PROTEÇÃO DE DADOS
E SEGURANÇA
CIBERNÉTICA PARA

COOPERATIVAS DE CRÉDITOS

Chenut

Nos últimos anos, as cooperativas de crédito têm desempenhado um papel cada vez mais importante no cenário financeiro, oferecendo uma alternativa sólida e confiável aos serviços bancários tradicionais. No entanto, com o crescimento do uso da tecnologia digital, surgem desafios complexos relacionados à proteção de dados pessoais, segurança cibernética e conformidade regulatória.

Neste e-book, que é fruto do compromisso do Chenut em fornecer informações atualizadas e relevantes, abordaremos tópicos essenciais que impactam diretamente as cooperativas de crédito no contexto jurídico atual: as determinações do BACEN, as boas práticas para o uso de inteligência artificial, as diretrizes legais aplicáveis ao marketing das cooperativas e as medidas de segurança da informação que devem ser implementadas.

Esperamos que este material forneça orientações práticas para as cooperativas de crédito enfrentarem os desafios jurídicos em um ambiente digital em constante evolução.

Estamos comprometidos em apoiar as cooperativas em sua jornada.

01 PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA PARA COOPERATIVAS DE CRÉDITOS

- A Resolução nº 4.658 do BACEN, a segurança cibernética e a proteção de dados
- Uso de decisões automatizadas e inteligência artificial para concessão de crédito
- Marketing: o que pode ou não ser feito na divulgação de produtos e serviços para cooperados?

02 O QUE NÃO PODE FALTAR PARA A SEGURANÇA DA INFORMAÇÃO?

03 O CHENUT

Proteção de dados e segurança
cibernética para cooperativas de créditos

A RESOLUÇÃO Nº 4.658 DO BACEN, A SEGURANÇA CIBERNÉTICA E A PROTEÇÃO DE DADOS

Testemunhamos nos últimos anos uma ascensão notável das discussões sobre regulação da proteção de dados pessoais no setor bancário, o qual cotidianamente processa um grande volume de dados financeiros. À medida que as instituições bancárias continuam a integrar tecnologias avançadas e coletar informações críticas de seus clientes, as preocupações com a segurança e privacidade desses dados têm aumentado consideravelmente.

Com o advento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) em 2018, as instituições financeiras tiveram que adequar suas práticas para assegurar o respeito à privacidade e estabelecer um nível adequação de proteção em seus ambientes. No entanto, para além da LGPD, o Banco Central do Brasil (BACEN) publicou também em 2018 a Resolução nº 4.658.

O propósito dessa resolução é estabelecer parâmetros de segurança e proteção de dados pessoais a serem observados pelas instituições autorizadas a funcionar pelo BACEN. Para tal, a resolução esclarece requisitos que devem ser observados nos programa de segurança cibernética e proteção de dados do setor bancário.

Além dos cuidados que uma instituição bancária deve ter em relação aos dados pessoais, os parâmetros de segurança devem ser estendidos a terceiros prestadores de serviços que, em decorrência de suas atividades, possam ter livre acesso aos dados. Nesse sentido, a resolução também estabelece critérios a serem observados na contratação de serviços de processamento e armazenamento de dados, inclusive aqueles de computação em nuvem.

Em seu papel de órgão regulador do sistema financeiro no Brasil, o BACEN historicamente atribui grande ênfase à responsabilidade das instituições financeiras. Em suas resoluções, o BACEN estabelece rigorosos requisitos de conformidade, controles internos e medidas de segurança para garantir que as instituições financeiras cumpram suas obrigações e protejam os interesses dos clientes, bem como a estabilidade do sistema financeiro como um todo.

No tema de segurança cibernética e proteção de dados, a postura do BACEN é igualmente severa: a resolução determina que na contratação de prestadores de serviços, a instituição contratante é responsável pela confiabilidade, integridade, disponibilidade, segurança e sigilo dos dados, bem como pelo cumprimento da legislação.

Ao considerar o impacto disso nas operações diárias das cooperativas de crédito, é fundamental focar a atenção em alguns aspectos específicos da resolução. Quanto à Política de Segurança Cibernética, a resolução determina que cooperativas de crédito podem adotar política de segurança cibernética única. Dessa forma, a definição e implementação de medidas de segurança pode ser feita de forma centralizada.

No mais, responsabilidades como cumprir com exigências regulatórias do BACEN (como relatórios anuais e comunicações formais exigidas na resolução) e atualizar anualmente a política (de forma a manter o nível de segurança da cooperativa à par do desenvolvimento tecnológico) podem ser concentradas no órgão central.

Dado que o órgão central detém uma série de responsabilidades cruciais relacionadas à segurança cibernética e à proteção de dados, é imperativo estabelecer um plano sólido para garantir o cumprimento das exigências regulatórias às quais as cooperativas de crédito estão sujeitas. A crescente complexidade das ameaças cibernéticas e a necessidade de proteger informações financeiras críticas tornam essas medidas de conformidade uma prioridade.

