
- suspensão parcial ou total das atividades de tratamento.

A existência de regulamentação setorial (como a Resolução Conjunta nº 6/2023 ou normas do *Open Finance*) não exclui a aplicação plena da LGPD nem limita o poder sancionador da ANPD. Mesmo quando o compartilhamento de dados decorre de dever regulatório, permanecem exigíveis:

- observância de finalidade, necessidade, adequação, segurança e responsabilização; e
- mecanismos efetivos de rastreabilidade, controle de acesso, auditoria e correção de dados.

O descumprimento de direitos dos titulares (atraso ou negativa na resposta a pedidos de acesso, retificação ou exclusão; compartilhamento indevido; manutenção de dados desatualizados; uso de sistemas automatizados sem garantir direitos do art. 20 da LGPD) pode configurar, simultaneamente:

- ilícitos civis, a serem discutidos no Judiciário; e
- infrações administrativas, sujeitas a sanções pela ANPD.

Desse modo, o regime atual combina dois planos de responsabilização:

- judicial indenizatório, conduzido sobretudo pelo STJ; e
- administrativo sancionador, sob supervisão da ANPD, com impacto direto sobre a continuidade e o modelo de tratamento de dados.

Além da dimensão sancionadora, a atuação da ANPD tende a se desenvolver também por meio de instrumentos de soft law, como guias orientativos, recomendações, modelos de boas práticas, mecanismos de governança e eventuais programas de certificação ou selos. Em setores intensivos em dados, como o de proteção ao crédito, prevenção a fraudes, monitoramento transacional e *Open Finance*, esses instrumentos podem desempenhar papel relevante na consolidação de padrões setoriais de transparência, segurança e avaliação de impacto, influenciando de forma indireta, porém significativa, o desenho de produtos e serviços e a gestão de riscos regulatórios pelas instituições.

Algumas experiências internacionais recentes, especialmente sob a aplicação do *General Data Protection Regulation (GDPR),* evidencia o endurecimento do controle regulatório sobre atividades de *credit scoring* e decisões automatizadas no setor financeiro. No caso SCHUFA (CJEU, dezembro de 2023), o Tribunal de Justiça da União Europeia entendeu que a atribuição automatizada de *score* de crédito por *bureau* pode configurar decisão individual automatizada, atraindo a incidência do art. 22 do GDPR, especialmente quando terceiros (como instituições financeiras) se apoiam fortemente nesse valor para estabelecer, executar ou encerrar relação contratual com o titular, com repercussões quanto ao direito à intervenção humana e às informações significativas sobre os critérios gerais aplicados[2]. Em paralelo, autoridades de proteção de dados alemãs aplicaram sanções em contextos de recusa automatizada de crédito sem transparência adequada, retenção excessiva de dados e ausência de base legal após o término da relação jurídica, reforçando os princípios de limitação temporal, necessidade e informação.

Há registros de atuação sancionatória e de investigações setoriais por autoridade regional alemã *(Hamburg Data Protection Authority – HmbBfDI)* em matéria de retenção/exclusão e governança do tratamento de dados no contexto de cobrança e bases de dados de crédito, reafirmando os princípios de limitação temporal e necessidade[3]. Esses referenciais indicam que, mesmo em ambientes altamente regulados por normas financeiras e de *Open Finance*, autoridades de proteção de dados mantêm escrutínio rigoroso sobre *credit scoring*, decisões automatizadas[4], compartilhamento e retenção de dados, cenário que pode servir de parâmetro comparativo para a evolução da atuação da ANPD no contexto brasileiro.

De qualquer forma, importante lembrar que o GDPR é distinto da LGPD em diversos aspectos, inclusive em relação a decisões automatizadas e proteção do crédito, de modo que não se recomenda importar literalmente decisões ou padrões legislativos externos, devendo-se avaliar a pertinência e compatibilidade com o sistema legal e especificidades do cenário brasileiro, ainda mais diante de precedentes já existentes no STJ sobre o tema

2.4. Bases legais: proteção ao crédito, obrigação legal e legítimo interesse

No setor financeiro e de proteção ao crédito, destacam-se, no art. 7º da LGPD, três bases legais principais:

- Proteção ao crédito (art. 7º, X)

  Sustenta o tratamento de dados pessoais para formação de histórico de crédito, manutenção de cadastros e uso de score, bem como em contextos de aplicação da Lei nº 12.414/2011.
- Cumprimento de obrigação legal ou regulatória (art. 7º, II)

  Fundamenta atividades de *KYC*, prevenção à lavagem de dinheiro, atendimento a normas do Banco Central e registros exigidos por regulação prudencial.
- Legítimo interesse do controlador (art. 7º, IX)

  Frequentemente invocado em contextos de prevenção a fraudes, monitoramento transacional, análises comportamentais e cruzamento de dados internos, desde que:
  - haja teste de balanceamento entre o interesse do controlador e os direitos do titular;
  - o tratamento seja limitado ao estritamente necessário; e
  - sejam implementadas salvaguardas técnicas e organizacionais.

No *Open Finance*, o compartilhamento de dados ocorre em um ambiente de coexistência entre:

- fluxos baseados em consentimento (iniciados pelo próprio titular);

- fluxos decorrentes de obrigação legal ou regulatória e de legítimo interesse, sobretudo em cenários de prevenção a fraudes e segurança do sistema.

A ANPD tem ressaltado, em guias e manifestações, a necessidade de que a escolha da base legal:

- seja motivadamente registrada;
- possa ser auditada; e
- esteja alinhada com documentação de riscos e medidas de mitigação.

Embora o STJ não tenha decidido diretamente casos sobre a escolha entre legítimo interesse e obrigação legal em *KYC*, monitoramento transacional ou *Open Finance*, sua jurisprudência sobre compartilhamento indevido de dados, falhas de segurança e disponibilização irregular reforça que definições equivocadas de base legal e ausência de controles adequados podem resultar em responsabilização civil objetiva.

3. Resumo dos pontos para reflexão pelo CNPD

A partir dos precedentes e dos aspectos normativos analisados, alguns eixos transversais podem orientar a atuação futura do Conselho:

3.1. *Score* de crédito x bancos de dados de crédito

- Como preservar, na prática, a distinção entre *score* (Tema 710/Súmula 550) e bancos de dados regidos pela Lei nº 12.414/2011 em ambientes de forte integração tecnológica?
- Em que medida essa distinção deve ser explicitada em orientações ao mercado (especialmente no que tange a bases legais, transparência e direitos dos titulares)?

3.2. Limites de compartilhamento e finalidade

- Como delimitar, de forma clara, o uso de dados para proteção ao crédito em contraste com usos para marketing, segmentação comercial ou outras finalidades econômicas?
- Seria desejável explicitar, em guias ou recomendações, critérios objetivos para reaproveitamento de dados de crédito em outras finalidades?

3.3. Dano moral presumido e padrões de responsabilização

- Como acomodar, em uma leitura sistêmica, a divergência entre Terceira e Quarta Turmas do STJ quanto ao reconhecimento de dano moral presumido em casos de disponibilização indevida de dados?
- Há espaço para o CNPD sugerir parâmetros mínimos de diligência e governança que possam servir como referência na avaliação de responsabilidade civil e administrativa?

3.4. Prevenção a fraudes, segurança da informação e dados sensíveis

- Quais balizas podem orientar a definição do que é “estritamente necessário” em tratamentos de dados para prevenção a fraudes, incluindo o uso de biometria e outros dados de alta criticidade?
- De que forma tratar, com proteção reforçada, situações que envolvam dados sensíveis e grupos vulneráveis (como crianças e adolescentes) no contexto de crédito e antifraude?

3.5. Decisões automatizadas e transparência (art. 20 da LGPD)

- Em que medida sistemas de *scoring* e de antifraude devem ser tratados como decisões automatizadas sujeitas ao art. 20 da LGPD, especialmente quando produzem efeitos relevantes (concessão ou negativa de crédito, bloqueios de operações, monitoramento contínuo)?
- Quais parâmetros poderiam orientar o "grau adequado" de transparência e explicabilidade em modelos complexos (estatísticos ou algorítmicos), sem comprometer segredos de negócio?

3.6. Bases legais em ecossistemas complexos (*KYC*, monitoramento, *Open Finance*)

- Quais critérios podem orientar a escolha entre proteção ao crédito, obrigação legal/regulatória, legítimo interesse e consentimento em fluxos com múltiplas finalidades (crédito, prevenção a fraudes, compliance, *Open Finance*)?
- Como incentivar práticas de documentação e testes de balanceamento que tornem essa escolha auditável perante a ANPD e demais autoridades?

3.7. Coordenação institucional e convergência regulatória

- De que modo ANPD, Banco Central, Senacon, Procons, Cade e outros órgãos podem convergir, dentro do escopo de sua atuação e considerando impactos sistêmicos, quanto a temas como prazo de retenção, compartilhamento entre instituições, e fronteira entre prevenção a fraudes e perfilização comercial?
- Qual poderia ser o papel específico do CNPD como espaço de articulação para evitar mensagens regulatórias conflitantes ao setor de crédito e serviços financeiros intensivos em dados?

Conselheiro responsável: Rodrigo Pironti

ANEXO III – Ata da Entrevista: Jéssica Abreu

ATA DE ENTREVISTA – 04/12/25

Data: 04/12/2025
Conselheiros: Rony Vainzof e Annette Pereira
Participantes: Kamilla Rodrigues e Tayná Araújo

ENTREVISTADA: JÉSSICA ABREU
Executive Legal Manager at Serasa Experian | Privacy | Positive Data | Regulation

---

As declarações aqui registradas refletem exclusivamente a percepção da entrevistada e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

1. Proteção do crédito e dados pessoais são indissociáveis. Não há como assegurar acurácia, estabilidade de mercado e prevenção à fraude sem tratamento robusto de dados.

2. Relevância macroeconômica e microeconômica: crédito impacta diretamente consumo, inclusão financeira, políticas públicas e redução de desigualdades regionais

3. Países desenvolvidos operam entre 100% (UE) e 200% (EUA) de relação crédito/PIB. É importante que o Brasil se espelhe nos países desenvolvidos e aproveite a oportunidade de desenvolvimento a partir da proteção do crédito.

4. Supremacia do interesse coletivo: dependência exclusiva de consentimento do tomador distorce o sistema, incentiva ocultação de informações e compromete a
5. precisão dos modelos.

6. Concedentes continuam em desvantagem frente ao tomador, especialmente se o modelo regulatório dependesse exclusivamente de consentimento. Titulares com maior letramento digital já selecionam quais dados expõem para se mostrar “bons pagadores”, o que distorce análise e amplia risco sistêmico.

7. A mudança do Cadastro Positivo do opt-in para o opt-out mostrou que modelos baseados em consentimento não geram escala nem precisão suficientes para a proteção do crédito.

8. Há uma oportunidade econômica estruturante para expansão sustentável se houver: segurança jurídica no uso de dados; acesso a informações consistentes e não enviesadas; e políticas públicas alinhadas a melhores práticas internacionais.

9. Não é possível operacionalizar concessão de crédito segura sem verificação robusta de identidade.

10. Separar juridicamente "proteção do crédito" e "prevenção à fraude" pode não refletir a realidade operacional.

11. Micro e pequenos empresários dependem de terceiros para análise; impor trilhas separadas (crédito × fraude) eleva custos, inviabiliza operações e fragiliza o ecossistema.

12. Fraudes afetam todo o mercado, punindo bons pagadores e encarecendo crédito, reforçando a dimensão coletiva da proteção ao crédito.

13. Biometria: banalização em ambientes de baixo controle (ex.: condomínios) sem governança mínima; descredito em grandes instituições, que possuem estruturas robustas de segurança, compliance e armazenamento; a regulação atual não pode penalizar quem tem governança madura, enquanto usos frágeis passam despercebidos; e o baixo letramento digital da população impede compreensão real sobre: onde dados são armazenados, qual tecnologia é utilizada e diferenças entre captura simples e soluções avançadas de prevenção à fraude.

14. Cresce a percepção equivocada de que "o titular controla tudo", gerando:

1. pedidos indevidos de exclusão de dados;
2. judicialização massiva;
3. risco de colapso regulatório para empresas menores a partir de um contencioso judicial e administrativo de massa.

15. Em conjunto com ações educativas, há a necessidade de mensagens públicas mais claras por parte dos órgãos responsáveis para evitar "interpretações absolutistas" sobre direitos dos titulares.

16. A análise do crédito vai além da concessão. As atividades abrangidas pela Base Legal de Proteção ao Crédito: a cadeia completa do crédito deve ser considerada, inclui:

1. Prospecção e segmentação, incluindo marketing responsável
2. Concessão
3. Gestão e monitoramento
4. Cobrança e recuperação

17. Publicidade sem alinhamento com políticas reais de crédito gera fricção com titulares e desperdício econômico.

18. Determinar público-alvo exige tratamento de dados alinhado ao risco e evita frustrações e consultas desnecessárias no CPF do consumidor.

19. Produtos e serviços que melhoram a higidez das bases integram proteção ao crédito.

20. Sem dados íntegros, todo o ecossistema se torna mais arriscado.

21. O parâmetro técnico para justificar uso de dados alternativos é a relevância estatística: se melhora a acurácia e protege a estabilidade de toda a cadeia do crédito, deixa de ser "excessivo" e passa a ser "necessário".

22. É preciso permitir experimentação regulatória para testar novas fontes de dados.

23. Dados alternativos podem proteger o próprio titular, antecipando riscos de superendividamento.

24. Crédito moderno é intrinsecamente baseado em IA, não apenas IA generativa, mas modelos estatísticos e machine learning tradicionais.

25. Governança envolve mapeamento completo das etapas, dados utilizados e finalidades; documentação das revisões, auditorias e reavaliações periódicas; monitoramento ativo de: vieses e discriminações ilícitas, e performance dos modelos.

26. Explicabilidade deve respeitar o equilíbrio entre direitos dos titulares, transparência e segredo de negócio (fórmulas, pesos e modelos proprietários).

27. Precedentes judiciais já reconhecem que explicação deve ocorrer sem violar modelos internos e o segredo de negócio.

Mensagens-Chave para o CNPD

1. Crédito é ativo estratégico para o país; limitações indevidas no uso de dados impossibilitam o desenvolvimento de soluções, a inclusão e o funcionamento de toda a economia.

2. Consentimento não deve ser a base central para tratamento de dados de crédito.

3. É essencial reforçar publicamente que direitos dos titulares têm limites, sobretudo quando entra em jogo o interesse coletivo.

4. O CNPD pode fomentar diretrizes que:
   1. reconheçam a cadeia completa do crédito;
   2. viabilizem uso responsável de dados alternativos;
   3. alinhem prevenção à fraude com proteção do crédito; e
   4. harmonizem explicabilidade de IA com proteção ao segredo de negócio.

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO IV – Ata da Entrevista: Elias Sfeir

ATA DE ENTREVISTA – 08/12/25

Data: 08/12/2025
Conselheiros: Rony Vainzof e Debora Sirotheau
Participante: Kamilla Rodrigues.

ENTREVISTADO: ELIAS SFEIR

Presidente da ANBC & Membro do Conselho Climático da Cidade de São Paulo & Conselheiro Certificado & Membro do ICCR e B Ready Banco Mundial

Sumário executivo da entrevista:

1. Contextualização e posicionamento institucional

- A ANBC representa os birôs de crédito brasileiros, todos certificados pelo Banco Central, e integra fóruns globais como ICCR, BIIA, Alacred e ACCIS, participando ativamente das discussões internacionais sobre crédito, dados e IA.
- O Brasil é benchmarking global em modelos de crédito e governança de dados, dialogando com diversos blocos econômicos (Europa, Ásia, Oriente Médio, América Latina).
- A perspectiva internacional comparada destaca como regulação, cultura e maturidade digital moldam modelos de crédito e proteção de dados:
    - Europa: foco em controle e proteção social; reconhece atraso competitivo.
    - Ásia: inovação, velocidade e prosperidade como motores; ampla cooperação multilateral.
    - EUA: inovação com escala de negócios.
    - África: criatividade e sobrevivência como drivers de inclusão.

2. Papel socioeconômico do crédito

- Crédito é mecanismo civilizatório basilar: relação entre quem dispõe de recursos e quem necessita. Três premissas essenciais:
    - Crédito não é direito adquirido.
    - Crédito não é renda.
    - Negativação não extingue a dívida após cinco anos.

- Três pilares estruturam a sustentabilidade do sistema:
    1. Consumo consciente
    2. Crédito responsável
    3. Educação financeira

A expansão do crédito fomenta prosperidade, inclusão e crescimento econômico. A diferença entre a relação crédito/PIB do Brasil (≈54%) e EUA (≈190%) reflete barreiras culturais, como a crença latino-americana de que "ocultar informação protege", ao contrário dos modelos anglo-saxões baseados em transparência.

3. Evolução global do crédito: quatro forças estruturantes

- Quatro vetores estratégicos que guiam a transformação do setor:
  1. Velocidade – decisão de crédito em tempo real.
  2. Simplicidade – experiência "one-click", especialmente avançada na Ásia.
  3. Customização – modelos aderentes ao perfil individual, suportados por dados alternativos.
  4. Segurança – elemento essencial para estabilidade sistêmica, precificação e confiança do consumidor.

- Fraude já representa 16% do PIB brasileiro e 14% global, elevando custo do crédito, retração do consumo e insegurança digital.

4. Uso de dados pessoais: redução de assimetria e impacto econômico

- Dados pessoais são fundamentais para:
  - identificação e autenticação;
  - análise de risco;
  - prevenção a fraudes;
  - melhor tomada de decisão;
  - redução de assimetrias e ampliação da liquidez de mercado.

4.1. Dados alternativos: tendência global

- Segundo estudo do Banco Mundial (SDD – Sex Disaggregation Data), há recomendações para uso ampliado de dados alternativos como: dados governamentais; empregabilidade; escolaridade; telecomunicações; energia; pré-pagos; biometria; metadados comportamentais.

- Em países africanos, onde há baixa disponibilidade de dados estruturados, tais modelos permitiram inclusão massiva e melhoria significativa na acuracidade de escoragem.

- No Brasil, apesar de o Cadastro Positivo ter 84% de cobertura da população economicamente ativa, as regiões Norte e Nordeste ainda sofrem com invisibilidade de crédito (60–64%). O titular tem direito a ser visível para crédito.

5. Princípio da necessidade e definição do que é "dado relevante"

- A relevância é definida por modelos estatísticos robustos e validados, não por percepções abstratas:
  - As bases passam por modelagem matemática, seguida de backtesting com amostras independentes.
  - Dados comportamentais, biométricos e de localização podem ser essenciais, desde que contextualizados e justificados.
  - Exemplos práticos mostram que elementos como movimentação do mouse ou velocidade de digitação permitem autenticação com alta precisão e mitigam fraude.
  - Dados irrelevantes são liability, e por isso birôs evitam coletá-los.

6. Inteligência Artificial: segurança, transparência e governança

- Os birôs utilizam IA há mais de 20 anos (redes neurais, modelos estatísticos). O desafio atual é IA generativa.
- Birôs não concedem crédito; fornecem ferramentas aos credores.
- O direito de revisão humana é exercido perante o credor, não com os birôs.
- Transparência deve ser responsável para não distorcer comportamento (ex.: divulgar peso exagerado de "conta de luz" pode levar titular a negligenciar outros pagamentos).
- Explicabilidade deve evoluir para "understandability": explicar somente o que o titular consegue compreender.
- Modelos são calibrados estatisticamente; vieses são verificados em testes empíricos.
- Exemplo global: estudos mostram que mulheres têm inadimplência até 20% menor; proibi-las como variável pode gerar injustiça e piorar modelos.
- O Banco Mundial pode recomendar uso responsável de variáveis de gênero para correção estatística — evidenciando que proibições rígidas podem prejudicar eficiência e equidade.

7. Direitos do titular, consentimento e segurança

- O Estado deve atuar quando a população não tem pleno entendimento dos riscos e benefícios, citando como exemplo a migração do Cadastro Positivo do opt-in para opt-out, que ampliou inclusão ,elevou scores para 78% da população e em setembro de 2025 de cada 100 pessoas que saiam do Cadastro Positivo, 95 retornam.

8. Visão regulatória: lacunas, avanços e diretrizes desejáveis

- A LGPD é considerada positiva, inovadora e equilibrada, especialmente pela inclusão da base legal de proteção ao crédito.
- O Brasil tem capacidade de calibrar regulação de forma dialogada.
- Risco: excesso de zelo pode gerar negação de cidadania digital — quem não tem dados não existe para o mercado.
- Regulação deve acompanhar, não preceder a inovação.

- Evitar transplantes automáticos de modelos europeus, que já reconhecem atraso competitivo.
- Priorizar:
    - uso proporcional e contextualizado de dados;
    - incentivo a dados alternativos para inclusão;
    - governança robusta e certificação de agentes;
    - educação digital, financeira e cibernética;
    - monitoramento baseado em risco real, não apenas potencial;
    - estímulo a autorregulação regulada (ex.: experiências da ANBC).

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO V – Ata da Entrevista: Diana Loureiro de Moura

ATA DE ENTREVISTA – 11/12/25

Data: 11/12/2025
Conselheiros: Rony Vainzof, Annette Pereira, Vitor Morais de Andrade e Debora Sirotheau
Participantes: Kamilla Rodrigues e Tayná Araújo

Entrevistada: DIANA LOUREIRO DE MOURA
Procuradora do Banco Central do Brasil

Sumário executivo da entrevista:

1. Abertura e contextualização

- Enquanto a ANPD atua com foco no indivíduo na proteção de dados pessoais, o BACEN opera sob uma lógica sistêmica, voltada ao equilíbrio do mercado de crédito como bem coletivo. Nesse contexto, proteção ao crédito e prevenção à fraude constituem dimensões interdependentes da estabilidade financeira.

2. Papel sistêmico do crédito e relação intrínseca com prevenção à fraude

- O crédito é mecanismo essencial de transferência de recursos dos agentes superavitários para os deficitários, viabilizando a atividade econômica.
- A análise de crédito não se limita à concessão tradicional; envolve momentos contínuos de avaliação, como compras atípicas no cartão, aumento de limites, monitoramento de comportamento etc.
- Sem dados (inclusive pessoais), não há como operacionalizar adequadamente qualquer etapa da gestão de risco.
- Proteção ao crédito e prevenção à fraude são “duas faces da mesma moeda”, inseparáveis na prática: prevenir fraude reduz inadimplência, diminui spreads, fortalece a saúde do sistema e gera crédito mais acessível e sustentável.

3. Visão sistêmica e impactos regulatórios

- Um erro individual na concessão de crédito ou uma fraude isolada não fica restrita à instituição que sofreu o evento; pode contaminar o mercado, afetando cessão de crédito, garantias, investidores e liquidez.
- A supervisão do BACEN considera denúncias individuais apenas como insumo para análise estrutural, não como casos isolados determinantes.
- Houve histórico de debates com a Senacon pela diferença natural entre a visão micro (consumidor individual) e a visão sistêmica (estabilidade do mercado).

4. Compartilhamento de dados e Resolução Conjunta nº 6

- A norma não altera a gestão de risco das instituições; esta continua complexa e própria a cada agente.
- A inovação está na interoperabilidade: colocar instituições "na mesma sala", permitindo troca padronizada de informações sobre suspeitas de fraude.
- A lógica é: fraudadores já trocam informações entre si; as instituições precisam ter a mesma capacidade colaborativa.
- Não houve, até agora, demanda institucional dentro do BACEN para ampliar o escopo de dados. Diana se dispôs a consultar área técnica sobre aprendizados e eventuais necessidades de evolução.
- Exigir consentimento para prevenção à fraude não faz sentido operacional nem jurídico, porque: fraudadores não darão consentimento; em serviços financeiros essenciais, o titular não tem real liberdade de escolha; todos os players exigem o mesmo procedimento; o consentimento acaba sendo um ato informativo e de transparência, e não um instrumento de autodeterminação;
- Há outras bases legais (interesse público, proteção do crédito, prevenção à fraude) plenamente suficientes para sustentar o tratamento de dados previsto na Resolução.

5. Interesse público e acesso à informação

A base legal de prevenção à fraude está ancorada no interesse público:

- A higidez do mercado reduz juros, democratiza crédito, reduz inadimplência e melhora condições econômicas para toda a sociedade.
- Esse racional diferencia o uso de dados para prevenção à fraude do consentimento típico do Open Finance, que é individual e competitivo.

6. Inteligência artificial, decisões automatizadas e explicabilidade

- O BACEN ainda **não regula limites de automação** nas análises de crédito.
- Não há, até o momento, evidências suficientes de problemas relevantes que demandem intervenção normativa.
- Contudo, há espaço para evoluir no tema de **explicabilidade**, equilibrando:
    - necessidade de transparência ao titular;
    - proteção de segredos de negócio;
    - risco de que divulgação excessiva permita que fraudadores burlem sistemas.

7. Considerações finais da especialista

- O ecossistema de crédito é interconectado, sensível e altamente dependente de dados.
- Restrições excessivas ao uso ou ao compartilhamento de dados podem elevar riscos sistêmicos e prejudicar o próprio consumidor.

- O avanço regulatório deve equilibrar proteção de dados, inovação, prevenção à fraude e estabilidade de mercado.

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

ANEXO VI – Ata da Entrevista: Luis Felipe Monteiro

ATA DE ENTREVISTA – 05/12/25

Data: 05/12/2025
Conselheiro: Rony Vainzof
Participantes: Kamilla Rodrigues, Joelson Vellozo, Maria Francioli, Mariana Moreno e Gilberto Fernandes

---

ENTREVISTADO: LUIS FELIPE MONTEIRO
Corporate Affairs - VP da Unico

---

1. Contexto e visão geral

- A Unico se posiciona como ID Tech brasileira líder global, operando em 20 países, com mais de 1 bilhão de verificações de identidade/ano.
- Modelo baseado em rede de verificação de identidade, funcionando como "vacina": uma fraude detectada em um cliente gera proteção preventiva para todo o ecossistema.
- Em 2025, a empresa afirma ter prevenido R$ 23 bilhões em fraudes, especialmente nos setores financeiro, varejo, e mais recentemente jogos/apostas.

2. Relevância dos dados pessoais na prevenção a fraudes

2.1. Mecanismo de funcionamento

- A validação biométrica ocorre no interesse do próprio titular, garantindo identidade e legitimidade da transação.
- Após o uso primário, os dados são utilizados para treinar modelos de detecção de fraude, equivalente ao processo de desenvolvimento de vacinas em saúde pública.
- O modelo gera três respostas essenciais por transação:
    1. Comprovação de vida (liveness): confirmar que há uma pessoa real, presente no momento da captura.
    2. Identidade: confirmação de que a face corresponde à pessoa declarada.
    3. Risco: detecção de padrão suspeito, seja tentativa de fraude ou vitimização do titular.

2.2. Dependência técnica do uso de biometria

- A biometria é, hoje, a tecnologia que melhor combina precisão, experiência do usuário e segurança.
- Para ambientes exclusivamente digitais (ex.: bancos digitais), não há alternativa mais consistente, principalmente em países com alto índice de fraudes — não há agência física para validar identidade.
- Fraudes sofisticadas cresceram (como deepfakes e ataques de injeção), demandando tecnologia de ponta e investimentos contínuos.

3. Situação atual da fraude no Brasil e o efeito sistêmico

- Crime organizado migrou para fraudes digitais de alta complexidade, com atuação transnacional.
- Cerca de 65% dos fraudadores atuam em rede, reforçando a importância de modelos de proteção também em rede.
- Fraude na iniciação de crédito ("default na primeira parcela") representa ~R$ 60 bilhões/ano, diretamente ligado à fraude de identidade.
- A redução dessa fraude é pilar para:
    - Inclusão financeira
    - Concorrência bancária
    - Redução estrutural do custo de crédito
    - Sucesso de infraestruturas como o Pix

4. Riscos da subutilização de dados pessoais

- Subutilizar ou restringir o uso de dados para prevenção à fraude geraria:
    - Aumento expressivo de perdas sistêmicas
    - Elevação de custos de crédito para toda população
    - Retrocesso no modelo bancário digital, com possível inviabilidade de operações 100% digitais
- Comparação internacional:
    - México: somente consentimento permitido: índices muito maiores de fraude e custo de crédito exorbitante.
    - Brasil: LGPD equilibrada, reconhecendo hipóteses adequadas, como prevenção à fraude, legítimo interesse (para dados não sensíveis) e execução de contrato.

5. Pontos críticos sobre regulação e LGPD

5.1. Avaliação geral

- A LGPD é considerada madura e tecnicamente bem calibrada para o ecossistema antifraude.
- As bases legais hoje existentes dão segurança jurídica essencial para a continuidade de modelos de proteção.

5.2. Riscos regulatórios identificados

- Propostas legislativas que:
    - Exijam consentimento obrigatório para biometria: o fraudador simplesmente pediria exclusão dos dados e reiniciaria o ciclo de ataques.
    - Imponham alternativas físicas obrigatórias para serviços 100% digitais – inviabilizando bancos digitais.
    - Regulem biometria de forma genérica, misturando uso banalizado (condomínios) com uso de alto risco e alta governança (sistema financeiro).
- Consequência: risco elevado de retrocesso sistêmico, com impacto em inovação, inclusão e segurança.

6. Oportunidades de evolução regulatória

- Evitar alterações desnecessárias na LGPD que possam fragilizar o ecossistema antifraude.

- Produzir políticas públicas que ampliem biometria onde há alto risco e baixo incentivo econômico privado, como Telecom (ativação de chips), que hoje é um vetor central de golpes.
- Maior aproximação entre ANPD e setores críticos, reforçando boas práticas, frameworks de governança e conscientização.

7. Expansões temáticas sugeridas

- Relevância da biometria facial para proteção de crianças e adolescentes em ambientes digitais.
    - Tecnologias permitem estimativa de idade com exclusão imediata dos dados.
    - Alternativas baseadas em *profiling* (conteúdos assistidos) são mais invasivas e menos precisas.
- Interesse da Unico em colaborar com GTs do CNPD relacionados ao ECA Digital.

8. Mensagens finais

- O Brasil tornou-se referência mundial em identificação digital e prevenção à fraude graças ao arcabouço regulatório atual.
- Há mais oportunidade do que risco no uso seguro de biometria — desde que mantidos os princípios de proporcionalidade, governança e minimização.
- Recomendações centrais:
    - Não fragilizar a legislação vigente.
    - Reconhecer a diferença entre usos legítimos e banalizados de biometria.

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO VII – Ata da Entrevista: Otávio Margonari Russo

ATA DE ENTREVISTA – 09/12/25

Data: 09/12/2025
Conselheiros: Rony Vainzof e Annette M. Pereira
Participante: Kamilla Rodrigues e Tayná Araújo

Entrevistado: OTAVIO MARGONARI RUSSO
Diretor de Combate a Crimes Cibernéticos da Polícia Federal

Sumário executivo da entrevista:

1. Visão Estruturante: Dados Pessoais como Ponto de Equilíbrio entre Liberdade e Segurança
   - Investigação e prevenção de crimes dependem necessariamente do acesso a dados pessoais.
   - A proteção de dados e a persecução penal não são objetivos antagonistas; quando bem calibradas, uma fortalece a outra.
   - Excesso de restrição pode asfixiar investigações, gerar sensação de impunidade e aumentar o crime.
   - Falta de limites pode expor cidadãos sem necessidade.

2. Impacto direto da LGPD no trabalho policial
2.1 Obrigações internas da PF
   - A PF possui área própria dedicada à governança de dados, garantindo confidencialidade, segurança e uso restrito às finalidades legais.
   - As exigências da LGPD "empurram" a PF para padrões cada vez mais elevados de proteção – avaliadas como positivas.

2.2 Potenciais dificuldades ligadas à disponibilização de dados por terceiros
   - O *ponto crítico* é na eventual ocorrência da interpretação restritiva da LGPD por parte de agentes privados, que pode dificultar ou atrasar o fornecimento de dados essenciais.
   - Sem fluxo adequado de informações, o país corre risco de voltar ao cenário de investigações fragmentadas, lentas e ineficazes.
   - Diversas iniciativas relevantes que envolvem o compartilhamento de informações para investigações dependem diretamente de correlação massiva de dados para identificar padrões criminosos, mapear organizações e antecipar tendências.

3. Riscos sistêmicos:
   - Criminosos invadem pequenos e médios e-commerces para furtar dados de cartões.
   - Esses dados abastecem marketplaces clandestinos de cartões, gerando fraudes em larga escala.
   - Crimes estão totalmente interligados: furto mediante fraude, estelionato, invasões, venda de bases, golpes em massa etc.

- Repressão fragmentada entre PF e polícias civis exige cooperação robusta e fluxo constante de inteligência.

4. Pilares de Combate a Crimes Cibernéticos da PF

4.1 Capacitação

- Formação massiva de policiais das 27 delegacias especializadas criadas no país.
- Expertise técnica é essencial para acompanhar o nível de sofisticação dos criminosos.

4.2 Áreas de repressão

- Tentáculos – Fraude bancária eletrônica.
- Rapina – Crimes de abuso sexual infantil.
- Núcleo especializado de crimes de ódio.
- Coordenação de crimes de alta tecnologia liderada por peritos especializados.

4.3 Prevenção

- Fraudes financeiras: foco em educação digital do usuário.
- Alta tecnologia: foco em jovens potenciais ofensores, para quebrar o "ciclo de escalada".
- Abuso sexual infantil: atuação junto a crianças, pais e educadores.

4.4 Cooperação

- Cooperação interna com polícias civis.
- Cooperação público-privada como pilar crítico (inclusive por meio de ACTs).
- Cooperação internacional (Europol, Interpol, FBI, países latino-americanos).
- Bases compartilhadas (ex.: plataforma MISP/capivara) enriquecem investigações globais.

5. Vazamento de Dados e Ransomware: Desafios, dilemas e caminhos

5.1 Círculo vicioso atual

- Empresas atacadas temem comunicar à PF ou à ANPD por receio de:
  - Multas,
  - Impacto reputacional,
  - Complexidades contábeis,
  - Percepção de "culpa" mesmo quando investem em segurança.
- Isso incentiva o crime e enfraquece a inteligência estatal.

5.2 Mudança no modus operandi dos grupos de ransomware

- Tendência global: migrar de criptografia para roubo silencioso de dados, seguido de extorsão.
- Motivo: ataques disruptivos chamam atenção e resultam em prisões.
- Tendência confirmada em eventos internacionais (ex.: CRI em Singapura).

5.3 Papel ativo da PF

- PF monitora, identifica e avisa empresas com credenciais vazadas.
- Participa de operações internacionais de desarticulação.
- Prende "afiliados" brasileiros que operam modelos *ransomware-as-a-service*.

5.4 Debate sobre pagamento de resgate

- Orientação global: não pagar.
- Pode haver exceções: casos de "vida ou morte" ou impacto crítico à sociedade.
- PF pode e deve ser acionada antes de qualquer decisão crítica.
- PF pode atuar, monitorar transações e investigar os criminosos.

- Frase síntese: *"Sempre veremos a empresa como vítima."*

6. Pontos de melhoria regulatória sugeridos pelo especialista

6.1 Interpretação da LGPD ajustada ao interesse público

- A LGPD não deve impedir a PF de receber dados em volume, velocidade e formato compatíveis com investigações modernas.
- É preciso evitar que a proteção de dados "mate" a persecução penal e comprometa a segurança coletiva.

6.2 Avaliar mitigação regulatória para empresas atacadas

- Comunicação tempestiva à PF deveria ser levada em conta pela ANPD na dosimetria de eventuais sanções.
- Evita penalizar duplamente a vítima e incentiva colaboração.

6.3 Aproximação institucional PF – ANPD – CNPD

- Importante haver maior integração estratégica.
- Reconhece ganhos de confiança, fluxo de informações e alinhamento de políticas públicas.

7. Conclusão

- O combate ao crime cibernético depende de dados, inteligência, cooperação e calibragem regulatória.
- Sem fluxo adequado de informações, ferramentas já consolidadas de combate ao crime podem perder potência e todo o sistema, como o financeiro, sofre.
- O CNPD tem papel fundamental em orientar diretrizes que permitam equilíbrio entre proteção e segurança coletiva.
- PF está aberta ao diálogo, colaboração e atuação conjunta com a ANPD e o CNPD.

ANEXO – RESPOSTAS ENVIADAS POR ESCRITO AO ROL DE PERGUNTAS

Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

A prevenção à fraude é condição sine qua non para sustentabilidade do sistema financeiro brasileiro. Quando a PF estruturou o combate sistemático às fraudes bancárias eletrônicas, o país enfrentava perdas anuais de milhões de reais com fraudes. A Polícia Federal recebia aproximadamente 4.000 notificações mensais de fraudes, gerando mais de 200.000 casos tramitando simultaneamente sem identificar autores.
Após a implementação de metodologia integrada de investigação, alcançou-se redução de inquéritos e aumento da efetividade das operações para desmantelamento das organizações criminosas. Entre 2018 e 2023, foram realizadas 572 operações policiais resultando em 208 prisões e 1.220 mandados de busca, demonstrando que prevenção efetiva protege não apenas recursos financeiros, mas viabiliza a confiança necessária para expansão dos serviços bancários eletrônicos sem comprometer a estabilidade sistêmica.

Qual a importância dos dados pessoais para proteção do crédito e demais atividades relacionadas ao tema?

A experiência da Polícia Federal demonstra que dados pessoais são elementos fundamentais para validação de identidade e detecção de contas fraudulentas que distorcem avaliações de risco. O trabalho investigativo da PF

recebe sistematicamente e legalmente dados das contas relacionadas as fraudes. Esses elementos permitem não apenas identificar fraudes, mas proteger o crédito legítimo ao distinguir transações genuínas de operações criminosas.
Dados transacionais e comportamentais viabilizam análise de padrões que seriam invisíveis em avaliações isoladas. A proteção ao crédito, portanto, depende intrinsecamente da capacidade de processar dados pessoais de forma integrada, identificando vítimas de fraude que precisam ter seu crédito protegido e criminosos que utilizam identidades falsas para obter crédito indevido.

Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?

A Polícia Federal demonstra que prevenção efetiva à fraude depende fundamentalmente de processamento integrado de dados transcionais e também pessoais. A Base Tentáculos centraliza dados que permitiram gerar milhares de investigações de casos de fraude. Atualmente, o ecossistema do Tentáculos integra sete grandes associações através de Acordos de Cooperação Técnica com FEBRABAN, ZETTA, ABRANET, ABBC, ACREFI, ABECS e ABRACAM.

Essa amplitude demonstra que dados transacionais e pessoais são insumo essencial não apenas para investigação, mas para prevenção proativa. O recebimento estruturado de dados permite identificar padrões emergentes evitando fraudes sistêmicas, protegendo simultaneamente vítimas potenciais e a estabilidade do sistema financeiro.

Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos?

A Polícia Federal utiliza análise de vínculos como metodologia central, processando dados e metadados para identificar as fraudes e respectivas organizações criminosas. Os dados e metadados revelam conexões invisíveis: mesmas contas beneficiárias vinculadas a múltiplas vítimas, agrupamentos geográficos suspeitos de saques, padrões de IP indicando acesso coordenado, e telefones ou endereços compartilhados entre contas.
Ferramentas de visualização transformam dados brutos em inteligência através de grafos de redes mostrando relacionamentos entre entidades, mapas de calor indicando concentração geográfica de fraudes, e cronologias temporais revelando padrões de execução. A descoberta investigativa de que grupos criminosos em regiões específicas alvejam sistematicamente determinados estados exemplifica como metadados permitem alocação estratégica de recursos investigativos e prevenção direcionada.

Quais são os riscos de subutilizar dados pessoais em processos antifraude (ex.: aumento de chargebacks, fraude sintética, falsidade ideológica e riscos sistêmicos)?

O modelo anterior ao sistema integrado da Polícia Federal ilustra dramaticamente as consequências da subutilização de dados. Quando cada fraude gerava inquérito individual, 4.000 notificações mensais resultaram em mais de 200.000 casos tramitando simultaneamente, consumindo recursos massivos sem identificar autores. Organizações criminosas operavam impunemente entre estados porque cada fraude era investigada isoladamente, impossibilitando identificação de grupos por trás dos crimes. As perdas anuais de milhões

persistiam apesar de investimentos em segurança, criando efeito cascata na confiança do consumidor e incerteza sobre riscos.

A subutilização de dados inviabiliza detecção de fraude sintética, onde criminosos combinam dados reais e fictícios criando identidades falsas e impede identificação de falsidade ideológica sistemática. Mais grave, impossibilita combate ao crime organizado transnacional, como demonstrado na Operação Redescobrimento que identificou R$10 milhões em de fraude contra vítimas em Portugal. Sem análise integrada de dados, o policiamento permanece reativo, fragmentado e ineficaz contra organizações criminosas sofisticadas que representam ameaça sistêmica ao sistema financeiro.

O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?

A infraestrutura da Polícia Federal demonstra convergência estrutural profunda entre proteção ao crédito e prevenção à fraude. A Plataforma Tentáculos funciona como portal único fornecendo inteligência, acesso aos dados de fraudes e recursos de análise de vínculos. Também substitui relatórios e notícias crime físicas por transmissão eletrônica, criando repositório único onde o mesmo conjunto de dados serve múltiplas finalidades investigativas e preventivas.

O ecossistema de parceiros revela convergência ainda mais clara: as sete associações com ACTs vigentes (FEBRABAN, ZETTA, ABRANET, ABBC, ACREFI, ABECS e ABRACAM) compartilham dados relacionados as fraudes que servem simultaneamente para análise e detecção de fraude. Elementos idênticos de dados permitem validação de identidade, análise comportamental, mapeamento geográfico e identificação de padrões sistêmicos. Os objetivos convergem naturalmente em reduzir assimetrias informacionais, proteger recursos financeiros, viabilizar transações eletrônicas seguras e desmantelar organizações criminosas que ameaçam tanto o crédito quanto a integridade transacional.

Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?

O modelo anterior ao sistema integrado demonstra as consequências da fragmentação. Milhares de inquéritos anuais com resultados mínimos, cada fraude investigada em silos isolados, impossibilidade de identificar padrões e desperdício em recursos caracterizavam a ineficiência. Organizações criminosas operavam impunemente porque conexões entre casos não eram identificadas, criminosos atuavam em múltiplos estados sem detecção e a taxa de prisões permanecia baixa.

A fragmentação de informações entre bancos mantendo dados isolados e Polícia Federal recebendo notificações desconectadas eliminava visão sistêmica, criando perda de escala e duplicação de esforços. As consequências eram diretas: perdas continuadas de milhões anuais, custos investigativos crescentes sem resultados, erosão da confiança no sistema bancário eletrônico e restrição do crédito por incerteza. Após integração, alcançou-se redução nas fraudes, prevenção de perdas financeiras, realização de mais de quinhentas operações com prisões de centenas de integrantes das organizações criminosas e estabelecimento de modelo replicável nacionalmente.

Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

A Polícia Federal opera com fundamentação legal sólida e abrangente. A Constituição Federal no Art. 144, §1º confere atribuição constitucional à PF para investigar infrações penais contra a ordem política e social e reprimir crimes praticados em detrimento de bens, serviços e interesses da União. A legislação criminal específica inclui o Código de Processo Penal para procedimentos investigativos, a Lei nº 12.850/2013 sobre Organizações Criminosas aplicável porque fraudes são praticadas por grupos estruturados permitindo técnicas especiais de investigação entre outras.

Na LGPD, o Art. 4º, III estabelece que a lei não se aplica ao tratamento de dados para segurança pública (alínea "a") e atividades de investigação e repressão de infrações penais (alínea "d"). O Art. 26, §1º permite transferência de dados do setor privado para público quando há execução descentralizada de atividade pública, previsão legal ou respaldo em contratos, e prevenção de fraudes com proteção do titular.

No âmbito do sigilo das operações de instituições financeiras, a Lei Complementar 105/2001 estabelece que não constitui violação do dever de sigilo a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa, conforme seu Art. 1 º, § 3o , inciso IV

Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?

A experiência da Polícia Federal demonstra equilíbrio exemplar entre os três pilares. O interesse público manifesta-se através de diversas operações policiais, resultando em centenas prisões e milhares mandados de busca.

A segurança dos titulares concretiza-se através de proteção direta às vítimas. O sistema identifica contas comprometidas e recupera valores através de bloqueios judiciais. O desmantelamento de grupos através das prisões e condenações cria efeito dissuasório robusto.

A estabilidade financeira é protegida através da cobertura de mais de 40 instituições bancárias, fintechs e empresas de cartões integradas à plataforma, viabilizando confiança no sistema bancário eletrônico. Salvaguardas robustas incluem base legal específica demonstrando proporcionalidade através de resultados mensuráveis que justificam o tratamento.

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO VIII – Ata da Entrevista: Leandro Miranda

ATA DE ENTREVISTA – 13/01/26

Data: 13/01/2026
Conselheiros: Rony Vainzof, Rodrigo Pironti e Vitor Moraes
Participante: Kamilla Rodrigues, Janaina Gomes e Tayná Araújo

---

ENTREVISTADO: LEANDRO ALVARENGA MIRANDA
Diretor Jurídico da Associação Nacional de Bureaus de Informação – ANBI

---

1. Atuação pessoal na construção da LGPD

- Participou ativamente da elaboração da LGPD desde as primeiras audiências públicas.
- Teve participação direta na criação da base legal específica de proteção ao crédito.
- Trabalhou juridicamente para que essa base legal existisse de forma autônoma na lei.

2. Origem e racionalidade da base legal de proteção ao crédito

- A base legal foi criada a partir de necessidades concretas do mercado brasileiro, não por simples reprodução da GDPR.
- O modelo europeu:
  - Não possui base legal específica de proteção ao crédito.
  - Opera com:
    - execução de contrato
    - legítimo interesse
- Esse modelo não é compatível com o Brasil, em razão de:
  - menor maturidade do mercado de crédito
  - menor maturidade tecnológica
  - maior incidência de fraudes
  - estrutura distinta de concessão de crédito (ex.: crédito consignado)

3. Limitações da base legal de execução de contrato

- A execução de contrato, se aplicada de forma estrita:
  - exigiria solicitação prévia do titular para consulta de dados.
- Isso:
  - inviabilizaria o modelo brasileiro de crédito
  - poderia causar quebra do mercado de crédito, especialmente no crédito consignado.
- Há uma dificuldade conceitual:
  - todo contrato envolve crédito
  - toda prestação a prazo é crédito
  - inadimplência não é claramente “fora” da execução contratual
- Por isso, a execução de contrato não é suficiente nem adequada como base única.

4. Crédito como atividade de interesse público

- Crédito não é uma relação contratual privada comum.
- É uma atividade:
  - de interesse público
  - estrutural para o desenvolvimento econômico e social
- Sem crédito:
  - há exclusão social
  - há desequilíbrio macroeconômico
- Dados:
  - mais de 6 trilhões de reais em crédito no Brasil
  - cerca de 54% do PIB está relacionado ao crédito
  - crédito às famílias representa cerca de 35% do PIB
- Uma interpretação apenas individualista:
  - prejudica o próprio consumidor
  - desorganiza o sistema econômico

5. Proteção ao crédito como política estrutural

- A proteção ao crédito:
  - não é atividade acessória
  - é política estrutural de país
- Abrange todo o ciclo do crédito, incluindo:
  - oferta de crédito
  - crédito pré-aprovado
  - execução do contrato
  - recuperação do crédito
- Deve ser analisada de forma integrada e contínua.

6. Base legal do legítimo interesse

- Considera a exigência de “legítima expectativa do titular”:
  - juridicamente problemática
  - conceitualmente frágil
- A expectativa de privacidade:
  - é individual
  - não comporta padrão de “homem médio”
- No legítimo interesse:
  - o titular pode se opor ao tratamento
  - isso pode fragilizar bancos de dados de crédito e antifraude
- Se aplicado à proteção ao crédito:
  - permitiria retirada de dados essenciais
  - geraria conflito entre direito individual e interesse coletivo

7. Combate à fraude

- O Brasil tem altíssima incidência de fraudes financeiras.
- Bancos de dados de crédito e antifraude:

  - não protegem apenas o mercado
  - protegem o próprio titular
- Fraudes atingem principalmente:
  - camadas mais vulneráveis
  - pessoas com menor capacidade de reação jurídica
- Combater fraude:
  - evita danos financeiros
  - evita negativação indevida
  - protege identidade do titular

8. Bancos de dados de proteção ao crédito

- Não se limitam à "negativação".
- Exercem funções como:
  - validação de identidade
  - confirmação cadastral
  - prevenção à fraude na fase pré-contratual
- "Negativação" é termo inadequado:
  - trata-se de apontamento de dívida informado por credor
  - o banco de dados não valida contrato nem valor

9. Cadastro Positivo

- Participou da discussão legislativa do Cadastro Positivo.
- Inicialmente foi criado em regime de opt-in:
  - resultou em baixíssima adesão
- Demonstra:
  - baixa maturidade da sociedade brasileira em dados pessoais
- Falta regulação efetiva:
  - ANPD poderia regular o Cadastro Positivo
  - Banco Central apenas homologa, não fiscaliza
- Há falhas práticas:
  - dados desatualizados
  - ausência de obrigação de envio de informações corretas

10. Dados e escoragem de crédito

- O problema não é o score em si.
- O problema central é quais dados alimentam o modelo.
- A fórmula é menos relevante do que a qualidade, pertinência e a proporcionalidade dos dados.
- Todo score
  - é estatístico
  - baseado em médias
  - não determina comportamento individual
- Sempre deveria ser complementado por outras informações.

11. Dados sensíveis e dados excessivos

- Dados sensíveis: não devem ser utilizados (ex.: religião).
- Dados considerados “excessivos”:
  - conceito impreciso
  - gera insegurança jurídica
- Dados como CEP:
  - são estatisticamente relevantes
  - refletem realidade socioeconômica
- A ausência de dados:
  - piora a análise
  - gera generalizações injustas

12. Estatística e risco de discriminação

- Dados estatísticos não são determinísticos.
- Sem dados suficientes:
  - o sistema aplica a “regra geral”
  - bons pagadores podem ser prejudicados
- Mais dados lícitos:
  - permitem distinções mais precisas
  - reduzem injustiças práticas

13. Biometria e dados cadastrais

- A LGPD permite biometria para combate à fraude.
- Se a lei permite o uso de dados mais sensíveis:
  - não faz sentido vedar dados cadastrais menos invasivos
- A permissão decorre da própria lógica da base legal de proteção ao crédito.

14. Oferta de crédito e crédito pré-aprovado

- Crédito pré-aprovado:
  - baseia-se em dados já disponíveis
  - não é marketing genérico
- Quando há oferta concreta:
  - surge expectativa jurídica
  - a oferta integra o contrato
- Diferente de:
  - “venha analisar seu crédito”
- O crédito pré-aprovado:
  - é instrumento de inclusão
  - pode reduzir superendividamento

15. Recuperação de crédito

- A proteção ao crédito inclui:

  - localização do devedor
  - recuperação do crédito
- Recuperar crédito:
  - devolve recursos à sociedade
  - mantém circulação econômica
- É interesse social que o crédito:
  - seja recuperado
  - volte a circular

16. Visão final

- A proteção ao crédito é contínua, integrada e de inequívoco interesse público;
- Simultaneamente protege a sociedade, o credor e o titular.
- Restringir excessivamente dados fragiliza o combate à fraude, aumenta custo do crédito e prejudica a inclusão financeira

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO IX – Ata da Entrevista: Iagê Miola

ATA DE ENTREVISTA – 20/01/26

Data: 20/01/2026
Conselheiros: Rony Vainzof, Debora Sirotheau, Annette Pereira, Vitor Moraes e Leonardo Ferreira
Participante: Davi Teófilo Nunes Oliveira, Kamilla Rodrigues e Tayná Araújo

---

ENTREVISTADO: IAGÊ MIOLA
Diretor da Agência Nacional de Proteção de Dados pessoais – ANPD

---

1. Considerações iniciais

- Relevância institucional do diálogo.
- Utilidade do documento prévio elaborado pelo GT, ressaltando que a leitura das perguntas já contribuiu para organizar e qualificar o debate.
- Os temas proteção do crédito e prevenção à fraude ainda não foram enfrentados diretamente pela ANPD. Estão no radar da agenda regulatória da ANPD, devendo ser enfrentados pelo Conselho Diretor em momento próximo.
- Suas contribuições deveriam ser entendidas como reflexões em construção, e não como posições consolidadas da Autoridade

2. Ênfase na necessidade de diagnóstico das práticas de mercado

- Como ponto transversal, a importância do esforço de diagnóstico da realidade do mercado.
- Enfatizou que diversas perguntas do GT buscam compreender:
  - quais práticas de tratamento de dados estão sendo efetivamente adotadas;
  - como se dão os usos concretos de dados pessoais para proteção do crédito e prevenção à fraude.
- Esse diagnóstico é essencial para:
  - fundamentar discussões regulatórias futuras;
  - evitar análises excessivamente abstratas;
  - permitir a construção de caminhos regulatórios mais aderentes à realidade.
- Esse tipo de insumo seria extremamente útil para a ANPD no futuro processo de normatização

3. Convergência prática entre proteção do crédito e prevenção à fraude

- Conforme indicado pelo GT, há uma dificuldade prática de separação entre as finalidades de proteção do crédito e prevenção à fraude.
- Há interesse institucional da ANPD em compreender como essa convergência ocorre concretamente, sob o ponto de vista operacional

4. Limites jurídicos impostos pela legislação

- Apesar da convergência prática, existem limites normativos objetivos impostos pela LGPD.
- O legislador optou por separar expressamente:

  - a hipótese legal de proteção do crédito; e
  - a hipótese legal de prevenção à fraude.
- Essa separação não pode ser ignorada no esforço interpretativo.
- A finalidade de proteção do crédito não autoriza, por si só, o tratamento de dados pessoais sensíveis.
- O tratamento de dados sensíveis tende a se enquadrar mais adequadamente na hipótese de prevenção à fraude.
- Reflexão central a necessidade de conciliar:
  - a realidade operacional do mercado; e
  - os limites jurídicos impostos pela legislação vigente.

5. Ônus argumentativo mais elevado na prevenção à fraude

- A hipótese legal de prevenção à fraude impõe um ônus argumentativo maior.
- Ressaltou que a legislação exige:
  - ponderação entre a finalidade do tratamento;
  - e a prevalência dos direitos e liberdades fundamentais do titular.
- Essa lógica se aproxima do modelo de ponderação previsto para o legítimo interesse.
- Esse aspecto diferencia substancialmente a prevenção à fraude da proteção do crédito.
- Há espaço para que o GT contribua com reflexões sobre:
  - como realizar essa ponderação na prática; e
  - possíveis diretrizes ou caminhos interpretativos para aplicação da hipótese legal.

6. Decisões automatizadas e aprendizado de máquina

- As questões levantadas pelo GT sobre decisões automatizadas são centrais e transversais a diversos setores.
- As perguntas formuladas refletem exatamente os dilemas enfrentados pela ANPD no contexto da agenda regulatória sobre decisões automatizadas.
- A experiência acumulada no setor de crédito pode fornecer exemplos concretos relevantes para a construção de orientações regulatórias mais amplas.
- Importância de compreender:
  - como os princípios da LGPD se aplicam concretamente;
  - como equilibrar necessidade de dados, não discriminação e governança de modelos.
- Exemplos práticos ajudam a tornar os princípios aplicáveis de forma menos abstrata.

7. Cooperação institucional no combate a fraudes

- O combate a fraudes é um problema complexo e sistêmico.
- Nenhuma instituição, isoladamente, possui ferramentas suficientes para enfrentar o problema.
- Necessidade de cooperação institucional, mencionando:
  - ANPD;
  - SENACON;
  - Banco Central;
  - eventual participação da Anatel.

- Há iniciativas já existentes de cooperação e a expectativa de fortalecimento desses arranjos.
- Respostas fragmentadas tendem a ser insuficientes diante da sofisticação das práticas criminosas.

8. Considerações finais

- Contribuições apresentadas como reflexões preliminares, voltadas a subsidiar o debate.
- Disponibilidade para continuar contribuindo com o GT em discussões futuras.
- Interesse institucional da ANPD em receber insumos qualificados e baseados na prática de mercado.

Atenciosamente,

Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO X – Ata da Entrevista: Livia Vieira

ATA DE ENTREVISTA – 29/01/26

Data: 29/01/2026
Conselheiros: Rony Vainzof, Annette Pereira, Vitor Moraes e Leonardo Ferreira
Participante: Flavio Luiz Damato Rocha de Souza e Tayná Araújo

ENTREVISTADA: LIVIA VEIRIA
Febraban

1. **Considerações iniciais**

- Foi ressaltada a relevância institucional do diálogo, bem como a importância de debater a base legal de proteção ao crédito sob a perspectiva de um setor altamente regulado e de grande complexidade operacional, como o Sistema Financeiro Nacional.
- Indicou-se que a proteção do crédito deve ser compreendida em sentido amplo, considerando não apenas a lógica interna das instituições financeiras, mas também seus efeitos sistêmicos sobre a economia e sobre a sociedade.

2. **Proteção do crédito como eixo sistêmico e estratégico**

- A base legal de proteção do crédito é relevante para a realidade brasileira, pois está conectada à necessidade de preservação da higidez do sistema financeiro, tema central para reguladores nacionais e internacionais, o que abrange a proteção do próprio titular-consumidor.
- Enfatizou-se que restrições indevidas podem gerar impactos em cadeia, inclusive com repercussões transnacionais, razão pela qual a proteção do crédito deve ser analisada como componente estrutural da estabilidade econômica.

3. Benefícios diretos ao consumidor e dimensão social da base legal

- A proteção do crédito não deve ser interpretada como mecanismo voltado exclusivamente ao concedente. Isso porque a utilização de dados para essa finalidade também protege o consumidor, ao permitir: crédito mais barato e acessível; análises mais precisas e fidedignas; distinção mais justa entre bons e maus pagadores; prevenção ao superendividamento; adequação de produtos ao perfil do cliente (*suitability*).

4. Ciclo de vida do crédito e multiplicidade de atividades abrangidas

- A entrevistada ressaltou que “proteção do crédito” abrange um conjunto amplo de atividades que compõem o ciclo de vida do crédito, incluindo: oferta e pré-aprovação; análise e concessão; autenticação do cliente; monitoramento de comportamentos atípicos; gestão do risco e deterioração do crédito; renegociação; e recuperação do crédito.

- Esse conjunto de atividades evidencia que a proteção do crédito deve ser tratada como processo contínuo e não como evento isolado.

5. Integração entre proteção do crédito, prevenção à fraude e segurança

- No contexto brasileiro, marcado por elevado nível de fraudes e tentativas de fraude, o uso de dados pessoais e metadados é relevante para autenticação, prevenção e monitoramento contínuo de transações.
- Mecanismos adicionais de validação (como confirmações por SMS ou verificações complementares) são frequentemente acionados diante de comportamentos atípicos, com o objetivo de garantir que a operação está sendo realizada pelo próprio titular.

6. Necessidade de alinhamento com a regulação financeira e prudencial

- A proteção do crédito possui conexão intrínseca com a regulação financeira, já que parte relevante das atividades do setor decorre de exigências prudenciais rígidas voltadas à mitigação de riscos sistêmicos.
- Qualquer discussão normativa ou orientativa da ANPD sobre o tema deve considerar essa interdependência e envolver diálogo com reguladores como Banco Central e CVM, para evitar efeitos adversos sobre a estabilidade do sistema.

7. Dados alternativos, precisão estatística e inclusão financeira

- O uso de dados alternativos e complementares é relevante tanto para modelagem de crédito quanto para prevenção à fraude, pois aumenta a precisão e permite maior aderência ao perfil real do consumidor. Isso pode ampliar a inclusão financeira, por exemplo, em públicos sem histórico bancário consolidado (como jovens), evitando negativas automáticas e permitindo análises mais individualizadas.

8. Minimização, ética e risco de discriminação

- O uso ampliado de dados deve ser orientado por pertinência, ética e observância dos princípios da LGPD, evitando discriminações ilícitas. Informações como endereço podem ter relevância legítima para adequação de produtos, microcrédito e garantias, desde que utilizadas em conjunto com outras variáveis e dentro de governança adequada.

9. Uso de biometria e medidas reforçadas de autenticação

- Biometria e mecanismos reforçados de validação para segurança têm importância para mitigar fraudes como roubo de sessão e operações sensíveis (ex.: troca de senha ou desvinculação de dados). Estes mecanismos protegem diretamente o consumidor, reduzindo prejuízos e consequências futuras decorrentes de operações fraudulentas.

10. Considerações finais

- O tema deve ser tratado como estratégico para o país, envolvendo equilíbrio entre proteção de dados, prevenção à fraude, estabilidade econômica e segurança cibernética. Interpretações excessivamente restritivas da base legal de proteção do crédito podem simplificar indevidamente a realidade do setor e gerar impactos sistêmicos relevantes.

Atenciosamente,
Rony Vainzof
Conselheiro Titular do CNPD – Setor Empresarial

ANEXO XI – Resposta ao ofício: ANBIMA

ANBIMA

Ao

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Aos cuidados de:

Sra. Lilian Manoela Cintra de Melo – Presidente do CNPD

Sr. Rony Vainzof – Conselheiro Titular de Coordenados do GT5 do CNPD

Ref: Solicitação de contribuição ao CNPD (GT5 – Proteção ao Crédito e Prevenção à Fraude).

Prezados Senhores,

Nos sentimos honrados com o recebimento da correspondência deste importante conselho e agradecemos a oportunidade de contribuição com tema tão relevante; entretanto, sendo o escopo das perguntas envolvendo crédito, entendemos que não somos, neste momento, a associação mais adequada para apresentar sugestões.

Nos colocando à disposição para discussão futuras, sempre que pudermos contribuir com temas relevantes para a sociedade.

Atenciosamente,

Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.

APROVADO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

← Escaneie para realizar a validação das assinaturas

Algoritmo
SHA-256 with RSA

Hash do documento original
CnuUxlxPmyGDmwDkum4kq4-qU_dbLibuF3jxyOdgMJI

Assinaturas	Data das assinaturas	Complemento
Assinado Eletronicamente por: Tiago Baptista da Silva E-mail: tiagosilva@anbima.com.br Papel: Representante Legal ANBIMA Representação: ANBIMA Associacao Brasileira das Entidades dos Mercados Financeiro e de Capitais	24/12/2025 às 07:02:06	IP 2804:18:153:4089:45c5:927:ab82:86ac4, 172.69.114.75 Latitude:-23.515107718061998 Longitude:-46.71369390224745
Assinado Eletronicamente por: Eliana Maria Gravaes Marino E-mail: eliana.marino@anbima.com.br Papel: Representante Legal ANBIMA Representação: ANBIMA Associacao Brasileira das Entidades dos Mercados Financeiro e de Capitais	29/12/2025 às 10:19:11	IP 177.137.199.67, 172.71.6.116 Latitude:-16.236863 Longitude:-39.003349

Para realizar a validação de assinaturas, acesse:https://esign.portaldedocumentos.com.br/validar-assinaturas e digite o código de validação: IDF6A6RJRRU9

pdsign_ Página 1 de 1

ANEXO XII – Resposta ao ofício: ANBC

Respostas ANBC às Perguntas do GT5 – Proteção ao Crédito e Prevenção à Fraude - CNPD

I) A Importância Socioeconômica do Crédito e da Prevenção à Fraude

1. Qual é a relevância do crédito para o desenvolvimento socioeconômico do Brasil?
O crédito é essencial para inclusão financeira, dinamização do consumo, incentivo ao empreendedorismo, expansão e desenvolvimento da economia. É instrumento de desenvolvimento nacional, redução de desigualdades e formalização econômica.

O GT5 destaca que crédito e prevenção à fraude são pilares complementares para estabilidade sistêmica e confiança digital.

A Pesquisa Febraban 2024 mostra que em 2023 foram realizadas 186 bilhões de transações bancárias, crescimento de 19% em relação ao ano anterior, com 70% via mobile banking e 96% das contratações de crédito já digitais.

O RCG Technical Note destaca que as fraudes financeiras são massivas e que classificações regulatórias equivocadas podem desincentivar inovação, prejudicando inclusão financeira.

2. Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

Previne perdas financeiras, reduz o risco para concedentes de crédito, fortalece a confiança nas transações digitais, estimula a inovação digital e garante segurança jurídica às operações de crédito, o que atrai investimentos e favorece a estabilidade do sistema financeiro. Ademais, as perdas com fraudes são muitas vezes repassadas aos clientes/consumidores.

II) Papel dos Dados Pessoais no Ecossistema de Crédito

3. Qual a importância dos dados pessoais para proteção do crédito e atividades relacionadas?
Dados pessoais viabilizam a avaliação de risco, a precificação do crédito e a prevenção ao superendividamento, permitindo decisões informadas e seguras. Sem tais dados seria impossível realizar avaliações de risco eficazes, conceder crédito de forma segura e justa, prevenir fraudes e, consequentemente, promover a inclusão financeira.

Os dados pessoais são insumos centrais para *scoring*, concessão responsável e detecção de comportamentos fraudulentos.

A Pesquisa Febraban 2024 evidencia que 96% das contratações de crédito ocorrem em canais digitais, o que exige governança robusta sobre dados pessoais.

O RCG Technical Note diferencia modelos determinísticos (ex.: regressão linear) de sistemas de IA de alto risco, reforçando que muitos modelos de crédito são explicáveis e auditáveis.

Assim, biometria, metadados e dados comportamentais são essenciais para mitigar riscos.

4. Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?

Aumenta a previsibilidade da capacidade de pagamento, reduz o custo do crédito, melhora a alocação de recursos e amplia o acesso financeiro. Com mais dados, os modelos de análise de crédito podem prever com maior precisão a probabilidade de inadimplência, permitindo ao credor "conhecer" melhor o tomador.

Assim, o risco percebido de cada operação diminui, o que pode se traduzir em um menor custo de captação de recursos para as instituições e, consequentemente, em taxas de juros mais competitivas para o tomador.

III) Dados Pessoais na Prevenção à Fraude

5. Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?

Permitem a validação de identidade, identificação de padrões suspeitos e combate eficaz à fraude sintética e falsidade ideológica. Também colaboram para a prevenção de cibercrimes.

6. Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos?

Biometria, metadados e dados comportamentais são essenciais para mitigar riscos.

A Pesquisa Febraban 2024 mostra que o Pix alcançou 114 milhões de usuários em 2023, alta de 16%, ampliando bancarização e também riscos de fraude. Renegociações de dívidas cresceram 33% no mobile e 40% no internet banking, evidenciando que operações de crédito e mitigação de risco ocorrem nos mesmos canais digitais.

O RCG Technical Note alerta que não se deve classificar indiscriminadamente biometria como “alto risco”, pois em contextos antifraude ela é indispensável.

7. Quais são os riscos de subutilizar dados pessoais em processos antifraude (ex.: aumento de chargebacks, fraude sintética, falsidade ideológica e riscos sistêmicos)?

Quando as organizações falham em aproveitar adequadamente o potencial dos dados pessoais (seja por limitações tecnológicas, regulatórias excessivamente restritivas, falta de expertise ou processos ineficientes), elas criam brechas que os fraudadores exploram habilmente.

Além do aumento de chargebacks, haverá menor capacidade de autenticação e, por consequência, a dificuldade em prever riscos, com a proliferação de fraudes e ilícitos.

IV) Convergência entre Proteção ao Crédito e Prevenção à Fraude

8. O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns?
Ambos dependem do uso de dados para identificar riscos, prevenir inadimplência e proteger o sistema financeiro de condutas ilícitas. Essa intrínseca relação entre crédito e fraude evidencia que a segurança do sistema financeiro não é uma preocupação secundária, mas sim uma parte integrante e simbiótica da própria concessão de crédito.

A Pesquisa Febraban 2024 mostra que renegociações de dívidas cresceram 33% no mobile e 40% no internet banking, evidenciando que operações de crédito e mitigação de risco ocorrem nos mesmos canais digitais.

O RCG Technical Note reforça que governança deve ser setorial e descentralizada, com autoridades como o Banco Central supervisionando compliance.

9. Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?
Fragmentação das soluções, aumento de custos, redução da eficácia operacional e elevação de riscos de fraude e inadimplência. Tratar crédito e fraude como finalidades separadas é ignorar a interdependência inerente a elas, resultando em um sistema mais caro, mais lento, menos seguro e menos inclusivo para todos. A integração é o caminho para otimizar os fluxos, maximizar o uso de insumos (especialmente dados pessoais) e alcançar os objetivos de crescimento econômico com segurança.

V) Atividades e Bases Legais Aplicáveis à Proteção ao Crédito

10. Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?

- Análise e avaliação de risco
- Score de crédito
- Prevenção ao superendividamento
- Atualização cadastral
- Compartilhamento com credores
- Prevenção e detecção de fraudes e outros ilícitos
- Cumprimento de obrigações legais e regulatórias

A Pesquisa Febraban 2024 mostra que a digitalização massiva exige clareza regulatória para evitar insegurança jurídica.

O RCG Technical Note lembra que o Cadastro Positivo (LC 166/2019) ampliou inclusão financeira e não deve ser tratado como atividade de alto risco.

11. Quais bases legais da LGPD suportam o tratamento para análise e concessão de crédito?

- Art. 7º, V – Proteção do crédito
- Art. 7º, II – Cumprimento de obrigação legal ou regulatória
- Art. 7º, I- Consentimento do titular
- Art. 7º, IX – Legítimo interesse (com cautela e documentação via RIPD)

VI) Bases Legais para Prevenção à Fraude

12. Quais bases legais amparam o tratamento de dados para prevenção a fraudes?

- Art. 7º, II – Obrigação legal
- Art. 7º, V – Exercício regular de direitos
- Art. 7º, IX – Legítimo interesse
- Art. 11, II, "a" – Dados sensíveis (em casos justificados)

O RCG Technical Note cita a Resolução Conjunta nº 6/23 (CMN/Bacen), que obriga compartilhamento de dados de fraude entre instituições financeiras.

A Pesquisa Febraban 2024 mostra que a expansão do Pix e mobile banking aumenta a superfície de ataque, reforçando a necessidade de bases legais claras.

13. Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?

Primeiramente, é importante esclarecer que "prevenção à fraude" não é, por si só, uma base legal autônoma na LGPD. Trata-se de uma **finalidade legítima** para o tratamento de dados, que precisa ser suportada por uma das bases legais previstas no Art. 7º (e, para dados sensíveis, no Art. 11º) da lei.

Deve-se harmonizar o interesse público – estabilidade do sistema financeiro, redução de custos sociais e manutenção da confiança digital- com os direitos e segurança dos titulares, aplicando transparência, proporcionalidade e minimização, conforme os princípios da LGPD.

VII) Princípios da LGPD Aplicáveis a ambos os contextos

14. Quais princípios devem orientar coleta, uso, minimização, retenção e compartilhamento de dados nesses tratamentos?

Finalidade, adequação, necessidade, livre acesso, qualidade dos dados, segurança, prevenção, transparência, não discriminação, responsabilização e prestação de contas.

Fonte: LGPD, art. 6º.

A Pesquisa Febraban 2024 mostra que 79% das transações já são digitais, exigindo equilíbrio entre minimização de dados e eficácia antifraude.

O RCG Technical Note sugere uso de dados sintéticos e differential privacy para reduzir riscos e viés em modelos de IA.

15. Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?

- Adoção de RIPD (art. 38) e teste de legítimo interesse (TLI)
- Definição clara e detalhada das finalidades
- Mapeamento completo dos dados e do ciclo de vida
- Minimização dos dados utilizados
- Desenvolvimento e validação rigorosa dos modelos
- Governança de dados e políticas internas robustas

16. Como operacionalizar transparência sem comprometer a efetividade de sistemas antifraude e de scoring?

- Informações claras sobre critérios gerais
- Canal de atendimento ao titular
- Preservação de segredos comerciais e industriais protegidos por lei (LGPD, art.9º, § 1º)
- Transparência por camadas
- Foco na explicação da lógica, não dá fórmula (LGPD, art. 20)
- Controles e auditorias internas

VII) Governança, Controles e Segurança

17. Quais frameworks de governança e gestão de riscos são recomendados para operações de crédito e antifraude?

- ISO/IEC 27001 (Segurança)
- ISO/IEC 27701 (Privacidade)
- NIST Cybersecurity Framework
- GRC (governança, risco e conformidade)
- LGPD + diretrizes da ANPD

A Pesquisa Febraban 2024 mostra que a confiança dos clientes no mobile banking só foi possível graças a investimentos em cibersegurança, criptografia e resposta a incidentes.

O RCG Technical Note defende governança descentralizada e códigos de conduta setoriais, com supervisão por autoridades como o Banco Central.

18. Quais controles técnicos e administrativos devem ser implementados para assegurar segurança da informação e mitigação de incidentes?

- Criptografia
- Gestão de acessos
- Programas de treinamento
- Data Governance/frameworks de governança
- Registro de logs
- Plano de resposta a incidentes

Fonte: LGPD, art. 46; art. 50.

A Pesquisa Febraban 2024 mostra que a confiança dos clientes no mobile banking só foi possível graças a investimentos em cibersegurança, criptografia e resposta a incidentes.

O RCG Technical Note defende governança descentralizada e códigos de conduta setoriais, com supervisão por autoridades como o Banco Central.

19. Como estruturar políticas de retenção, registro de logs, auditoria e accountability?

- Logs mantidos conforme prazos legais
- Auditorias regulares
- Políticas formais de retenção
- Inventário de dados e mapeamento do ciclo de vida
- Registro das operações de tratamento (art. 37 da LGPD)
- Procedimentos de descarte seguro

IX) DECISÕES AUTOMATIZADAS E INTELIGÊNCIA ARTIFICIAL

20. Quais são decisões automatizadas mais comuns em crédito e antifraude?

Em crédito: aprovação ou negação de pedidos de crédito, definição de limites, taxas de juros e encargos.

Em antifraude: bloqueio ou aprovação de transações em tempo real, bloqueio ou suspensão de contas, verificação automatizada de identidade.

O RCG Technical Note diferencia modelos determinísticos (regressão linear) de IA adaptativa, reforçando que nem todo sistema de crédito é de alto risco.

A Pesquisa Febraban 2024 mostra que contratações e renegociações já são digitais e automatizadas em larga escala, exigindo explicabilidade e mitigação de vieses.

21. Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?

A explicabilidade refere-se à capacidade de compreender *por que* um modelo de inteligência artificial chegou a uma determinada decisão. Em modelos complexos (conhecidos como "caixas-pretas", como redes neurais profundas), essa compreensão não é óbvia. Por isso, sempre que possível, devem ser utilizados modelos mais simples como árvores de decisão, regressões logísticas/lineares, que são naturalmente mais fáceis de interpretar, especialmente para decisões de menor impacto ou quando a precisão de um modelo mais complexo não é estritamente necessária.

A Governança Algorítmica estabelece as políticas e processos para implementar a explicabilidade e a mitigação de vieses de forma sistemática.

A Mitigação de Vieses é um objetivo chave que tanto a explicabilidade (para entender o viés) quanto a governança (para implementar as soluções) buscam alcançar.

É fundamental a existência de controles eficazes, com rigor na documentação e uma cultura organizacional que valorize a ética e a justiça algorítmica tanto quanto a eficiência e o lucro.

22. Quais diretrizes devem orientar o uso de IA generativa e machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos?

Conformidade com a LGPD e outras regulamentações, além de equilíbrio entre inovação tecnológica e responsabilidade ética e legal.

23. Como equilibrar transparência e explicabilidade com segredos de negócio?

O Art. 20 garante o direito de o titular solicitar a revisão de decisões automatizadas e obter informações sobre os critérios e procedimentos utilizados. Contudo, o Art. 9º, §1º, ao tratar do direito do titular à informação, ressalta que esse direito deve ser exercido "observados os segredos comercial e industrial".

Para obter esse equilíbrio seguem algumas diretrizes: (a) adoção da transparência por camadas; (b) implementação da intervenção humana ("human in the loop); (c) documentação interna robusta e governança algorítmica; (d) educação e conscientização interna.

ANEXO XIII – Resposta ao ofício: ABRID

ABRID
Associação Brasileira das Empresas de Tecnologia em Identificação Digital

Ofício nº 001/2026-ABRID Brasília, 09 de janeiro de 2026.

Ao Senhor
RONY VAINZOF
Conselheiro Titular e Coordenador do GT5
Conselho Nacional de Proteção de Dados Pessoais e Privacidade - CNPD

Assunto: Referente a Portaria nº 05/25 do Conselho Nacional de Proteção de Dados Pessoais e Privacidade (CNPD). GT5 – Proteção ao Crédito e Prevenção à Fraude. Solicitação de Contribuição. Apoio e Considerações Pertinentes

Senhor Conselheiro,

1. A Associação Brasileira das Empresas de Tecnologia em identificação Digital (ABRID), criada em 2007, congrega grandes empresas brasileiras e estrangeiras - com atuação no Brasil - de tecnologia em identificação digital, a fim de representá-las diante das autoridades e da sociedade brasileira.

2. As associadas atuam na área de identificação digital através de tecnologias de *smart cards*, certificação digital, identificação biométrica, impressos de segurança, integração de sistemas, entre outras.

3. Há quase duas décadas, a ABRID tem trabalhado em cooperação com instituições públicas e privadas de modo a apoiar e subsidiar técnica e institucionalmente essas Instituições e os entes do governo brasileiro, sobretudo em busca de sistemas de identificação seguros e eficientes para o Brasil.

4. Nesse sentido, recebemos com satisfação a solicitação formulada por esse CNPD para que apresentemos nossas contribuições para as discussões em curso, as quais seguem:

I) A importância socioeconômica do crédito e da prevenção à fraude para o Brasil

1. Qual a relevância do crédito para o desenvolvimento socioeconômico do Brasil?

O mercado de crédito é um dos principais canais de transmissão da política monetária e de financiamento do investimento produtivo; estudos mostram que maior assimetria de

CLSW 105, Bl. A, salas 104 a 106, Sudoeste, Brasília-DF, 70670-431, (61) 3234-6282, www.abrid.org.br

informação gera menor volume de empréstimos, *spreads* mais altos e queda prolongada da atividade econômica[1]. Isso significa que, sem crédito em volume e preço adequados, micro e pequenas empresas tendem a enfrentar racionamento e dificuldade de expansão, com impacto direto sobre emprego, crescimento econômico e arrecadação tributária. Em 2024, o estoque de crédito ampliado às famílias e empresas superou R$ 10 trilhões, algo em torno de 90% do PIB[2], mostrando que praticamente "um PIB inteiro" circula via intermediação de crédito e mercado de capitais, com impacto sobre renda, arrecadação e inclusão financeira.

2. Qual a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

A fraude gera medo, insegurança, perda de confiança e um elevado custo social para o país. Por isso, a prevenção à fraude é crucial para o desenvolvimento socioeconômico do Brasil porque atrai a confiabilidade do mercado e, por consequência, maiores investimentos, bem como contribui para arrecadação e contratações.

Estudo da Serasa Experian mostra que somente as tentativas de fraudes bancárias e em cartões, se não tivessem sido barradas em 2024, poderiam gerar prejuízo estimado de R$ 51,6 bilhões, valor que, se preservado, poderia ser direcionado a crédito, investimento e consumo em vez de perdas e provisões de risco[3].

Mais recentemente, entre julho de 2024 e junho de 2025, 24 milhões de pessoas foram vítimas de golpes financeiros envolvendo o PIX ou boletos bancários, com um prejuízo de quase 29 bilhões de reais, segundo o Fórum Brasileiro de Segurança Pública[4].

Esses volumes elevam o custo operacional e o risco percebido pelos bancos, que respondem com *spreads* maiores e políticas de crédito mais restritivas, reduzindo liquidez e encarecendo o financiamento para famílias e empresas. Trabalhos recentes em gestão de risco e fraudes no setor financeiro sintetizam essa lógica: a gestão proativa de riscos operacionais e de fraude é "essencial para a continuidade e integridade das operações", pois fraudes

---

[1] BARBOSA, Renato Cesar Ottoni; MARÇAL, Emerson Fernandes. The impacts of information asymmetry in determining bank spreads. **Revista Gestão & Políticas Públicas**, São Paulo, Brasil, v. 1, n. 2, p. 113–130, 2011. DOI: 10.11606/issn.2237-1095.v1p113-130. Disponível em: https://revistas.usp.br/rgpp/article/view/97838. Acesso em: 5 jan. 2026.
SOUTO, Gabriel Araújo. Cadastro Positivo: a solução para o combate à assimetria informacional no setor bancário brasileiro?. **Revista da Procuradoria-Geral do Banco Central**, *[S. l.]*, v. 13, n. 1, p. 75–88, 2019. DOI: 10.58766/rpgbcb.v13i1.1016. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1016. Acesso em: 5 jan. 2026.

[2] O crédito ampliado às empresas atingiu R$6,6 trilhões (56,0% do PIB), com expansão de 18,7% no ano, influenciada pelo crescimento de 26,3% nos empréstimos externos e de 27,6% em títulos de dívida.
O crédito ampliado às famílias alcançou R$4,2 trilhões (35,5% do PIB) em 2024, com expansão de 10,6%, refletindo a elevação de 12,1% na carteira de empréstimos do SFN. Disponível em: https://www.bcb.gov.br/content/estatisticas/hist_estatisticasmonetariascredito/202501_Texto_de_estatisticas_monetarias_e_de_credito.pdf

3 SERASA EXPERIAN. Tentativas de fraudes bancárias cresceram 10,4% em 2024 e poderiam gerar prejuízo de até R$ 51,6 bilhões, revela Serasa Experian - Serasa Experian. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraudes-bancarias-cresceram-104-em-2024-e-poderiam-gerar-prejuizo-de-ate-r-516-bilhoes-revela-serasa-experian/>. Acesso em: 6 jan. 2026.
4 RÁDIO SENADO. Mais de 24 milhões de pessoas foram vítimas de golpes pelo PIX. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2025/08/18/mais-de-24-milhoes-de-pessoas-foram-vitimas-de-golpes-pelo-pix>.

recorrentes elevam provisões, pressionam capital regulatório e limitam a capacidade de oferta de crédito.[5]

II) Papel dos dados pessoais no ecossistema de crédito

3. Qual a importância dos dados pessoais para proteção do crédito e demais atividades relacionadas ao tema?

Só é possível a proteção do crédito com tratamento de dados pessoais. Ou seja, o tratamento de dados pessoais é essencial para proteção do crédito porque permite avaliar riscos de forma precisa, possibilitando reduzir inadimplência e expandir o volume de financiamento com juros menores, alavancando crescimento econômico. Por isso que a lei brasileira 13.709/2018 (LGPD) foi vanguardista ao trazer a base legal específica da proteção do crédito como uma das hipóteses do art. 7. O que deveria ser um exemplo a ser seguido por outros países.

Segundo estudo do Banco Central do Brasil (BCB) sobre os efeitos do Cadastro Positivo[6], quando o mercado dispõe de dados completos (cadastrais e comportamentais), o crédito cresce, o *spread* cai e, consequentemente, bilhões de reais adicionais podem ser injetados na economia brasileira de forma assertiva e sustentável.

No Brasil, o BCB e a literatura econômica apontam que estruturas de informação ineficientes elevam o *spread* bancário, restringem liquidez e tornam o sistema financeiro menos sustentável, sobretudo em ciclos de estresse[7]. Birôs de crédito e cadastros positivos, ao consolidar históricos de pagamento, ampliam a base de informação e permitem inclusão de consumidores antes "invisíveis", o que aumenta a taxa de bancarização e o acesso a financiamentos para consumo, habitação e capital de giro.[8]

Dessa forma, pode-se identificar que os dados pessoais (por exemplo: identificação, renda, histórico de pagamento) são o insumo para reduzir a assimetria informacional, permitindo que o sistema financeiro mantenha a oferta de crédito e a liquidez mesmo em ciclos de estresse, o que protege a estabilidade e o crescimento econômico.

4. Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?

O uso de dados pessoais (cadastrais, financeiros e comportamentais) reduz assimetrias informacionais vez que viabiliza maior assertividade do titular/solicitante diante da análise ampla de uma base de dados. Assim, a identificação mais assertiva do risco permite que o

5 CARLOS, S. Gerenciamento de riscos em processos de operações financeiras: análise comparativa de riscos e práticas mitigadoras em modelos normalizados. UFPB, 2025.
6 Análise dos efeitos do Cadastro Positivo. [s.l: s.n.]. Disponível em: <https://www.bcb.gov.br/content/publicacoes/Documents/outras_pub_alfa/analise_dos_efeitos_do_cadastro_positivo.pdf >. Acesso em: 6 jan. 2026.
7 Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Febraban_2023_Estudo_do_Spread.pdf
8 CNN Brasil. **Mais de 13 milhões de pessoas entraram no cadastro positivo desde 2020, aponta Serasa.** Disponível em: <https://www.cnnbrasil.com.br/economia/financas/mais-de-13-milhoes-de-pessoas-entraram-no-cadastro-positivo-desde-2020-aponta-serasa/ >. Acesso em: 5 jan. 2026.

sistema financeiro empreste mais, com menor perda esperada e melhor formação de preços[9] – via Cadastro Positivo, bureaus e *Open Finance* –, há ganhos concretos em liquidez, redução da inadimplência e eficiência alocativa do crédito.

Estudo da Serasa Experian sobre o Cadastro Positivo[10], uma das primeiras medidas para redução de assimetrias informacionais, já estimava em 2019 que, com o uso amplo de dados comportamentais de pagamento, poderia haver injeção de cerca de R$ 1,3 trilhão adicionais na economia, elevando a relação crédito/PIB de 47,4% para 67,0%. Esse resultado é, essencialmente, um efeito de liquidez: dados mais completos sobre milhões de consumidores permitem transformar capacidade de pagamento "oculta" em operações de crédito elegíveis, aumentando o volume de dinheiro emprestado sem, em tese, aumentar o risco agregado.

O mesmo estudo ainda já afirmava que 22,6 milhões de pessoas com "score baixo" não o possuíam por histórico negativo, mas por "insuficiência de informação" e que, com o Cadastro Positivo suprindo dados de contas e pagamentos, tornariam essa população elegível e com melhores condições ao crédito. Ou seja, ao distinguir quem é de fato arriscado de quem apenas "não tem dados", esses sistemas reduzem o erro de seleção típico de mercados com alta assimetria, canalizando crédito para perfis com menor probabilidade de default e, portanto, reduzindo inadimplência estrutural.

Portanto, se um credor tiver informações creditícias mais completas sobre o tomador de empréstimo, o banco poderá alocar com mais precisão o valor do risco, afastando-o da taxa de juros mais alta em decorrência da assimetria informacional e resultando em um produto de valor melhor para o cliente[11], e por fim, aumentando a eficiência de todo mercado, criando um círculo virtuoso para a economia.

III) Papel dos dados pessoais na prevenção à fraude e outros ilícitos

5. Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?

Só é possível melhorar os mecanismos de prevenção à fraude com tratamento de dados pessoais de forma cada vez mais completa e assertiva. A combinação de muitas informações históricas (de mais recentes para mais antigas) é o que faz com que os sistemas de anti-fraude possam discernir quando é a pessoa e quando não é a pessoa por métodos que avaliam "desvios de conduta", e identificam comportamentos atípicos associados àquele usuário específico (individualizado).

---

[9] EDUARDO, C. O impacto esperado do Open Finance no mercado de crédito e na economia do Brasil. Disponível em: <https://repositorio.fgv.br/items/051100c6-9491-4cac-b311-0334863cae52>.

[10] SERASA EXPERIAN. **Cadastro Positivo pode favorecer 137 milhões de brasileiros**. Disponivel em: <https://www.serasaexperian.com.br/conteudos/cadastro-positivo-pode-favorecer-137-milhoes-de-brasileiros/>. Acesso em: 8 jan. 2026.

[11] MERRILL, Howard J. III. **Consequences of Information Asymmetry on Corporate Risk Management**. Applied Economics Theses, n. 21, 2017. Disponível em: https://pdfs.semanticscholar.org/3c5b/fa4604b1b63ea081a0f5f9ca84a0b2dc54bf.pdf.

Portanto, os dados pessoais possuem papel extremamente importante na prevenção à fraude, uma vez que, além de permitirem a identificação e autenticação dos titulares, contribuem para definir quando não é a pessoa, quando é alguém tentando ser a pessoa, inclusive com situações que podem envolver relação de proximidade ou conveniência (familiar ou terceiro com cargo de confiança). Pois mais importante que saber quando é a pessoa é saber todas as vezes que não é, ou seja, que pode até parecer, mas não é. E este nível de acurácia e sofisticação só é alcançado quando potencializado pelo conhecimento exaustivo dos dados pessoais do titular.

Deste modo, o tratamento de dados pessoais permite, por exemplo:

- Identificação e autenticação do titular, evitando o uso indevido da identidade, falsidade ideológica, golpes financeiros e fraudes digitais e analógicas;

- Rastreabilidade das operações, possibilitando a detecção e redução de ilícitos; e

- Responsabilização e prova, permitindo a identificação de autores de ilícitos e a fundamentação de investigações administrativas, civis e penais.

Com efeito, é certo que o regular e necessário tratamento de dados pessoais por autoridades públicas, instituições financeiras e agentes de mercado autorizados não só pode como deve ser realizado para mitigar fraudes e demais ilícitos correlatos que costumeiramente se valem de opacidade e inexatidão informacional para sua consecução.

6. Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos?

Os dados comportamentais, biométricos e metadados são fundamentais para mitigação das fraudes, principalmente de falsidades ideológicas, e permitem que as organizações ultrapassem o modelo comum de verificação de identidade. A junção desses dados torna possível analisar quem é o usuário e também "como", "quando", "de onde" e em que contexto ele realiza a sua interação, e, principalmente, contribui com o "pool de dados" necessários para gerar distinção (saber quem não é a pessoa).

Inclusive, a própria Resolução BCB nº 501/2025, dispõe que instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil e instituições de pagamento integrantes do Sistema de Pagamento Brasileiro (SPB), podem utilizar informações provenientes de sistemas eletrônicos e bases de dados de caráter público ou privado, reforçando assim, a legitimidade do uso desses dados para fins de prevenção a fraudes, golpes e outros ilícitos.

Deste modo, possibilitar que a organização tenha essa visão ampliada dos dados viabiliza a avalição **de padrões, contexto e intenção**, criando uma camada de segurança mais refinada e eficaz na mitigação de fraudes, golpes e outros ilícitos, o que é essencial com o aumento dos golpes usando *deepfake*.

Assim, quando a instituição dispõe de tais dados pessoais, pode-se dizer que há uma mudança estrutural no modelo de prevenção a fraudes, ou seja, a empresa sai de uma abordagem padronizada para um modelo contextual.

Nesse sentido, adotando um modelo contextual, a empresa conseguirá tomar decisões mais precisas, possibilitando de forma significativa a capacidade de identificar comportamentos anômalos antes mesmo da concretização de uma fraude, golpe ou de um ilícito.

Para melhorar a compreensão, destacam-se os seguintes tipos de dados:

- Dados Comportamentais: correspondem às informações relacionadas como o usuário interage com os sistemas, plataformas e serviços ao longo do tempo, possibilitando a identificação de padrões como por exemplo, horários e frequência de acesso, rotina de transações bancárias, etc.

- Dados Biométricos: são dados que dispõe sobre características físicas ou comportamentais únicas de um indivíduo. São subdivididos em biometria física (facial, impressão digital, voz, íris) e biometria comportamental.
  O uso de dado biométrico, como, por exemplo, fator de autenticação, fortalece a confirmação da identidade do usuário, essencial para a redução de fraudes de identidade.

- Metadados: são dados contextuais que descrevem o ambiente onde a transação ou interação ocorre, como por exemplo, o endereço de IP, MAC *Address*, porta lógica e geolocalização.

Importante constatar que o uso de algoritmos biométrico robustos, com alta acurácia, testados internacionalmente por entidades reconhecidas, como o NIST (National Institute of Standards and Technology), garantem o funcionamento adequado das verificações biométricas. Além disso, os sistemas de coleta, comunicação e armazenamento biométrico devem seguir os altos padrões de segurança, como por exemplo do ISO (International Organization for Standardization).

Portanto, é forçoso concluir que o uso combinado e estruturado desses dados potencializa significativamente a possibilidade de redução de fraudes pelas organizações, sendo, portanto, fundamental o seu tratamento integrado.

7. Quais são os riscos de subutilizar dados pessoais em processos antifraudes (ex. aumento de *chargebacks*, fraude sintética, falsidade ideológica e riscos sistêmicos)?

A utilização adequada de dados pessoais constitui elemento indispensável para a efetividade dos processos de prevenção a fraudes. A subutilização compromete a capacidade de identificação de riscos, o que pode facilitar e favorecer a ocorrência de fraudes, golpes e atos ilícitos.

Em um cenário nos quais os dados pessoais não são empregados de forma integrada, cada informação é analisada de maneira isolada, impedindo a correlação entre identidade, comportamento e contexto. Isso reduz significativamente a capacidade dos sistemas antifraude de identificar padrões complexos e inconsistências sutis, típicas de fraudes modernas.

Do ponto de vista operacional, essa limitação se reflete no aumento de *chargebacks*, uma vez que as transações são, na maioria das vezes, aprovadas sem a necessária e imprescindível análise contextual.

Deste modo, a ausência de correlação entre o perfil histórico do usuário, seu comportamento esperado e o contexto da operação inviabiliza a identificação de anomalias relevantes ao risco do negócio.

Adicionalmente, é importante destacar que a subutilização dos dados pessoais favorece a proliferação de fraude sintética[12], que ocorre quando um fraudador consegue criar uma identidade do zero a partir da combinação de dados reais ou falsos.

Nessa hipótese, por exemplo, sem o cruzamento estruturado dos dados cadastrais, comportamentais e contextuais, essas identidades conseguem superar qualquer controle básico, permanecendo tais contas ativas por período indevido, acumulando prejuízo as empresas.

Conforme estudo do Serasa Experian "*a perda financeira está bastante relacionada na dificuldade em identificar o fraudador, uma vez que eles realizam diversos testes para descobrir qual o padrão que a empresa determinou para considerar que aquelas ações são de uma pessoa legítima*".

Dessa forma, o tratamento de dados pessoais não constitui excesso, mas requisito essencial para a efetividade dos controles antifraude, contribuindo para redução de perdas financeiras, bem como uma melhor a experiência dos seus titulares.

IV) Convergência entre proteção ao crédito e prevenção à fraude

8. O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?

Uma das principais evidências de que o crédito e a fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco é a própria integração de dados e tecnologia aplicada de forma contínua ao longo da jornada do titular do dado.

Essa integração não é apenas desejável, mas sim fundamental, pois na prática, o ideal é que os processos de identificação de fraude já estejam incorporados ao fluxo de análise de crédito desde o início, ou seja, antes mesmo da oferta do crédito ser aprovada, múltiplos dados pessoais (por exemplo, dados comportamentais, metadados e dados contextuais, dentre outros) são cruzados para verificar se a solicitação está alinhada com os padrões legítimos do indivíduo.

Nesse sentido, quando esses dados são integrados e compartilhados de forma legítima e integrada, a instituição passa a ter uma visão abrangente e precisa do risco envolvido em cada camada da sua operação.

Isso é exatamente o que se observa nas tendências mais atuais de prevenção e combate a fraudes: a convergência entre análise de risco de crédito, prevenção à fraude e combate à

[12] Fonte: Fraude de identidade sintética: o que é e como ela pode afetar o seu negócio

lavagem de dinheiro, com uso de tecnologia avançada para cruzar informações de múltiplas origens. [13]

Também reforça essa percepção a própria Resolução BCB nº 6 de 2023, que 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 BCB.

Logo, a integração dos dados possibilita ganhos significativos e relevantes para uma organização, uma vez que poderá ter facilitado a precisão analítica, a velocidade na detecção de eventual fraude, ou ato ilícito, bem como possibilita uma maior eficiência operacional.

9. Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?

O tratamento da concessão de crédito e da prevenção à fraude como trilhas independentes pode gerar impactos diretos tanto na efetividade dos controles, como na eficiência operacional e na capacidade de gestão de riscos das instituições financeiras.

Uma das principais consequências é a impossibilidade de construir uma visão detalhada, uniforme e contínua do cliente ao longo de toda a sua jornada, o que compromete a identificação precoce de fraudes e ilícitos.

A separação dessas finalidades, na prática, gera impedimento na integração dos dados pessoais e decisões de risco. Informações relevantes permanecem fragmentadas em silos distintos — como dados cadastrais em um fluxo, dados comportamentais em outro e informações contextuais em sistemas isolados — dificultando a correlação entre eventos. Essa fragmentação reduz significativamente a capacidade de identificar padrões complexos e sinais fracos de fraude, que normalmente só se tornam evidentes quando analisados de forma conjunta.

Como consequência direta, os mecanismos de prevenção à fraude passam a operar de maneira limitada e com assertividade afetada, uma vez que decisões são tomadas com base em conjuntos incompletos de dados.

Além disso, a ausência de integração dos dados pessoais compromete a detecção de fraudes mais sofisticadas, como por exemplo, a fraude sintética e o uso indevido de identidades de terceiros.

Deste modo, tratar concessão de crédito e prevenção à fraude e proteção como trilhas separadas pode resultar em uma ineficiência operacional, menor assertividade na detecção de ilícitos e maior exposição a perdas financeiras e riscos sistêmicos. Em contrapartida, a integração dessas finalidades permite decisões mais precisas, atuação preventiva e uma gestão de riscos mais robusta, alinhada às exigências regulatórias e legais, bem como à complexidade crescente das fraudes contemporâneas.

[13] Fonte: Maiores tendências em fraudes e crimes financeiros em 2025 (SERASA)

V) Atividades e bases legais aplicáveis à proteção ao crédito

10.Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?

As seguintes atividades de tratamento podem ser englobadas na base legal de proteção do crédito:

(a) Análise de risco/score de crédito, incluindo a modelagem de *credit scoring* que visa atribuir uma pontuação de risco a um titular com base em dados históricos de pagamentos e comportamento financeiro, e a avaliação de capacidade de pagamento, considerando a renda e os compromissos financeiros assumidos.
(b) Gestão da Inadimplência, contando com a negativação de titulares devedores e consultas a bases de dados de terceiros para verificar débitos pendentes de um prospecto.
(c) Prevenção ao superendividamento, mediante análise contínua de comportamento financeiro do cliente para identificar sinais de insolvência e evitar concessão de novos créditos que possam comprometer a subsistência do titular analisado.
(d) Gestão do Cadastro Positivo, com o processamento das obrigações financeiras liquidadas ou em andamento para formar o histórico de bom pagador.
(e) Localização de devedores e atividades de cobrança (fase pré-judicial): considerando que crédito não se resume ao momento da concessão, mas sim compreende a concessão, a manutenção e a recuperação, localizar um titular devedor é uma etapa intrínseca à proteção da operação de crédito efetuada. Além disso, a localização do devedor permite a notificação do titular antes de uma negativação formal, conforme o CDC.

11.Quais bases legais da LGPD suportam o tratamento de dados para análise e concessão do crédito?

Para uma governança robusta no setor financeiro ou comercial é preciso considerar as diferentes etapas do fluxo de análise e concessão de crédito ((i) prospecção e pré-análise; (ii) processamento da solicitação e formalização e (iii) análise de risco para a determinação da base legal que as fundamente. Sob este prisma, temos as seguintes bases legais aplicáveis:

(a) Fase inicial de prospecção e análise: Legítimo interesse (art. 7º, IX, LGPD) para o uso de dados de titulares prospectos para ofertas de crédito (pré-aprovados) e para o uso de dados coletados de fontes externas não públicas para uma análise inicial antes da solicitação formal do cliente.
(b) Processamento da solicitação e formalização: Procedimentos preliminares ao contrato (art. 7º, V, LGPD), para o uso dos dados do titular solicitante do crédito, e o Cumprimento de Obrigação Legal ou Regulatória (art. 7º, II, LGPD) para o uso de dados exigidos pelo Banco Central e leis de prevenção à lavagem de dinheiro (PLD, Lei 9.613/98).
(c) Análise de risco: Proteção ao crédito (art. 7º, X, LGPD), para o uso de dados do titular para consultas aos *bureaus* e geração de *score* de crédito, e a Prevenção à Fraude e

Segurança do Titular (art. 11, II, "g", LGPD), para o uso de dados sensíveis (biometria) para autenticação e validação de identidade durante a concessão do crédito.

VI) Bases legais aplicáveis à prevenção à fraude

12.Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?

As bases legais a seguir amparam os usos de dados pessoais para prevenir fraudes:

(a) Legítimo Interesse (art. 7º, IX, LGPD), para proteção do patrimônio e segurança da plataforma do Controlador.
(b) Cumprimento de Obrigação Legal ou Regulatória (art. 7º, II, LGPD), para cumprir as exigências legais e regulatórias definidas pelo BACEN, CVM ou COAF.
(c) Execução de Contrato ou procedimentos preliminares relacionados a contrato (art. 7º, V, LGPD), para garantir que a transação solicitada pelo titular seja legítima.
(d) Garantia da Prevenção à Fraude e Segurança do Titular (art. 11, II, "g", LGPD), para proteger o titular de ter seus dados utilizados por terceiros.
(e) Exercício regular de direitos, inclusive em contrato e em processos judiciais, administrativos e arbitrais (Art. 7º, VI e art. 11, II, "d", LGPD), na proteção jurídica do Controlador.

13.Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?

A interpretação da prevenção à fraude sob a ótica do interesse público vai além do princípio de economicidade e iniciativas de redução de custos operacionais no sistema financeiro, que opera na base da fé pública. É um pilar que sustenta e fortalece a confiança nas instituições financeiras e na própria economia do país, além de permitir o exercício da Cidadania Digital.

Uma fraude não é apenas uma perda financeira, mas sim uma violação de direitos fundamentais do cidadão impactado. Uma identidade roubada pode causar o descontrole do cidadão sobre sua própria vida civil.

Se as ocorrências de fraudes forem elevadas, o sistema financeiro torna-se tão burocrático que acaba por excluir as populações mais vulneráveis e encarece o crédito, por isso o próprio Banco Central do Brasil trata acertadamente a prevenção à fraude como uma questão de segurança sistêmica.

VII) Princípios da LGPD aplicáveis a ambos os contextos

14. Quais princípios devem orientar a coleta, uso, minimização, retenção e compartilhamento de dados nesses tratamentos?

O tratamento de dados pessoais no contexto de prevenção à fraude e concessão de crédito deve observar, de forma rigorosa, os princípios previstos no artigo 6º da LGPD, em especial:

- **Princípio da qualidade dos dados (art. 6º, V):** os dados utilizados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e finalidade do tratamento. No contexto antifraude, isso significa que informações cadastrais, comportamentais, biométricos e contextuais devem ser corretos e atualizados para permitir uma avaliação de risco confiável e possibilitar a mitigação de fraude e atos ilícitos.
- **Princípio da transparência (art. 6º, VI):** os titulares devem ter acesso a informações claras sobre a coleta, uso, compartilhamento e finalidades de seus dados. Essa transparência é fundamental para manter a confiança do indivíduo, mesmo em fluxos de análise de risco contínuos e preventivos.
- **Princípio da não discriminação (art. 6º, IX):** o tratamento não pode ser utilizado para fins discriminatórios ilícitos ou abusivos, devendo os modelos de análise de risco considerar critérios objetivos, históricos e comportamentais, sem viés ou preconceito.
- **Princípio da segurança (art. 6º, VII):** o agente de tratamento deve utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão

Adicionalmente, importante considerar o **princípio da minimização (art. 6º, II)**, o qual estabelece que o tratamento deve se limitar ao mínimo necessário para atingir a finalidade definida.

No entanto, no cenário em discussão, a aplicação desse princípio requer interpretação contextual: quanto mais complexos e sofisticados forem os riscos de fraude, maior será a necessidade de dados adicionais para permitir uma análise precisa e preventiva. Ou seja, a minimização não significa limitar arbitrariamente a coleta de informações, mas sim **garantir que os dados necessários para cada avaliação de risco sejam utilizados**, respeitando a finalidade e a segurança do titular.

Portanto, o tratamento contínuo e integrado de dados pessoais, dentro de um modelo proporcional e governado, não apenas atende à LGPD, mas reforça a eficácia na prevenção de fraudes, ao mesmo tempo em que preserva a segurança e a confiança dos titulares.

15. Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?

A proporcionalidade, a necessidade e a adequação em modelos de risco integrados são asseguradas por meio de uma governança estruturada de dados e modelos, alinhada à finalidade específica de prevenção a fraudes e gestão de riscos, com controles técnicos, jurídicos e operacionais claramente definidos.

O princípio da necessidade é garantido pela utilização dos dados necessários para a avaliação de risco, definidos a partir de mapeamento prévio de ameaças, evitando coletas excessivas ou desconectadas da finalidade antifraude.

De outro lado, a adequação é assegurada pela correlação dos dados utilizados com resultados mensuráveis de mitigação de risco, por meio de testes de efetividade, validação de modelos, monitoramento contínuo de performance (*ex.: redução de fraude*, *chargebacks e falsos positivos*) e revisão periódica dos sinais utilizados.

Por fim, a proporcionalidade é aplicada por meio de modelos dinâmicos e baseados em risco, nos quais a profundidade da análise, o volume de dados processados e o nível de fricção imposto ao usuário variam conforme o score de risco da operação, adotando medidas escalonadas (*risk-based approach*).

Tais princípios são reforçados por mecanismos de governança, como por exemplo: (i) segregação de finalidades e minimização de dados; (ii) documentação técnica e jurídica dos modelos; (iii) auditorias internas; (iv) explicabilidade das decisões automatizadas e (v) políticas de retenção e descarte compatíveis com o risco.

Dessa forma, os modelos de risco integrados permanecem eficazes no combate a ilícitos, ao mesmo tempo em que preservam direitos dos titulares, asseguram conformidade regulatória e mantêm a confiança no ecossistema.

16. Como operacionalizar transparência sem comprometer a efetividade de sistemas antifraude e de *scoring*?

Os controladores devem assegurar transparência ativa no tratamento de dados pessoais, mesmo quando utilizam sistemas sofisticados de prevenção à fraude, *scoring* de crédito e análise de risco.

Para tanto, recomenda-se adotar algumas práticas, como por exemplo, (i) disponibilização de Aviso de Privacidade abrangente e acessível: o documento deve ser elaborado com informações claras sobre a finalidade do tratamento, os tipos de dados tratados, prazos de retenção e medidas de segurança adotadas. Além disso, o aviso deve estar disponível de forma pública e fácil acesso ao titular e demais interessados, incluindo um canal eficaz para exercício dos direitos dos titulares, conforme dispõe a LGPD e (ii) Transparência compatível com eficácia do sistema: a comunicação ao titular não precisa detalhar cada modelo, regra ou algoritmo específico utilizado no *scoring* ou na detecção de fraude, evitando comprometer a efetividade operacional e a segurança do sistema.

Tais abordagens permitem ao titular e terceiros interessados compreenderem a finalidade, tipo de dado e medidas de proteção, sem prejudicar a atuação preventiva e proativa da organização.

Além disso, é importante destacar novamente a integração contínua dos dados pessoais, visto que a coleta e o uso de dados devem ser proporcionais à finalidade. A respectiva integração contínua permitirá maior assertividade na detecção de fraudes e *scoring* de crédito, equilibrando eficácia operacional e conformidade legal e regulatória.

Desta forma, a transparência operacionalizada de forma clara, proporcional e contextualizada permite que os sistemas financeiros utilizem todas as fontes de dados necessários para proteger o negócio e os seus clientes, mantendo assim a efetividade de prevenção de fraudes e *scoring* de crédito, sem comprometer e/ou violar princípios dispostos na LGPD.

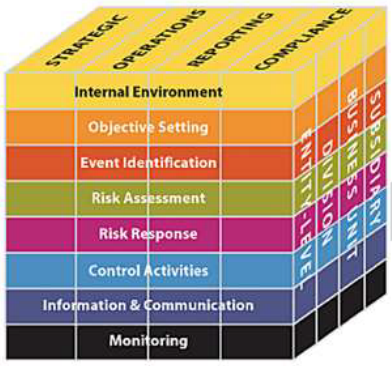
VIII) Governança, controles e segurança

17.Quais *frameworks* de governança e gestão de riscos são recomendados para operações de crédito e antifraude?

Os frameworks recomendados são baseados nas boas práticas internacionais e na regulamentação específica da área de atuação da empresa.

Dentre as boas práticas internacionais estão:

a) o COSO ERM, para alinhar a cultura organizacional de forma integrada com abordagem tridimensional, focando em atividades, áreas de negócio e unidades de negócio.



b) ISO 31.000:2018 – Gestão de riscos – Diretrizes.
c) ISO 27.005:2022 – Gestão de riscos de segurança da informação.

Para empresas atuantes no mercado financeiro, por ex. instituições de pagamento, há regulamentações específicas a serem observadas pelo programa de governança das operações de crédito e antifraude, como:

a) BACEN, Resolução Conjunta 6/2023, que estabelece o compartilhamento obrigatório de informações de fraude entre instituições, visando a construção de inteligência coletiva do sistema financeiro.
b) BACEN, Resolução BCB nº 142/2021, disciplina controles para prevenção de fraudes em serviços de pagamento.
c) BACEN, Resolução BCB nº 265/2022, atualizada pela Resolução BCB nº 447/2024, que define a estrutura de gerenciamento de riscos para instituições de pagamento.

18.Quais controles técnicos e administrativos devem ser implementados para assegurar a segurança da informação e mitigação de incidentes?

Os controles a serem implementados devem ser aptos a proteger as informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de uso inadequado ou ilícito, bem como as medidas

aconselháveis dado o estado da tecnologia, garantindo a confidencialidade, integridade e disponibilidade das informações, incluindo:

a) medidas administrativas como Avisos de Privacidade, Política de Segurança da informação, Política de Gestão de Identidades e Controles de Acessos, Política de Uso Aceitável de Recursos Tecnológicos e Comunicações, Política de Uso Responsável de Inteligência Artificial, Política de Cópia de Segurança (backup) e Recuperação, Plano de Resposta a incidentes, Plano de Continuidade de Negócios, Política de Segurança desde a Concepção (*Security by Desing)* entre outras.
b) medidas técnicas como autenticação, mecanismos de criptografia, detecção de intrusão, prevenção de vazamentos de informações (DLP), mecanismos de proteção contra softwares maliciosos (antivírus e *antispywares*), mecanismos de rastreabilidade, cópias de backup, monitoramento de vulnerabilidades de recursos de tecnológicos e de comunicações, controles de acesso, gestão de identidades e implementação de perfis de privilégios, mecanismos de proteção de rede (segmentação de rede – isolamento de ambientes de produção e de testes, *firewalls*, portais cautivos na rede WAN), gerenciamento de certificados digitais e seus usos, definição de requisitos técnicos para a integração de sistemas por meio de APIs, monitoramento de informações de interesse na *Deep Web* e *Dark Web*, conforme Resolução CMN 5.274/2025).

19.Como estruturar políticas de retenção, registro de logs, auditoria e *accountability*

Para a estruturação destas políticas, é importante observar:

a) Retenção de dados (Prolongada): Considerada a atuação em proteção ao crédito e prevenção de fraudes como atividades envolvidas em forte ambiente regulatório, o tratamento de dados deve ser realizado, excepcionalmente, de forma contínua, permanente e expansiva, pois o histórico de informações a respeito de determinado titular de dados contribui para o combate à fraude de forma mais assertiva, considerando que novos dados surgem continuamente a partir de dados já existentes. Ou seja, em casos de prevenção à fraude, a coleta contínua não significa coleta excessiva, mais inerente à própria natureza da finalidade antifraude, cuja retenção prolongada de dados é defensável em razão de padrões e fraudes que são identificadas a posteriori, a partir do histórico de informações.
b) Registro de *logs*: Embora o Marco Civil de Internet defina 6 (seis) meses de retenção para *logs* das aplicações, novamente a observação de legislações e regulamentações específicas aplicáveis à área financeira é relevante para a governança de registros. Por exemplo, a Lei de Lavagem de Dinheiro (Lei 9.613/98) estabelece o prazo mínimo de 5 (cinco) anos de retenção de *logs* de transações financeiras, contados a partir do enceramento da conta ou da conclusão da transação. Entretanto, conforme previsão legal, a Autoridade competente (BCB) pode ampliar esse prazo e temos diversos prazos para retenção de logs, desde 5 (cinco) anos, conforme Resolução CMN 4.893/2021 até os casos de investigações relacionadas a fraudes, em que os *logs* devem ser mantidos por 10 (dez) anos, conforme Resolução Conjunta BCB 6/2023 e *logs* de transações financeiras por período mínimo de 10 (dez) anos, conforme Circular BCB3.978/2020 e atualizações.

c) Auditoria: deve ser observada a Resolução BCB 93/2021, atualizada pela Resolução BCB 368/2024, para o planejamento e execução de auditorias internas nas administradoras de consórcio, nas instituições de pagamento, nas sociedades corretoras de títulos e valores mobiliários, nas sociedades distribuidoras de títulos e valores mobiliários e nas sociedades corretoras de câmbio autorizadas a funcionar pelo BCB.
d) *Accountability*: visando a responsabilização e transparência, as instituições financeiras devem nomear um diretor responsável pela segurança cibernética na instituição junto ao BCB, nos termos da Resolução CMN 4.893/2021 e suas atualizações, além de demonstrarem sua governança através de auditorias periódicas, evidenciando estarem preparadas para o cumprimento da legislação e regulamentação da área de atuação de forma diligente, inclusive sobre comunicação de incidentes ao BCB, tais como indícios de fraude em até 24h após identificar um indício ou tentativa de fraude.

IX) Decisões automatizadas e Inteligência Artificial

20. Quais são decisões automatizadas mais comuns em crédito e antifraude?

Nos cenários de crédito e antifraude, são muitas as decisões que, atualmente, já são realizadas de forma automatizada sem que haja, necessariamente, intervenção humana.

Dentre essas, destacam-se a aprovação ou reprovação de propostas, a definição de limite, taxa de juros e prazo, bem como ajustes de limite e estratégias de cobrança; e, em antifraude, a autorização ou negação de transações, a aprovação ou bloqueio de cadastros, a exigência de autenticação adicional e o bloqueio preventivo de contas.

Importante esclarecer que, ainda que tratando-se de decisões automatizadas, são necessárias definições de parâmetros auditáveis a serem observados quando da tomada de decisão. Outrossim, viável em primeiro nível a revisão de decisões automatizada por soluções de inteligência artificial e revisão humana em segundo nível, observando *accountability*.

21. Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?

Para lidar adequadamente com explicabilidade, governança algorítmica e mitigação de vieses em modelos de crédito e antifraude, é recomendável adotar um conjunto integrado de medidas técnicas, organizacionais e jurídicas.

A explicabilidade decorre diretamente da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), especialmente do art. 20[14], que garante ao titular o direito à informação clara sobre decisões tomadas unicamente com base em tratamento automatizado de dados

[14] LGPD, Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

pessoais, inclusive aquelas destinadas à definição de perfis de crédito e à prevenção à fraude.

Tal dever é reforçado pelos princípios da transparência, finalidade e necessidade previstos no art. 6º do mesmo dispositivo legal.

De outro lado, a governança algorítmica encontra fundamento no princípio da responsabilização e prestação de contas do art. 6º, X, bem como no dever de manutenção de registros das operações de tratamento (art. 37 da LGPD).

A mitigação de vieses e discriminação, por sua vez, é imposta pelo princípio da não discriminação previsto no art. 6º, IX, da LGPD, que veda o uso de dados pessoais para fins discriminatórios ilícitos ou abusivos. Esse dever é reforçado pelo Código de Defesa do Consumidor (Lei nº 8.078/1990), especialmente pelo art. 6º, III e VI, que asseguram informação adequada e proteção contra práticas abusivas, e pelo art. 39, que proíbe condutas discriminatórias na concessão de crédito. No plano constitucional, a exigência decorre do art. 5º, caput, que consagra o princípio da igualdade, e do art. 170, que impõe a harmonização entre livre iniciativa e proteção do consumidor.

Importante utilizar no treinamento de IA dados mais diversos em conjunto com técnicas de amostragem equilibradas, pode garantir que os dados representem uma variedade de grupos demográficos por exemplo e evitar que uma tomada de decisão reproduza ou amplifique vieses sociais.

Ainda, antes de implementar soluções de IA necessário incorporação de medidas de governança com avaliação inclusive de imparcialidade em *datasets* de treinamento das IA. Identificar as limitações de representação e possíveis correlações prejudiciais ou discriminatórias entre dados auxilia a não reprodução dos vieses sociais.

Para tanto, em especial quando se trata de decisões automatizadas, necessário que se realize um acompanhamento constante dos resultados fornecidos, sendo essencial sua verificação para que sejam identificados, quando houver, resultados que se afastem da realidade e possuam caráter discriminatório.

Logo, conclui-se que a adoção de modelos explicáveis, governança algorítmica estruturada e mecanismos de mitigação de vieses não é apenas uma boa prática técnica, mas um dever jurídico, indispensável para a conformidade legal.

22. Quais diretrizes devem orientar o uso de IA generativa e machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos?

As diretrizes que devem orientar o uso da IA generativa e *machine learning* nas situações expostas devem abranger questões jurídicas, regulatórias e técnicas, especialmente no contexto financeiro e de prevenção a ilícitos.

Quando abordamos tratamento de dados pessoais, este deve estar amparado em uma base legal válida, nos termos do art. 7º da LGPD, ressaltando que o uso de IA generativa para análise de risco, KYC e antifraude deve ser limitado ao estritamente necessário, em observância ao princípio da necessidade previsto na lei supracitada.

Além disso, essencial destacar também o princípio da exaustão. Este, no contexto do *machine learning*, refere-se a uma abordagem na análise de dados que busca maximizar o uso de todos os dados disponíveis.

Apenas dessa forma será possível que as ferramentas de IA generativa consigam aprender de forma completa e, consequentemente, tomar decisões de forma mais assertiva possível. É certo que, caso a ferramenta não tenha acesso à todas as informações, essa estará mais sujeita a erros e alucinações.

Ademais, considerando o art. 20, §1º da LGPD, o controlador, a fim de prestar informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada deve informar ao titular: a) a fonte dos dados que são utilizados e quais parâmetros que podem influenciar no resultado, incluindo, se existem etapas intermediárias e como o sistema decide com base nas variáveis; b) as tecnologias utilizadas que sustentam o processo de decisão automatizada (IA, *machine learning*, algoritmos, modelos de linguagem); c) os possíveis efeitos da tomada de decisão automatizada para o titular dos dados; d) linguagem clara e acessível evitando o termos técnicos ou termos complexos.

Logo, deve-se observar o princípio da explicabilidade, ou seja, os titulares devem ter acesso a explicações sobre como e porque a decisão automatizada foi tomada pelo controlador, incluindo informações sobre as fontes de dados/entradas, processos e/ou lógicas que levaram ao resultado, para que possam entender a saída, incluindo como tomam decisões, fazem previsões ou recomendações, garantindo que as decisões possam ser compreendidas e analisadas pelo titul**ar.**

23. Como equilibrar transparência e explicabilidade com segredos de negócios?

É imperioso afirmar, por primeiro, que nenhum dos princípios apresentados na legislação é absoluto ou mantém predominância sobre os demais, de sorte que a ponderação hermenêutica no caso concreto é, na maior parte das vezes, o melhor e mais adequado condutor para uma decisão assertiva e juridicamente adequada.

Com efeito, para viabilizar um equilíbrio da transparência e explicabilidade com segredos de negócios é essencial implementar sistemas robustos de registro das operações, combinados com mecanismos de versionamento de modelos e conjunto de dados, observando, também, regramentos internos previstos e em vigor dentro das corporações.

Estes controles técnicos devem ser complementados por uma estrutura de governança que inclui a instituição de uma comissão multidisciplinar para avaliação contínua das finalidades declaradas e realização de avaliações de impacto à proteção de dados (RIPD) e/ou avaliação de impacto algorítmico, antes da implementação de novos tratamentos, sempre que cabível (a exemplo, no caso de sistemas classificados como de alto risco).

De outro lado, vale ressaltar que o princípio da transparência, crucial para a observância às obrigações impostas pela LGPD, exige que os titulares tenham visibilidade adequada sobre o tratamento de seus dados pessoais.

ABRID
Associação Brasileira das Empresas de Tecnologia em Identificação Digital

Para evitar a falta de transparência com o tratamento de dados dos usuários de tais sistemas, os avisos de privacidade devem especificar claramente quais dados serão tratados, bem como conter previsão expressa de que tais dados serão usados para instrução algorítmica.

Esta transparência deve se estender também aos casos de compartilhamento entre empresas do mesmo grupo econômico, garantindo que o titular tenha ciência completa sobre a destinação de seus dados.

Reitero os protestos de elevada estima e consideração.

Atenciosamente,

ABRID ASSOCIACAO BRASILEIRA DAS EMPRESAS DE TECNO:09104543000123

Assinado de forma digital por ABRID ASSOCIACAO BRASILEIRA DAS EMPRESAS DE TECNO:09104543000123
Dados: 2026.01.09 21:12:30 -03'00'

CÉLIO DE SIQUEIRA RIBEIRO
Presidente Executivo

ANEXO XIV – Resposta ao ofício: ANBI

ANBI

À
Presidência do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD
Aos cuidados do
Conselheiro Rony Vainzof
Coordenador do GT5 – Proteção ao Crédito e Prevenção à Fraude

A Associação Nacional dos Bureaus de Informação – ANBI, entidade representativa do setor de bureaus de informação, proteção ao crédito e prevenção à fraude no Brasil, apresenta a presente manifestação institucional no âmbito do Grupo de Trabalho instituído pela Portaria CNPD nº 05/2025, dedicado ao estudo da Proteção ao Crédito e da Prevenção à Fraude mediante o uso de dados pessoais.

A ANBI reconhece a relevância singular deste Grupo de Trabalho, por se tratar da primeira iniciativa formal do Conselho Nacional de Proteção de Dados voltada especificamente à interpretação, ao alcance e à operacionalização da base legal da proteção ao crédito prevista na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). Trata-se de oportunidade institucional inédita para consolidar uma leitura técnica, econômica e jurídica coerente com a função sistêmica do crédito na economia brasileira e com a finalidade protetiva da própria LGPD.

Desde sua concepção legislativa, a base legal da proteção ao crédito prevista no art. 7º, inciso X, da LGPD foi desenhada como uma exceção funcional às limitações do tratamento de dados fundadas exclusivamente na execução de contrato. A experiência prática demonstrava que a restrição do tratamento de dados apenas ao momento contratual inviabilizava a própria existência do crédito responsável, pois o risco relevante surge antes da contratação, se prolonga durante a vigência da relação creditícia e somente se extingue com o adimplemento integral da obrigação.

Nesse contexto, registra-se que o subscritor desta manifestação, na qualidade de Diretor Jurídico da ANBI, atuou pessoalmente no processo legislativo que culminou na inclusão expressa da base legal da proteção ao crédito na LGPD, participando das discussões técnicas e das justificativas apresentadas ao Congresso Nacional. A fundamentação central para sua inclusão foi exatamente a constatação de que a execução de contrato, isoladamente, não seria base jurídica suficiente para sustentar o ecossistema de crédito, sobretudo diante da necessidade de proteger o crédito desde a fase de oferta, com destaque para o crédito consignado, até as etapas de monitoramento, prevenção à fraude, recuperação e cobrança.

A proteção ao crédito, portanto, jamais foi concebida como um evento pontual, mas sim como um processo contínuo, estruturado em ciclos de risco, cuja fragmentação normativa compromete tanto a segurança jurídica quanto a proteção efetiva do titular de dados. A interpretação restritiva dessa base legal não apenas fragiliza o sistema financeiro, como também expõe o próprio titular a riscos de superendividamento, fraude, usurpação de identidade e exclusão financeira.

Essa leitura funcional e sistêmica encontra paralelo claro no Direito Comparado. No âmbito do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), embora não exista uma base legal expressamente denominada "proteção ao crédito", o tratamento de dados para fins de avaliação de risco, prevenção à fraude e estabilidade financeira é amplamente admitido com fundamento no legítimo interesse (art. 6º, 1, "f"), na proteção de interesses vitais do sistema financeiro e em normas setoriais específicas, como as relacionadas à prevenção à lavagem de dinheiro e à fraude. A Autoridade Europeia de Proteção de Dados reconhece que a análise prévia de risco e a mitigação de fraude são condições essenciais para o funcionamento responsável do crédito.

Nos Estados Unidos, a California Consumer Privacy Act (CCPA) e sua evolução normativa (CPRA) também reconhecem expressamente a legitimidade do uso de dados pessoais para prevenção de fraudes, segurança, verificação de identidade e atividades compatíveis com a expectativa razoável do consumidor, inclusive no contexto financeiro e creditício. A legislação norte-americana parte do pressuposto de que a restrição excessiva ao uso de dados nesses contextos gera mais danos do que proteção, ao aumentar fraudes e reduzir a eficiência econômica.

O modelo brasileiro, ao optar por criar uma base legal autônoma de proteção ao crédito, foi além dessas experiências internacionais, oferecendo uma solução normativa mais clara, específica e adaptada à realidade nacional. Essa escolha legislativa não foi acidental, mas resultado direto do reconhecimento de que crédito e prevenção à fraude são atividades de interesse público, com impacto direto na estabilidade econômica, na inclusão financeira e na proteção do consumidor.

À luz desse contexto, a ANBI entende que a atuação do GT5 deve se orientar por uma interpretação teleológica, sistêmica e economicamente informada da LGPD, capaz de harmonizar proteção de dados pessoais, combate à fraude, segurança jurídica e desenvolvimento do mercado de crédito. Qualquer leitura que restrinja artificialmente a proteção ao crédito a fases isoladas do ciclo creditício contraria não apenas a lógica econômica, mas também a própria razão de ser da base legal introduzida no texto da LGPD.

Com essa premissa institucional, a ANBI apresenta, a seguir, suas respostas específicas aos quesitos formulados no ofício do GT5, colocando-se à disposição para

aprofundar tecnicamente os pontos tratados e contribuir de forma contínua com os trabalhos do Conselho Nacional de Proteção de Dados.

I. A IMPORTÂNCIA SOCIOECONÔMICA DO CRÉDITO E DA PREVENÇÃO À FRAUDE PARA O BRASIL

1. Qual é a relevância do crédito para o desenvolvimento socioeconômico do Brasil?

O crédito constitui um instrumento estruturante do desenvolvimento econômico e social brasileiro, sendo condição indispensável para o funcionamento do mercado de consumo, do investimento produtivo, do empreendedorismo e da inclusão financeira. Em economias marcadas por elevada desigualdade de renda e restrições históricas de acesso a capital, como a brasileira, o crédito assume papel ainda mais relevante ao viabilizar a antecipação de consumo essencial, o financiamento da atividade empresarial e a mitigação de choques econômicos individuais e familiares.

Sob a ótica macroeconômica, a relevância do crédito é expressiva e mensurável. Dados do Banco Central do Brasil indicam que o saldo total das operações de crédito do Sistema Financeiro Nacional ultrapassou R$ 6,4 trilhões em 2024, com crescimento anual superior a 10%, abrangendo crédito às famílias e às empresas (Banco Central do Brasil, Estatísticas Monetárias e de Crédito, 2024). O estoque de crédito no Brasil corresponde atualmente a aproximadamente 54% do Produto Interno Bruto, enquanto o crédito às famílias representa cerca de 35% do PIB, evidenciando a centralidade do crédito na dinâmica econômica nacional (Banco Central do Brasil, Relatório de Economia Bancária, 2024).

A ausência de crédito, ou sua concessão de forma desestruturada e temerária, produz efeitos adversos relevantes, como retração do consumo, aumento da informalidade econômica, elevação estrutural das taxas de juros e exclusão financeira de parcelas significativas da população. Esses efeitos atingem de forma mais intensa as camadas C e D, para as quais o crédito formal frequentemente representa a única alternativa viável para acesso a bens duráveis, educação, saúde, reorganização financeira e até mesmo subsistência em momentos de instabilidade econômica.

Do ponto de vista jurídico-regulatório, o crédito não pode ser compreendido apenas como uma relação contratual privada entre partes isoladas. Trata-se de atividade de inequívoco interesse público, cuja estabilidade afeta diretamente o sistema financeiro, o equilíbrio macroeconômico e a proteção do próprio consumidor. Essa compreensão está presente em diversos ordenamentos estrangeiros e foi expressamente incorporada pelo

legislador brasileiro ao prever, na Lei Geral de Proteção de Dados Pessoais, uma base legal específica para a proteção do crédito (art. 7º, X), reconhecendo sua natureza sistêmica, contínua e estrutural.