Esse planejamento estratégico não apenas ajuda a fortalecer a segurança das cooperativas, mas também a manter a confiança dos cooperados. No entanto, é fundamental notar que algumas medidas dependem da implementação no nível micro – ou seja, no dia a dia de cada cooperativa e com respeito a suas particularidades (considerando, por exemplo, o volume de cooperados e a cultura institucional).

Dentre essas medidas, podemos citar a conscientização dos funcionários nos temas de segurança da informação e proteção de dados pessoais. O desconhecimento das equipes quanto aos riscos de segurança e os cuidados a serem observados contribui para que ataques de engenharia social sejam um dos tipos mais comuns de ataque cibernético e uma das principais causas de incidentes de segurança.

Esses ataques geralmente consistem no envio de conteúdos com o objetivo de convencer a pessoa a clicar em um link ou fazer download de um arquivo, permitindo assim a entrada de invasores em seu computador. Assim, para evitar incidentes de segurança ou vazamentos de dados pessoais, é fundamental assegurar que as equipes tenham conhecimento das regras e boas práticas a serem observadas no dia a dia.

Quando se trata de incidentes, outra importante ação a ser conduzida por cada cooperativa consiste justamente em garantir que todos os colaboradores saibam identificar suspeitas de incidente e como agir nessa situação.

Infelizmente, incidentes de segurança acontecem. Considerando a sensibilidade das operações realizadas no setor bancário, é fundamental que em uma situação de incidente, a resposta seja rápida e organizada. Para que isso se concretize, é essencial que as equipes estejam plenamente preparadas e devidamente instruídas.

Ademais, as cooperativas devem ser capazes de ter um olhar crítico para sua operação em termos de segurança e proteção de dados. Esses temas têm evoluído rapidamente no sentido técnico e no sentido regulatório. A cada ano, novos entendimentos da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e do BACEN se consolidam no assunto.

Nesse contexto, verificar periodicamente as práticas de segurança cibernética e proteção de dados pessoais é fundamental para que as cooperativas se mantenham sempre em conformidade com as exigências do setor.

Segurança cibernética e proteção de dados pessoais são peças-chave na busca da excelência em segurança para as cooperativas. Garantir que todas as medidas estejam atualizadas e alinhadas com as regulamentações vigentes não apenas fortalece a confiança dos membros e parceiros, mas também ajuda a construir uma reputação sólida em um cenário cada vez mais digital e interconectado.

Proteção de dados e segurança
cibernética para cooperativas de créditos

USO DE DECISÕES AUTOMATIZADAS E INTELIGÊNCIA ARTIFICIAL PARA CONCESSÃO DE CRÉDITO

O uso de inteligências artificiais e softwares de decisões automatizadas revolucionou a tomada de decisão sobre concessão de crédito por instituições bancárias.

A decisão acerca de para quais pessoas conceder crédito e em qual valor e as análises de risco nela implicadas tem um passado reconhecidamente burocrático. O processo envolvia uma ampla coleta de dados de diversas fontes. Os riscos relacionados à oferta de crédito eram analisados de forma manual para cada solicitante e a decisão final era tomada caso a caso.

Atualmente, instituições bancárias em todo o mundo implementam sistemas automatizados que são capazes de processar uma massiva quantidade de dados e regras por segundo. Para além da mera automatização do trabalho humano, a utilização de inteligências artificiais e outras técnicas de machine learning permite a correlação de padrões de forma detalhada e minuciosa, elevando o grau de acurácia das decisões. Em termos de oferta de crédito, decisões mais acuradas significam menos riscos assumidos.

Com essas novas tecnologias, um processo de tomada de decisão arriscado, que historicamente demandou uma imensa quantidade de tempo e burocracia das instituições bancárias, pode ser feito em questão de minutos.

Tempo é, certamente, uma unidade bastante relevante no atendimento no setor financeiro. Em especial quando observamos a proposta das cooperativas de crédito, que propõe justamente um atendimento humanizado e uma aproximação aos cooperados, situação em que a celeridade na tomada de decisão pode ser fundamental para assegurar um bom atendimento.

No entanto, a implementação de toda tecnologia deve considerar os riscos de sua utilização. No caso de tecnologias de tomada de decisões de crédito automatizadas, os riscos jurídicos em termos de proteção de dados pessoais e atendimento às exigências regulatórias do BACEN devem ser compreendidos. O que muda no dia a dia das cooperativas?

Em primeiro momento, cabe relembrar que a LGPD garante aos titulares o direito à revisão de decisões automatizadas que possam afetar seus interesses, incluindo menção explícita a decisões sobre o perfil de crédito.

Embora a ANPD não tenha emitido regulamentações adicionais sobre o tema, as cooperativas podem receber a qualquer momento uma solicitação de exercício desse direito. Assim, é importante assegurar a possibilidade de revisão humana da solicitação de crédito e da decisão automatizada em prazo razoável.