A proteção ao crédito manifesta-se ao longo de todo o ciclo da relação creditícia, que se inicia antes da contratação, na fase de análise e oferta responsável de crédito, passa pela concessão e acompanhamento da operação e se estende até a recuperação ou liquidação da obrigação. A oferta de crédito, inclusive por meio de comunicações direcionadas, crédito pré-aprovado e outros instrumentos informativos, quando baseada em análise técnica adequada, não constitui prática abusiva ou meramente mercadológica, mas sim instrumento legítimo de proteção do crédito e do titular, pois permite apresentar produtos compatíveis com a capacidade financeira do consumidor, com melhores condições de taxa, prazo e previsibilidade.

Nesse contexto, instrumentos como o Cadastro Positivo exercem papel relevante ao reduzir assimetrias informacionais e permitir que o histórico de bom pagador seja considerado na análise de risco, beneficiando diretamente os titulares com redução do custo do crédito e ampliação do acesso a condições mais favoráveis (Banco Central do Brasil, Relatório de Economia Bancária, 2023). Esses mecanismos são particularmente relevantes para consumidores historicamente excluídos do sistema financeiro formal, contribuindo para inclusão financeira e estabilidade econômica.

Essa lógica é coerente com a Lei nº 14.181/2021 (Lei do Superendividamento), que parte do pressuposto de que o crédito deve ser ofertado de forma responsável, com informação adequada, análise prévia de risco e orientação financeira, justamente para evitar o endividamento excessivo e proteger o consumidor. Não há combate efetivo ao superendividamento sem sistemas de crédito capazes de avaliar dados, estruturar ofertas compatíveis e acompanhar a relação creditícia ao longo do tempo.

É importante destacar que não se defende o uso indiscriminado ou desproporcional de dados pessoais, mas sim seu uso responsável, proporcional e aderente à realidade econômica e social do país, em conformidade com os princípios da LGPD. Uma interpretação excessivamente restritiva da base legal da proteção ao crédito, ao limitar indevidamente o tratamento de dados necessários à análise, à oferta e à proteção do crédito, tende a produzir efeitos contrários aos pretendidos: aumento do risco sistêmico, elevação das taxas de juros, retração da oferta de crédito e maior exclusão financeira.

Esses efeitos recaem, de forma direta, sobre os próprios titulares de dados, que passam a ter menos acesso ao crédito ou acesso mais caro e restrito, com menor

possibilidade de reorganização financeira, consolidação de dívidas e melhoria de sua condição econômica. Assim, a restrição excessiva não protege o titular; ao contrário, agrava sua vulnerabilidade econômica, especialmente entre as camadas C e D da população.

Dessa forma, a relevância socioeconômica do crédito no Brasil exige um ambiente regulatório que harmonize a proteção de dados pessoais com a segurança jurídica, a eficiência econômica e a inclusão financeira, reconhecendo o crédito como um processo contínuo, de interesse público, voltado à estabilidade do sistema, à proteção do consumidor e ao desenvolvimento sustentável do país.

Diante desse cenário, a proteção ao crédito deve ser compreendida como política estrutural de desenvolvimento econômico e social, e não como atividade acessória ou meramente privada. A interpretação da LGPD nesse contexto deve preservar a funcionalidade do crédito ao longo de todo o seu ciclo, garantindo segurança jurídica, eficiência econômica e proteção efetiva do titular. Leituras excessivamente restritivas da base legal da proteção ao crédito tendem a produzir efeitos contrários aos objetivos da própria lei, ao restringir o acesso ao crédito, elevar seu custo e aprofundar desigualdades, com impactos negativos não apenas para o mercado, mas para a sociedade brasileira como um todo.

2. Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

A prevenção à fraude é componente indissociável da proteção ao crédito e da própria estabilidade do sistema econômico. O crescimento contínuo das fraudes financeiras, digitais e identitárias no Brasil gera impactos sistêmicos profundos, que extrapolam a relação individual entre credor e devedor e afetam diretamente consumidores, empresas, o sistema financeiro e o Estado.

Dados setoriais indicam a magnitude do problema. Segundo a Federação Brasileira de Bancos, as tentativas de fraudes bancárias no Brasil ultrapassaram R$ 40 bilhões por ano, considerando fraudes evitadas e consumadas, com crescimento relevante impulsionado pela digitalização dos serviços financeiros (FEBRABAN, Relatório de Tecnologia Bancária, 2023). No mesmo sentido, estudos de mercado apontam que o Brasil figura de forma recorrente entre os países com maior incidência de fraudes digitais e golpes financeiros, especialmente envolvendo uso indevido de dados pessoais e engenharia social (Serasa Experian, Indicador de Tentativas de Fraude, 2023).

Esses custos não permanecem restritos às instituições financeiras. As perdas decorrentes de fraudes são internalizadas nos modelos de risco, refletindo-se diretamente no aumento do custo do crédito, em critérios mais restritivos de concessão e na exclusão de perfis considerados mais vulneráveis. O efeito prático é a elevação das taxas de juros, a redução da oferta de crédito formal e o fortalecimento de alternativas informais e mais arriscadas de financiamento, com impactos negativos para a economia e para a inclusão financeira.

A prevenção à fraude atua, portanto, ao longo de todo o ciclo do crédito, desde a fase prévia de identificação e validação do titular, passando pela oferta e concessão responsável, pelo monitoramento da operação, até a fase de recuperação do crédito. A ausência de mecanismos eficazes de prevenção compromete todas essas etapas, elevando o risco sistêmico e tornando o crédito mais caro e menos acessível.

Do ponto de vista do titular de dados, a prevenção à fraude representa forma concreta de proteção de direitos fundamentais, especialmente da identidade, do patrimônio e da dignidade econômica. Fraudes não afetam apenas instituições financeiras; afetam diretamente indivíduos que se veem endividados por operações que não realizaram, têm seus nomes negativados injustamente, enfrentam restrições de crédito e percorrem longos e complexos processos para recomposição de sua situação financeira. Esses efeitos são particularmente graves para consumidores das classes C e D, que dispõem de menor capacidade de absorver choques financeiros e menores recursos para defesa administrativa ou judicial.

Além disso, a recorrência de fraudes compromete a confiança no ecossistema digital e financeiro, elemento essencial para a modernização da economia, a inovação e a ampliação de serviços digitais. Ambientes nos quais a fraude é elevada e mal controlada afastam investimentos, desestimulam a adoção de novas tecnologias e frequentemente levam a respostas regulatórias mais rígidas, que podem gerar efeitos colaterais indesejados sobre eficiência econômica e direitos individuais.

No plano internacional, tanto o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) quanto legislações como a California Consumer Privacy Act (CCPA) reconhecem expressamente a prevenção à fraude e a segurança como finalidades legítimas e necessárias do tratamento de dados pessoais, partindo da premissa de que a subutilização desses dados tende a gerar mais danos do que benefício, ao ampliar riscos sistêmicos e prejuízos aos próprios titulares.

O ordenamento jurídico brasileiro adotou posição ainda mais clara ao reconhecer, por meio da LGPD, uma base legal específica para a proteção ao crédito, justamente porque compreendeu que crédito e fraude são fenômenos estruturalmente conectados. A prevenção à fraude não é atividade acessória ou excepcional, mas elemento essencial para o funcionamento responsável do mercado de crédito, para a redução do custo financeiro e para a proteção do consumidor.

É importante destacar que não se defende o uso indiscriminado de dados pessoais, mas sim seu tratamento responsável, proporcional e aderente às finalidades de proteção do crédito e prevenção à fraude, em conformidade com os princípios da LGPD. Uma interpretação excessivamente restritiva dessas finalidades tende a produzir efeitos contraproducentes: aumento do risco, elevação das taxas, retração da oferta de crédito e maior vulnerabilidade dos próprios titulares.

Portanto, a prevenção à fraude deve ser compreendida como atividade essencial de interesse público, indispensável ao desenvolvimento econômico sustentável, à estabilidade financeira, à inclusão social e à proteção efetiva dos consumidores brasileiros ao longo de todo o ciclo do crédito.

Assim, a prevenção à fraude deve ser reconhecida como atividade essencial de interesse público e econômico, indissociável da proteção ao crédito e da estabilidade do sistema financeiro. Fragilizar os mecanismos antifraude por meio de interpretações restritivas do tratamento de dados não reduz riscos, mas os transfere para consumidores legítimos, eleva custos e compromete a confiança no mercado. A proteção efetiva do titular exige, necessariamente, um ambiente capaz de prevenir ilícitos de forma eficiente, proporcional e tecnicamente adequada.

II. O PAPEL DOS DADOS PESSOAIS NO ECOSSISTEMA DE CRÉDITO

3. Qual a importância dos dados pessoais para a proteção do crédito e demais atividades relacionadas ao tema?

Os dados pessoais constituem o insumo técnico central do ecossistema de crédito, sendo indispensáveis para a avaliação de risco, para a concessão responsável e para a proteção do próprio titular de dados. Em um mercado de crédito de grande escala e elevada complexidade como o brasileiro, o tratamento estruturado de dados é condição necessária para substituir decisões arbitrárias ou puramente intuitivas por análises técnicas, previsíveis e auditáveis. Sem o uso adequado desses dados, o crédito se aproxima de um

exercício de especulação, incompatível com a segurança jurídica, a estabilidade financeira e a efetiva proteção do consumidor.

A proteção ao crédito pressupõe, de forma concreta, a capacidade de identificar corretamente o titular, compreender sua situação econômico-financeira, verificar sua elegibilidade para diferentes modalidades de crédito, estruturar ofertas compatíveis com sua capacidade de pagamento e acompanhar o cumprimento das obrigações assumidas ao longo do tempo. Essas atividades exigem o tratamento organizado de dados pessoais cadastrais, financeiros e comportamentais e, em determinados contextos de maior risco, dados biométricos, sempre em observância aos princípios da finalidade, adequação, necessidade, segurança e prevenção previstos na Lei Geral de Proteção de Dados Pessoais.

Essa lógica se aplica a todo o ciclo do crédito, incluindo a fase pré-contratual de análise e oferta responsável, a concessão propriamente dita, o monitoramento da operação, a prevenção à fraude e a eventual recuperação do crédito. A oferta de crédito, inclusive por meio de mecanismos como crédito pré-aprovado e comunicações direcionadas, quando baseada em dados adequados e análise técnica, constitui instrumento legítimo de proteção ao crédito e ao titular, pois permite reduzir assimetrias informacionais, apresentar produtos mais adequados e contribuir para a redução do custo financeiro.

A experiência brasileira demonstra que a restrição indevida ao uso de dados pessoais no crédito não reduz riscos, mas os redistribui de forma assimétrica e socialmente regressiva. Quando instituições passam a operar com menor qualidade informacional, os modelos de risco tendem a se tornar mais conservadores, elevando taxas de juros, reduzindo prazos, exigindo garantias adicionais e excluindo perfis considerados mais vulneráveis. O resultado prático é a diminuição do acesso ao crédito formal, especialmente para consumidores das classes C e D, e o fortalecimento de alternativas informais de financiamento, geralmente mais onerosas e menos protegidas juridicamente (Banco Central do Brasil, Relatório de Economia Bancária).

Instrumentos como o Cadastro Positivo evidenciam a importância dos dados pessoais para a eficiência do mercado de crédito. Ao permitir que o histórico de adimplemento seja considerado, o Cadastro Positivo contribui para a redução de assimetrias informacionais e para a oferta de crédito em condições mais favoráveis aos bons pagadores, com impacto direto na redução do custo do crédito e na ampliação da inclusão financeira (Banco Central do Brasil, Relatório de Economia Bancária; Lei nº 12.414/2011). Esse efeito é particularmente relevante para consumidores que, sem dados estruturados, seriam tratados de forma indistinta e penalizados com condições mais gravosas.

Do ponto de vista normativo, a LGPD reconheceu expressamente essa realidade ao prever, no art. 7º, inciso X, a base legal da proteção ao crédito, afastando a exigência de consentimento e superando as limitações inerentes à execução de contrato. Essa opção legislativa foi essencial para garantir que o tratamento de dados pudesse ocorrer antes da contratação, durante a relação creditícia e após o seu término, enquanto subsistirem riscos legítimos associados ao crédito concedido. Trata-se de reconhecimento explícito de que a proteção ao crédito é um processo contínuo e não um evento pontual.

No direito comparado, observa-se lógica convergente. O Regulamento Geral de Proteção de Dados da União Europeia (GDPR) admite amplamente o tratamento de dados pessoais para avaliação de risco, segurança e proteção do sistema financeiro com base no legítimo interesse, reconhecendo que a qualidade e a disponibilidade de dados são condições para a justiça e a eficiência do crédito. Nos Estados Unidos, a California Consumer Privacy Act (CCPA) e legislações setoriais financeiras partem do pressuposto de que o uso de dados para fins de crédito, segurança e prevenção à fraude é compatível com a expectativa razoável do consumidor, desde que observado o princípio da proporcionalidade.

É importante ressaltar que não se defende o uso indiscriminado de dados pessoais, mas sim seu tratamento responsável, proporcional e aderente às finalidades legítimas de proteção do crédito, prevenção à fraude e inclusão financeira. Interpretações excessivamente restritivas tendem a produzir efeitos contraproducentes, como aumento do risco sistêmico, elevação das taxas de juros e exclusão financeira, atingindo diretamente os próprios titulares de dados que a regulação busca proteger.

Assim, os dados pessoais não são um elemento acessório, mas o alicerce técnico da proteção ao crédito, sem o qual não há concessão responsável, prevenção eficaz à fraude, redução do custo financeiro nem inclusão financeira sustentável ao longo de todo o ciclo do crédito.

Dessa forma, os dados pessoais devem ser compreendidos como o alicerce técnico da proteção ao crédito, sem o qual não há concessão responsável, prevenção à fraude nem inclusão financeira sustentável. A opção do legislador ao criar uma base legal específica na LGPD reflete o reconhecimento de que a proteção de dados não pode ser dissociada da realidade econômica do crédito. Restringir indevidamente o uso responsável desses dados compromete a eficiência do sistema e prejudica diretamente os próprios titulares, que passam a enfrentar crédito mais caro, mais escasso e menos adequado ao seu perfil.

4. Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?

A assimetria informacional é um dos principais fatores estruturais de ineficiência nos mercados de crédito. Quando o credor dispõe de informações limitadas ou imprecisas sobre a capacidade de pagamento, o histórico financeiro ou a identidade real do solicitante, o risco passa a ser precificado de forma genérica e conservadora, resultando em custos mais elevados, menor oferta de crédito e restrições de acesso, especialmente para perfis considerados mais vulneráveis.

O uso estruturado e responsável de dados pessoais permite reduzir significativamente essas assimetrias, tornando a análise de risco mais precisa, individualizada e aderente à realidade econômica do tomador. Esse efeito é central para a liquidez do mercado de crédito, pois aumenta a previsibilidade de retorno das operações, reduz a necessidade de provisões excessivas e amplia a disposição das instituições em conceder crédito, movimentando a economia como um todo.

Os impactos dessa lógica não se limitam às pessoas físicas. Empresas, especialmente micro, pequenas e médias, dependem de crédito para capital de giro, investimento, expansão de atividades e manutenção de empregos. A qualidade das informações utilizadas na análise de risco influencia diretamente o acesso dessas empresas ao crédito formal. Ambientes com alta assimetria informacional tendem a restringir financiamento produtivo, reduzir investimentos e comprometer a geração de empregos, com efeitos negativos sobre o desenvolvimento econômico nacional.

No plano da inadimplência, modelos de crédito baseados em dados de qualidade permitem identificar padrões de risco, evitar concessões temerárias e direcionar produtos compatíveis com o perfil econômico do tomador. O crédito consignado é exemplo emblemático dessa lógica, ao utilizar dados confiáveis de renda e margem consignável para reduzir substancialmente o risco de inadimplemento, ao mesmo tempo em que amplia o acesso ao crédito com taxas estruturalmente mais baixas. O mesmo raciocínio se aplica a modalidades como crédito pré-aprovado e produtos baseados no Cadastro Positivo, que beneficiam bons pagadores e reduzem o custo financeiro.

Sob a ótica da eficiência de mercado, a adequada utilização de dados pessoais promove alocação mais racional do capital, reduz subsídios cruzados indevidos e evita que consumidores e empresas de baixo risco financiem, de forma indireta, operações de alto risco mal avaliadas. Isso gera benefícios sistêmicos relevantes, como maior concorrência,

inovação em produtos financeiros, expansão do crédito produtivo e redução estrutural do custo do crédito, com impacto positivo para toda a economia.

É importante reconhecer que o crédito não constitui um direito subjetivo do consumidor, mas sim uma liberalidade do concedente. Ainda assim, é indubitável que o crédito desempenha papel essencial no desenvolvimento social individual e coletivo. O acesso a crédito em condições justas é fator determinante para inclusão financeira, mobilidade social, estímulo ao empreendedorismo e dinamização da economia. Para as camadas C e D, em particular, o crédito estruturado e responsável frequentemente representa a diferença entre integração ao sistema formal e dependência de soluções informais mais caras e arriscadas.

A subutilização ou restrição indevida do uso de dados pessoais produz efeitos adversos relevantes. A ausência de informações suficientes leva ao endurecimento generalizado das políticas de crédito, ao aumento de exigências garantidoras, à elevação de taxas e à exclusão de perfis que poderiam ser atendidos de forma segura. Em termos sistêmicos, isso enfraquece a liquidez do mercado, amplia a inadimplência estrutural e reduz o impacto positivo do crédito sobre o crescimento econômico.

Por essa razão, legislações internacionais e organismos reguladores reconhecem que a proteção de dados pessoais não pode ser dissociada da eficiência econômica, devendo ser interpretada de forma a permitir o uso responsável, proporcional e tecnicamente necessário dos dados em modelos de risco. A Lei Geral de Proteção de Dados Pessoais, ao criar uma base legal específica para a proteção ao crédito, alinhou-se a essa compreensão, oferecendo um arcabouço normativo apto a reduzir assimetrias informacionais sem sacrificar os direitos dos titulares.

Uma interpretação excessivamente restritiva dessa base legal, ao comprometer a utilização de dados essenciais à análise de risco, pode produzir efeitos econômicos severos, com aumento do custo do crédito, retração do financiamento produtivo, redução de investimentos e prejuízos diretos aos próprios titulares de dados e ao desenvolvimento do país como um todo.

Conclui-se, portanto, que a redução de assimetrias informacionais por meio do uso responsável de dados pessoais é condição indispensável para a liquidez, a eficiência e a sustentabilidade do mercado de crédito. Embora o crédito não constitua um direito subjetivo, ele é instrumento essencial de desenvolvimento individual e coletivo. Interpretações que inviabilizem análises técnicas adequadas tendem a gerar efeitos

macroeconômicos severos, como retração do crédito produtivo, aumento de taxas e redução de investimentos, com prejuízos diretos para consumidores, empresas e para o país.

III. O PAPEL DOS DADOS PESSOAIS NA PREVENÇÃO À FRAUDE E A OUTROS ILÍCITOS

5. Qual a importância dos dados pessoais para a prevenção à fraude, a outros ilícitos e às demais atividades relacionadas?

Os dados pessoais são elemento estruturante e indispensável para a prevenção à fraude, a outros ilícitos e para a segurança das relações econômicas contemporâneas. Em um ambiente de contratação massivamente digital, a fraude moderna é, em grande medida, uma fraude de identidade, de comportamento ou de engenharia social. Por isso, sem correta identificação e validação do titular, não há contratação segura, não há crédito legítimo e não há proteção jurídica mínima do mercado. A prevenção à fraude é, portanto, condição prévia para a própria existência de relações contratuais válidas e para a integridade do crédito.

A prevenção eficaz de ilícitos exige capacidade de detectar inconsistências cadastrais, indícios de falsidade ideológica, uso indevido de dados de terceiros, simulação de perfis e manipulações destinadas a induzir o concedente ao erro. Esses riscos não podem ser mitigados adequadamente sem tratamento de dados pessoais, pois a lógica antifraude depende de comparar, correlacionar e validar informações para distinguir operações legítimas de tentativas de fraude. A subutilização desses dados, ou a eliminação indevida de instrumentos de validação, torna o sistema operacionalmente "cego" para o risco e amplia tanto perdas quanto danos aos próprios titulares.

O legislador brasileiro reconheceu a centralidade dessa atividade ao desenhar, na LGPD, um regime que não trata prevenção à fraude como exceção marginal, mas como finalidade legítima de alta relevância social e econômica. A própria disciplina de dados pessoais sensíveis demonstra essa opção: o art. 11 prevê hipóteses legais de tratamento sem consentimento quando necessário para finalidades legítimas, e o sistema normativo da LGPD permite, na prática, que operações de proteção ao crédito e prevenção a fraudes sejam realizadas sem autorização do titular quando preenchidos os requisitos legais e respeitados os princípios de finalidade, necessidade, adequação, segurança, prevenção e responsabilização. Isso ocorre porque, no mundo real, exigir consentimento como regra para mecanismos antifraude inviabilizaria a proteção efetiva do titular e a própria segurança do mercado.

Essa estrutura não existe para favorecer o agente econômico em detrimento do consumidor; ao contrário, ela protege simultaneamente o titular, o concedente e o ambiente econômico. O titular é protegido contra usurpação de identidade, contratações indevidas, endividamento fraudulento e negativação injusta, que frequentemente geram longa "dor de cabeça" para regularização e recomposição da vida financeira. O concedente é protegido contra perdas e inadimplência fraudulenta. E o mercado é protegido porque, se o crédito não é pago ou recuperado, ele não retorna ao circuito econômico nas mesmas condições, tornando-se mais caro e mais restrito, já que o risco passa a ser precificado e repassado aos consumidores legítimos.

Em termos macroeconômicos, fraudes elevadas degradam a confiança, aumentam custos operacionais, ampliam provisões e tendem a reduzir a oferta de crédito ou elevar seu custo. Isso afeta de modo especialmente severo os consumidores das camadas C e D e também empresas, sobretudo as menores, que dependem de crédito para capital de giro e geração de empregos. Assim, uma interpretação excessivamente restritiva que impeça ou fragilize o tratamento de dados indispensável à prevenção à fraude não apenas prejudica o mercado, mas prejudica diretamente os próprios titulares, que passam a enfrentar maior exposição a golpes e, ao mesmo tempo, menor acesso ao crédito ou crédito mais caro.

No direito comparado, regimes como o GDPR e a CCPA também reconhecem a prevenção à fraude e a segurança como finalidades legítimas e essenciais, justamente porque a restrição desproporcional a esses mecanismos tende a aumentar danos reais ao consumidor e instabilidade econômica. A conclusão é objetiva: a prevenção à fraude não é um "uso tolerado" de dados pessoais, mas atividade essencial de interesse público e econômico, indispensável para a proteção da identidade do titular, para a segurança jurídica das contratações e para a sustentabilidade do ecossistema de crédito ao longo de todo o seu ciclo.

Em síntese, a prevenção à fraude depende necessariamente do tratamento adequado de dados pessoais e constitui condição básica para a validade das relações contratuais e para a segurança do crédito. O regime jurídico da LGPD reconhece essa realidade ao permitir o tratamento de dados, inclusive sensíveis, quando indispensável para a proteção do crédito e a prevenção de ilícitos. Interpretar essas hipóteses de forma excessivamente restritiva não fortalece a proteção do titular; ao contrário, amplia sua exposição a fraudes, encarece o crédito e compromete a sustentabilidade de todo o ecossistema econômico.

6. Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e a mitigação de fraudes, golpes e outros ilícitos?

A sofisticação crescente das fraudes financeiras exige instrumentos igualmente avançados de detecção e mitigação de riscos. Nesse contexto, dados comportamentais, biométricos e metadados exercem papel central, pois permitem verificar não apenas quem é o titular que pretende contratar, mas se o comportamento apresentado é compatível com sua identidade declarada, com seu histórico conhecido e com o padrão esperado para aquela operação de crédito.

Os dados comportamentais são fundamentais para a identificação de fraudes financeiras modernas, que raramente se apresentam de forma explícita. Desvios relevantes em padrões de navegação, horários de acesso, frequência de tentativas, tipo de dispositivo, localização aproximada, velocidade de interação e sequência de ações são amplamente utilizados para detectar fraudes automatizadas, contas sintéticas e golpes baseados em engenharia social. Sem o monitoramento de perfil comportamental, torna-se impossível distinguir operações legítimas de transações fraudulentas sofisticadas.

Os metadados complementam essa análise ao fornecer contexto técnico essencial, como origem de conexões, recorrência de eventos suspeitos, correlação entre operações aparentemente isoladas e identificação de tentativas coordenadas de fraude. Esses elementos são indispensáveis para análises antifraude em escala, especialmente no crédito digital, no qual a contratação ocorre de forma remota e instantânea.

Os dados biométricos, em especial a biometria facial, representam atualmente um dos meios mais eficazes de combate à fraude de identidade em ambientes de alto risco, como abertura de contas, concessão de crédito remoto, validação de operações sensíveis e recuperação de crédito. A biometria facial permite verificar a presença real do titular, reduzir drasticamente fraudes por uso de documentos furtados ou dados vazados e proteger tanto o consumidor quanto o concedente de crédito. Seu uso não substitui outros mecanismos, mas atua de forma complementar, reduzindo falsos positivos e falsos negativos nos modelos de risco.

A importância do monitoramento de perfil e do uso desses dados é reconhecida pelo próprio Poder Judiciário brasileiro. Em diversos casos envolvendo fraudes em cartões, transferências e operações atípicas, os tribunais têm entendido que a ausência de bloqueio ou de mecanismos de detecção de transações fora do padrão caracteriza falha na prestação do serviço, por se tratar de risco inerente à atividade financeira. Esse entendimento pressupõe, de forma implícita, que o fornecedor dispõe, e deve dispor, de mecanismos de

análise comportamental e contextual para identificar operações suspeitas. Sem dados comportamentais e biométricos, esse dever se torna inexequível.

No plano normativo, a LGPD reconhece expressamente a sensibilidade desses dados, impondo requisitos reforçados de segurança, governança e accountability, especialmente para dados biométricos (art. 11). Contudo, não há proibição absoluta ao seu uso. Ao contrário, o legislador admitiu seu tratamento quando estritamente necessário para finalidades legítimas, como a prevenção à fraude e a proteção do crédito, justamente por reconhecer que essas atividades envolvem segurança econômica e proteção do próprio titular.

No direito comparado, essa compreensão é amplamente consolidada. O GDPR admite o uso de dados biométricos para fins de segurança e prevenção à fraude quando necessário e proporcional, sendo prática corrente em sistemas financeiros europeus o uso de biometria facial para onboarding digital e validação de identidade, inclusive sob supervisão das autoridades de proteção de dados. Países como Reino Unido, Espanha e Alemanha utilizam biometria facial em processos de verificação remota de identidade no setor financeiro, com base em orientações da European Banking Authority (EBA) e autoridades nacionais de proteção de dados.

Nos Estados Unidos, sob a CCPA e normas setoriais financeiras, o uso de biometria e dados comportamentais para prevenção à fraude e segurança é amplamente admitido, sendo prática comum em bancos, fintechs e bureaus de crédito, desde que observados limites claros de finalidade, retenção e segurança. Em todos esses ordenamentos, parte-se do reconhecimento de que fraudes financeiras não podem ser combatidas com instrumentos analógicos em um ambiente digital.

É importante enfatizar que estamos tratando exclusivamente de uso de dados no contexto de crédito e prevenção à fraude, e não de monitoramento de comportamento social genérico ou desvinculado de risco econômico. O tratamento desses dados tem finalidade específica, legítima e delimitada, vinculada à proteção da identidade do titular, à validade das contratações e à sustentabilidade do mercado de crédito.

Diante desse cenário, dados comportamentais, biométricos e metadados devem ser compreendidos como instrumentos essenciais de proteção do crédito e de prevenção à fraude, e não como exceções toleradas pelo sistema jurídico. Fragilizar ou restringir indevidamente seu uso, especialmente da biometria facial, compromete a capacidade de identificar riscos, amplia fraudes de identidade, eleva custos operacionais e encarece o crédito para consumidores legítimos. A interpretação da LGPD deve preservar a

possibilidade de uso responsável, proporcional e tecnicamente necessário desses dados, sob pena de expor o titular a maiores riscos e comprometer a estabilidade de todo o ecossistema de crédito.

7. Quais são os riscos de subutilizar dados pessoais em processos antifraude?

A subutilização de dados pessoais em processos antifraude gera riscos sistêmicos relevantes, que afetam simultaneamente os titulares de dados, os agentes econômicos e a estabilidade do mercado de crédito. A ausência ou limitação excessiva de informações compromete a capacidade de identificar fraudes cada vez mais sofisticadas, reduz a efetividade dos mecanismos de prevenção e amplia a incidência de golpes bem-sucedidos, com impactos econômicos e sociais significativos.

Um dos efeitos mais imediatos da subutilização de dados é o aumento de fraudes de identidade, chargebacks, fraudes sintéticas e falsidade ideológica, fenômenos que prosperam justamente em ambientes com lacunas informacionais. Modelos antifraude que operam com dados insuficientes tendem a apresentar dois comportamentos igualmente nocivos: tornam-se excessivamente permissivos, permitindo a concretização de fraudes relevantes, ou excessivamente restritivos, bloqueando operações legítimas e excluindo usuários idôneos do sistema financeiro formal.

Para o titular de dados, a subutilização representa um paradoxo regulatório. Em vez de protegê-lo, a restrição excessiva ao uso responsável de dados amplia sua exposição a fraudes, dificulta a identificação tempestiva de ilícitos e prolonga os efeitos negativos decorrentes de golpes, como endividamento indevido, negativação injusta, restrição de crédito e longos processos administrativos ou judiciais para recomposição da situação financeira. Esses impactos são especialmente severos para consumidores das camadas C e D, que dispõem de menor capacidade de absorver prejuízos e menor acesso a mecanismos eficazes de reparação.

Do ponto de vista do concedente de crédito, a subutilização de dados eleva perdas operacionais, amplia custos de recuperação e exige provisões mais conservadoras. Esses custos não permanecem isolados, sendo inevitavelmente repassados ao mercado, na forma de aumento de taxas de juros, redução de prazos, maior seletividade na concessão e retração da oferta de crédito. O resultado é um sistema menos eficiente, mais caro e menos inclusivo.

No plano macroeconômico, esses efeitos se traduzem em redução da liquidez do mercado de crédito, enfraquecimento do financiamento produtivo, impacto negativo sobre

empresas, especialmente micro, pequenas e médias, e prejuízos à geração de empregos. Instituições passam a operar com margens de segurança artificialmente elevadas, penalizando consumidores e empresas de baixo risco para compensar fraudes que poderiam ser mitigadas com melhor uso de dados.

Além disso, a subutilização de dados pessoais dificulta o cumprimento do próprio dever de diligência esperado dos agentes econômicos. O Poder Judiciário brasileiro, ao analisar casos de fraudes financeiras, tem reconhecido reiteradamente que a identificação e o bloqueio de operações atípicas integram o risco da atividade, pressupondo a existência de mecanismos eficazes de monitoramento de perfil e comportamento. A restrição injustificada desses instrumentos coloca o fornecedor em situação de maior exposição jurídica, ao mesmo tempo em que fragiliza a proteção do consumidor.

No direito comparado, observa-se convergência no reconhecimento de que a proteção de dados não deve operar em oposição à prevenção à fraude. O GDPR, a CCPA e normas setoriais financeiras partem da premissa de que a subutilização de dados em contextos antifraude aumenta riscos sistêmicos e danos aos próprios titulares, exigindo interpretações equilibradas que permitam o uso responsável, proporcional e tecnicamente necessário dos dados pessoais.

Dessa forma, a subutilização de dados pessoais em processos antifraude não representa ganho real de proteção ao titular, mas sim fragilização do sistema, aumento de riscos e encarecimento do crédito. A LGPD, ao reconhecer a proteção ao crédito e a prevenção a ilícitos como finalidades legítimas, oferece um arcabouço normativo apto a evitar esse desequilíbrio, desde que interpretado de forma técnica, sistêmica e alinhada à realidade econômica. Restringir indevidamente o uso responsável de dados compromete a efetividade da prevenção à fraude, prejudica consumidores legítimos e afeta negativamente a estabilidade do mercado de crédito como um todo.

IV. CONVERGÊNCIA ENTRE PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

8. O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?

No modelo contemporâneo de gestão de risco, a proteção ao crédito e a prevenção à fraude constituem dimensões indissociáveis de um mesmo ecossistema operacional, estruturado para garantir não apenas a segurança do mercado financeiro, mas também a proteção econômica do titular de dados e a estabilidade das relações contratuais. Ambas as atividades compartilham os mesmos fluxos informacionais, tecnologias, bases de

dados e mecanismos analíticos, orientados à concessão responsável, à mitigação de riscos e à preservação do equilíbrio econômico do sistema.

A análise de crédito moderna não se limita à verificação estática de capacidade de pagamento. Ela incorpora, de forma integrada, validação de identidade, confirmação e atualização de informações cadastrais, análise de comportamento, monitoramento de padrões de uso e detecção de inconsistências — elementos tradicionalmente associados à prevenção à fraude. Da mesma forma, os sistemas antifraude dependem de dados financeiros, históricos de adimplemento, padrões de relacionamento creditício e contexto econômico para diferenciar operações legítimas de práticas ilícitas. Na prática, trata-se do mesmo conjunto de dados e do mesmo modelo de risco, aplicado a finalidades complementares.

Essa convergência se manifesta de forma clara ao longo de todo o ciclo do crédito, desde a fase pré-contratual de análise e oferta responsável, passando pela concessão, acompanhamento da operação, prevenção de ilícitos e eventual recuperação do crédito. Não é tecnicamente possível separar, de forma estanque, o risco de inadimplência do risco de fraude, pois ambos impactam diretamente a viabilidade econômica da operação e a proteção do titular.

A integração entre crédito e antifraude é especialmente relevante no contexto da oferta responsável de crédito, incluindo modalidades como crédito consignado, crédito pré-aprovado e produtos baseados em análise prévia de risco. O tratamento adequado de dados pessoais nessas etapas permite estruturar ofertas compatíveis com o perfil econômico do consumidor, reduzir taxas de juros, ajustar prazos e aumentar a previsibilidade do pagamento. Esse processo beneficia diretamente o titular, ao evitar concessões inadequadas e reduzir o custo financeiro, e protege o concedente ao mitigar riscos operacionais.

O Cadastro Positivo é exemplo emblemático dessa lógica integrada. Ao permitir que o histórico de bom pagador seja considerado, ele reduz assimetrias informacionais, amplia o acesso ao crédito em condições mais favoráveis e incentiva comportamentos financeiros responsáveis. Esse mecanismo só é viável porque existe tratamento contínuo de dados pessoais ao longo de todo o ciclo do crédito, reforçando a convergência estrutural entre proteção ao crédito e prevenção à fraude.

Essa abordagem também está alinhada às políticas públicas de combate ao superendividamento. A Lei nº 14.181/2021 pressupõe a existência de sistemas capazes de analisar dados, orientar a oferta de produtos financeiros, monitorar a capacidade de pagamento e evitar concessões incompatíveis com a realidade econômica do consumidor.

Não há combate efetivo ao superendividamento sem modelos de crédito baseados em dados e integrados a mecanismos de prevenção de ilícitos.

No plano internacional, essa convergência é amplamente reconhecida. Tanto o GDPR quanto a CCPA partem da premissa de que avaliação de risco, segurança, integridade do sistema financeiro e prevenção à fraude integram um mesmo contexto funcional, legitimando o uso proporcional de dados pessoais para essas finalidades. O legislador brasileiro, ao prever na LGPD uma base legal específica para a proteção ao crédito, adotou solução ainda mais clara e adequada à realidade nacional, reconhecendo expressamente a natureza sistêmica e contínua dessas atividades.

Diante desse cenário, crédito e fraude não podem ser tratados como trilhas paralelas ou desconectadas, mas como componentes interdependentes de um único modelo de risco. Tentativas de separação artificial comprometem a eficiência do sistema, elevam custos, ampliam riscos e prejudicam diretamente os titulares de dados, que passam a enfrentar crédito mais caro, mais restrito e maior exposição a ilícitos. A interpretação da LGPD deve preservar essa integração estrutural, assegurando proteção efetiva ao titular, segurança jurídica às operações e estabilidade ao mercado de crédito.

9. Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?

A separação artificial entre proteção ao crédito e prevenção à fraude produz consequências práticas profundamente negativas, tanto do ponto de vista operacional quanto econômico e social. Ao fragmentar atividades que, na prática, compartilham os mesmos dados, sistemas e objetivos, os modelos de risco passam a operar com informações incompletas, desconectadas da realidade econômica, comportamental e contextual dos consumidores, comprometendo sua eficiência e confiabilidade.

Do ponto de vista operacional, essa fragmentação eleva significativamente os erros decisórios. De um lado, amplia-se o risco de concessão de crédito a agentes fraudulentos, que exploram lacunas informacionais e inconsistências entre sistemas. De outro, aumenta-se a negativa injustificada de crédito a consumidores legítimos, que deixam de ser corretamente avaliados por ausência de uma visão integrada de risco. O resultado é o aumento dos custos operacionais, da inadimplência, inclusive fraudulenta, e das provisões de risco, com reflexo direto na elevação das taxas de juros e na retração da oferta de crédito em condições adequadas.

Para o titular de dados, especialmente aquele pertencente às camadas C e D, os efeitos são ainda mais gravosos. A restrição indevida ao uso integrado de dados impede o

acesso a modalidades de crédito mais vantajosas, como crédito pré-aprovado com taxas menores, consolidação de dívidas, renegociações estruturadas ou ofertas compatíveis com sua real capacidade financeira. Isso dificulta a reorganização econômica, agrava situações de superendividamento e reduz oportunidades de inclusão financeira justamente para quem mais depende do crédito formal.

Além disso, a ausência de uma visão integrada de crédito e fraude enfraquece políticas de orientação financeira e crédito responsável, pois inviabiliza a análise global da situação do consumidor e a oferta de produtos adequados ao seu perfil. A interpretação excessivamente restritiva, portanto, não protege o titular; ao contrário, retira instrumentos essenciais para sua estabilização financeira, aumentando sua exposição a soluções informais, mais caras e menos protegidas juridicamente.

Sob a ótica regulatória e institucional, essa fragmentação gera insegurança jurídica, desestimula investimentos em inovação tecnológica e favorece práticas excessivamente conservadoras, que sacrificam eficiência econômica, inclusão financeira e desenvolvimento produtivo em nome de uma proteção meramente formal de dados. Ambientes regulatórios instáveis ou contraditórios tendem a reduzir a concorrência, elevar custos e limitar a evolução de soluções antifraude e de crédito mais seguras e eficientes.

Diante disso, tratar proteção ao crédito e prevenção à fraude como trilhas separadas não apenas ignora a realidade operacional do mercado, como produz efeitos contrários aos objetivos de proteção do titular e de estabilidade econômica. A integração dessas finalidades é condição necessária para crédito responsável, redução de riscos, eficiência de mercado e inclusão financeira. A interpretação da LGPD deve, portanto, reconhecer essa interdependência estrutural, sob pena de comprometer a efetividade da regulação, encarecer o crédito e prejudicar os próprios titulares que se busca proteger.

V. ATIVIDADES E BASES LEGAIS APLICÁVEIS À PROTEÇÃO AO CRÉDITO

10. Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?

A base legal da proteção ao crédito prevista no art. 7º, inciso X, da Lei Geral de Proteção de Dados Pessoais deve ser interpretada de forma ampla, sistêmica e funcional, compatível com a realidade do mercado de crédito e com a finalidade que motivou sua criação pelo legislador. A proteção ao crédito não se limita ao momento da contratação, mas envolve um conjunto contínuo de atividades necessárias para que o crédito seja concedido, acompanhado e recuperado de forma responsável e segura.

Nesse contexto, estão abrangidas pela base legal da proteção ao crédito as atividades de análise prévia de risco, verificação e validação de identidade, avaliação da capacidade financeira, conferência e atualização cadastral, definição de elegibilidade para produtos, bem como a oferta responsável de crédito. Essas etapas são essenciais para que o crédito seja concedido em condições compatíveis com o perfil do titular, reduzindo riscos de inadimplência, evitando endividamento excessivo e promovendo maior previsibilidade econômica.

A proteção ao crédito também engloba o monitoramento da relação creditícia ao longo do tempo, a prevenção à fraude, a atualização contínua das informações relevantes, a renegociação de obrigações, a recuperação do crédito e a cobrança realizada de forma regular e proporcional, até o efetivo adimplemento da obrigação. Todas essas atividades integram um mesmo processo econômico e jurídico, voltado à preservação da saúde do sistema de crédito e à proteção do titular.

A oferta de crédito, inclusive nas modalidades de crédito consignado e crédito pré-aprovado, integra plenamente esse conceito quando baseada em análise técnica adequada e orientada à melhoria das condições financeiras do consumidor. Não se trata de prática mercadológica desvinculada do risco, mas de instrumento legítimo de proteção do crédito, que permite apresentar alternativas mais adequadas, com melhores taxas, prazos compatíveis e menor risco de superendividamento.

O funcionamento do Cadastro Positivo reforça essa compreensão ao permitir que dados de adimplemento sejam utilizados em benefício do próprio titular, ampliando o acesso ao crédito em condições mais favoráveis e reduzindo assimetrias informacionais. De forma coerente, a Lei do Superendividamento parte do pressuposto de que a análise prévia, a oferta responsável e o acompanhamento da relação creditícia são elementos centrais para a proteção do consumidor e para a prevenção de situações de endividamento excessivo.

Restringir a base legal da proteção ao crédito a fases pontuais ou a modalidades específicas, como apenas o crédito consignado, desconsidera a lógica sistêmica adotada pelo legislador e compromete a eficácia do modelo de proteção construído pela LGPD. A proteção ao crédito exige uma visão integrada e contínua, capaz de refletir a realidade econômica do país e de proteger, de forma efetiva, tanto o titular de dados quanto o funcionamento saudável do mercado.

Dessa forma, a base legal da proteção ao crédito deve abranger todas as atividades necessárias ao ciclo completo do crédito, desde a análise e a oferta responsável

até a recuperação e o encerramento da relação creditícia. Interpretações restritivas enfraquecem a proteção do titular, aumentam riscos, encarecem o crédito e reduzem a eficiência do mercado. A aplicação técnica e sistêmica do art. 7º, inciso X, da LGPD é condição essencial para assegurar crédito responsável, inclusão financeira e estabilidade econômica.

11. Quais bases legais da LGPD suportam o tratamento de dados para análise e concessão do crédito?

A base legal da proteção ao crédito, prevista no art. 7º, inciso X, da Lei Geral de Proteção de Dados Pessoais, constitui o fundamento jurídico central e estruturante para o tratamento de dados pessoais no contexto da análise, da oferta e da concessão de crédito. A sua criação não foi acidental, mas resultado de uma escolha legislativa consciente, voltada a superar as limitações da base da execução de contrato, que não alcança de forma adequada a fase pré-contratual nem as atividades posteriores ao inadimplemento.

A proteção ao crédito exige tratamento contínuo de dados ao longo de todo o ciclo da relação creditícia. Antes da contratação, para permitir análise de risco, definição de elegibilidade e oferta responsável. Durante a relação, para acompanhamento, prevenção à fraude e atualização de informações. E após o inadimplemento, para possibilitar renegociação, recuperação do crédito e encerramento adequado da relação. A base legal do art. 7º, inciso X, foi desenhada exatamente para dar sustentação jurídica a esse fluxo contínuo, assegurando segurança jurídica às operações e proteção efetiva aos titulares.

Outras bases legais previstas na LGPD podem atuar de forma complementar em situações específicas, como o cumprimento de obrigação legal ou regulatória, especialmente em setores supervisionados, ou o legítimo interesse, desde que haja compatibilidade com a finalidade e observância dos princípios da lei. No entanto, essas bases não substituem nem esvaziam a centralidade da proteção ao crédito como fundamento próprio e autônomo para o tratamento de dados nesse contexto.

Reduzir a proteção ao crédito a uma combinação residual de bases genéricas distorce o desenho normativo adotado pelo legislador brasileiro e compromete a coerência do sistema. Ao prever expressamente essa base legal, o legislador reconheceu o crédito como atividade de interesse público, essencial à estabilidade financeira, à inclusão social, ao funcionamento da economia e à proteção do consumidor, especialmente em um país com profundas desigualdades e forte dependência do crédito para mobilidade social e desenvolvimento produtivo.

Essa opção normativa posiciona o Brasil de forma avançada no cenário internacional, ao oferecer maior clareza e segurança jurídica do que modelos que dependem exclusivamente do legítimo interesse, como no GDPR, ou de exceções setoriais fragmentadas, como ocorre nos Estados Unidos sob a CCPA. Ao mesmo tempo, a LGPD preserva integralmente os princípios da finalidade, necessidade, proporcionalidade, transparência e segurança, deixando claro que não se trata de autorização irrestrita, mas de um regime jurídico próprio, equilibrado e compatível com a realidade econômica do país.

Assim, a correta interpretação das bases legais da LGPD no contexto do crédito exige reconhecer a proteção ao crédito como eixo central do tratamento de dados, capaz de sustentar juridicamente a análise, a oferta e a concessão responsável de crédito. Interpretações restritivas que desconsiderem essa opção legislativa não ampliam a proteção do titular, mas fragilizam o sistema, encarecem o crédito e reduzem o acesso a soluções financeiras adequadas, com prejuízos diretos para consumidores, empresas e para o desenvolvimento econômico nacional.

VI. BASES LEGAIS APLICÁVEIS À PREVENÇÃO À FRAUDE

12. Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?

O tratamento de dados pessoais para fins de prevenção à fraude encontra amparo em múltiplas bases legais previstas na Lei Geral de Proteção de Dados Pessoais, que devem ser interpretadas de forma sistemática, funcional e coerente com a finalidade protetiva do ordenamento jurídico e com o interesse público envolvido. A prevenção à fraude não constitui atividade marginal ou excepcional, mas elemento essencial para a segurança das relações econômicas, para a proteção do titular de dados e para a estabilidade do mercado.

Em primeiro lugar, a base legal da proteção ao crédito, prevista no art. 7º, inciso X, da LGPD, abrange naturalmente as atividades de prevenção à fraude quando estas se inserem no ciclo do crédito. A fraude representa risco direto ao crédito concedido, à sua recuperação e à própria viabilidade econômica da operação. Por essa razão, sua prevenção integra o próprio conceito de proteção ao crédito, não podendo ser tratada como atividade acessória ou dissociada do modelo de risco.

Além disso, o tratamento de dados pessoais para prevenção à fraude pode ser legitimado pelo cumprimento de obrigação legal ou regulatória, nos termos do art. 7º, inciso II, especialmente em setores regulados como o financeiro. Nesses contextos, existem deveres normativos expressos relacionados à prevenção de ilícitos, à mitigação de riscos

operacionais, ao combate à lavagem de dinheiro, ao financiamento do terrorismo e a outras práticas fraudulentas, que exigem tratamento contínuo e estruturado de dados pessoais.

O legítimo interesse, previsto no art. 7º, inciso IX, também pode ser aplicado em determinadas situações, desde que realizado o devido teste de balanceamento e demonstrado que o tratamento é necessário, proporcional e compatível com as expectativas legítimas do titular. No contexto antifraude, esse balanceamento tende a ser favorável, pois o tratamento busca evitar danos concretos e relevantes ao próprio titular, como fraudes de identidade, endividamento indevido e prejuízos patrimoniais de difícil reparação.

No que se refere a dados pessoais sensíveis, inclusive dados biométricos, a LGPD prevê hipóteses específicas de tratamento no art. 11, admitindo seu uso quando indispensável para finalidades legítimas como a prevenção à fraude e a proteção do crédito, desde que observados requisitos reforçados de segurança, governança, minimização e responsabilização. Essa previsão demonstra o reconhecimento, pelo legislador, de que determinadas atividades de segurança econômica e proteção do titular não podem ser inviabilizadas pela exigência de consentimento, sob pena de esvaziar sua efetividade.

No direito comparado, observa-se compreensão convergente. O Regulamento Geral de Proteção de Dados da União Europeia admite expressamente o tratamento de dados para prevenção à fraude com fundamento no legítimo interesse e na proteção da integridade do sistema financeiro. Nos Estados Unidos, a California Consumer Privacy Act e legislações setoriais reconhecem a fraude e a segurança como exceções legítimas às restrições gerais de tratamento. O modelo brasileiro, ao conjugar bases legais específicas e gerais, oferece um arcabouço normativo claro, robusto e proporcional, apto a sustentar juridicamente as atividades antifraude.

Dessa forma, a correta interpretação das bases legais da LGPD demonstra que a prevenção à fraude está plenamente amparada no ordenamento jurídico brasileiro. Leituras excessivamente restritivas, que ignorem essa arquitetura normativa, não fortalecem a proteção de dados, mas fragilizam a segurança econômica, ampliam riscos sistêmicos e prejudicam os próprios titulares, que passam a enfrentar maior exposição a ilícitos e um mercado de crédito mais caro e restrito.

13. Como interpretar a base legal de prevenção à fraude à luz do interesse público, da segurança dos titulares e da estabilidade financeira?

A interpretação da base legal aplicável à prevenção à fraude deve partir do reconhecimento de que se trata de atividade de inequívoco interesse público, cuja finalidade

ultrapassa a proteção de interesses individuais e alcança a segurança da coletividade, a estabilidade da economia e o regular funcionamento do sistema financeiro. A fraude, especialmente em larga escala, não é um evento isolado, mas um fenômeno sistêmico que compromete a confiança no mercado, eleva custos, reduz o acesso ao crédito e gera impactos sociais amplos e duradouros.

Sob a perspectiva da segurança dos titulares, a prevenção à fraude constitui verdadeira medida de proteção de direitos fundamentais, como o direito ao patrimônio, à identidade, à honra e à dignidade econômica. Fraudes de identidade, contratações indevidas e operações não reconhecidas produzem efeitos que vão muito além do prejuízo financeiro imediato, afetando a vida civil do titular, seu acesso ao crédito, sua reputação e sua estabilidade econômica. Impedir ou dificultar o tratamento de dados necessário à detecção de fraudes significa, na prática, expor o titular a riscos concretos e recorrentes, muitas vezes de difícil ou demorada reparação.

A estabilidade financeira também depende diretamente da existência de mecanismos eficazes de prevenção à fraude. Sistemas financeiros permeáveis a ilícitos tendem a se tornar mais caros, mais restritivos e menos inclusivos. O aumento de fraudes eleva perdas operacionais, exige provisões mais conservadoras e leva ao repasse de custos ao mercado, na forma de juros mais altos, maior seletividade na concessão e retração do crédito produtivo. Esses efeitos não recaem apenas sobre instituições financeiras, mas sobre toda a sociedade, afetando consumo, investimento, geração de empregos e crescimento econômico.

Nesse contexto, a interpretação das bases legais da LGPD aplicáveis à prevenção à fraude deve ser teleológica, sistêmica e orientada à efetividade, e não meramente formal. A proteção de dados pessoais não pode ser compreendida de forma isolada, desconectada de seus impactos econômicos e sociais. A própria LGPD reconhece que a proteção de dados deve conviver com outras finalidades legítimas do ordenamento jurídico, entre elas a segurança, a prevenção de ilícitos e a proteção do crédito.

A LGPD não foi concebida para inviabilizar a prevenção à fraude ou enfraquecer mecanismos essenciais de segurança econômica. Ao contrário, buscou disciplinar essas atividades de forma responsável, proporcional e transparente, assegurando governança, minimização de dados e responsabilização, sem comprometer a proteção material dos titulares nem a estabilidade do sistema financeiro. Interpretações excessivamente restritivas, que desconsiderem o interesse público envolvido, acabam por produzir o efeito inverso ao pretendido, fragilizando a proteção do titular, ampliando riscos sistêmicos e encarecendo o crédito para toda a sociedade.

Dessa forma, a base legal de prevenção à fraude deve ser interpretada como instrumento legítimo de proteção coletiva, de segurança dos titulares e de preservação da estabilidade financeira, compatível com os princípios da LGPD e indispensável ao funcionamento saudável do ecossistema de crédito e da economia nacional.

VII. PRINCÍPIOS DA LGPD APLICÁVEIS AOS CONTEXTOS DE CRÉDITO E ANTIFRAUDE

14. Quais princípios devem orientar a coleta, o uso, a minimização, a retenção e o compartilhamento de dados nesses tratamentos?

Os tratamentos de dados pessoais no contexto da proteção ao crédito e da prevenção à fraude devem ser orientados pelos princípios estabelecidos na Lei Geral de Proteção de Dados Pessoais, de forma integrada e funcional, considerando a natureza contínua dessas atividades e seu impacto direto sobre a segurança econômica e a proteção do titular. Entre esses princípios, destacam-se a finalidade, a adequação, a necessidade, a transparência, a segurança, a prevenção e a responsabilização.

A finalidade deve ser clara, específica e legítima, vinculada à proteção do crédito, à prevenção à fraude, à concessão responsável e à proteção do próprio titular de dados. Esses tratamentos não podem ser desviados para usos incompatíveis, como exploração meramente mercadológica desvinculada do risco creditício. A correta delimitação da finalidade é essencial para garantir previsibilidade ao titular e segurança jurídica aos agentes envolvidos.

A adequação exige que os dados tratados sejam compatíveis com essas finalidades, considerando o contexto econômico da operação e o risco envolvido. Já o princípio da necessidade impõe que sejam utilizados apenas os dados efetivamente requeridos para a análise de risco, a identificação de inconsistências e a detecção de ilícitos, sem excessos, mas também sem restrições artificiais que comprometam a eficácia dos mecanismos de proteção.

A retenção de dados deve observar critérios objetivos e proporcionais, vinculados ao ciclo do crédito, às obrigações legais e regulatórias aplicáveis e à existência de riscos residuais legítimos. A eliminação prematura de dados pode inviabilizar a prevenção à fraude, dificultar a defesa do titular e do agente econômico e comprometer a recuperação do crédito. Por outro lado, a retenção excessiva e desproporcional deve ser evitada por meio de políticas claras de governança, revisão periódica e controle de acesso.

O compartilhamento de dados deve ocorrer de forma controlada, transparente e segura, preferencialmente entre agentes que integrem legitimamente o ecossistema de crédito e antifraude. Esse compartilhamento deve estar limitado a finalidades compatíveis, amparado por instrumentos contratuais adequados, com deveres de confidencialidade, padrões de segurança da informação e mecanismos de responsabilização bem definidos. A circulação responsável de dados, quando bem governada, fortalece a prevenção à fraude, reduz assimetrias informacionais e beneficia diretamente os titulares.

Os princípios da segurança e da prevenção exigem a adoção de medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, incidentes e usos indevidos, especialmente considerando a sensibilidade econômica das informações tratadas. A responsabilização impõe que os agentes demonstrem conformidade com a LGPD por meio de políticas internas, registros de tratamento, avaliações de impacto quando cabíveis e mecanismos efetivos de controle e auditoria.

Assim, a aplicação dos princípios da LGPD nesses contextos não deve ser meramente formal, mas orientada à efetividade da proteção do titular e à estabilidade do sistema de crédito. A observância equilibrada desses princípios permite conciliar proteção de dados, segurança econômica e inclusão financeira, evitando tanto o uso indiscriminado quanto a restrição excessiva que fragiliza a prevenção à fraude e encarece o crédito.

15. Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?

A proporcionalidade, a necessidade e a adequação em modelos integrados de crédito e prevenção à fraude devem ser asseguradas por meio de governança estruturada, controles internos consistentes e revisão contínua dos modelos de risco utilizados. Esses princípios não se materializam de forma abstrata, mas por meio de processos concretos que demonstrem a relação direta entre os dados tratados, os riscos mitigados e a finalidade legítima do tratamento.

É fundamental que os agentes de tratamento realizem o mapeamento completo dos fluxos de dados, identifiquem as categorias de informações utilizadas em cada etapa do ciclo do crédito e documentem as finalidades específicas associadas a esses tratamentos. Sempre que aplicável, devem ser conduzidas análises de impacto à proteção de dados, acompanhadas de políticas claras de minimização, retenção e descarte, capazes de demonstrar que apenas os dados necessários estão sendo utilizados e pelo tempo estritamente adequado.

A necessidade deve ser avaliada à luz do risco concreto que se busca mitigar. Em contextos de maior risco, como concessão remota de crédito, prevenção à fraude de identidade ou operações financeiras sensíveis, o uso de dados mais robustos pode ser plenamente justificado. Em situações de menor risco, os modelos devem ser ajustados para utilizar informações menos invasivas. Essa calibragem contínua é essencial para preservar o equilíbrio entre proteção de dados e segurança econômica.

A adequação exige que os dados tratados sejam compatíveis com a finalidade declarada e com as expectativas legítimas do titular no contexto da relação econômica. Isso inclui transparência quanto à existência de modelos de risco, aos tipos de dados utilizados e às consequências práticas dessas análises, especialmente quando envolvem decisões automatizadas ou semiautomatizadas.

Os modelos de risco devem ser constantemente avaliados para reduzir excessos, evitar vieses ou discriminações indevidas e assegurar que decisões automatizadas funcionem como instrumentos de apoio qualificado à tomada de decisão humana, e não como mecanismos opacos ou inflexíveis. A proporcionalidade, nesse contexto, não se mede apenas pela quantidade de dados coletados, mas pela qualidade do uso, pela correlação efetiva com a mitigação de riscos e pelo benefício concreto proporcionado à proteção do titular.

Assim, assegurar proporcionalidade, necessidade e adequação em modelos integrados exige uma abordagem dinâmica e responsável, baseada em governança, revisão contínua e responsabilidade demonstrável. Quando bem estruturados, esses modelos permitem conciliar proteção de dados, prevenção à fraude e eficiência do crédito, promovendo segurança jurídica, inclusão financeira e estabilidade econômica sem sacrificar os direitos dos titulares.

16. Como operacionalizar transparência sem comprometer a efetividade de sistemas antifraude e de scoring?

A transparência nos sistemas de prevenção à fraude e de scoring de crédito deve ser interpretada de forma funcional, proporcional e orientada à proteção material do titular, e não como exigência de divulgação irrestrita de lógicas internas, parâmetros técnicos ou mecanismos sensíveis de detecção de risco. A finalidade da transparência, nesse contexto, é permitir que o titular compreenda por que seus dados são tratados, para quais objetivos, quais direitos lhe assistem e como pode exercê-los, sem comprometer a segurança do sistema nem a eficácia das ferramentas de proteção ao crédito.

Esse entendimento encontra respaldo direto na jurisprudência consolidada do Superior Tribunal de Justiça, especialmente na Súmula 550, segundo a qual a utilização de sistemas de credit scoring é lícita, desde que assegurados ao consumidor o direito à informação e à correção de dados, resguardado o segredo empresarial. Ao reconhecer a validade desses sistemas, o STJ deixou claro que a transparência exigida não se confunde com a divulgação integral dos modelos, fórmulas matemáticas, pesos atribuídos ou critérios específicos de cálculo, justamente porque essa exposição comprometeria a utilidade e a segurança do próprio sistema.

A operacionalização adequada da transparência pode ser realizada por meio de políticas de privacidade claras, redigidas em linguagem acessível, que expliquem as finalidades gerais do tratamento, as categorias de dados utilizadas, a existência de mecanismos de análise de risco e prevenção à fraude, bem como os direitos do titular e os canais disponíveis para atendimento, correção e revisão. Esse nível de informação permite compreensão suficiente do tratamento, sem revelar informações técnicas sensíveis.

Da mesma forma, é possível assegurar transparência por meio de canais efetivos de atendimento ao titular, capazes de fornecer explicações em nível adequado sobre decisões que impactem sua relação creditícia, como negativa de crédito, bloqueio de operação ou necessidade de validações adicionais. Essas explicações devem se concentrar nos critérios gerais considerados, tais como histórico financeiro, perfil de risco, inconsistências cadastrais ou padrões atípicos de comportamento, sem a divulgação de regras específicas, limiares de decisão ou mecanismos de detecção que possam ser explorados por fraudadores.

Exigir transparência absoluta, com abertura integral de modelos e parâmetros, além de contrariar a orientação do STJ, produziria efeitos contraproducentes. Sistemas antifraude e de scoring dependem justamente da assimetria informacional em relação a agentes mal-intencionados, e sua exposição excessiva fragilizaria a prevenção a ilícitos, ampliaria riscos sistêmicos e prejudicaria os próprios titulares, que passariam a enfrentar maior incidência de fraudes e um mercado de crédito mais caro e restritivo.

Esse equilíbrio também é reconhecido no direito comparado. O GDPR admite limites à transparência quando sua aplicação irrestrita compromete a segurança, a prevenção à fraude ou outros interesses públicos relevantes. A CCPA segue lógica semelhante ao prever exceções destinadas à proteção da integridade dos sistemas e à prevenção de ilícitos. A LGPD deve ser interpretada de forma coerente com essas premissas e com a jurisprudência nacional consolidada.

Assim, a transparência nos sistemas de crédito e antifraude deve ser real, proporcional e orientada à efetividade, garantindo informação adequada ao titular sem inviabilizar ferramentas essenciais de proteção econômica. Esse modelo, longe de fragilizar direitos, assegura a validade jurídica dos sistemas de scoring, protege o titular contra fraudes, preserva o segredo empresarial e contribui para a estabilidade do mercado, em plena consonância com a LGPD e com o entendimento consolidado do Superior Tribunal de Justiça.

VIII. GOVERNANÇA, CONTROLES E SEGURANÇA

17. Quais frameworks de governança e gestão de riscos são recomendados para operações de crédito e antifraude?

As operações de crédito e de prevenção à fraude exigem frameworks de governança robustos, integrados e baseados em risco, capazes de articular proteção de dados pessoais, segurança da informação, gestão de riscos, conformidade regulatória e estabilidade operacional. Trata-se de atividades contínuas, sensíveis e de impacto sistêmico, que demandam estruturas de governança maduras, verificáveis e alinhadas às melhores práticas internacionais.

No plano técnico e operacional, recomenda-se a adoção de padrões internacionais amplamente reconhecidos, como o ISO 31000, voltado à gestão de riscos corporativos, que permite estruturar processos decisórios baseados em risco de forma transversal e alinhada à estratégia do negócio. No campo da segurança da informação, as normas ISO/IEC 27001 e 27002 permanecem referência essencial para a definição de controles técnicos e organizacionais voltados à proteção de dados, especialmente em ambientes de alto risco econômico e financeiro.

No âmbito específico da privacidade e proteção de dados pessoais, a ISO/IEC 27701 se destaca como framework de governança ao estruturar um sistema de gestão da privacidade integrado à segurança da informação, com foco em accountability, avaliação de riscos à privacidade e conformidade regulatória com legislações como a LGPD e o GDPR. Em operações críticas, a adoção de práticas alinhadas à ISO 22301, voltada à continuidade de negócios, também se mostra relevante para assegurar a resiliência dos sistemas de crédito e antifraude diante de incidentes operacionais, cibernéticos ou sistêmicos.

Além das normas ISO, é altamente recomendável a adoção de frameworks desenvolvidos por autoridades públicas e organismos regulatórios internacionais, que

refletem a visão institucional dos reguladores sobre gestão de riscos e segurança. Nesse contexto, o NIST Cybersecurity Framework, amplamente utilizado nos Estados Unidos e reconhecido internacionalmente, oferece diretrizes práticas para identificação, proteção, detecção, resposta e recuperação frente a riscos cibernéticos e fraudes, sendo especialmente relevante para operações financeiras e de crédito intensivas em dados.

No cenário europeu, orientações emitidas por autoridades de proteção de dados e supervisores financeiros reforçam essa abordagem baseada em risco e governança. O European Data Protection Board (EDPB), ao tratar de accountability, segurança e prevenção de ilícitos sob o GDPR, enfatiza a necessidade de estruturas organizacionais capazes de demonstrar conformidade contínua, com avaliações de impacto, controles proporcionais e revisão periódica de modelos de risco. Da mesma forma, diretrizes da European Banking Authority (EBA) sobre gestão de riscos operacionais e de TIC reforçam a integração entre segurança, prevenção à fraude e estabilidade financeira.

Também merecem destaque regulações recentes como o Digital Operational Resilience Act (DORA) da União Europeia, que estabelece requisitos de governança, gestão de riscos e resiliência operacional para entidades financeiras, reconhecendo que a segurança dos sistemas, a prevenção a incidentes e a proteção de dados são elementos indissociáveis da estabilidade do mercado financeiro.

No plano da proteção de dados, legislações como o GDPR e a CCPA, embora adotem modelos distintos, convergem ao exigir estruturas de governança capazes de demonstrar responsabilidade, proporcionalidade e controle efetivo dos riscos, especialmente em atividades de alto impacto como crédito e prevenção à fraude. Em ambos os regimes, a conformidade não se resume ao cumprimento formal de regras, mas à capacidade de demonstrar que riscos são identificados, mitigados e continuamente monitorados.

Assim, a adoção combinada de normas técnicas internacionais, frameworks regulatórios públicos e orientações de autoridades estrangeiras fortalece a governança das operações de crédito e antifraude, assegurando proteção efetiva aos titulares, segurança jurídica aos agentes econômicos e estabilidade ao sistema financeiro. Trata-se de abordagem alinhada ao princípio da accountability da LGPD e compatível com as melhores práticas globais, capaz de sustentar modelos de risco eficientes, proporcionais e socialmente responsáveis.

ANBI

18. Quais controles técnicos e administrativos devem ser implementados para assegurar segurança da informação e mitigação de incidentes?

Os controles técnicos e administrativos adotados em operações de crédito e de prevenção à fraude devem ser proporcionais ao volume, à sensibilidade e ao impacto potencial dos dados tratados, considerando que essas atividades envolvem riscos econômicos relevantes e exposição direta dos titulares a danos patrimoniais e identitários. Essa abordagem baseada em risco está expressamente alinhada à Lei Geral de Proteção de Dados Pessoais e às orientações emitidas pela Autoridade Nacional de Proteção de Dados, bem como às boas práticas internacionais de segurança e governança.

A própria experiência brasileira com o Cadastro Positivo constitui evidência concreta da viabilidade técnica e regulatória desses controles. O Cadastro Positivo opera há anos com grande volume de dados financeiros, envolvendo milhões de titulares, sob supervisão regulatória específica, com regras claras de governança, segurança, compartilhamento e responsabilização. Ao longo desse período, não se verificaram incidentes sistêmicos relevantes que colocassem em risco os titulares ou a estabilidade do mercado, o que demonstra a maturidade do setor e a eficácia dos controles técnicos e administrativos já implementados. Esse histórico reforça que a proteção de dados, quando bem governada, é plenamente compatível com operações de crédito em larga escala.

Do ponto de vista técnico, devem ser adotados controles de acesso baseados em perfis e no princípio do menor privilégio, autenticação forte para ambientes críticos, criptografia de dados em repouso e em trânsito, segregação de ambientes, monitoramento contínuo, registro de logs e processos estruturados de gestão de vulnerabilidades. Essas medidas estão em consonância com as normas ISO/IEC 27001 e 27002, amplamente reconhecidas como referência internacional em segurança da informação, e refletem o estado da técnica exigido para operações sensíveis.

No que se refere à gestão de incidentes, frameworks como a ISO/IEC 27035, voltada especificamente à resposta a incidentes de segurança da informação, e o NIST Cybersecurity Framework, adotado globalmente em setores críticos e financeiros, fornecem diretrizes claras para identificação, detecção, contenção, resposta e recuperação. Esses modelos enfatizam a importância de processos documentados, testes periódicos e melhoria contínua, elementos essenciais em ambientes expostos a fraudes sofisticadas e ataques cibernéticos recorrentes.

Sob a ótica administrativa e organizacional, é indispensável a existência de políticas internas claras de segurança da informação e proteção de dados, programas de

treinamento contínuo para colaboradores, definição formal de responsabilidades e mecanismos de supervisão interna. A ANPD, assim como autoridades europeias como a Agencia Española de Protección de Datos (AEPD) e a Commission Nationale de l'Informatique et des Libertés (CNIL), reiteram que falhas organizacionais e humanas figuram entre as principais causas de incidentes, o que torna a governança e a cultura de segurança elementos centrais da mitigação de riscos.

No contexto brasileiro, as normas e orientações do Banco Central do Brasil, especialmente aquelas relacionadas à gestão de riscos operacionais, segurança cibernética e continuidade de negócios no Sistema Financeiro Nacional, reforçam essa mesma lógica. Essas regulações partem do pressuposto de que a segurança da informação e a prevenção a incidentes não são apenas obrigações de conformidade, mas componentes essenciais da estabilidade financeira e da proteção do consumidor.

O compartilhamento de dados com terceiros deve ser protegido por instrumentos contratuais robustos, com cláusulas específicas de confidencialidade, segurança da informação, proteção de dados, deveres de cooperação em caso de incidentes e padrões mínimos de controle. Essa exigência é reiterada tanto pela ANPD quanto por autoridades estrangeiras como elemento essencial da accountability.

A mitigação de incidentes exige, ainda, a existência de planos formais de resposta, com fluxos claros de comunicação interna, critérios objetivos de avaliação de impacto, procedimentos de contenção e recuperação e, quando aplicável, mecanismos de comunicação a titulares e autoridades competentes. A capacidade de resposta organizada e tempestiva é fator determinante para reduzir danos, preservar direitos e manter a confiança no sistema de crédito.

Assim, a adoção de controles técnicos e administrativos alinhados às orientações da ANPD, às regulações setoriais do Banco Central, às normas técnicas internacionais como ISO e NIST e à experiência consolidada do Cadastro Positivo demonstra que o setor de crédito e antifraude possui maturidade regulatória e operacional suficiente para tratar dados pessoais de forma segura, proporcional e responsável. Longe de representar fragilidade, esse histórico evidencia que a combinação entre governança, tecnologia e supervisão é capaz de proteger os titulares, prevenir fraudes e assegurar a estabilidade do ecossistema de crédito, em plena consonância com os princípios da LGPD.

19. Como estruturar políticas de retenção, registro de logs, auditoria e accountability?

A estruturação de políticas de retenção, registro de logs, auditoria e accountability deve partir de uma abordagem baseada em risco, compatível com a natureza contínua das operações de crédito e de prevenção à fraude. Essas políticas não podem ser genéricas ou meramente formais, devendo refletir o ciclo completo do crédito, as obrigações legais e regulatórias aplicáveis e os riscos residuais legítimos associados às atividades desenvolvidas.

As políticas de retenção de dados devem ser definidas com base em critérios objetivos, considerando o ciclo da relação creditícia, os prazos prescricionais, as obrigações legais e regulatórias, bem como a necessidade de prevenção à fraude, defesa de direitos e recuperação do crédito. A eliminação de dados deve ocorrer de forma segura, controlada e documentada, após o esgotamento das finalidades legítimas, evitando tanto a retenção excessiva e desproporcional quanto a eliminação prematura, que pode comprometer investigações, auditorias, a prevenção de ilícitos e a própria proteção do titular. Essa lógica é coerente com os princípios da LGPD e com orientações da ANPD, que reconhecem a necessidade de retenção proporcional ao risco e à finalidade.

O registro de logs e a manutenção de trilhas de auditoria constituem elementos centrais da governança e da segurança da informação. Esses registros são indispensáveis para assegurar rastreabilidade das operações, investigação de incidentes de segurança, apuração de fraudes e demonstração de conformidade perante autoridades e titulares. Os logs devem registrar acessos, alterações, consultas e eventos relevantes, ser protegidos contra acessos não autorizados, alterações indevidas ou exclusões, e mantidos por período compatível com sua finalidade e com os riscos envolvidos. Essa prática é amplamente recomendada por normas técnicas como a ISO/IEC 27001, a ISO/IEC 27002 e a ISO/IEC 27035, bem como pelo NIST Cybersecurity Framework, especialmente nos domínios de detecção, resposta e recuperação.

As auditorias internas e, quando aplicável, externas, desempenham papel fundamental na verificação contínua da aderência das operações às políticas estabelecidas, à LGPD e às boas práticas de mercado. Auditorias periódicas permitem identificar falhas, corrigir desvios, aprimorar controles e demonstrar comprometimento com a melhoria contínua da governança. Autoridades europeias, como a CNIL e a AEPD, reiteram que a existência de auditorias documentadas e recorrentes é elemento relevante na avaliação da conformidade e da diligência dos agentes de tratamento.

ANBI

A accountability, princípio estruturante da LGPD, deve se materializar por meio de documentação consistente e acessível, incluindo registros de atividades de tratamento, políticas internas, relatórios de risco, avaliações de impacto quando aplicáveis, planos de resposta a incidentes e evidências de treinamento e conscientização. Essa documentação deve permitir que o agente de tratamento demonstre, de forma clara e verificável, que adotou medidas técnicas e administrativas adequadas, proporcionais e alinhadas às finalidades legítimas do tratamento.

No contexto brasileiro, essa abordagem também dialoga com regulações setoriais do Banco Central do Brasil, que exigem registros, rastreabilidade, controles internos e capacidade de auditoria em operações financeiras e de crédito, reconhecendo que esses elementos são essenciais para a estabilidade do sistema financeiro e para a proteção do consumidor.

Assim, a correta estruturação de políticas de retenção, logs, auditoria e accountability não se resume ao cumprimento formal da LGPD, mas representa instrumento essencial de governança, transparência responsável e gestão de riscos. Quando bem implementadas, essas políticas fortalecem a proteção dos titulares, viabilizam a prevenção à fraude, asseguram segurança jurídica aos agentes econômicos e contribuem para a estabilidade e a confiança no ecossistema de crédito.

IX. DECISÕES AUTOMATIZADAS E INTELIGÊNCIA ARTIFICIAL

20. Quais são as decisões automatizadas mais comuns em crédito e antifraude?

As decisões automatizadas em operações de crédito e de prevenção à fraude são utilizadas de forma ampla e estruturada ao longo de todo o ciclo do crédito, sempre como parte de modelos integrados de gestão de risco, e não como mecanismos isolados ou autônomos. Esses sistemas atuam principalmente na organização, correlação e análise de grandes volumes de dados, permitindo identificar riscos, inconsistências e padrões relevantes que subsidiam a tomada de decisão.

No contexto do crédito, as decisões automatizadas são empregadas em etapas como análise inicial de elegibilidade, classificação de risco, definição de faixas de limite e condições compatíveis com o perfil financeiro do titular, bem como no acompanhamento contínuo da relação creditícia. Esses modelos permitem avaliar capacidade de pagamento, histórico de adimplemento, comportamento financeiro e outros indicadores objetivos, com a finalidade de adequar a oferta de crédito à realidade econômica do consumidor, evitando

concessões incompatíveis e contribuindo diretamente para o crédito responsável e para a prevenção do superendividamento.

Na prevenção à fraude, as decisões automatizadas são utilizadas para validação de identidade, análise de comportamento transacional, identificação de padrões atípicos, detecção de inconsistências cadastrais e monitoramento contínuo de eventos suspeitos. Esses mecanismos são essenciais em ambientes digitais e de alto volume, nos quais a atuação exclusivamente manual seria incapaz de oferecer proteção efetiva contra fraudes sofisticadas e escaláveis. A automação permite respostas rápidas, proporcionais e direcionadas, reduzindo riscos tanto para as instituições quanto para os próprios titulares de dados.

Essas decisões automatizadas são estruturadas de forma a cumprir integralmente o art. 20 da LGPD. Os agentes de tratamento mantêm procedimentos formais que asseguram ao titular o direito de obter informações claras e adequadas sobre os critérios gerais utilizados nos processos decisórios, bem como o direito de solicitar revisão das decisões que afetem seus interesses. A revisão é realizada por meio de intervenção humana qualificada, com análise contextualizada do caso concreto, possibilidade de correção de dados e reavaliação da decisão, sem prejuízo da preservação da segurança do sistema e do segredo empresarial.

A governança desses modelos inclui salvaguardas técnicas e organizacionais específicas, como documentação dos critérios gerais de decisão, validação periódica dos modelos, monitoramento de desempenho, mitigação de vieses, controles de acesso, registro de logs e trilhas de auditoria. Essas medidas asseguram que as decisões automatizadas sejam proporcionais, adequadas e alinhadas às finalidades legítimas de proteção ao crédito, prevenção à fraude e proteção do titular.

A jurisprudência brasileira consolidou a legitimidade desses modelos ao reconhecer que sistemas de credit scoring e decisões automatizadas baseadas em métodos estatísticos são lícitos, desde que respeitados os direitos de informação, correção e revisão, sem exigência de divulgação de fórmulas, pesos ou regras internas que comprometam a eficácia e a segurança dos sistemas. Esse entendimento dialoga diretamente com o regime do art. 20 da LGPD, que não exige transparência absoluta, mas sim transparência funcional e proteção efetiva dos direitos do titular.

No plano internacional, essa abordagem é consistente com a prática europeia sob o GDPR, que admite decisões automatizadas em contextos de risco financeiro e prevenção à fraude, desde que acompanhadas de salvaguardas, possibilidade de intervenção humana

e medidas de governança adequadas. Nos Estados Unidos, modelos semelhantes são utilizados há décadas, com exigência de mecanismos de contestação e correção, mas preservando a integridade técnica dos sistemas.

Assim, as decisões automatizadas mais comuns em crédito e antifraude devem ser compreendidas como instrumentos técnicos de apoio à decisão, inseridos em estruturas de governança maduras, transparentes em nível adequado e plenamente compatíveis com a LGPD. Quando corretamente implementadas, essas decisões protegem o titular contra fraudes, evitam concessões irresponsáveis, contribuem para o combate ao superendividamento e fortalecem a estabilidade do sistema de crédito, cumprindo função econômica e social relevante.

21. Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?

A explicabilidade, a governança algorítmica e a mitigação de vieses em modelos automatizados de crédito e prevenção à fraude devem ser tratadas como elementos estruturantes da gestão de risco, e não como obrigações isoladas ou meramente formais. Esses modelos operam em contextos de alto impacto econômico e social, o que exige controles contínuos, documentação adequada e mecanismos efetivos de supervisão humana.

A explicabilidade deve ser compreendida em nível funcional e proporcional. Não se exige, nem seria adequado, a divulgação integral de modelos matemáticos, algoritmos, códigos-fonte ou pesos atribuídos às variáveis, o que comprometeria a segurança do sistema, o segredo empresarial e a própria eficácia dos mecanismos antifraude e de scoring. A explicabilidade exigida pela LGPD e pelas boas práticas internacionais consiste na capacidade de explicar, de forma clara e compreensível, os critérios gerais utilizados, os fatores relevantes considerados na decisão e as consequências práticas para o titular, permitindo a compreensão do processo decisório sem expor mecanismos sensíveis.

Nesse sentido, os agentes de tratamento devem ser capazes de demonstrar, tanto para autoridades quanto para titulares, quais categorias de dados são utilizadas, quais finalidades orientam o modelo, como os dados contribuem para a avaliação de risco e de que forma decisões podem ser revistas. Essa abordagem está alinhada ao art. 20 da LGPD, bem como à jurisprudência nacional que reconhece a licitude de sistemas de scoring desde que assegurados direitos de informação, correção e revisão, sem comprometimento da integridade técnica dos modelos.

ANBI

A governança algorítmica deve ser estruturada de forma integrada à governança de dados, à gestão de riscos e à estratégia institucional. Isso envolve a documentação dos modelos utilizados, a definição clara de responsabilidades, a validação periódica de desempenho, a revisão de premissas e a supervisão por equipes multidisciplinares, envolvendo áreas jurídica, de compliance, tecnologia, risco e negócios. Modelos automatizados não devem operar de forma opaca ou desassistida, mas sob monitoramento contínuo e com possibilidade de ajustes sempre que necessário.

A mitigação de vieses exige processos técnicos e organizacionais permanentes. Isso inclui a realização de testes periódicos para identificar efeitos desproporcionais ou discriminatórios, a análise de impacto sobre diferentes perfis de titulares e a revisão das variáveis utilizadas, de modo a evitar correlações indevidas ou resultados incompatíveis com a finalidade legítima do modelo. A mitigação de vieses não se limita à exclusão de determinadas variáveis, mas envolve avaliação contextual, qualidade dos dados, calibração contínua e monitoramento dos resultados produzidos ao longo do tempo.

Essas práticas são coerentes com as orientações internacionais sob o GDPR, que exige medidas adequadas para proteger os direitos dos titulares em decisões automatizadas, bem como com frameworks técnicos amplamente reconhecidos, como aqueles recomendados por autoridades europeias e por organismos como o NIST, que reforçam a necessidade de auditoria, governança e melhoria contínua em sistemas automatizados de alto impacto.

Assim, lidar adequadamente com explicabilidade, governança algorítmica e mitigação de vieses requer uma abordagem madura, baseada em risco, transparência funcional e supervisão humana efetiva. Quando bem estruturados, esses mecanismos permitem conciliar inovação tecnológica, proteção de dados, prevenção à fraude e crédito responsável, assegurando que os modelos automatizados atuem de forma legítima, proporcional e alinhada à LGPD e às melhores práticas regulatórias internacionais.

22. Quais diretrizes devem orientar o uso de IA generativa e machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos?

O uso de tecnologias de inteligência artificial generativa e de machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos deve ser orientado por diretrizes claras de finalidade legítima, proporcionalidade, segurança, explicabilidade funcional e controle humano significativo, observando-se sempre o impacto concreto dessas soluções sobre os titulares e sobre o ecossistema de crédito.

A experiência regulatória europeia, especialmente com o AI Act, oferece contribuições relevantes nesse sentido ao adotar uma abordagem baseada em risco, distinguindo aplicações de baixo, médio e alto impacto. Esse modelo é positivo porque reconhece que nem todo uso de IA apresenta o mesmo nível de risco e que os requisitos de governança devem ser calibrados de acordo com a finalidade, o contexto e os potenciais efeitos da tecnologia. Em atividades como prevenção à fraude, análise de risco e segurança financeira, o AI Act reconhece a legitimidade do uso de IA, desde que acompanhada de salvaguardas adequadas.

Ao mesmo tempo, é essencial que essa lógica seja aplicada de forma proporcional e pragmática, evitando a imposição de estruturas de governança excessivamente complexas que possam inviabilizar a inovação ou criar barreiras de entrada para pequenas e médias empresas. A governança deve ser adequada ao porte da organização, à complexidade do modelo e ao impacto real da decisão automatizada, sob pena de concentrar o mercado, reduzir a concorrência e, paradoxalmente, prejudicar os próprios titulares.

No plano prático, recomenda-se que sistemas de IA generativa e machine learning sejam utilizados prioritariamente como ferramentas de apoio qualificado à decisão, especialmente em decisões de maior impacto, assegurando controle humano efetivo, possibilidade de revisão e mecanismos claros de contestação, em consonância com o art. 20 da LGPD. A automação deve fortalecer a tomada de decisão, e não substituí-la de forma cega ou irreversível.

A finalidade do uso da IA deve estar claramente delimitada à proteção do crédito, à prevenção à fraude, à validação de identidade e à segurança das operações. A proporcionalidade exige que o volume de dados, o grau de sofisticação do modelo e as exigências de governança sejam compatíveis com o risco tratado. A segurança demanda proteção contra acessos indevidos, manipulação de dados, ataques adversariais e uso fora do escopo autorizado.

A explicabilidade, conforme reconhecido tanto pelo AI Act quanto pelo GDPR, deve ser funcional e orientada a resultados. Não se exige a abertura de modelos, códigos ou dados de treinamento, mas a capacidade de explicar critérios gerais, objetivos do sistema e efeitos práticos das decisões, de forma compreensível para autoridades e titulares, preservando a segurança e o segredo empresarial.

Também é recomendável a realização de testes periódicos de desempenho, robustez e vieses, com ajustes proporcionais sempre que identificados riscos relevantes.

Esses testes devem ser compatíveis com a escala da operação e com os recursos disponíveis, evitando exigências que apenas grandes players consigam cumprir.

Assim, as diretrizes para o uso de IA generativa e machine learning em crédito e antifraude devem buscar o equilíbrio entre inovação, proteção de dados, segurança econômica e inclusão financeira. A incorporação dos princípios positivos do AI Act, combinada com a flexibilidade e a proporcionalidade da LGPD, permite construir um ambiente regulatório eficaz, que fortaleça a prevenção à fraude e o crédito responsável sem engessar o mercado ou excluir pequenas e médias empresas do ecossistema de inovação.

23. Como equilibrar transparência e explicabilidade com segredos de negócio?

O equilíbrio entre transparência, explicabilidade e proteção de segredos de negócio é elemento central para a legitimidade e a sustentabilidade dos sistemas de crédito, scoring e prevenção à fraude. A transparência excessiva ou mal calibrada pode comprometer a segurança dos sistemas, facilitar práticas fraudulentas e inviabilizar modelos legítimos de negócio, gerando efeitos contrários à proteção dos próprios titulares de dados.

A legislação brasileira e a jurisprudência consolidada reconhecem esse equilíbrio. No julgamento do Recurso Especial nº 1.419.697/RS, o Superior Tribunal de Justiça afirmou expressamente a licitude dos sistemas de credit scoring e reconheceu que a exigência de transparência não implica a divulgação de fórmulas matemáticas, pesos, variáveis específicas ou critérios técnicos detalhados. O Tribunal foi claro ao afirmar que a preservação do segredo empresarial é condição necessária para a própria eficácia desses sistemas e para a proteção do mercado contra comportamentos oportunistas e fraudulentos.

Nesse sentido, a transparência exigida deve ser funcional e orientada à proteção material do titular, e não à exposição irrestrita dos mecanismos internos de decisão. O titular deve ter acesso a informações claras sobre a existência do tratamento automatizado, suas finalidades, as categorias de dados utilizadas, os critérios gerais considerados e os impactos práticos da decisão, bem como meios efetivos de correção e revisão. Isso atende plenamente ao art. 20 da LGPD, sem comprometer a segurança do sistema ou os segredos de negócio.

A explicabilidade, portanto, não se confunde com abertura de modelos, códigos-fonte, bases de treinamento ou parâmetros internos. Ela se materializa na capacidade de explicar a lógica decisória em nível adequado, permitindo compreensão e contestação legítima, mas preservando a integridade técnica, a inovação e a vantagem competitiva dos agentes econômicos.

ANBI

Essa compreensão é amplamente reconhecida no direito comparado. O GDPR admite limites claros à transparência quando a divulgação irrestrita compromete a segurança, a prevenção à fraude ou outros interesses legítimos, incluindo segredos comerciais. A CCPA, nos Estados Unidos, segue a mesma lógica ao permitir exceções à divulgação de informações quando necessárias para proteger a integridade dos sistemas e os interesses comerciais legítimos. O AI Act europeu, ao tratar de sistemas de IA utilizados em contextos sensíveis, reforça que a explicabilidade deve ser proporcional ao risco e compatível com a proteção de segredos comerciais e direitos de propriedade intelectual.

Esse equilíbrio é particularmente relevante para a inovação, sobretudo no contexto de pequenas e médias empresas. Exigências desproporcionais de transparência técnica tendem a favorecer apenas grandes players com maior capacidade jurídica e tecnológica, concentrando o mercado, reduzindo a concorrência e, em última instância, prejudicando os próprios titulares, que passam a enfrentar menos opções, crédito mais caro e menor inclusão financeira.

Assim, a interpretação da LGPD deve buscar uma harmonização entre transparência, segurança e inovação, assegurando que os titulares sejam informados e protegidos sem inviabilizar ferramentas legítimas de gestão de risco, combate à fraude e concessão responsável de crédito. A proteção de segredos de negócio não representa um privilégio indevido, mas um componente essencial da segurança do sistema, da prevenção de ilícitos e da estabilidade do ecossistema de crédito.

Quando corretamente calibrado, esse equilíbrio fortalece simultaneamente os direitos dos titulares, a inovação responsável e a eficiência econômica, em plena consonância com a LGPD, com a jurisprudência do STJ e com as melhores práticas regulatórias internacionais.

CONSIDERAÇÕES FINAIS DA ANBI

A ANBI compreende que a proteção ao crédito e a prevenção à fraude constituem atividades contínuas, integradas e de inequívoco interesse público, indispensáveis ao funcionamento do sistema financeiro, à inclusão econômica da população e à proteção efetiva dos titulares de dados pessoais. Crédito e fraude não são fenômenos isolados, mas dimensões interdependentes de um mesmo ecossistema de risco, cuja adequada regulação impacta diretamente o desenvolvimento socioeconômico do país.

ANBI

Ao longo das contribuições apresentadas, restou evidenciado que o tratamento de dados pessoais no ciclo do crédito, desde a oferta responsável, passando pela concessão, monitoramento, renegociação e recuperação, até a prevenção a ilícitos, é condição necessária para reduzir assimetrias informacionais, combater fraudes, mitigar o superendividamento e promover acesso a crédito em condições mais justas e compatíveis com a realidade financeira dos consumidores. Essa lógica protege não apenas o mercado, mas sobretudo o próprio titular, que passa a ter maior segurança, previsibilidade e dignidade econômica.

Uma interpretação excessivamente restritiva da base legal da proteção ao crédito, dissociada da prevenção à fraude e da realidade operacional do setor, tende a produzir efeitos contrários aos objetivos da LGPD. Ao limitar de forma artificial o uso responsável de dados, essa abordagem encarece o crédito, reduz a oferta, amplia a exclusão financeira e afeta de maneira mais severa as camadas economicamente vulneráveis, dificultando a reorganização financeira e agravando o superendividamento. Nesse cenário, a proteção de dados se torna meramente formal, enquanto a proteção material do titular é enfraquecida.

O legislador brasileiro, ao instituir de forma expressa a base legal da proteção ao crédito na LGPD, reconheceu a natureza estrutural dessas atividades e buscou superar as limitações inerentes a outras bases legais, como a execução de contrato ou o consentimento. Essa escolha normativa conferiu segurança jurídica a um ecossistema essencial ao desenvolvimento econômico, alinhando o Brasil às melhores práticas internacionais, mas com solução ainda mais clara e adequada à realidade nacional.

As respostas também demonstram que o setor de crédito e prevenção à fraude opera sob elevado grau de maturidade regulatória e técnica, com governança estruturada, adoção de padrões internacionais, mecanismos de accountability, controles de segurança e experiência consolidada, como evidenciado pelo histórico do Cadastro Positivo. A utilização de decisões automatizadas, modelos de scoring, machine learning e, de forma controlada, inteligência artificial, ocorre com salvaguardas compatíveis com a LGPD, com respeito ao art. 20, com possibilidade de revisão humana, mitigação de vieses e preservação do segredo empresarial, conforme reconhecido pela jurisprudência do Superior Tribunal de Justiça e pelo direito comparado.

Nesse contexto, cabe ao Conselho Nacional de Proteção de Dados, por meio dos trabalhos do GT5, consolidar uma interpretação técnica, sistêmica e equilibrada da base legal da proteção ao crédito, que concilie proteção de dados pessoais, segurança econômica, inovação responsável e inclusão financeira. Essa interpretação deve estar alinhada às melhores práticas internacionais, como o GDPR, o AI Act e a experiência norte-americana,

ANBI

mas calibrada à realidade brasileira, evitando soluções que, embora bem-intencionadas, produzam efeitos econômicos e sociais adversos.

A ANBI reafirma seu compromisso com a proteção de dados pessoais, com o crédito responsável e com a prevenção eficaz à fraude, e se coloca à disposição para continuar contribuindo de forma técnica e construtiva com os trabalhos deste Grupo de Trabalho, colaborando para o fortalecimento de um ambiente regulatório seguro, proporcional e favorável ao desenvolvimento sustentável do país.

São Paulo, 21 de janeiro de 2026

LEANDRO ALVARENGA MIRANDA:30239291816

Assinado de forma digital por LEANDRO ALVARENGA MIRANDA:30239291816
Dados: 2026.01.21 13:25:18 -03'00'

Leandro Alvarenga Miranda
Diretor Jurídico
Associação Nacional dos Bureaus de Informação – ANBI

ANEXO XV – Resposta ao ofício: Febraban e ABECS

abecs

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

OFÍCIO Nº ED-0003/2026

São Paulo, 20 de janeiro de 2026

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD)
A/C do GT5 – Proteção ao Crédito e Prevenção à Fraude

Ref.: Solicitação de contribuição ao CNPD (GT5 – Proteção ao Crédito e Prevenção à Fraude)

Prezados,

1 A Federação Brasileira de Bancos ("FEBRABAN") e Associação Brasileira das Empresas de Cartões de Crédito e Serviços ("ABECS"), associações civis sem fins lucrativos representativas do setor financeiro, vêm apresentar suas contribuições acerca da solicitação do GT5 – Proteção ao Crédito e Prevenção à Fraude, do CNPD.

2 Esperamos que nossas contribuições possam auxiliar qualitativamente na solicitação feita pelo CNPD, através do GT-5.

3 Permanecemos à disposição para quaisquer esclarecimentos ou contribuições que se façam necessários.

vicente.dechiara@febraban.org.br
Assinado
D4Sign
Luís Vicente Magni De Chiara
Diretor-executivo de Assuntos Jurídicos

roberta.buso@febraban.org.br
Assinado
D4Sign
Roberta Gaspar Buso
Gerente Jurídica

Associação Brasileira das Em[illegible]édito e Serviços – ABECS

marcelot@abecs.org.br
Assinado
D4Sign
Marcelo Takeyama
Diretor Jurídico, Autorregulação e Compliance

I) A importância socioeconômica do crédito e da prevenção à fraude para o Brasil

1. **Qual é a relevância do crédito para o desenvolvimento socioeconômico do Brasil?**

O crédito é um dos principais motores do desenvolvimento socioeconômico do Brasil. Ele viabiliza investimentos, permite que empresas expandam suas operações, financiem inovação e gerem empregos. Para as famílias brasileiras, o crédito possibilita a aquisição de bens, acesso à moradia, educação e realização de projetos pessoais, contribuindo para a melhoria da qualidade de vida e para o aumento do consumo, que movimenta a economia.

Além disso, o crédito é fundamental para a inclusão financeira, especialmente em regiões e públicos tradicionalmente excluídos do sistema bancário. O aumento do acesso ao crédito está diretamente relacionado à participação na economia formal, permitindo que mais pessoas tenham oportunidades de prosperidade. No contexto macroeconômico, o crédito fortalece a liquidez do mercado, facilita a circulação de capital e contribui para a estabilidade financeira. Em momentos de crise, bancos públicos e privados desempenham papel estratégico ao ampliar a oferta de crédito, ajudando empresas e famílias a superar dificuldades e impulsionando a retomada do crescimento.

Por fim, o crédito direcionado para setores estratégicos, como infraestrutura, sustentabilidade e inovação, tem potencial de transformar a sociedade, promovendo desenvolvimento regional, geração de empregos qualificados e avanços tecnológicos. Dessa forma, o crédito é um pilar essencial para o progresso econômico, pois impulsiona a competitividade, promove o desenvolvimento social e sustentável e contribui para a construção de um Brasil mais moderno, justo e competitivo.

2. **Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?**

Em um cenário de crescente digitalização, fraudes representam riscos sistêmicos que afetam consumidores, instituições e a economia como um todo. A prevenção à fraude é um vetor estratégico para o desenvolvimento socioeconômico do Brasil, pois fortalece a confiança, protege direitos, reduz perdas e garante a sustentabilidade do sistema financeiro. Investir continuamente em tecnologias como inteligência artificial e análise comportamental contribui para um ecossistema estável e seguro,

estimulando o uso de serviços financeiros e impulsionando a inovação e o crescimento econômico.

II) Papel dos dados pessoais no ecossistema de crédito

3. Qual a importância dos dados pessoais para proteção do crédito e demais atividades relacionadas ao tema?

A Lei Geral de Proteção de Dados Pessoais (LGPD) prevê a Proteção ao Crédito como uma das bases legais para o tratamento de dados pessoais (Art. 7º, X). Isso significa que é possível tratar dados pessoais para atividades relacionadas ao crédito, inclusive para garantir a segurança das operações de crédito, em observância aos princípios e diretrizes da norma.

Além disso, o tratamento responsável dos dados pessoais, seguindo a LGPD, e outras regras de proteção de dados, é indispensável para garantir decisões justas, seguras e transparentes, protegendo tanto o consumidor quanto as instituições financeiras e de pagamento.

O uso de dados pessoais é essencial para atividades relacionadas ao crédito e permite, inclusive, a análise precisa do perfil do cliente, avaliação e gerenciamento de risco, concessão responsável de crédito e prevenção à inadimplência, além de todas as demais atividades relacionadas, como recuperação de crédito. Dados como histórico de pagamentos, renda, dados cadastrais, CPF e restrições de crédito, dentre outros, além da avaliação de informações relacionadas e que se utilizam de dados pessoais, como o score de crédito, são fundamentais para que as instituições financeiras e de pagamento possam tomar decisões informadas, reduzir assimetrias informacionais e aumentar a liquidez e estabilidade sistêmica do mercado, possibilitando o melhor gerenciamento do risco de crédito e de seus impactos sistêmicos, fortalecendo o setor financeiro, a economia e possibilitando a concessão de crédito de forma mais segura e inclusiva.

4. Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?

A utilização de dados pessoais, conforme as diretrizes da LGPD e outras normas de proteção de dados, é essencial para reduzir assimetrias informacionais, pois fornece informações detalhadas sobre os titulares. Quando instituições acessam informações como histórico de pagamentos, renda, dívidas, restrições cadastrais, comportamento de consumo, dentre outros, conseguem avaliar com maior

assertividade o risco de inadimplência de cada pessoa. Isso diminui a dependência de critérios genéricos ou subjetivos, impacta positivamente a liquidez do mercado, reduz a inadimplência e aumenta a eficiência das operações financeiras, tornando a análise de crédito mais justa e personalizada.

Ao reduzir as assimetrias informacionais, o uso dos dados pessoais facilita a concessão de crédito para quem realmente tem capacidade de pagamento, evitando que "bons" pagadores sejam excluídos por falta de informação ou que "maus" pagadores tenham acesso a crédito sem o devido controle. Com dados mais completos, as instituições conseguem precificar melhor o risco, ajustar taxas de juros e ampliar a oferta de crédito, o que aumenta a circulação de recursos na economia.

Além disso, a eficiência do mercado é aprimorada, já que decisões baseadas em dados reduzem custos operacionais, evitam fraudes e diminuem a inadimplência. O uso responsável dos dados pessoais, aliado à conformidade com a LGPD, fortalece a confiança dos consumidores e das empresas, promovendo um ambiente mais transparente, competitivo e sustentável. Dessa forma, o tratamento adequado dos dados pessoais é um dos principais motores para o equilíbrio entre inovação, segurança e inclusão financeira no Brasil.

III) Papel dos dados pessoais na prevenção à fraude e outros ilícitos

5. Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?

Os dados pessoais são fundamentais para a prevenção à fraude e outros ilícitos, pois permitem identificar, autenticar e monitorar transações com segurança, reduzindo riscos e garantindo a integridade do sistema financeiro. Informações como CPF, biometria, histórico de transações, dados cadastrais, dados comportamentais, dentre outros são essenciais para validar identidades e detectar padrões suspeitos, possibilitando o uso agregado de tecnologias avançadas como inteligência artificial, monitoramento de transações e padrões e *onboarding* digital para mitigar vulnerabilidades. Além disso, a correta utilização desses dados, alinhada à LGPD, bem como outras regras de proteção de dados, assegura equilíbrio entre prevenção eficaz e respeito à privacidade, fortalecendo a confiança do consumidor e garantindo um ambiente econômico moderno, inclusivo e resiliente.

6. **Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos?**

A combinação de dados comportamentais, biométricos e metadados é considerada uma prática essencial para fortalecer mecanismos de prevenção à fraude e atender às exigências regulatórias, conforme as diretrizes da LGPD bem como outras regras de proteção de dados. Dados comportamentais permitem monitorar padrões de uso e identificar desvios que indicam risco, como acessos em horários atípicos ou transações fora do perfil do cliente. Dados biométricos, por sua vez, garantem autenticação forte e reduzem vulnerabilidades relacionadas à identidade, dificultando ataques de engenharia social e fraudes sintéticas. Já os metadados fornecem contexto adicional, incluindo informações sobre dispositivos, localização e rede, que possibilitam análises cruzadas para detectar inconsistências e uso indevido. A integração dessas três camadas cria um sistema antifraude mais inteligente e responsivo, capaz de atuar em tempo real, assegurando rastreabilidade, transparência e conformidade regulatória, além de proteger o patrimônio dos clientes. Por exemplo, a análise de padrões de compra, reconhecimento facial e análise de localização podem identificar tentativas de fraude em tempo real, tornando os processos mais seguros e eficientes.

7. **Quais são os riscos de subutilizar dados pessoais em processos antifraude (ex.: aumento de chargebacks, fraude sintética, falsidade ideológica e riscos sistêmicos)?**

Subutilizar dados pessoais em processos antifraude traz riscos relevantes para o mercado como um todo e para os próprios titulares. A ausência de informações detalhadas pode aumentar o número de *chargebacks* - devoluções de valores por transações contestadas - o que prejudica a liquidez das empresas e eleva os custos operacionais.

A falta de informações pessoais pode favorecer a ocorrência de falsidade ideológica, fraude sintética e golpes, permitindo que pessoas se passem por outras para obter crédito ou realizar transações ilícitas.

Além disso, a subutilização dos dados pode gerar riscos sistêmicos, como o aumento da inadimplência, a perda de confiança no sistema financeiro e a exposição das instituições a sanções regulatórias e danos reputacionais. Por isso, o uso responsável, seguro e eficiente dos dados pessoais é indispensável para a saúde do mercado, a proteção dos consumidores e o desenvolvimento socioeconômico do Brasil. A abordagem adotada deve ser integrada e responsável, garantindo que todos

os dados pessoais coletados sejam utilizados de forma eficiente, segura e em conformidade com a LGPD e com as normas do Banco Central do Brasil ("Bacen") e demais reguladores do setor financeiro. Os processos devem seguir princípios de finalidade, transparência e segurança, assegurando que cada dado seja tratado conforme orienta a lei. Além disso, devem ser alocados investimentos contínuos em tecnologia avançada e monitoramento inteligente para prevenir ilícitos, proteger o patrimônio dos clientes e das instituições e manter a integridade do ecossistema financeiro.

IV) Convergência entre proteção ao crédito e prevenção à fraude

8. **O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?**

Ambos dependem de dados pessoais, comportamentais e de monitoramento para garantir decisões seguras. Por exemplo, no processo de concessão de crédito, as instituições precisam avaliar o perfil do cliente, histórico de pagamentos, capacidade de pagamento e possíveis restrições, utilizando informações cadastrais, comportamentais e externas (como dados de bureaus de crédito, dentre outras). Esses mesmos dados são fundamentais para os sistemas de prevenção à fraude, que buscam identificar tentativas de golpes e outros ilícitos.

Além disso, o objetivo comum é proteger o titular, a instituição e todo o sistema contra perdas financeiras, seja por inadimplência ou por fraudes, e garantir a sustentabilidade do negócio. A eficiência desses processos depende da capacidade de identificar riscos rapidamente, mitigar ameaças e tomar decisões seguras, equilibrando a concessão de crédito responsável com a proteção contra ilícitos. Por isso, crédito e fraude são áreas que atuam de forma colaborativa, compartilhando dados, tecnologias e estratégias para fortalecer o sistema financeiro, para reduzir custos, dar respostas mais rápidas a ameaças emergentes e proteger clientes e empresas.

9. **Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?**

A ausência de integração entre os fluxos de dados aumenta a chance de inconsistências e desinformação sobre o titular, dificultando a validação de identidades e a detecção de comportamentos suspeitos.

Além disso, separar as trilhas pode comprometer a experiência do cliente, pois ele pode ser submetido a múltiplas etapas de verificação, solicitações redundantes de

documentos e abordagens divergentes entre áreas, tornando o processo mais burocrático e complexo. A integração é fundamental para uma abordagem holística e eficaz, focada na proteção do titular, das instituições e do sistema como um todo, contribuindo para a sua estabilidade.

V) Atividades e bases legais aplicáveis à proteção ao crédito

10. Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?

Diversas atividades de tratamento podem ser englobadas na base legal de proteção ao crédito, visto que para garantir a avaliação adequada do risco de crédito do titular (que é uma das atividades, mas não a única relacionada a essa base legal), é necessário a coleta, classificação, acesso, transmissão, processamento, armazenamento, compartilhamento, transferência e extração de dados pessoais em diversas etapas do processo. De forma exemplificativa, pode-se detalhar algumas dessas atividades relacionadas à avaliação de risco de crédito e outras atividades relacionadas à proteção do crédito:

- **Análise de crédito**: coleta, consulta e processamento de dados pessoais (como CPF, nome, endereço, renda, histórico de pagamentos, restrições cadastrais, dados comportamentais e informações de cadastro positivo) e de score de crédito para avaliar o risco de inadimplência e decidir sobre a oferta e concessão de crédito ao consumidor.
- **Concessão de crédito**: oferta e concessão efetiva do crédito, com a gestão durante todo o seu ciclo de vida.
- **Gestão do risco de crédito**: monitoramento contínuo do comportamento financeiro do cliente, atualização de informações cadastrais, acompanhamento de pagamentos e identificação de sinais de inadimplência ou fraude, além do gerenciamento do risco de crédito como um todo, e não apenas focado no titular, mas no risco de crédito da instituição e do mercado, incluindo fornecimento de informações e consultas ao SCR – Sistema de Informações de Crédito do Banco Central do Brasil e outras atividades de gerenciamento de risco de crédito, inclusive considerando as normas regulamentares dos órgãos reguladores financeiros, como políticas de crédito, limites de crédito e atividades relacionadas.
- **Bancos de dados de proteção ao crédito**: fornecimento de informações e verificação de restrições, registros de inadimplência, cadastro positivo, protestos

etc., junto a bureaus de crédito como Serasa, SPC, Quod, entre outros e/ou cartórios, por exemplo.

- **Modelagem estatística e score de crédito**: uso de dados pessoais para modelos matemáticos, políticas de crédito e algoritmos que estimam o risco de crédito e capacidade de pagamento.
- **Concessão e gestão de financiamentos, empréstimos e cartões**: oferta, análise de propostas, simulação de operações, contratação, acompanhamento de contratos.
- **Recuperação de crédito**: atividades como avaliação, constituição, gerenciamento e/ou execução de garantias de operações de crédito e de outras transações que envolvem risco financeiro, além de cobrança de dívidas, renegociações, localização do devedor e/ou de bens e outras medidas de recuperação de crédito, inclusive judiciais e/ou extrajudiciais.
- **Cessão de crédito**: Realização de transações envolvendo crédito, como a cessão e aquisição de operações de crédito e recebíveis.

Um dos principais pontos que deve ser levado em consideração é que a base legal de proteção do crédito não se resume aos cadastros de crédito, como cadastro positivo e outros cadastros de inadimplência, ou à avaliação de risco de crédito. A proteção do crédito é bem mais ampla e engloba todas as atividades descritas acima e tantas outras relacionadas ao crédito e a transações que envolvem risco financeiro.

11. Quais bases legais da LGPD suportam o tratamento de dados para análise e concessão do crédito?

Além da base legal da proteção ao crédito, outras bases legais previstas na LGPD podem ser aplicadas, observando os princípios de tal norma, conforme o contexto da operação e da atividade de tratamento:

Execução de contrato (art. 7º, V, da LGPD): permite o tratamento de dados para a execução de contrato do qual o titular seja parte, inclusive de procedimentos preliminares relacionados ao contrato, como avaliações prévias, propostas e contratos de financiamento, empréstimos ou cartões de crédito.

Cumprimento de obrigação legal ou regulatória (art. 7º, II, da LGPD): autoriza o tratamento de dados para atender obrigações legais e/ou regulatórias, inclusive as decorrentes de normas e requisições de órgãos como Bacen, CMN – Conselho Monetário Nacional, CVM - Comissão de Valores Mobiliários, ANPD e demais autoridades.

Legítimo interesse (art.7º, IX, da LGPD): permite o tratamento de dados pessoais para finalidades legítimas atreladas ao apoio e promoção de atividades do controlador e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, como por exemplo, para o direcionamento de ofertas adequadas ao titular, observando riscos de crédito e/ou de superendividamento.

Consentimento (art. 7º, I, da LGPD): embora não seja obrigatório para proteção ao crédito, pode ser utilizado em situações em que o titular autoriza expressamente o uso de seus dados pessoais, como no Open Finance.

Exercício regular de direitos em processo judicial, administrativo ou arbitral (art. art. 7º, I, da LGPD): no caso de medidas necessárias, inclusive anteriores, a processos que envolvam crédito.

VI) Bases legais aplicáveis à prevenção à fraude

12. Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?

Quando falamos de tratamento de dados pessoais para prevenção às fraudes, algumas bases legais podem ser utilizadas, a depender da natureza dos dados (pessoais ou sensíveis). Neste sentido, a LGPD possibilita o tratamento com fundamento em algumas bases legais, como:

Cumprimento de obrigação legal ou regulatória (art. 7º, II e art. 11, II. "a", da LGPD): quando o tratamento é decorrente de legislação e/ou de normas e requisições do Bacen, CMN, ANPD ou outras autoridades, especialmente em processos de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo e gerenciamento de riscos de fraude e operacionais.

Execução de contrato (art. 7º, V, da LGPD): quando o tratamento é necessário para validar identidades, autenticar transações e garantir a segurança de operações relacionadas a contratos com o titular, inclusive previamente à sua contratação.

Legítimo interesse (art.7º, IX, da LGPD): permite o tratamento de dados pessoais para finalidades legítimas atreladas ao apoio e promoção de atividades do controlador e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de

serviços que o beneficiem, como por exemplo, o tratamento de dados pessoais para preservar a segurança das transações realizadas pelo titular.

Garantia da prevenção à fraude e à segurança do titular (art.11, II, g, da LGPD): nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, como, por exemplo, a autenticação de biometria facial na abertura de conta de corrente para prevenir a abertura de conta fraudulenta.

Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (art.11, II, d, da LGPD): no caso de contratos e processos que envolvam fraude e segurança e dados sensíveis.

13. Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?

A base legal de prevenção à fraude, interpretada à luz do interesse público, da segurança dos titulares e da estabilidade financeira, deve ser vista como um instrumento que equilibra a proteção dos direitos individuais com a necessidade coletiva de manter um ambiente econômico seguro e confiável, o qual também beneficia o titular e toda a sociedade.

O interesse público está diretamente relacionado à redução de crimes financeiros, à proteção do patrimônio dos cidadãos e das instituições, bem como à preservação da confiança no sistema bancário e comercial. Ao permitir o tratamento de dados pessoais para prevenir fraudes, a legislação busca evitar prejuízos que afetam não apenas indivíduos, mas também empresas e o próprio funcionamento do mercado.

Neste sentido, o tratamento de dados pessoais fundado na finalidade de prevenção a fraudes é essencial para garantir a estabilidade financeira do mercado e a segurança dos titulares, evitando prejuízos financeiros individuais e que reflitam no interesse público. Portanto, deve-se considerar o interesse público na proteção do sistema financeiro, a segurança dos titulares e a necessidade de garantir a estabilidade do ecossistema, sempre com transparência, proporcionalidade e respeito aos direitos fundamentais.

VII) Princípios da LGPD aplicáveis a ambos os contextos

14. Quais princípios devem orientar a coleta, uso, minimização, retenção e compartilhamento de dados nesses tratamentos?

Os princípios que devem orientar a coleta, uso, minimização, retenção e compartilhamento de dados pessoais em tratamentos voltados para crédito e prevenção à fraude devem ser os já definidos pela Lei Geral de Proteção de Dados Pessoais (art.6º da LGPD) e que refletem as melhores práticas internacionais de governança de dados. Dentre estes princípios, exemplifica-se os seguintes:

- O princípio da **finalidade** dispõe que os dados sejam coletados e tratados para propósitos legítimos, assim como ocorre nas situações de proteção ao crédito e prevenção a fraudes;
- O princípio da **adequação** dispõe que os tratamentos dos dados estejam alinhados com as informações dadas aos titulares com o contexto da operação.
- O princípio da **transparência** obriga as organizações a informar aos titulares sobre os tratamentos realizados e a respectivas finalidades.
- O princípio da **não discriminação** proíbe o uso dos dados para fins discriminatórios ilícitos ou abusivos.

Esses princípios devem ser aplicados de forma contínua e revisados periodicamente.

15. Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?

A proporcionalidade e a necessidade devem ser ponderadas a depender do contexto do tratamento. Nas hipóteses de tratamento de dados pessoais fundamentados na proteção ao crédito e prevenção a fraudes, quantidade de dados tratados atende ao princípio da necessidade e sua redução arbitrária e sem fundamento pode gerar prejuízos à finalidade legítima, visto que para estas finalidades os dados pessoais são essenciais para o aperfeiçoamento do funcionamento dos modelos de riscos, evitando a concessão de crédito desproporcional ao titular ou em desacordo com o risco de crédito e/ou a ocorrência de fraudes. De toda forma, para zelar por estes pontos, é importante o registro da operação de tratamento; avaliações de impacto à proteção de dados, quando aplicável; revisões periódicas dos fluxos de dados; auditorias internas e validação dos critérios quando necessário; garantindo assim, o tratamento dos dados necessários e a manutenção de dados atualizados para atingir os objetivos.

A adequação, por sua vez, implica que o tratamento dos dados seja alinhado com as finalidades informadas ao titular, de acordo o contexto da operação. Para isso, é importante zelar pela transparência nas políticas de privacidade, informar os titulares sobre o uso dos dados pessoais, adotar medidas de segurança robustas e permitir mecanismos de revisão e contestação das decisões automatizadas, quando aplicável.

16. Como operacionalizar transparência sem comprometer a efetividade de sistemas antifraude e de scoring?

Para os tratamentos relacionados a proteção ao crédito e prevenção às fraudes, a transparência pode ser observada por meio de políticas de privacidade, comunicação objetiva e acessível sobre o uso dos dados e disponibilização de canais de atendimento para esclarecimento de dúvidas e exercício de direitos. Porém, tal transparência não pode extrapolar limites de segredos comerciais e/ou expor informações que possam comprometer a segurança ou a eficácia do tratamento e/ou dos sistemas.

VIII) Governança, controles e segurança (SI)

17. Quais frameworks de governança e gestão de riscos são recomendados para operações de crédito e antifraude?

A adoção de práticas reconhecidas globalmente que integrem governança sólida, gestão contínua de riscos e conformidade regulatória é recomendada, mas não deve ser imposta, ficando a cargo do controlador definir as medidas mais adequadas. Certificações como ISO 27001:2022, ISO 27701:2025, ISO 31000:2018, 27017, 27018, NIST e PCI, por exemplo, reforçam o compromisso com a Segurança e Privacidade da Informação dos titulares, garantindo que processos de governança de segurança da informação (avaliação de risco de segurança, SOC (Security Operation Center), tratamento de incidentes de segurança da informação, arquitetura de segurança da informação, vulnerabilidade no ambiente computacional, gestão de acessos lógicos) e seus processos de governança de tratamento de dados pessoais, estão em conformidade com os requisitos das normas. O foco deve ser em controles robustos, monitoramento em tempo real, uso de tecnologia avançada, observando as diretrizes e normas de órgãos reguladores do sistema financeiro, tais como o Bacen.

18. Quais controles técnicos e administrativos devem ser implementados para assegurar segurança da informação e mitigação de incidentes?

Para assegurar a segurança da informação e mitigar incidentes é fundamental implementar controles técnicos e administrativos que atuem de forma integrada e contínua. Entre os controles técnicos, destacam-se o gerenciamento de acessos (com autenticação forte e restrição ao menor privilégio necessário), a criptografia de dados, o

monitoramento contínuo de sistemas e redes, a realização de backups regulares, o uso de firewalls, sistemas de detecção e prevenção de intrusões, além da atualização frequente de softwares e correção de vulnerabilidades.

No âmbito administrativo, é essencial estabelecer políticas claras de segurança da informação e privacidade, promover treinamentos e campanhas de conscientização para os colaboradores, realizar avaliações periódicas de riscos, manter planos de resposta a incidentes bem definidos e testados e garantir auditorias regulares. A gestão de ativos de informação, a classificação dos dados conforme sensibilidade, e a documentação dos processos também são práticas recomendadas.

19. Como estruturar políticas de retenção, registro de logs, auditoria e accountability?

A definição dos prazos de retenção dos dados e dos logs, deve estar alinhado à legislação vigente, a boas práticas de governança, à estratégia de gestão de riscos das instituições e às finalidades e contexto de tratamento. Os logs devem ser armazenados em ambiente seguro, com controles de acesso restritos e evidências de configuração e tempo de retenção definidos.

A auditoria deve ser realizada de forma periódica, para monitorar a aplicação das políticas, gerar relatórios detalhados e validar a conformidade dos controles implementados.

IX) Decisões automatizadas e Inteligência Artificial

20. Quais são decisões automatizadas mais comuns em crédito e antifraude?

As decisões automatizadas em prevenção à fraude são suportadas por inteligência de dados estruturada em dois pilares: (i) criação de variáveis especializadas e (ii) geração de scores antifraude.

No primeiro pilar, desenvolve-se variáveis que permitem segmentar riscos com maior precisão, como habitualidade de Wi-Fi, geolocalização, indicadores de acesso remoto, sinais de malware e contadores de transações. Essas variáveis ajudam a inferir *modus operandi* e direcionar ações como validação biométrica ou bloqueio preventivo. No segundo pilar, utiliza-se scores antifraude, que podem consolidar diversas variáveis em um único índice de risco (0 a 1000, por exemplo), calculado por

modelos de machine learning e inteligência artificial. Esses scores permitem decisões ágeis e escaláveis, como negativas de transações, desafios de autenticação (biometria, QR Code, senhas), temporização com validação via SMS ou WhatsApp e, em casos críticos, bloqueio de conta. Todo o processo é suportado por ferramentas analíticas avançadas e motores de risco que operam em tempo real, garantindo explicabilidade, rastreabilidade e conformidade com LGPD e normas do Bacen e demais reguladores do setor financeiro.

Com essas informações, é possível verificar a elegibilidade do cliente e realizar a pré-aprovação, em decorrência da verificação automática de impedimentos cadastrais (CPF irregular, apontamentos internos/externos) e regras de políticas para liberar ou barrar a proposta comercial.

Além disso, na modelagem de risco e decisão (Decisioning), os modelos de risco de crédito atuais que estruturam a tomada de decisão já contam com uso de algoritmos que combinam técnicas avançadas de machine learning com abordagens mais sofisticadas de inteligência artificial, como a criação de variáveis explicativas derivadas de dados não estruturados por meio de redes neurais profundas e arquiteturas baseadas em *_transformers_*. Essas técnicas permitem extrair padrões complexos de comportamento, enriquecer os modelos com sinais provenientes de textos, imagens e dados transacionais, além de melhorar a capacidade preditiva e a personalização das decisões. Com isso, a esteira evolui para um ecossistema de *decision intelligence*, onde modelos adaptativos, aprendizado contínuo e explicabilidade garantem decisões mais ágeis, precisas e alinhadas às políticas de risco e compliance.

Portanto, de forma geral, pode-se exemplificar algumas decisões automatizadas como as necessárias para: análise de perfil de risco; concessão de crédito; detecção de transações suspeitas; bloqueio preventivo e validação de identidade por biometria e/ou comportamento.

21. Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?

Para lidar com explicabilidade, governança algorítmica e mitigação de vieses em modelos de risco (crédito e antifraude), a abordagem precisa combinar disciplina regulatória, engenharia de dados, modelos e práticas organizacionais claras.

A utilização de ferramentas que realizam uma análise da presença de vieses em bases de dados utilizadas para treino dos modelos de crédito e de antifraude é uma das formas empregadas pelas instituições para realizar um monitoramento de

performance do modelo. Além disso, existem métodos amplamente conhecidos no mercado e que são utilizados para a explicabilidade desses modelos, como SHAP Values e Lime. O SHAP Values é um método que indica o nível de contribuição de cada variável utilizada para a previsão do resultado de um modelo. Em um modelo de detecção de diabetes, por exemplo, variáveis como nível de glicose no sangue e idade são muito influentes no resultado expedido pelo modelo (tem diabetes ou não). O Lime, ao contrário do SHAP que foca em uma compreensão global do modelo e de seu conjunto de dados, é um método que se dedica a explicar a previsão do modelo para instâncias individuais. Seguindo o exemplo anterior, o LIME indica a probabilidade de um paciente específico ter ou não diabetes e quais as variáveis que mais influenciaram nessas probabilidades (ex: nível de glicose e de pressão arterial). Dessa forma, a utilização de ferramentas de análise de viés em conjunto com métodos de explicabilidade de modelos de inteligência artificial são formas de lidar com a explicabilidade, governança algorítmica e mitigação de vieses nesses modelos.

Além das ferramentas, o tema ainda pode ser tratado através do estabelecimento de planos de governança específicos que visam definir métricas de acompanhamento e redução de vieses. Esse plano deve contemplar três frentes: primeiro, diagnosticar o cenário atual, mapeando o ambiente regulatório (LGPD, Bacen, Marco Legal da IA, quando houver etc.) e identificando pontos críticos de viés nos fluxos internos; segundo, definir metas e métricas de conformidade, estabelecendo indicadores claros para monitorar a equidade ao longo do ciclo de vida dos modelos; e, por fim, especificar processos e responsabilidades, detalhando checkpoints de auditoria, práticas de MLOps e mecanismos de governança que assegurem transparência, explicabilidade e mitigação contínua de vieses.

22. Quais diretrizes devem orientar o uso de IA generativa e machine learning em análises de risco, validação de identidade e detecção de comportamentos suspeitos?

No contexto de crédito e prevenção a fraudes, há uma predominância de utilização de modelos de inteligência artificial tradicional, uma vez que a prioridade é a geração de uma probabilidade que auxiliará na decisão de concessão de crédito ou de medidas de mitigação para prevenção à fraude. Dessa forma, já existem diretrizes bem definidas e consolidadas para técnicas de machine learning utilizadas nesses meios, como a utilização de métodos de explicabilidade (SHAP Values e Lime), a definição de políticas internas e determinações do Bacen sobre variáveis utilizáveis em cada um desses contextos, estabelecimento de formas de monitoramento de performance desses

modelos, com previsões de escalonamento e revisão, e possibilidade de contestação de decisões automatizadas.

Em relação à IA Generativa, apesar de, atualmente, possuir pouca aplicação no campo de crédito e de prevenção à fraude, já existem, também, ferramentas e técnicas que auxiliam na avaliação das interações geradas pelos modelos em fatores como segurança, privacidade, viés, toxicidade e ataque. Como exemplos, existem frameworks que elencam os principais riscos no uso de modelos de IA Generativa[1], ferramentas de avaliações retroalimentadas pelos próprios modelos de IA Generativa[2] e técnicas que podem ser aplicadas no próprio desenvolvimento dos modelos que aumentam a sua acurácia, eficiência e robustez[3]. De maneira geral, esse conjunto orienta um uso responsável de modelos de IA generativa, e se alinha com práticas e regulações já existentes, como privacidade *by design*, Lei Geral de Proteção de Dados (LGPD) e o *AI Act* Europeu. Além disso, vale ressaltar que, quando aplicável, no início do desenvolvimento, pode haver um fluxo de supervisão humana do resultado desses modelos para a construção de conjuntos de dados verdadeiros e verificados (*ground truth*) para incrementar a robustez dessas técnicas e ferramentas empregadas.

Portanto, de forma geral, devem ser observados os princípios éticos, transparência, segurança, privacidade e conformidade regulatória, realizando validação dos modelos, com testes de desempenho, vieses e robustez e assegurando a aderência às normas e regulamentos (ex: LGPD, Bacen).

23. **Como equilibrar transparência e explicabilidade com segredos de negócio?**

A transparência não pode extrapolar limites de segredos comerciais e/ou expor informações que possam comprometer a segurança ou a eficácia do tratamento, do titular, da instituição e/ou do modelo. A disponibilização de informações deve se ater a explicações básicas referentes ao modelo utilizado – por exemplo: objetivo do modelo, fatores que mais influenciaram a decisão, limites e salvaguardas, sem expor parâmetros, regras operacionais e sinais antifraude que comprometam a efetividade. Essas diretrizes

[1] *"Risk Taxonomy, Mitigation, and Assessment Benchmarks of Large Language Model Systems"*, de Tianyu Cui, Yanling Wang, Chuanpu Fu, Yong Xiao, Sijia Li, Xinhao Deng, Yunpeng Liu, Qinglin Zhang, Ziyi Qiu, Peiyang Li, Zhixing Tan, Junwu Xiong, Xinyu Kong, Zujie Wen, Ke Xu, Qi Li. Acessado em https://arxiv.org/html/2401.05778v1, em 30 de dezembro de 2025.

[2] *"Buffer of Thoughts: Thought-Augmented Reasoning with Large Language Models"*, de Ling Yang, Zhaochen Yu, Tianjun Zhang, Shiyi Cao, Minkai Xu, Wentao Zhang, Joseph E. Gonzalez, Bin Cui. Acessado em https://arxiv.org/pdf/2406.04271, em 30 de dezembro de 2025.

[3] *"Meta-Rewarding Language Models: Self-Improving Alignment with LLM-as-a-Meta-Judge"*, de Tianhao Wu, Weizhe Yuan, Olga Golovneva, Jing Xu, Yuandong Tian, Jiantao Jiao, Jason Weston, Sainbayar Sukhbaatar, acessado emhttps://arxiv.org/pdf/2407.19594, em 30 de dezembro de 2025.

já são amplamente difundidas em modelos de crédito e prevenção à fraude, em que há uma governança interna específica para cuidar, revisar e validar esses modelos e que permite uma definição clara dos níveis de informação que podem ser disponibilizados ao público geral sem comprometer a segurança desses modelos.

De forma geral, o equilíbrio entre transparência, explicabilidade e a proteção de segredos de negócio exige uma abordagem estruturada, baseada em princípios de governança, confidencialidade e comunicação responsável. Para garantir os direitos dos titulares de dados e, ao mesmo tempo, proteger informações estratégicas e sensíveis, exemplifica-se algumas formas:

- Políticas claras de transparência: Disponibilizar informações objetivas sobre a existência dos modelos automatizados e finalidades, critérios gerais de decisão e direitos dos titulares, sem expor detalhes técnicos, algoritmos proprietários ou parâmetros sensíveis que possam comprometer a segurança ou a competitividade da instituição.
- Comunicação acessível: Utilizar canais de atendimento e documentos explicativos que permitam ao titular compreender, de forma clara e resumida, como suas informações são utilizadas e quais são as salvaguardas implementadas, sem revelar informações confidenciais ou estratégicas.
- Segregação de informações: Garantir que relatórios de explicabilidade e respostas a titulares sejam elaborados de modo a separar informações essenciais para o exercício de direitos daqueles dados classificados como segredo de negócio, conforme contratos e políticas internas de confidencialidade.
- Justificativas: Quando a divulgação de determinada informação puder comprometer segredos comerciais, apresentar justificativas fundamentadas, alinhadas à legislação e aos contratos, explicando os limites da transparência e os motivos da restrição.
- Treinamento e governança: Capacitar equipes para identificar informações sensíveis e aplicar corretamente as políticas de confidencialidade, além de manter processos de revisão e auditoria para garantir o cumprimento das obrigações legais e contratuais.

D4Sign by ZUCCHETTI

19 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 21 de January de 2026, 15:42:50

ntp.br

ED-0003 - Compilado - GT 5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO A FRAUDES - Abecs e FBB final 1
Código do documento 437022f8-7fb9-4a07-9f61-a7e86798e30c

Assinaturas

Luis Vicente Magni De Chiara
vicente.dechiara@febraban.org.br
Assinou

ROBERTA GASPAR BUSO
roberta.buso@febraban.org.br
Assinou

Marcelo Takeyama
marcelot@abecs.org.br
Assinou

Eventos do documento

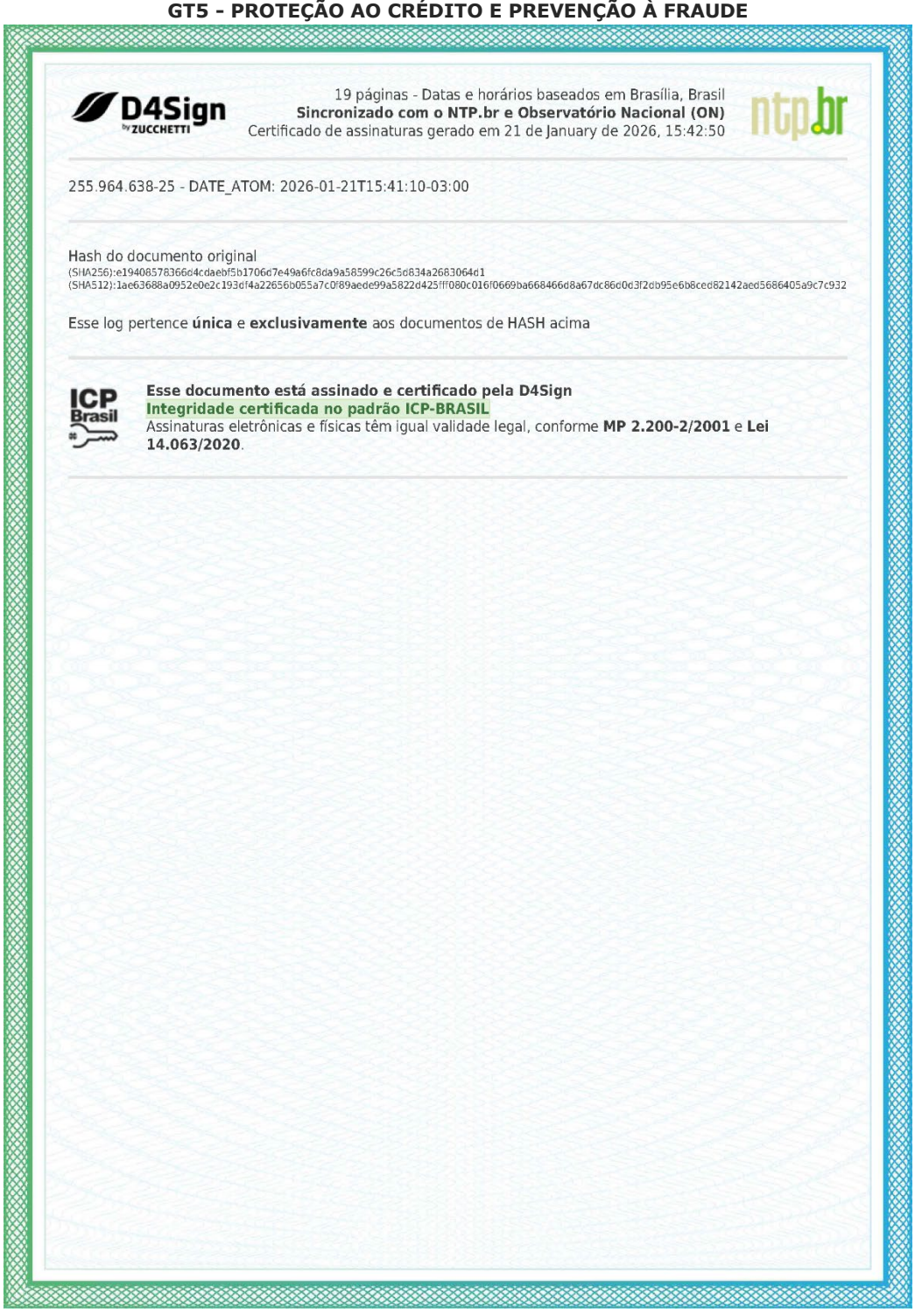
20 Jan 2026, 09:48:22
Documento 437022f8-7fb9-4a07-9f61-a7e86798e30c **criado** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). Email:paula.mesquita@febraban.org.br. - DATE_ATOM: 2026-01-20T09:48:22-03:00

20 Jan 2026, 09:51:37
Assinaturas **iniciadas** por PAULA MESQUITA (9ce8a91a-16d2-4874-ab0e-0a0538f2bc0b). Email: paula.mesquita@febraban.org.br. - DATE_ATOM: 2026-01-20T09:51:37-03:00

20 Jan 2026, 11:05:32
LUIS VICENTE MAGNI DE CHIARA **Assinou** - Email: vicente.dechiara@febraban.org.br - IP: 18.228.157.120 (ec2-18-228-157-120.sa-east-1.compute.amazonaws.com porta: 12256) - Documento de identificação informado: 293.346.478-09 - DATE_ATOM: 2026-01-20T11:05:32-03:00

20 Jan 2026, 21:30:08
ROBERTA GASPAR BUSO **Assinou** (5ddcce9a-9c5d-493b-92ca-05a9e2f52f9c) - Email: roberta.buso@febraban.org.br - IP: 18.228.157.120 (ec2-18-228-157-120.sa-east-1.compute.amazonaws.com porta: 47020) - Documento de identificação informado: 306.633.378-79 - DATE_ATOM: 2026-01-20T21:30:08-03:00

21 Jan 2026, 15:41:10
MARCELO TAKEYAMA **Assinou** - Email: marcelot@abecs.org.br - IP: 200.212.179.66 (200.212.179.66 porta: 23060) - Geolocalização: -23.594853863906113 -46.68107307847902 - Documento de identificação informado:



D4Sign by ZUCCHETTI

19 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 21 de January de 2026, 15:42:50

ntp.br

255.964.638-25 - DATE_ATOM: 2026-01-21T15:41:10-03:00

Hash do documento original
(SHA256):e194085783666d4cdaebf5b1706d7e49a6fc8da9a58599c26c5d834a2683064d1
(SHA512):1ae63688a0952e0e2c193df4a22656b055a7c0f89aede99a5822d425fff080c016f0669ba668466d8a67dc86c0d3f2db95e6b8ced82142aed5686405a9c7c932

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

ICP Brasil

Esse documento está assinado e certificado pela D4Sign
Integridade certificada no padrão ICP-BRASIL
Assinaturas eletrônicas e físicas têm igual validade legal, conforme **MP 2.200-2/2001** e **Lei 14.063/2020**.

ANEXO XVI – Resposta Zetta

Zetta

Proteção ao Crédito e Prevenção à Fraude envolvendo Dados Pessoais

Brasília (DF), 21 de janeiro de 2025

A **Zetta**, associação que representa empresas de tecnologia constituídas como plataformas de serviços financeiros digitais, vem, por meio do presente documento, encaminhar suas contribuições ao Grupo de Trabalho instituído pela Portaria CNPD nº 05/2025, dedicado ao desenvolvimento de proposições sobre Proteção ao Crédito e Prevenção à Fraude envolvendo Dados Pessoais, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD).

As manifestações aqui apresentadas são elaboradas em resposta ao Ofício encaminhado a esta associação, que convidou a Zetta a contribuir com os estudos do referido Grupo de Trabalho por meio do envio de posicionamentos técnicos e institucionais, organizados a partir dos blocos temáticos propostos.

A Zetta agradece a oportunidade de colaborar com o CNPD em tema de elevada relevância para o ecossistema digital e financeiro, especialmente no que se refere à promoção da proteção de dados pessoais, à prevenção de fraudes e ao adequado funcionamento dos instrumentos de proteção ao crédito, à luz da Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normas aplicáveis.

Além das respostas objetivas aos questionamentos formulados, a Zetta se reserva o direito de indicar observações complementares e referências técnicas que entende contribuírem para o aprofundamento do debate, em consonância com a possibilidade expressamente indicada no Ofício.

Por fim, a associação registra ciência de que as contribuições encaminhadas poderão ser tornadas públicas como parte do anexo ao Relatório Final do GT5, em observância aos princípios de transparência que orientam a atuação do CNPD.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

Zetta

Sumário Executivo

O **crédito** é um pilar fundamental do desenvolvimento socioeconômico brasileiro, viabilizando consumo, investimento, inclusão financeira e redução de desigualdades. Em um sistema financeiro cada vez mais digital, sua oferta eficiente, segura e inclusiva depende do **tratamento responsável e proporcional de dados pessoais** ao longo de todo o ciclo de vida das operações de crédito.

A base legal de **proteção ao crédito** prevista no art. 7º, inciso X, da LGPD não se limita à análise pontual de inadimplência ou à atribuição de scores no momento da contratação. Trata-se de um **fluxo contínuo e integrado de gestão de risco**, que abrange desde a prospecção e oferta responsável, a verificação de identidade (KYC), a avaliação e o monitoramento do risco, a prevenção ao superendividamento, até as atividades de cobrança e recuperação de crédito.

Nesse contexto, no mercado financeiro e de pagamentos, a **prevenção à fraude** é **indissociável da proteção ao crédito**. Fraude e risco de crédito compartilham dados, infraestrutura tecnológica e modelos analíticos, pois a concessão de crédito a fraudadores, inclusive por meio de identidades sintéticas ou uso indevido de dados de terceiros, resulta inevitavelmente em inadimplência, perdas financeiras e aumento do risco sistêmico. Tratar fraude como finalidade autônoma gera ineficiências, eleva spreads e restringe o acesso ao crédito, afetando especialmente populações mais vulneráveis.

O uso combinado, proporcional e transparente de **dados tradicionais e informações relevantes** (cadastrais, comportamentais, contextuais e digitais), aliado a modelos avançados de **Inteligência Artificial**, é essencial para reduzir assimetrias informacionais, cumprir obrigações prudenciais do Banco Central, prevenir fraudes e ampliar a **inclusão financeira**, especialmente de indivíduos sem histórico bancário tradicional. Essa abordagem é compatível com a regulação prudencial brasileira, padrões internacionais (Basileia, OCDE, Banco Mundial) e a jurisprudência nacional.

Interpretações excessivamente restritivas da LGPD, que limitem a proteção ao crédito à análise estática de inadimplência, tendem a produzir efeitos adversos relevantes: aumento do custo do crédito, exclusão financeira, enfraquecimento da prevenção à fraude e maior risco sistêmico. Em contraste, uma **interpretação sistemática e finalística**, alinhada à Constituição, à legislação consumerista e à regulação financeira, permite conciliar proteção de dados, segurança jurídica, eficiência econômica e inovação.

Diante disso, a Zetta defende que a base legal de proteção ao crédito legitima o tratamento de dados pessoais necessário, proporcional e responsável para todas as atividades inerentes à gestão do risco de crédito, incluindo a prevenção à fraude, o monitoramento contínuo e a estabilidade do sistema financeiro, com adequada governança, transparência funcional e supervisão humana. Essa interpretação fortalece a confiança no ecossistema digital, promove a concorrência, reduz custos e contribui para um mercado de crédito mais justo, seguro e inclusivo no Brasil.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

Zetta

SUMÁRIO

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5 - PROTEÇÃO AO CRÉDITO E PREVENÇÃO À FRAUDE

Zetta

1) A importância socioeconômica do crédito e da prevenção à fraude para o Brasil

1.1) Qual é a relevância do crédito para o desenvolvimento socioeconômico do Brasil?

O crédito desempenha um papel essencial no desenvolvimento socioeconômico dos países, havendo ampla evidência empírica sobre esse assunto (ver Demirguç and Levine, 2008), seja com dados *cross-country*, seja com dados de séries temporais para países específicos. Em uma amostra com dados do BIS e do Banco Mundial para 40 países, incluindo o Brasil, a correlação entre PIB per capita e crédito ao setor privado é de 75% (dados de 2024, último ano disponível). No caso específico do Brasil, há uma correlação de cerca de 85% entre concessões reais de crédito para pessoas físicas e PIB. A importância do crédito deriva de diversos canais sobre a atividade econômica: maior consumo e investimento, maior inclusão financeira, redução de desigualdades regionais, aumento da competitividade no sistema bancário e impulsionamento de inovações tecnológicas.

Promoção da Inclusão Financeira

O acesso ao crédito facilita a inclusão financeira, especialmente nas regiões mais carentes, como o Norte e Nordeste, onde a penetração de serviços financeiros tradicionais é menor. Iniciativas como o Pix (sistema de pagamento instantâneo) desempenham um papel crucial nesse processo. A implementação do Pix ajudou a aumentar a participação de áreas historicamente desassistidas pelo sistema bancário, resultando em um aumento significativo na bancarização da população. Graças à transformação digital do sistema financeiro e do crédito, o número de usuários de serviços financeiros no Brasil cresceu de 76,3 milhões em 2018 para 163,3 milhões em 2025, representando um aumento de 114%[1]. Estudo feito por pesquisadores do BIS, com dados de 101 países, mostra que pagamentos digitais impulsionam a atividade econômica: cada aumento de 1 p.p. no uso desses meios está associado, em média, a um acréscimo de 0,1 p.p. na taxa de crescimento do PIB per capita em dois anos. A parcela de adultos que usa pagamentos digitais no Brasil passou de 57,9% em 2017 para 77,4% em 2024.

Redução de Assimetrias de Informação

O Cadastro Positivo e o Open Finance ajudam a reduzir a assimetria de informações no mercado de crédito, permitindo que consumidores e empresas de menor porte tenham mais acesso a crédito com melhores condições. Essas medidas são especialmente benéficas para os grupos mais vulneráveis e para pequenas e médias empresas, que antes enfrentavam dificuldades em acessar crédito devido à falta de dados financeiros históricos.

Pesquisas globais indicam que 70% das organizações que adotam Machine Learning avançado concordam que a melhoria na precisão permite ampliar o acesso ao crédito para consumidores que seriam rejeitados por modelos tradicionais. Além disso, o uso de dados alternativos (como pagamentos de serviços públicos e telecomunicações) processados por esses modelos é citado por 68% dos tomadores de decisão como fator chave para incluir segmentos desassistidos[2].

Aumento da Competitividade e Redução de Juros

A implementação de políticas de portabilidade de crédito e a regulamentação das fintechs aumentaram a concorrência no setor bancário. A maior competitividade entre instituições financeiras têm levado à redução das taxas de juros, com efeitos significativos na redução dos spreads bancários e na diminuição do custo do crédito, o que é benéfico para

[1] ZETTA; TENDÊNCIAS CONSULTORIA INTEGRADA. *Inovação e inclusão financeira: a revolução silenciosa do Banco Central do Brasil*. São Paulo, set. 2025. Estudo. Disponível em: https://somoszetta.org.br. Acesso em: 16/12/2025.

[2] HEATON, Paul. Machine Learning Divide in Credit Risk. In: RESPONSIBLE USE OF AI IN CREDIT RISK MANAGEMENT: Balancing Innovation, Risk, and Regulation. [S.l.]: International Committee on Credit Reporting (ICCR); World Bank Group, 16 dez. 2025. Apresentação de slides. Disponível mediante requisição. Baseado em pesquisa conduzida pela Forrester Consulting para a Experian em julho de 2025.

consumidores e empresas, especialmente para microempresas e negócios familiares. Estudo recente do Banco Central revelou que a portabilidade de crédito resultou em uma redução de 5% no spread bancário em municípios com mais de uma instituição financeira[3].

A precisão superior dos modelos de Inteligência Artificial não gera apenas benefícios operacionais, mas estabilidade sistêmica e eficiência de capital. Estudos indicam que a melhor predição de probabilidade de inadimplência (*Probability of Default - PD*) por modelos de ML pode gerar economias de capital regulatório entre 17% e 25%, liberando recursos para novas concessões de crédito e reduzindo perdas esperadas[4].

Impulso ao Crescimento Econômico

O crédito acessível também desempenha um papel vital no crescimento econômico ao facilitar o consumo e o investimento, o que se traduz em um aumento do PIB potencial. O crédito mais barato e mais acessível permite que famílias e empresas invistam em consumo e expansão, impulsionando a atividade econômica de maneira geral. Comparando a correlação entre a taxa de crescimento de cada uma das 12 atividades do Sistema de Contas Nacionais Trimestrais (IBGE) com a taxa de crescimento do consumo das famílias e da formação bruta de capital fixo (investimento) um ano à frente, nota-se que o desempenho da atividade financeira é o que tem correlação mais forte com o consumo e o investimento. Portanto, a atividade financeira – com grande destaque para a concessão de crédito – é aquela cujo desempenho, individualmente, antecipa melhor o comportamento dessas variáveis relevantes para a economia como um todo.

Inovações Tecnológicas e Novos Modelos de Negócios

A adoção de tecnologias de transformação digital, como a inteligência artificial, e o avanço das fintechs no Brasil têm levado à transformação do sistema financeiro. Isso não só melhora a eficiência das transações, mas também cria novas oportunidades de negócios, com menor custo e maior acessibilidade. As fintechs têm se mostrado particularmente eficazes em alcançar segmentos de mercado negligenciados pelos bancos tradicionais .

Plano de Ação Prático

Para continuar a promover o desenvolvimento socioeconômico por meio do crédito, o Brasil deve:

(a) Expandir ainda mais a implementação de infraestruturas públicas digitais como o Open Finance e o Pix, integrando o sistema financeiro a novas e mais diversas bases de dados públicas para melhorar o acesso a serviços financeiros digitais.

(b) Estimular a educação financeira para garantir que os consumidores façam pleno uso da portabilidade de crédito e outros benefícios de maior competitividade no mercado.

(c) Continuar apoiando e regulamentando fintechs para promover a inclusão financeira e reduzir as barreiras de entrada para novas empresas, especialmente em áreas menos atendidas.

(d) Aprofundar a digitalização do sistema financeiro, garantindo que as populações em áreas remotas ou de baixa renda tenham acesso a serviços financeiros modernos.

Essas iniciativas continuarão a fortalecer a economia brasileira e a reduzir desigualdades, tornando o sistema financeiro mais inclusivo, competitivo e eficiente.

---

[3] Idem.

[4] ALONSO-ROBISCO, Andrés. Artificial Intelligence and Credit Risk: Accuracy vs. Interpretability. In: RESPONSIBLE USE OF AI IN CREDIT RISK MANAGEMENT: Balancing Innovation, Risk, and Regulation. [S.l.]: International Committee on Credit Reporting (ICCR); World Bank Group, 16 dez. 2025. Apresentação de slides. Citando: ALONSO-ROBISCO, A.; CARBÓ, J. M. Machine learning in credit risk: measuring the economic impact. Banco de España Working Paper, 2022.

1.2) Qual é a relevância da prevenção à fraude para o desenvolvimento socioeconômico do Brasil?

No sistema financeiro brasileiro, a prevenção à fraude é um componente estrutural da gestão de risco de crédito. Fraudes aumentam perdas esperadas e inesperadas, elevam custos operacionais e de capital regulatório e, como consequência, pressionam o spread bancário e o custo final do crédito. Instituições com modelos antifraude maduros conseguem precificar melhor o risco, reduzir a inadimplência estrutural e ofertar crédito mais barato e sustentável.

Fraudes como falsidade ideológica, roubo de identidade, fraude documental, contas laranja e fraudes promovidas pelo próprio tomador impactam diretamente o risco de crédito, pois distorcem a avaliação da capacidade e da intenção de pagamento; geram inadimplência não associada a risco econômico real; contaminam bases históricas usadas em modelos de score. O resultado é o aumento artificial da perda esperada (*EL – Expected Loss*) da fórmula regulatória de gestão prudencial do risco da contraparte.

O custo do crédito incorpora, de forma simplificada, as taxas de juros como resultado do custo de captação, mais as despesas operacionais, mais as perdas esperadas, mais o custo de capital, mais a margem da instituição financeira. Portanto, as fraudes elevam principalmente as perdas esperadas que são calculadas pela multiplicação da 'probabilidade de inadimplência' (PD ou *Probability of Default*), pela 'perda em caso de inadimplência (LGD ou *Loss Given Default*) e pela 'exposição na inadimplência' (ED ou *Exposure at Default*).

A atividade de prevenção contra fraudes no fluxo de proteção ao crédito no contexto do mercado financeiro impacta, assim, nas despesas operacionais (investigação, *chargeback*, atendimento) e no custo de capital (maior volatilidade e risco residual), com efeitos sistêmicos no mercado de crédito tais como spreads mais altos para a carteira, inclusive para bons pagadores.

Quando a atividade de prevenção a fraudes no fluxo de proteção ao crédito não é executada de forma adequada — seja por falhas operacionais, seja, sobretudo, pela falta de acesso a dados de qualidade ou pela insegurança jurídica e regulatória no tratamento de dados pessoais relevantes para essas atividades —, clientes com bom perfil de crédito acabam por subsidiar operações com maior risco de inadimplência ou fraude. Como consequência, ocorre exclusão financeira, com a negativa cautelar de crédito, e os produtos financeiros tornam-se mais caros e restritivos. Esse cenário é especialmente relevante no Brasil, onde a assimetria de informação é elevada e uma parcela significativa da população possui histórico de crédito limitado.

Essas são as razões pelas quais a adequada mensuração do risco, habilitada pelo acesso a dados pessoais de qualidade, torna-se crucial para o desenvolvimento socioeconômico do Brasil.

2) Papel dos dados pessoais no ecossistema de crédito

2.1) Qual a importância dos dados pessoais para proteção do crédito e demais atividades relacionadas ao tema? Quais atividades vão além da atribuição do score de crédito?

Os dados pessoais são essenciais para a proteção do crédito porque viabilizam a gestão adequada, responsável e contínua do risco de crédito ao longo de todo o ciclo de vida da relação creditícia, e não apenas no momento da atribuição de um score.

Segundo o Estudo Técnico, sem o tratamento de dados pessoais (dados tradicionais e dados alternativos, que aqui denominaremos de dados relevantes na forma da regulação prudencial do sistema financeiro) não há como reduzir assimetrias de informação, prevenir fraudes, evitar o superendividamento, precificar corretamente o crédito nem preservar a estabilidade do sistema financeiro. Não há crédito sem conhecimento e não há conhecimento sem informação, e os dados pessoais são o principal insumo para a formação de confiança entre credor e tomador.

Os dados pessoais permitem a redução de assimetrias informacionais, um dos maiores

entraves ao acesso ao crédito, em especial para empréstimos sem garantia onde os dados são o verdadeiro "colateral" e é a modalidade que potencialmente é a mais acessível para a população. Os dados pessoais também permitem uma avaliação mais precisa do risco de inadimplência, indo além do histórico negativo, proporcionam mais inclusão financeira, especialmente para pessoas "invisíveis ao crédito", ou seja, sem histórico ou em ocupações informais. Os dados também possibilitam uma precificação mais justa, levando a taxas proporcionais ao risco real e habilitam as instituições a prevenir crises sistêmicas conforme exigências prudenciais do Banco Central do Brasil e padrões de Basileia.

Os dados pessoais podem ser classificados em dados tradicionais e dados relevantes. As informações tradicionais consistem no histórico de crédito, dados de SCR, birôs, inadimplência, dentre outros. Já as informações relevantes podem ser dados cadastrais, comportamentais, dados digitais, tais como presença na internet, dados de dispositivo e dados de contexto, além de outros dados que aumentam a capacidade preditiva de modelos de risco de crédito. Uma adequada proteção ao crédito exige o uso combinado e responsável desses dois grupos de dados.

O conceito jurídico-técnico de "proteção ao crédito" não se limita ao score ou à avaliação pontual de capacidade de pagamento. A proteção ao crédito é um fluxo contínuo, composto por várias etapas, todas legitimadas pela base legal do art. 7º, X, da LGPD. A tabela abaixo esquematiza as etapas desse fluxo:

Fluxo da proteção ao crédito					
Pré-aplicação	**Cadastro e autenticação (KYC/AML)**	**Avaliação do risco de inadimplência**	**Monitoramento do desempenho do crédito**	**Prevenção ao superendividamento**	**Cobrança e recuperação de crédito**
Direcionamento de ofertas adequadas ao perfil do consumidor Evita concessão irresponsável e garante cumprimento de regras de suitability	Verificação de identidade Prevenção de fraudes, uso de documentos falsos, e identidade de terceiros	Modelagem de risco mais ampla que o score Análise de renda, comportamento, contexto e exposição total	Identificação da deterioração da qualidade creditícia Revisões periódicas exigidas pelas normas prudenciais do BCB	Avaliação contínua do comprometimento de renda Cumprimento da Lei do Superendividamento e do CDC	Planejamento de estratégias de cobrança Estimativa de perdas esperadas Recuperação de ativos problemáticos

Portanto, a gestão do risco de crédito envolve uma série de atividades de tratamento de dados pessoais que vão além da mera verificação da capacidade de adimplemento contratual do consumidor. Ou seja, o score é apenas uma ferramenta, não a finalidade e inclui a noção de "proteção sistêmica" do crédito, num fluxo contínuo e multidisciplinar, abarcando atividades específicas de tratamento de dados com finalidades que convergem, sendo elas prevenção contra fraudes, gestão do risco sistêmico, governança, estabilidade financeira e interesse social.

2.2) Como o uso dos dados pessoais reduz assimetrias informacionais e impacta liquidez, inadimplência e eficiência de mercado?

Em mercados de crédito, dados pessoais reduzem assimetrias informacionais porque permitem estimar o risco de forma mais precisa e granular do que "médias" de grupo. Isso tem três efeitos econômicos principais:

a) **Liquidez**: a oferta de crédito e a velocidade de concessão tendem a aumentar com uma melhor mensuração de risco. Ou seja, mais tomadores "bons" deixam de ser tratados como "médios"e passam a receber propostas viáveis; além disso, processos ficam mais automatizáveis e portáveis (ex.: Open Finance com compartilhamento via APIs mediante autorização);

b) **Inadimplência:** A inadimplência tende a cair com informação compartilhada e histórico positivo, permitindo com que credores precifiquem e aprovem dentro de critérios prudenciais mais eficientes, disciplinando o comportamento com menos "apostas" no escuro.

c) **Eficiência:** A eficiência de mercado melhora. Spreads e perdas esperadas podem diminuir, a competição tende a aumentar com menor barreira de entrada informacional e o preço do crédito tende a convergir para curvas de risco mais realistas. No Brasil, o Banco Central estimou redução média de 10,4% no spread em crédito pessoal não consignado para novos tomadores quando havia pontuação no Cadastro Positivo em relação a consumidores sem pontuação[5].

Do ponto de vista jurídico-institucional, é relevante notar que a LGPD prevê base legal específica para "proteção do crédito", que autoriza o tratamento de dados pessoais sem consentimento, quando aplicável, o que sinaliza que o ordenamento reconhece o papel econômico do uso responsável desses dados, sem afastar princípios como finalidade, necessidade e transparência.

O acesso a dados pessoais diversos melhora a calibração de risco e reduz inadimplência, possibilitando o aumento de liquidez no mercado de crédito ao diminuir custos operacionais e incertezas, podendo resultar na queda de spreads bancários e no fomento à concorrência. O aumento do fluxo de informações exige contrapesos para evitar externalidades negativas. A eficiência econômica deve ser balanceada com a proteção à privacidade, respeitando a proporcionalidade e a finalidade dos dados conforme a LGPD, além de mitigar riscos de discriminação algorítmica e concentração de mercado. Para que a redução da assimetria gere valor real, é indispensável uma governança de dados e privacidade sólida que garanta a qualidade dos dados, a segurança da informação e mecanismos transparentes de contestação para o consumidor.

3) Papel dos dados pessoais na prevenção à fraude e outros ilícitos

3.1) Qual a importância dos dados pessoais para prevenção à fraude, outros ilícitos e demais atividades relacionadas?

A utilização de dados pessoais constitui elemento estrutural e indispensável das estratégias de prevenção à fraude, repressão a ilícitos e gestão de risco no sistema financeiro digital contemporâneo. Em um ambiente marcado pela digitalização intensiva dos serviços financeiros, a capacidade de verificar identidades, monitorar comportamentos e identificar anomalias em tempo real depende, de forma intrínseca, do tratamento responsável e tecnicamente qualificado de um conjunto amplo de dados, que extrapola informações cadastrais básicas..

A prevenção à fraude não se configura como um processo isolado, mas como parte indissociável da gestão do risco de crédito e do ciclo de vida de produtos financeiros. A separação rígida entre dados utilizados para análise de crédito e aqueles destinados à prevenção à fraude revela-se ineficaz na prática, uma vez que a concessão de crédito a fraudadores, inclusive por meio de uso de identidades sintéticas ou de terceiros, resulta, invariavelmente, em inadimplência e prejuízos sistêmicos. Assim, a verificação da autenticidade

[5] BANCO CENTRAL DO BRASIL. *Análise dos efeitos do Cadastro Positivo*. Brasília: Banco Central do Brasil, abril de 2021.

da identidade e da intenção do solicitante representa a primeira linha de defesa tanto da instituição financeira quanto do próprio titular dos dados.

Nesse contexto, o tratamento de dados pessoais é essencial para o cumprimento das obrigações regulatórias de Conheça Seu Cliente (KYC) e de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/CFT). Dados cadastrais, documentais e biométricos são fundamentais para mitigar riscos de falsidade ideológica, enquanto o uso de informações complementares e metadados, como endereço de IP, geolocalização, características do dispositivos e padrões comportamentais, permitem identificar inconsistências e sinais de fraude, com mudanças abruptas de localização ou uso de dispositivos atípicos.

A incorporação de técnicas de inteligência artificial e machine learning potencializa esse processo ao viabilizar a análise de volume relevante de dados transacionais e comportamentais, permitindo a detecção de anomalias e padrões ilícitos que seriam imperceptíveis à análise humana. Esses mecanismos são fundamentais para a identificação de fraudes em pagamentos, lavagem de dinheiro, financiamento ao terrorismo e ataques cibernéticos estruturados, inclusive aqueles baseados em engenharia social e cooptação de colaboradores.

O cenário brasileiro de segurança digital atingiu um nível crítico de sofisticação, conforme evidenciado por recentes operações policiais, como a operação "DeGenerative AI", conduzida pela Polícia Civil do Distrito Federal, que revelou a atuação de organizações criminosas especializadas no uso de deepfakes, biometria sintética e automação avançada para a prática de fraudes em larga escala, inclusive engenharia social. Esse contexto demonstra que a fraude contemporânea deixou de se restringir à falsificação documental tradicional, assumindo caráter sistêmico, cibernético e altamente tecnológico, baseado na exploração de vulnerabilidades digitais, especialmente vulnerabilidades comportamentais.Diante desse cenário, o tratamento estruturado, em múltiplas camadas de verificação, de dados pessoais torna-se condição necessária para a prevenção, detecção e mitigação de fraudes e outros ilícitos. A prevenção à fraude deixa, assim, de ser mera boa prática de mercado e passa a constituir requisito essencial à integridade, à continuidade e à confiança do sistema financeiro digital, com impactos diretos na proteção dos titulares de dados, na preservação da boa-fé nas relações econômicas e na mitigação de riscos sistêmicos.

Esse entendimento encontra respaldo nas políticas públicas federais e na regulação prudencial do Sistema Financeiro Nacional. Iniciativas do Ministério da Justiça e Segurança Pública, como o programa "Celular Seguro" e os acordos firmados no âmbito da Aliança de Combate a Fraudes Bancárias Digitais, reconhecem expressamente o tratamento de dados pessoais para fins de segurança e prevenção a fraudes como matéria de ordem pública, orientada à proteção do cidadão e do interesse coletivo. Tais iniciativas se estruturam sobre pilares com o aprimoramento contínuo dos mecanismos de prevenção, o compartilhamento responsável de dados entre agentes públicos e privados, o suporte às investigações, a capacitação institucional, e a promoção do letramento digital.

Em convergência, o Banco Central do Brasil, por meio da Resolução Conjunta nº 6/23, consolidou o entendimento de que as instituições do Sistema Financeiro Nacional devem implementar mecanismos estruturados de prevenção, detecção e mitigação de fraudes, incorporando essas medidas à governança corporativa, à gestão de riscos e à segurança operacional A norma reconhece a legitimidade do uso de dados pessoais de forma responsável, proporcional e tecnicamente fundamentada, em plena compatibilidade com a LGPD.

Dessa forma, tanto sob a ótica das políticas públicas, proteção de dados e da regulação setorial, evidencia-se que o tratamento de dados pessoais para fins de prevenção à fraude não apenas é relevante, mas constitui instrumento necessário para a tutela do interesse público, a proteção efetiva dos titulares de dados e a preservação da estabilidade e da confiança no sistema financeiro digital brasileiro. A viabilidade de um sistema de crédito e de serviços financeiros digitais seguros, eficientes e resilientes depende, de maneira indissociável, do tratamento responsável, proporcional e tecnicamente qualificado de dados pessoais, orientado à gestão de riscos e à prevenção de ilícitos.

3.2) Como dados comportamentais, biométricos e metadados contribuem para a identificação de riscos e mitigação de fraudes, golpes e outros ilícitos? Quais são os riscos de subutilizar dados pessoais em processos antifraude (ex.: aumento de chargebacks, fraude sintética, falsidade ideológica e riscos sistêmicos)?

O tratamento de dados comportamentais, biométricos e de metadados exerce papel central na identificação e mitigação de fraudes, golpes e outras práticas ilícitas, especialmente diante da crescente sofisticação das ameaças digitais, como deepfakes, fraudes sintéticas e o uso indevido de identidades digitais. Quando utilizados de forma responsável e em estrita observância aos princípios e às bases legais previstos na Lei Geral de Proteção de Dados (LGPD), esses dados constituem instrumentos essenciais para a segurança do sistema financeiro e digital, a proteção dos titulares de dados e a integridade das operações.

Esse entendimento encontra respaldo em experiências regulatórias internacionais consolidadas. No âmbito da União Europeia, a Strong Customer Authentication (SCA), prevista na Diretiva (UE) 2015/2366 (PSD2) e detalhada nos Regulatory Technical Standards (RTS) da Autoridade Bancária Europeia (EBA), estabelece a obrigatoriedade da autenticação forte do cliente em operações eletrônicas, baseada na combinação de ao menos dois fatores independentes (conhecimento, posse e inerência) incluindo, expressamente, elementos biométricos e comportamentais. A SCA reconhece que o uso estruturado e proporcional desses dados é condição necessária para elevar os padrões de segurança, reduzir fraudes e preservar a confiança no ecossistema financeiro digital.

A título exemplificativo, o uso de biometria para verificação de identidade contribui de maneira significativa para a prevenção de fraudes digitais e de ataques altamente sofisticados, incluindo aqueles baseados em deepfakes. Assim, a utilização desses dados para fins de prevenção à fraude e proteção do titular, desde que necessária, legítima e proporcional à finalidade específica, em conformidade com as diretrizes regulatórias nacionais e internacionais, bem como com orientações setoriais reconhecidas a exemplo da Cartilha sobre Dados Biométricos da Zetta[6], revela-se não apenas legítima, mas essencial.

A subutilização de dados pessoais em mecanismos de prevenção a fraudes pode gerar riscos relevantes à integridade do sistema financeiro e digital, dentre os quais se destacam:

(a) Aumento de chargebacks e perdas financeiras, uma vez que a ausência de dados robustos compromete a acurácia das análises e decisões relacionadas à verificação de transações;

(b) Fraude sintética, caracterizada pela combinação estruturada de dados reais com informações falsificadas para a criação de identidades parcialmente artificiais. A detecção desse tipo de fraude torna-se significativamente mais complexa na ausência não apenas de dados suficientes, mas também de tecnologias antifraude tecnicamente qualificadas e devidamente validadas. Sua mitigação efetiva demanda, além do uso responsável de dados pessoais robustos, a adoção de padrões técnicos capazes de reduzir vieses algorítmicos e de promover a adequada tropicalização das soluções tecnológicas à realidade demográfica, social e comportamental da população brasileira, marcada por elevada diversidade e assimetrias digitais;

(c) Falsidade ideológica, consistente na criação ou manipulação de documentos e identidades com o objetivo de ocultar ou distorcer a verdadeira identidade do titular;

(d) Riscos sistêmicos, incluindo a perda de confiança no sistema financeiro e digital, a maior exposição a ataques coordenados e recorrentes, bem como potenciais danos reputacionais e prejuízos econômicos de grande magnitude.

[6] ZETTA. *Dados Biométricos no Setor Financeiro e de Pagamentos*. STIVELBERG, D.; VAINZOF, R.; LIMA, C. (Orgs.). Disponível aqui.

4) Convergência entre proteção ao crédito e prevenção à fraude

4.1) O que evidencia que crédito e fraude compartilham fluxos, insumos e objetivos comuns no modelo atual de risco?

A evidência de que crédito e fraude compartilham fluxos, insumos e objetivos decorre da indissociabilidade técnica, operacional e econômica da gestão de riscos no modelo financeiro contemporâneo[7][8]. A separação rígida entre análise de crédito, tradicionalmente associada à capacidade de pagamento, e prevenção à fraude, voltada à autenticidade e à intenção do agente, mostra-se ineficaz na prática, uma vez que ambas convergem para o mesmo objetivo: garantir a solvabilidade das obrigações financeiras, mitigando perdas financeiras, a sustentabilidade do negócio[9] e a prevenção ao superendividamento.

No modelo moderno de risco adotado pelas instituições financeiras, crédito e fraude deixaram de ser domínios independentes porque avaliam o mesmo comportamento do cliente em tempo real, utilizam os mesmos dados, sinais e infraestrutura tecnológica e operam decisões sequenciais ou simultâneas sobre uma mesma transação. Na essência, a fraude representa o risco de não pagamento por intenção maliciosa, enquanto o risco de crédito reflete o não pagamento por incapacidade financeira, sendo ambos materializados nos mesmos eventos operacionais.

Essa integração se manifesta, primeiramente, nos fluxos de decisão. O gerenciamento de risco ocorre de forma orquestrada e contínua ao longo do ciclo de vida do crédito, desde a pré-aplicação e o onboarding até o monitoramento da carteira e a recuperação de ativos. A verificação de identidade e autenticidade constitui a etapa inicial e condicionante da concessão de crédito, uma vez que um crédito concedido a um fraudador resulta, inevitavelmente, em inadimplência. As decisões seguem uma lógica encadeada (identidade, autenticidade, intenção, capacidade, limite e precificação) em que a detecção de anomalias comportamentais durante o uso do produto serve tanto para bloquear fraudes quanto para identificar a deterioração da capacidade de pagamento.

A integração também é evidente nos insumos utilizados, especialmente dados e sinais comportamentais. Crédito e fraude se apoiam nas mesmas fontes centrais, diferenciando-se apenas pela hipótese causal associada ao risco. Dados de comportamento, histórico transacional, geolocalização, endereço de IP, características do dispositivo, padrões de uso e sinais de rede alimentam simultaneamente modelos de detecção de fraude e de avaliação de risco de crédito. Um mesmo sinal pode indicar comportamento fraudulento coordenado ou, alternativamente, instabilidade financeira e estresse de liquidez, demonstrando que o insumo é comum, embora a interpretação varie conforme o contexto.

No plano analítico e tecnológico, os modelos modernos convergem em forma e finalidade. Algoritmos de machine learning utilizam bases compartilhadas de dados e features para otimizar métricas econômicas agregadas, como perda esperada, taxa de aprovação, valor do ciclo de vida do cliente ajustado ao risco e margem líquida pós-perda. A ocorrência de fraude impacta diretamente indicadores clássicos de crédito, como a probabilidade de default observada, a severidade da perda e as curvas de desempenho da carteira, tornando impraticável avaliar a performance de crédito de forma dissociada do controle de fraude.

Por fim, a convergência se consolida nos objetivos estratégicos. O objetivo final não é minimizar fraude isoladamente nem maximizar aprovação de crédito de forma desarticulada, mas maximizar o valor econômico esperado com controle do risco total. Isso exige o equilíbrio entre fricção, crescimento e perdas, reconhecendo que decisões excessivamente restritivas reduzem

[7] BASEL COMMITTEE ON BANKING SUPERVISION (BCBS). *Basel Core Principles for Effective Banking Supervision*. BIS, 2012.

[8] BASEL COMMITTEE ON BANKING SUPERVISION (BCBS). *Principles for the Sound Management of Operational Risk*. BIS, 2011.

[9] SAUNDERS, Anthony; ALLEN, Linda. *Credit Risk Management in and out of the Financial Crisis*. Wiley, 2010.

fraude, mas aumentam chum e reduzem valor no longo prazo, enquanto decisões excessivamente permissivas ampliam crescimento à custa de inadimplência e fraudes. O trade-off, portanto, é global e não segmentado por silos organizacionais.

Na prática, essa visão integrada se materializa em arquiteturas unificadas de dados, com camadas compartilhadas de eventos e features, decisões orquestradas por regras e modelos encadeados ou em ensemble, métricas econômicas comuns entre crédito e fraude e mecanismos de aprendizado cruzado, nos quais eventos de fraude retroalimentam modelos de crédito e vice-versa.

Em síntese, no mercado financeiro crédito e fraude são faces de uma mesma lógica de gestão de riscos[10]: avaliam o mesmo cliente, no mesmo momento, com os mesmos dados, para decidir se é economicamente racional assumir determinado risco financeiro. A separação entre ambos é, em grande medida, uma convenção organizacional; a integração, por sua vez, constitui uma necessidade técnica, econômica e operacional do sistema financeiro moderno.

4.2) Quais são as consequências práticas de tratar essas finalidades como trilhas separadas?

Tratar proteção ao crédito e prevenção à fraude como trilhas independentes gera ineficiências operacionais, distorções econômicas e aumento de risco sistêmico. A separação artificial fragmenta fluxos decisórios que, na prática, avaliam o mesmo evento econômico, a saber, a solvabilidade de uma obrigação financeira, a partir de hipóteses distintas (incapacidade versus intenção maliciosa).

Do ponto de vista operacional, a segregação resulta em decisões inconsistentes e sequenciais não coordenadas, aumentando fricção, latência e custo por transação. Um crédito aprovado sem validação antifraude robusta tende a materializar inadimplência certa, enquanto bloqueios antifraude excessivamente conservadores reduzem a taxa de aprovação e inclusão financeira, mesmo para tomadores solventes.

Sob a ótica econômica, a fragmentação eleva perdas esperadas, custos operacionais duplicados e consumo de capital regulatório, pressionando spreads e afetando negativamente bons pagadores, que passam a subsidiar ineficiências do sistema. No agregado, essa abordagem amplia a exclusão financeira, reduz eficiência alocativa e compromete o equilíbrio entre crescimento, risco e estabilidade.

Do ponto de vista prudencial, a separação contraria os princípios de gestão integrada de riscos exigidos pelos Acordos de Basileia e pela regulação do Banco Central do Brasil, enfraquecendo a capacidade de detecção de riscos emergentes e ampliando vulnerabilidades sistêmicas[11].

5) Atividades e bases legais aplicáveis à proteção ao crédito

5.1) Quais atividades de tratamento podem ser englobadas na base legal de proteção do crédito?

A interpretação do art. 7º, inciso X, da LGPD indica que a base legal de proteção do crédito abrange um conjunto amplo e integrado de atividades de tratamento de dados pessoais, necessárias para viabilizar todo o ciclo de vida do crédito, e não apenas a análise pontual de inadimplência no momento da contratação.

[10] COSO. *Enterprise Risk Management – Integrating with Strategy and Performance*. 2017.

[11] BASEL COMMITTEE ON BANKING SUPERVISION. *Principles for the Sound Management of Operational Risk*. Basel: BIS, 2011; BASEL COMMITTEE ON BANKING SUPERVISION. *Basel Core Principles for Effective Banking Supervision*. Basel: BIS, 2012; COSO. *Enterprise Risk Management – Integrating with Strategy and Performance*. New York: COSO, 2017.

Sob uma leitura alinhada às normas prudenciais[12]/[13]/[14]/[15] do Conselho Monetário Nacional e do Banco Central do Brasil, a proteção do crédito compreende as etapas de prospecção responsável, concessão, gestão, monitoramento e recuperação do crédito, desde que o tratamento seja estritamente necessário, proporcional e compatível com a finalidade creditícia.

Nesse sentido, enquadram-se na base legal de proteção do crédito as seguintes atividades:

(a) a fase de **pré-aplicação e prospecção responsável**, voltada à oferta adequada de produtos de crédito conforme o perfil de risco do público-alvo, com o objetivo de evitar práticas predatórias e o superendividamento. Inclui-se aqui o uso de modelos estatísticos para cálculo de escores de conversão e direcionamento responsável e em linha com o perfil do consumidor para ofertas de crédito.

(b) na etapa de **concessão e onboarding**, são tratados dados para avaliação da capacidade de pagamento, análise de risco de inadimplência e verificação da autenticidade da identidade e do pleito do solicitante. Essa fase envolve o cálculo de escores de pedido (*application score*), a consulta a bureaus de crédito e a validação de informações cadastrais, inclusive com terceiras partes se necessário, sendo essencial para decisão sobre concessão, limites e condições do crédito.

(c) durante a **gestão e monitoramento do contrato**, o tratamento de dados permite o acompanhamento contínuo do comportamento de pagamento, a identificação de sinais de deterioração do perfil de risco e a revisão de limites de crédito. São utilizados, para esse fim, escores comportamentais (*behavioral scores*) e outros modelos preditivos voltados à prevenção da inadimplência e à sustentabilidade da relação creditícia.

(d) na fase da **cobrança e recuperação**, os dados pessoais subsidiam estratégias proporcionais de contrato, negociação e renegociação de dívidas, bem como o uso de escores de cobrança (*collection scores*), o registro e atualização de informações junto a sistemas de proteção ao crédito e o compartilhamento com empresas especializadas ou escritórios jurídicos, quando necessário à recuperação de valores legitimamente devidos.

A base legal também sustenta o desenvolvimento e uso de modelos estatísticos e de *credit scoring*, incluindo treinamento, teste e calibração de algoritmos de inteligência artificial e *machine learning*, com uso de dados históricos e atuais. Nesse contexto, é admissível o tratamento de dados alternativos ou "informações relevantes"[16], como histórico de pagamentos de serviços, dados de telecomunicações e sinais comportamentais, especialmente para viabilizar a inclusão financeira de pessoas sem histórico bancário tradicional, desde que observados os princípios da necessidade, transparência e não discriminação.

Além disso, integram o escopo da proteção do crédito as consultas e o enriquecimento de bases de dados, como o acesso ao Cadastro Positivo, bureaus de crédito e, quando

---

[12] BRASIL. Conselho Monetário Nacional. *Resolução CMN nº 4.557, de 23 de fevereiro de 2017. Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.* Diário Oficial da União, Brasília, DF, 01º mar. 2017.

[13] BRASIL. Conselho Monetário Nacional. *Resolução BCB nº 265, de 25 de novembro de 2022. Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de instituição classificada como Tipo 3 enquadrada no Segmento 2 – S2, Segmento 3 – S3 ou Segmento 4 – S4.* (Redação dada, a partir de 1º/1/2025, pela Resolução BCB nº 447, de 19/12/2024).

[14] BRASIL. Conselho Monetário Nacional. Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. (Redação dada pela Resolução CMN nº 5.274, de 18/12/2025).

[15] BRASIL. Banco Central do Brasil. Resolução Conjunta nº 6, de 23 de maio de 2023. Dispõe sobre requisitos para prevenção, detecção e mitigação de fraudes. Diário Oficial da União, Brasília, DF, 24 maio de 2023.

[16] Res. nº 4.557/17: "Art. 23. A estrutura de gerenciamento de que trata o art. 7º deve prever, adicionalmente, para o risco de crédito: (...) V - utilização de **informações relevantes** e consistentes para avaliação e mensuração do risco de crédito; Res. CMN nº 265/22: "Art. 21. A estrutura de gerenciamento de que trata o art. 5º deve prever, adicionalmente, para o risco de crédito: (...) V - utilização de **informações relevantes** e consistentes para avaliação e mensuração do risco de crédito; (...)".

tecnicamente justificado, a validação de informações junto a fontes externas para confirmação de renda, endereço ou identidade, sempre com foco na segurança e na mitigação de riscos da operação.

Embora a LGPD preveja base legal específica para prevenção à fraude, no contexto financeiro a prevenção à fraude é indissociável da proteção do crédito. A concessão de crédito a um fraudador resulta, necessariamente, em perda creditícia, de modo que a verificação da identidade, o uso de escores de fraude e de autenticidade e a detecção de comportamentos atípicos durante a solicitação de crédito integram a lógica de proteção do crédito e de gestão prudencial de riscos.

Registre-se que a Agência Nacional de Proteção de Dados (ANPD), em manifestações técnicas preliminares, como a Nota Técnica nº 19/2023, sinalizou interpretação mais restritiva da base legal, limitando-a à análise de risco de inadimplência no momento da contratação. Contudo, o setor financeiro sustenta que tal leitura não reflete a gestão integrada de riscos exigida pela regulação prudencial, podendo elevar o custo do crédito, comprometer a prevenção à inadimplência e dificultar a inclusão financeira. A posição técnica do setor defende o reconhecimento do ciclo completo do crédito — da prospecção responsável à cobrança — como escopo legítimo da base legal do art. 7º, X, da LGPD e, como decorrência, a legitimação do uso de informações relevantes e necessárias para o cumprimento adequado de todo o ciclo aqui descrito.

Em síntese, a base legal de proteção do crédito autoriza o tratamento de dados pessoais necessário para avaliar risco, conceder crédito, prevenir inadimplência, gerir contratos e recuperar valores devidos, desde que observados os princípios da finalidade, necessidade (que na regulação prudencial ganha contornos de "informações relevantes"), proporcionalidade, transparência, segurança e os direitos dos titulares, incluindo o direito à supervisão humana significativa e, quando for o caso, a revisão de decisões tomadas unicamente no tratamento automatizado de dados pessoais (ver mais sobre essa discussão no **item 9.1**). Essa interpretação é compatível com a LGPD, com a regulação do Sistema Financeiro Nacional e com a proteção do próprio titular de dados, ao assegurar um sistema de crédito mais seguro, responsável e sustentável.

5.2) Quais bases legais da LGPD suportam o tratamento de dados para análise e concessão do crédito?

O tratamento de dados pessoais para análise e concessão de crédito é sustentado por um conjunto integrado e complementar de bases legais da LGPD, cuja aplicação varia conforme a finalidade específica, o tipo de dado tratado e a etapa do ciclo de vida da relação creditícia.

A base legal estruturante é o art. 7º, X, da LGPD (proteção do crédito), que autoriza o tratamento de dados pessoais necessário à avaliação de risco, concessão, gestão, monitoramento e recuperação do crédito, em consonância com a regulação prudencial do Sistema Financeiro Nacional. Essa base abrange não apenas a análise de inadimplência, mas também atividades funcionalmente indissociáveis da integridade do crédito, como a prevenção à fraude em cadastros eletrônicos, a verificação de identidade, a validação da autenticidade das informações cadastrais e a mitigação de riscos de falsidade ideológica e uso indevido de identidades.

De forma complementar, aplicam-se as seguintes bases legais:

- Art. 7º, V (execução de contrato ou procedimentos preliminares), especialmente nas fases de onboarding e análise de propostas de crédito iniciadas pelo próprio titular;
- Art. 7º, II (cumprimento de obrigação legal ou regulatória), para tratamentos exigidos por normas do Banco Central do Brasil, do Conselho Monetário Nacional, pela legislação consumerista e por regras de KYC, PLD/CFT e segurança operacional;

- Art. 7º, IX (legítimo interesse), de forma subsidiária e condicionada à realização de teste de balanceamento, em atividades acessórias voltadas à prevenção do superendividamento, à melhoria contínua de modelos de risco e à governança do sistema;
- Art. 11, II, "g" (proteção do crédito), para o tratamento de dados pessoais sensíveis estritamente necessários à análise e concessão do crédito, bem como à prevenção à fraude em cadastros eletrônicos, à verificação de identidade e à segurança do titular, desde que observados controles reforçados de proporcionalidade, minimização, segurança e governança.

A inclusão do art. 11, II, "g", é particularmente relevante em contextos que envolvem dados biométricos e outros dados sensíveis utilizados para validação de identidade, autenticação e prevenção de fraudes, cuja finalidade última é assegurar a integridade do cadastro, a proteção do titular e a sustentabilidade da operação de crédito. O uso desses dados, contudo, deve observar salvaguardas técnicas e organizacionais reforçadas, em linha com as boas práticas setoriais consolidadas na Cartilha da Zetta sobre Tratamento de Dados Biométricos[17], que estabelece diretrizes de necessidade, adequação, segurança da informação, prevenção de vieses, transparência funcional e governança ao longo do ciclo de vida desses dados. Tais diretrizes reforçam a compatibilidade do uso responsável de biometria com a LGPD e com a regulação prudencial, especialmente quando orientado à proteção do titular e à integridade do sistema de crédito.

Essa leitura sistemática reflete a natureza integrada do risco de crédito no ambiente financeiro digital e assegura compatibilidade entre a LGPD, a regulação prudencial e o interesse público na estabilidade, eficiência e inclusão do sistema de crédito.

6) Bases legais aplicáveis à prevenção à fraude

6.1) Quais bases legais amparam o tratamento de dados pessoais para prevenção a fraudes?

O tratamento de dados pessoais para prevenção a fraudes é amparado por bases legais expressas e convergentes na LGPD e na regulação setorial. Assim, a depender do contexto, da natureza e do escopo da atividade de tratamento de dados, a base legal aplicável poderá ser a do Art. 7º, II, para cumprimento de obrigações legais e regulatórias de KYC, PLD/CFT e segurança operacional; a do Art. 7º, IX, quando presentes interesses legítimos relacionados à segurança do titular, prevenção de ilícitos e integridade do sistema, desde que respeitado o teste de balanceamento; a do Art. 7º, X, na medida em que a prevenção à fraude é indissociável da proteção do crédito no contexto financeiro; ou a base legal do Art. 11, II, "g", para tratamento de dados sensíveis estritamente necessários à prevenção à fraude e segurança do titular, como biometria, observadas salvaguardas reforçadas.

6.2) Como interpretar a base legal de prevenção à fraude à luz do interesse público, segurança dos titulares e estabilidade financeira?

A base legal de prevenção à fraude deve ser interpretada de forma teleológica, sistêmica e orientada ao interesse público, reconhecendo seu papel estruturante na proteção dos titulares de dados e na estabilidade do sistema financeiro.

A fraude digital contemporânea gera externalidades negativas relevantes: elevação de custos, exclusão financeira, deterioração da confiança e risco sistêmico. O tratamento responsável de dados pessoais para prevenção de fraudes não protege apenas a instituição, mas o próprio titular, evitando uso indevido de sua identidade, perdas financeiras e danos reputacionais.

Sob a ótica prudencial, a prevenção à fraude integra a gestão de riscos exigida pelo

[17] ZETTA. *Dados Biométricos no Setor Financeiro e de Pagamentos*. STIVELBERG, D.; VAINZOF, R.; LIMA, C. (Orgs.). Disponível aqui.

Banco Central e pelos padrões internacionais de supervisão, sendo condição para a resiliência operacional e financeira das instituições. A LGPD, ao prever bases legais específicas e princípios de proporcionalidade e necessidade, não pretende inviabilizar atividades essenciais à segurança econômica, mas sim disciplinálas.

Assim, a interpretação adequada deve conciliar proteção de dados, segurança jurídica e eficiência econômica, evitando leituras excessivamente restritivas que ampliem riscos sistêmicos e prejudiquem os próprios titulares.

7) Princípios da LGPD aplicáveis a ambos os contextos

7.1) Quais princípios devem orientar a coleta, uso, minimização, retenção e compartilhamento de dados nesses tratamentos?

O tratamento de dados pessoais no fluxo de proteção ao crédito deve observar princípios globais de uso responsável da tecnologia em relatórios de crédito, como por exemplo aqueles preconizados pelo Banco Mundial e pelo *International Committee on Credit Reporting* (ICCR). Estes incluem: Justiça (Fairness), assegurando que a tecnologia não discrimine grupos de consumidores; Responsabilidade (Accountability), garantindo governança sobre tecnologias internas e terceirizadas; Transparência, tornando as técnicas explicáveis e compreensíveis; e Segurança e Robustez, mantendo a integridade dos dados[18]. A aplicação desses princípios fortalece a conformidade com a LGPD e a confiança no sistema.

Adicionalmente, o uso de modelos e tecnologias analíticas no contexto de proteção ao crédito deve observar as diretrizes internacionais de Model Risk Management, conforme estabelecido pelos Acordos de Basileia[19] e pelas orientações de Supervisory Review (SR)[20] do Federal Reserve. Tais referenciais exigem que instituições financeiras implementem estruturas formais de governança de modelos, incluindo validação independente, monitoramento contínuo de desempenho, gestão de vieses, documentação completa e controles proporcionais ao impacto regulatório e ao risco do modelo. O alinhamento a essas práticas contribui para a mitigação de riscos prudenciais, reforça a transparência e a rastreabilidade das decisões automatizadas e complementa os princípios de uso responsável da tecnologia e de proteção de dados pessoais.

No contexto brasileiro, esses princípios encontram-se internalizados no arcabouço prudencial e regulatório por meio da Resolução CMN nº 4.557/2017, que institui a estrutura de gerenciamento de riscos e o processo de supervisão prudencial em linha com o Pilar 2 de Basileia; da Resolução CMN nº 4.658/2018, que estabelece requisitos de governança e segurança cibernética aplicáveis às infraestruturas tecnológicas e aos dados utilizados em modelos; bem como das Resoluções CMN nº 4.966/2021 e BCB nº 85/2021, que reforçam exigências de governança, validação, monitoramento e controle de modelos, inclusive no âmbito de risco operacional e de provisões baseadas em perda esperada. De forma complementar, a Lei nº 13.709/2018 (LGPD) assegura transparência e revisão de decisões automatizadas, fortalecendo a convergência entre o regime prudencial, a proteção de dados pessoais e o uso responsável de modelos analíticos no crédito.

---

[18] MASUNDA, Collen. ICCR paper on Responsible Use of Technology. In: RESPONSIBLE USE OF AI IN CREDIT RISK MANAGEMENT: Balancing Innovation, Risk, and Regulation. [S.l.]: International Committee on Credit Reporting (ICCR); World Bank Group, 16 dez. 2025. Apresentação de slides. Baseado no documento Responsible Use of Technology in Credit Reporting (White Paper), ICCR, 2022.

[19] BASEL COMMITTEE ON BANKING SUPERVISION. *Principles for effective risk data aggregation and risk reporting*. Basel: Bank for International Settlements, 2013; BASEL COMMITTEE ON BANKING SUPERVISION. *Supervisory guidance on model risk management*. Basel: Bank for International Settlements, 2023.

[20] BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM; OFFICE OF THE COMPTROLLER OF THE CURRENCY. *Supervisory guidance on model risk management (SR 11-7 / OCC 2011-12)*. Washington, D.C.: Federal Reserve System, 2011.

7.2) Como assegurar proporcionalidade, necessidade e adequação em modelos de risco integrados?

A proporcionalidade, a necessidade e a adequação no tratamento de dados pessoais em modelos integrados de crédito e prevenção à fraude não podem ser avaliadas de forma abstrata ou ex ante, por categorias fixas de dados, devendo ser analisadas caso a caso, à luz da atividade específica exercida dentro da finalidade geral do fluxo de proteção ao crédito.

O fluxo de proteção ao crédito compreende múltiplas atividades (como verificação de identidade, prevenção à fraude, avaliação de risco, monitoramento comportamental e prevenção ao superendividamento) cada uma com objetivos técnicos distintos, perfis de risco próprios e exigências informacionais específicas. A necessidade de um dado deve, portanto, ser aferida em relação à atividade concreta, e não de forma genérica ou dissociada do contexto operacional e econômico em que o tratamento ocorre.

Nesse sentido, uma abordagem regulatória excessivamente prescritiva, baseada em listas ex ante de dados permitidos ou proibidos, mostra-se inadequada em ambientes dinâmicos e intensivos em tecnologia. Um dado que não demonstra utilidade preditiva hoje pode tornar-se necessário amanhã, à medida que evoluem técnicas analíticas, padrões de fraude, modelos econométricos ou o próprio comportamento do mercado. A rigidez normativa tende a cristalizar ineficiências, reduzir acurácia, ampliar riscos sistêmicos e, paradoxalmente, prejudicar a proteção de direitos fundamentais ao elevar exclusão financeira e custos de crédito.

Por essa razão, a regulação deve assumir caráter essencialmente principiológico e funcional, orientada por critérios como finalidade legítima, relevância econômica, impacto sobre direitos fundamentais e mitigação de riscos, e não por categorias estáticas de dados. A verificação da necessidade e da proporcionalidade deve ocorrer ex post, com base em validações técnicas e econométricas, capazes de demonstrar se o uso do dado:

(a) melhora significativamente a acurácia do modelo;

(b) reduz fraude, inadimplência ou exclusão financeira; e

(c) não gera impactos discriminatórios desproporcionais.

Esse modelo é compatível com os referenciais internacionais de Model Risk Management e com a supervisão prudencial baseada em resultados, adotada pelos Acordos de Basileia, nos quais a legitimidade de modelos não decorre da natureza dos insumos isoladamente, mas da robustez dos controles, da performance observada e da mitigação de efeitos adversos.

Do ponto de vista da proteção de dados, essa abordagem reforça a tutela de direitos fundamentais, ao deslocar o foco do controle formalista para a avaliação concreta de impactos, exigindo governança, documentação, testes de vieses, auditoria e mecanismos de contestação eficazes. A proporcionalidade deixa de ser meramente declaratória e passa a ser empiricamente verificável, em consonância com o princípio da precaução substantiva.

Em síntese, assegurar proporcionalidade, necessidade e adequação em modelos integrados de risco exige uma regulação orientada por princípios, evidência empírica e controle ex post, capaz de acompanhar a evolução tecnológica sem comprometer a proteção dos titulares, a estabilidade do sistema financeiro e a eficiência econômica do crédito.

7.3) Como operacionalizar a transparência sem comprometer a efetividade de sistemas antifraude e de scoring?

A transparência deve ser funcional, contextual e orientada ao titular, e não técnica ou exaustiva. O dever de informar deve focar em categorias de dados, fatores relevantes de decisão e direitos de contestação, sem exigir a exposição de modelos, pesos ou regras específicas.

A abertura excessiva de lógica decisória compromete a segurança do sistema, facilita engenharia reversa e aumenta fraude ("gaming"). A transparência efetiva é aquela que permite

ao titular compreender impactos relevantes sobre sua vida financeira e exercer seus direitos, preservando a integridade, segurança e competitividade do sistema.

8) Governança, controles e segurança

8.1) Quais frameworks de governança e gestão de riscos são recomendados para operações de crédito e antifraude?

A governança e a gestão de riscos em operações de crédito e prevenção à fraude devem se apoiar em frameworks integrados, reconhecidos internacionalmente e compatíveis com a regulação prudencial, capazes de endereçar, de forma coordenada, riscos financeiros, operacionais, tecnológicos, cibernéticos, algorítmicos e de direitos fundamentais.

No plano da gestão integrada de riscos corporativos e financeiros, destacam-se:

(a) os Acordos de Basileia, especialmente o Pilar 2, que exige estrutura formal de gerenciamento de riscos, definição de apetite a risco, testes de estresse e supervisão contínua;

(b) o COSO Enterprise Risk Management (ERM), que integra risco, estratégia e desempenho organizacional;

(c) a ISO 31000, que estabelece princípios e diretrizes para a gestão transversal de riscos, aplicável a riscos financeiros, operacionais e tecnológicos.

No que se refere à governança de modelos, dados e sistemas analíticos, recomenda-se a adoção de:

(a) o Model Risk Management Framework (SR 11-7), utilizado por autoridades supervisoras para validação independente, monitoramento contínuo, controle de vieses e gestão do ciclo de vida de modelos estatísticos e de machine learning;

(b) o NIST Artificial Intelligence Risk Management Framework (AI RMF), que fornece diretrizes estruturadas para identificação, avaliação, mitigação e governança de riscos associados a sistemas de IA, incluindo riscos de opacidade, robustez, viés, segurança e impactos adversos sobre direitos fundamentais, adotando abordagem baseada em risco, princípios e resultados, compatível com controle ex post.

No campo da segurança da informação e cibersegurança, essenciais para a integridade do crédito e a prevenção de fraudes digitais, são especialmente relevantes:

(a) ISO/IEC 27001, como framework central de gestão de segurança da informação;

(b) ISO/IEC 27002, que detalha controles de segurança da informação aplicáveis a ambientes financeiros e digitais;

(c) ISO/IEC 27005, voltada à gestão de riscos de segurança da informação;

(d) ISO/IEC 27032, específica para diretrizes de cibersegurança em ambientes interconectados;

(e) ISO/IEC 27701, que estende a ISO 27001 para a gestão de privacidade e proteção de dados pessoais;

(f) ISO 22301, para gestão de continuidade de negócios e resiliência operacional, especialmente relevante para incidentes cibernéticos de larga escala.

A adoção combinada desses frameworks permite às instituições estruturar uma governança robusta, coerente com as exigências do Banco Central do Brasil, da LGPD e de padrões internacionais, assegurando accountability, rastreabilidade, resiliência operacional e proteção efetiva dos titulares, sem comprometer eficiência, inovação e inclusão financeira.

8.2) Quais controles técnicos e administrativos devem ser implementados para assegurar segurança da informação e mitigação de incidentes?

Devem ser implementados controles integrados de governança, risco e tecnologia, alinhados à regulação prudencial, à LGPD e a padrões internacionais, com foco em prevenção, detecção e resposta a incidentes.

Controles Administrativos e de Governança

(a) Modelo de Três Linhas de Defesa: Segregação clara entre gestão operacional, funções independentes de risco/compliance e auditoria interna (Res. CMN nº 4.557/2017), garantindo *accountability* e supervisão contínua.

(b) Supervisão Humana Significativa (Human-on-the-loop): Acompanhamento humano em todo o ciclo de vida dos modelos (concepção, treinamento, validação e monitoramento), mitigando vieses, falhas algorítmicas e riscos legais, em linha com as práticas de Model Risk Management.

(c) Ética e Mitigação de Vieses: Validações periódicas para identificar e corrigir discriminações indevidas, assegurando que decisões automatizadas ou semi-automatizadas sejam justas, inclusivas e éticas.

(d) Responsabilização e Governança de Terceiros: Políticas formais de accountability para tecnologias internas e fornecedores, exigindo padrões de segurança e controles equivalentes.

Controles Técnicos e Operacionais

(a) Monitoramento Contínuo e Resposta em Tempo Real: Uso de IA para detecção proativa de anomalias, fraudes e ataques cibernéticos, com capacidade de resposta automatizada em milissegundos para reduzir perdas e riscos sistêmicos.

(b) Verificação em Múltiplas Camadas e Privacy by Design: Combinação de biometria e análise comportamental integrada a técnicas de preservação de privacidade (como criptografia e anonimização), prevenindo identidades sintéticas conforme boas práticas internacionais.

(c) Explicabilidade e Transparência: Implementação de técnicas que permitam interpretar as decisões dos modelos, garantindo o direito do titular à revisão e explicação de decisões automatizadas, conforme preconiza a LGPD.

(d) Testes de Estresse e Robustez: Avaliação periódica com dados sintéticos para validar a resiliência frente a cenários adversos e mudanças de padrão de fraude, assegurando estabilidade operacional.

(e) Gestão de Risco Cibernético: Adoção de frameworks (ISO/IEC 27001/27002) e conformidade com as políticas de segurança cibernética do CMN/BCB, garantindo a tríade CID (Confidencialidade, Integridade e Disponibilidade).

8.3) Como estruturar políticas de retenção, registro de logs, auditoria e accountability?

(a) Políticas de retenção e registro de logs (rastreabilidade): Registro completo do ciclo de decisão pela manutenção de logs que permitam reconstruir integralmente decisões automatizadas, incluindo inputs relevantes, versão do modelo, parâmetros, regras vigentes e output, conforme boas práticas de Model Risk Management e exigências de auditoria prudencial.

(b) Gestão do ciclo de vida dos dados: retenção alinhada a prazos legais, regulatórios e prescricionais do setor financeiro (auditoria, prevenção à fraude e supervisão), com descarte seguro ou anonimização quando cessada a finalidade, em observância aos princípios da necessidade e proporcionalidade da LGPD.

(c) Accountability e documentação: Responsabilidade por tecnologias internas e terceirizadas: adoção de governança que assegure accountability integral sobre modelos, dados e decisões, inclusive de fornecedores, com contratos prevendo padrões de segurança, transparência funcional e direito de auditoria, conforme princípios do ICCR e regulação prudencial.

(d) Documentação de modelos: produção e atualização de documentação de Model Risk Management, relatórios regulatórios, registros de validação e evidências de conformidade.

(e) Auditoria e monitoramento contínuo: Auditorias periódicas de performance e vieses por meio de testes recorrentes de acurácia, estabilidade e detecção de *data drift* e *model drift*, com foco em impactos discriminatórios e deterioração de performance, em linha com exigências de supervisão prudencial e princípios da LGPD.

9) Decisões automatizadas e Inteligência Artificial

9.1) Quais são as decisões automatizadas mais comuns em crédito e antifraude?

As decisões automatizadas ou semi-automatizadas mais comuns nos setores de crédito e antifraude cobrem todo o ciclo de vida do relacionamento com o cliente, desde a prospecção até a recuperação de ativos. Essas decisões são sustentadas por modelos estatísticos, *Machine Learning* (ML) e, mais recentemente, modelos fundacionais e/ou Inteligência Artificial Generativa (GenAI).

Nem toda decisão suportada por sistemas de IA será totalmente automatizada, dependendo muito da realidade operacional da instituição. O mercado financeiro é submetido a uma carga regulatória significativa. Em especial para decisões de crédito e prevenção à fraudes. As normas setoriais exigem governanças adequadas para a gestão do risco tecnológico e de outros riscos associados e integrados com o uso de IA em atividades finalísticas como crédito.

Assim, além de governanças específicas com requisitos sobre validações de modelos, avaliações de capacidade preditiva, obrigações de perfilamento, análises de vieses, relatórios de impacto de privacidade e supervisão com auditoria, as instituições ainda estão submetidas à supervisão de reguladores especializados, como o próprio Banco Central (no caso de crédito), a Comissão de Valores Mobiliários (CVM) (no caso de distribuição em mercados) e a Agência Nacional de Proteção de Dados (ANPD) para o uso de dados pessoais, dentre outros. Portanto, as decisões suportadas por modelos de IA nunca ocorrem num vácuo de governança ou supervisão, sendo complexo afirmar tratarem-se de decisões unicamente automatizadas.

Independentemente disso, e como exposto anteriormente, as decisões de negócio no ciclo de vida da proteção ao crédito perseguem uma finalidade única (garantir a solvabilidade das obrigações financeiras), subdividida em diversas atividades parciais cujas decisões convergem para esse fim. São elas:

(a) **verificação de identidade e autenticidade (*onboarding*):** no momento do cadastro, sistemas de IA podem apoiar em decisões sobre se a identidade apresentada é genuína, cruzando dados cadastrais, biometria e informações do dispositivo para prevenir pleitos fraudulentos de crédito via identidade sintética ou uso de documentos falsos.

(b) **aprovação ou rejeição de propostas:** com base no escore de risco e nas políticas da instituição, o sistema apoia em decisões sobre concessão ou negativa de crédito. Evidência empírica indica que modelos de aprendizado de máquina, como *Random Forest* e *XGBoost*, superam métodos tradicionais, incluindo regressão logística, na predição de inadimplência, apresentando maior acurácia preditiva e melhor

desempenho[21].

(c) **definição de limites de crédito:** algoritmos determinam o valor máximo de crédito a ser concedido (ex: limite do cartão). O uso de IA permite ajustar esses limites de forma dinâmica; modelos mais sofisticados podem sugerir aumentos de limites para clientes com bom comportamento que, em modelos tradicionais, teriam limites menores[22/23].

(d) **precificação ajustada ao risco (taxa de juros):** trata-se de decisão sobre qual taxa de juros aplicar a um cliente específico. Sistemas avançados permitem a personalização das taxas, oferecendo condições melhores para perfis de menor risco e ajustando o preço para compensar riscos mais elevados.

(e) **recomendação de produtos (*cross-sell/up-sell*):** modelos analisam o perfil do cliente para decidir qual produto financeiro oferecer e em que momento (ex.: oferta de empréstimo pessoal), aumentando as taxas de conversão.

(f) **detecção de fraudes em tempo real:** monitoramento contínuo de transações para decidir, em milissegundos, se uma operação deve ser aprovada, bloqueada ou enviada para análise humana. Isso envolve identificar anomalias no comportamento transacional e padrões de ataque.

(g) **gestão de cobrança e recuperação:** decisões sobre qual estratégia de cobrança utilizar para clientes inadimplentes (qual canal usar, qual oferta de negociação executar), visando maximizar recuperação de ativos.

Na prática, a distinção entre análise de crédito e prevenção à fraude é tênue, pois ambas visam proteger a instituição financeira de perdas e garantir a segurança do titular da conta (e dos dados). Uma decisão suportada por sistemas de IA que seja eficaz, deve incluir, intrinsecamente, a verificação de autenticidade para evitar a concessão de empréstimos a fraudadores, o que resultaria em inadimplência certa. O uso de IA Generativa tem expandido essas capacidades, permitindo a análise de dados não estruturados (como textos e imagens de documentos) para refinar tanto as decisões de crédito quanto a detecção de fraudes complexas, como *deep fakes*[24].

9.2) Como lidar com explicabilidade, governança algorítmica e mitigação de vieses nesses modelos?

Para lidar com os desafios de explicabilidade, governança algorítmica e mitigação de vieses em modelos de IA para crédito, a Zetta recomenda ao Conselho Nacional de Proteção de Dados (CNPD) uma abordagem fundamentada na precaução substantiva e na análise de impacto baseada em resultados. A exigência de transparência absoluta ou de revisão humana para cada decisão automatizada pode inviabilizar o uso de tecnologias que, comprovadamente, promovem a inclusão financeira.

Recomendamos, assim, uma abordagem baseada em três pilares: (1) explicabilidade focada em "por que importa" e não "como funciona"; (2) reconhecimento do papel da supervisão humana e institucional na governança de algoritmos; (3) mitigação de vieses e inclusão via dados alternativos.

Explicabilidade

A explicabilidade exigida pelo Art. 20 da LGPD não deve ser interpretada como a necessidade de explicar a causalidade de cada dado utilizado, mas sim de fornecer informações úteis sobre a lógica da decisão.

(a) Modelos avançados de *Machine Learning* (ML) e *Deep Learning* muitas vezes operam

[21] AGARWAL, Sumit et al. *Financial Inclusion and Alternate Credit Scoring for the Millennials: Role of Big Data and Machine Learning in Fintech*. 2020, p. 21–25; Tabela 8.

[22] TRINDADE, André; HORTA, Lucca. *O valor dos dados de mídia social para o setor financeiro*. Manuscrito não publicado, 2024.

[23] ALLIANCE FOR FINANCIAL INCLUSION. *Alternative data for credit scoring*. Kuala Lumpur: AFI, 2025, p. 3; p. 18–19.

[24] WORLD ECONOMIC FORUM. *Artificial intelligence in financial services*. Geneva: World Economic Forum, 2025, p. 8–10; p. 15–16.

como "caixas-pretas", identificando correlações estatísticas complexas que não possuem uma explicação intuitiva ou causal imediata para humanos. Exigir uma justificativa causal para cada input (ex: por que a compra de um item específico ou o horário de uso do celular afeta o score) pode degradar a acurácia do modelo e impedir a descoberta de padrões que favorecem a inclusão de quem não tem histórico bancário tradicional.

Embora modelos fundacionais apresentem maior complexidade técnica, o uso dessas tecnologias não implica, por si só, a impossibilidade de explicação ou supervisão adequada. O potencial trade-off entre desempenho e interpretabilidade permanece reconhecido em nível conceitual, porém pode ser substancialmente mitigado por meio de uma arquitetura de controles adequada, delimitação clara de escopo, mecanismos de explicação funcional e supervisão humana proporcional ao risco[25].

(b) Foco na acurácia e benefício social: Assim como na medicina, onde sistemas de IA diagnosticam doenças com alta precisão sem que se possa explicar causalmente cada pixel da imagem analisada, no crédito deve-se priorizar a confiabilidade do resultado (acurácia na predição de inadimplência) e o benefício social (concessão de crédito) em detrimento de uma explicabilidade técnica detalhada que é muitas vezes inatingível e ineficaz.

(c) Informação Significativa: A transparência deve focar em informar ao titular as categorias de dados que influenciaram a decisão e os principais fatores de risco, permitindo o contraditório, sem exigir a abertura do código-fonte ou da fórmula matemática, protegendo o segredo comercial e evitando a manipulação do sistema (*gaming*).

Governança

É crucial distinguir entre revisão humana de cada decisão individual e a supervisão humana do sistema como um todo. A regulação deveria priorizar a segunda.

(d) Exigir revisão humana para cada decisão (como a concessão de um microcrédito ou o aumento de um limite de cartão) é operacionalmente inviável e pode anular os ganhos de escala e eficiência que permitem a redução de custos e taxas de juros. Em muitos casos, a revisão humana é menos precisa e mais enviesada que a decisão algorítmica.

(e) Modelo de Três Linhas de Defesa: As instituições financeiras já operam sob rigorosos regulamentos do Banco Central (Resolução CMN nº 4.557/2017) que exigem uma estrutura de gerenciamento de riscos robusta. Isso inclui a definição de apetite de risco, testes de estresse e auditoria interna, garantindo que os modelos sejam monitorados continuamente quanto à sua performance e segurança.

(f) Human-on-the-loop: A governança deve focar na supervisão humana durante o cido de vida do modelo (concepção, treinamento, validação e monitoramento), garantindo que ele opere dentro de parâmetros éticos e legais, em vez de intervir em cada transação individual ("human-in-the-loop").

Inclusão

O uso de IA e dados alternativos é a ferramenta mais eficaz para corrigir os vieses de exclusão presentes no sistema financeiro tradicional.

[25] A literatura econômica recente do Banco de Espanha demonstra que o trade-off entre precisão e interpretabilidade pode ser mitigado. O uso de modelos de ML restritos (ex: restrições de monotonicidade) permite manter alta capacidade preditiva — superior aos modelos tradicionais — preservando a interpretabilidade necessária para a supervisão. Além disso, técnicas post-hoc como SHAP (Shapley values) e LIME podem ser empregadas para oferecer explicações locais sobre decisões específicas, cumprindo o requisito de transparência funcional sem expor segredos industriais complexos. (ALONSO-ROBISCO, Andrés. Artificial Intelligence and Credit Risk: Accuracy vs. Interpretability. In: RESPONSIBLE USE OF AI IN CREDIT RISK MANAGEMENT: Balancing Innovation, Risk, and Regulation. [S.l.]: International Committee on Credit Reporting (ICCR); World Bank Group; Banco de España, 16 dez. 2025. Apresentação de slides disponível mediante requisição.

(g) Estudos demonstram que modelos de crédito baseados apenas em dados tradicionais (bureaus) tendem a excluir populações jovens, de baixa renda e minorias. A incorporação de dados alternativos (como pagamentos de varejo, telecomunicações, dentre outros) via IA aumenta a taxa de aprovação para clientes sem histórico bancário ("*thin-files*") de 16% para até 48%, sem aumentar significativamente a inadimplência[26].

(h) A avaliação de vieses deve focar nos resultados (impacto desproporcional) e não apenas nos inputs. Testes de estresse e monitoramento contínuo devem ser utilizados para identificar se o modelo está perpetuando discriminações históricas, permitindo ajustes nos parâmetros ou nos dados de treinamento[27].

Em síntese, a Zetta entende que a regulação de sistemas de IA aplicados ao crédito deve buscar um equilíbrio pragmático entre proteção de direitos, inovação tecnológica e promoção da inclusão financeira. Uma interpretação excessivamente formalista da explicabilidade ou a imposição de revisão humana caso a caso tende a produzir efeitos contraproducentes, restringindo o acesso ao crédito justamente para os grupos historicamente excluídos.

Ao adotar uma abordagem orientada por resultados, ancorada na precaução substantiva, na supervisão humana contínua e em mecanismos robustos de governança já consolidados no sistema financeiro, o CNPD pode assegurar transparência significativa, mitigação efetiva de vieses e proteção ao titular de dados, sem inviabilizar modelos que demonstram ganhos claros de eficiência, acurácia e impacto social positivo. Essa escolha regulatória é essencial para que a IA seja não apenas compatível com a LGPD, mas também um instrumento legítimo de inclusão, concorrência e desenvolvimento econômico.

9.3) Como equilibrar transparência e explicabilidade com segredos de negócio?

O equilíbrio entre transparência, explicabilidade e segredo de negócio no uso de técnicas de *Machine Learning* (ML) e inteligência artificial (IA) para crédito deve ser alcançado por meio da transparência funcional e da precaução substantiva[28]. A abertura irrestrita de algoritmos ou a exigência de explicações causais detalhadas para cada dado pode inviabilizar modelos matemáticos complexos que são motores da inclusão financeira e da redução de custos no Brasil.

A capacidade de processar dados via IA é diferencial que permite às empresas de tecnologia financeira operarem com custos mais baixos e maior alcance. Em 2024, o volume de crédito concedido por fintechs cresceu 68%, atingindo R$ 35,5 bilhões. No mesmo período, 67% dessas empresas passaram a desenvolver ou estudar soluções baseadas em IA, mais que o dobro do observado no ano anterior[29]. A automação e o uso de IA, ao reduzirem custos operacionais entre 20% e 40%, contribuem para que fintechs operem com estruturas mais eficientes, o que se reflete em taxas de juros mais competitivas em relação ao mercado tradicional[30].

Ademais, evidências indicam que a entrada e expansão de fintechs intensificam a concorrência no setor financeiro, pressionando o mercado em geral a reduzir spreads e margens. Estimativas do FMI apontam reduções da ordem de até 2,9 pontos percentuais em contextos comparáveis, com reflexos positivos sobre as taxas de juros ao consumidor. Esses

[26] LEE, Jung Youn; YANG, Joonhyuk; ANDERSON, Eric T. *Who benefits from alternative data for credit scoring? Evidence from Peru*. SSRN Working Paper, 2025, p. 11–13; p. 22–24.

[27] ZETTA. *A revolução dos entrantes: competitividade e inclusão financeira*. São Paulo: Zetta, 2022, p. 22–25; p. 32–35; p. 78–79.

[28] MARANHÃO, Juliano. *A proteção de dados à luz da IA responsável: a Lei Geral de Proteção de Dados sob a ótica da Inteligência Artificial Responsável*. [S.l.: s.n.], 2025.

[29] PWC Brasil; ABCD - Associação Brasileira de Crédito Digital. *Pesquisa Fintechs de Crédito Digital 2025:* inovação e maturidade diante de novos desafios. São Paulo: PwC Brasil; ABCD, 2025.

[30] SERVIÇO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS (SEBRAE). *Relatório de inteligência: impacto das novas tecnologias no acesso ao crédito*. Curitiba: Sebrae/PR, 2025.

efeitos reforçam a importância da preservação da inteligência competitiva e do segredo de negócio como instrumentos de promoção de concorrência e eficiência no mercado financeiro[31].

A exigência de "explicar tudo" (causalidade entre cada dado e a decisão) é tecnicamente incompatível com modelos avançados de ML, que identificam correlações não intuitivas para humanos mas altamente preditivas. Assim como a IA descobriu novos antibióticos através de padrões moleculares que humanos até hoje não conseguem explicar causalmente[32], modelos de crédito podem identificar padrões de solvência em dados alternativos que não possuem uma relação de causa e efeito óbvia, mas que favorecem a inclusão de quem não tem histórico bancário.

A regulação, nesse sentido, deve adotar a "precaução substantiva": se o modelo é acurado, não discriminatório e amplia o acesso ao crédito (o resultado social), a falta de uma explicação detalhada sobre como cada variável interna interage (o processo) não deve ser impedimento para seu uso. Exigir a explicabilidade total forçaria o uso de modelos estatísticos rudimentares, prejudicando a precisão e a inclusão.

A base legal da proteção ao crédito (art. 7º, X, LGPD), portanto, não deve ser limitada apenas à análise de inadimplência (score). A gestão de risco integrada é um processo contínuo que inclui a prevenção a fraudes (verificação de identidade e autenticidade), o monitoramento e a cobrança quando necessário. Dados demonstram que o uso de informações comportamentais e de dispositivos (fingerprinting) podem ser fundamentais para o avanço da eficácia das medidas de prevenção contra fraudes, protegendo tanto a instituição quanto o titular dos dados.

Para garantir transparência sem expor segredos comerciais, a segurança e a higidez do sistema financeiro, reputamos relevante que, antes da regulamentação da base legal da proteção ao crédito e da regulamentação sobre decisões automatizadas (Art. 20, LGPD), a ANPD e o BCB conduzam uma análise de impacto regulatório via sandbox, testando se as exigências de explicabilidade propostas são tecnicamente viáveis sem limitar a capacidade preditiva dos modelos, uma obrigação regulatória decorrente das normas prudenciais do próprio sistema financeiro[33].

Ademais, é importante que a regulamentação reconheça e legitime os procedimentos de priorização de supervisão humana relevante, a exemplo das políticas de riscos que preveem monitoramento contínuo de performance e vieses por equipes técnicas, em vez de revisões humanas individualizadas caso a caso, em homenagem ao princípio da precaução substantiva. Uma exigência de revisão humana caso a caso é impraticável em escala e muitas vezes menos precisa que a decisão suportada por máquina.

A transparência deve ser funcional e efetiva, permitindo que o cidadão se informe sobre as categorias de dados que podem impactar sua vida financeira para que ele possa gerenciar seu comportamento, sem exigir a abertura do "código-fonte" da modelagem de risco, algo ininteligível. Os modelos de crédito são ativos intelectuais essenciais para a competição e a redução de juros no Brasil.

---

[31] ASSOCIAÇÃO BRASILEIRA DE FINTECHS; ASSOCIAÇÃO BRASILEIRA DE CRÉDITO DIGITAL; AMPP; ZETTA. *Fintechs em fatos, não em versões*. [S.l.: s.n.], [2024 ou 2025].

[32] KISSINGER, Henry A.; SCHMIDT, Eric; HUTTENLOCHER, Daniel. *The age of AI: and our human future*. Paperback edition. London: John Murray Publishers, 2022, p. 9–11.

[33] NOGUEIRA, Rafaela; STIVELBERG, Daniel. *O futuro do crédito: como garantir que decisões automatizadas sejam justas e transparentes*. JOTA, 06 nov. 2025. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-futuro-do-credito-como-garantir-que-decisoes-automatizadas-sejam-justas-e-transparentes. Acesso em: 28 de dezembro de 2025.