Além disso, os consumidores podem solicitar informações sobre os critérios e procedimentos utilizados no processo de tomada de decisão automatizada. Neste caso, será necessário fornecer informações claras e adequadas mediante solicitação, porém sempre protegendo e não revelando segredos de negócio.

É importante notar que, tratando-se de tecnologias de inteligência artificial orientadas por quantidades massivas de dados e por um reconhecimento de padrões oriundo de aprendizados na fase de treinamento da inteligência artificial, os critérios decisórios nem sempre podem ser facilmente compreendidos. Estes são desafios que devem ser considerados quando se utilizando tais tecnologias.

De forma ampla, um dos princípios da LGPD é a transparência. De acordo com esse princípio, devem ser garantidas informações claras, precisas e acessíveis sobre o uso de dados aos titulares, que devem ser informados sobre as finalidades de utilização de seus dados e a forma de tratamento. Desta feita, quando da utilização de decisões automatizadas em um processo de análise de crédito, é fundamental incluir essa informação na Política de Privacidade ou em outro documento ou nota de caráter informativo.

Para além da transmissão de informações e do atendimento ao direito de revisão, alguns outros critérios devem ser observados para utilização dessas tecnologias em conformidade com a legislação de proteção de dados e as regulamentações do BACEN.

Considerando que parte significativa dos softwares e sistemas de decisões automatizadas são terceirizados, é fundamental assegurar que o fornecedor esteja em conformidade com a legislação e possui medidas de segurança adequadas para realizar o tratamento de dados pessoais pretendido.

Cabe ressaltar, conforme regulamentação do BACEN, que instituições bancárias podem ser responsabilizadas pelos serviços prestados por correspondentes (prestadores de serviços em geral) e devem assegurar a integridade, a confiabilidade, a segurança e o sigilo das transações realizadas por terceiros sob sua contratação.

Para além do estabelecimento de contrato contendo os requisitos mínimos de segurança, recomenda-se auditar previamente à contratação e periodicamente os fornecedores em termos de proteção de dados e segurança da informação. Além disso, é fundamental assegurar que as bases de dados estejam devidamente treinadas – compreendendo qual a origem dos dados utilizados e como ocorreu o processo de treinamento, até mesmo para evitar vieses indesejados na tomada de decisão.

A inovação representada pelo uso dessas tecnologias não pode ser ignorada. No entanto, os riscos existem e devem ser tratados. Ao centralizar a responsabilidade nas instituições financeiras, o BACEN exige papel ativo dessas instituições na tomada das medidas de segurança e conformidade necessárias para utilização dessas tecnologias.

Proteção de dados e segurança
cibernética para cooperativas de créditos

MARKETING: O QUE PODE OU NÃO SER FEITO NA DIVULGAÇÃO DE PRODUTOS E SERVIÇOS PARA COOPERADOS?

O relacionamento com associados é parte da essência das cooperativas de crédito. Nesse ramo, setores de comunicação e divulgação em todo o Brasil implicam seus esforços na manutenção de um relacionamento ativo, transparente e personalizado com os associados.

Diferentemente do marketing voltado para busca de novos cooperados, os associados já possuem uma relação com a cooperativa. Se por um lado, a importância de um bom relacionamento nesse contexto torna-se maior, por outro é inegável a ampliação das possibilidades de comunicação e personalização do atendimento.

Parte significativa dessas possibilidades relacionam-se diretamente ao fato de que a cooperativa já possui uma série de informações sobre o cooperado, incluindo canais de contato (e-mail, aplicativo) e informações sobre a vida financeira do cooperado que permitem a individualização do atendimento.

Para além do fácil acesso ao cooperado, torna-se possível delinear qual o perfil de cada pessoa (por suas movimentações financeiras) e direcionar ofertas de produtos e serviços pelos quais ela possa se interessar. Com a tecnologia e o uso das informações disponíveis, as ações de marketing e divulgação ganham um caráter personalizado para cada cooperado, permitindo uma especialização dessas ações jamais vista antes no setor bancário.

Hoje em dia, a grande maioria dos aplicativos bancários já possui seções de divulgação: “adquira X reais de crédito” ou “invista no rendimento Y”. Essas abordagens são justamente tentativas personalizadas, inclusive em termos de valores, de buscar adesão dos cooperados a novos produtos e serviços.

No entanto, o que diz a LGPD sobre essa prática? Quais questões devemos levar em consideração ao realizar ações de divulgação com os cooperados?

Primeiramente, não podemos cair na falsa sensação de que, como os cooperados já cederam seus dados pessoais para a cooperativa, podemos utilizá-los livremente e para qualquer finalidade. É fundamental observar alguns pontos de atenção quando realizamos esse tipo de uso “secundário” de dados, ou seja, utilizamos os dados coletados anteriormente para uma nova finalidade (marketing e divulgação), diversa da que motivou a coleta (abertura da conta pelo cooperado, por exemplo).

A regra de ouro da LGPD é a transparência. Uma das principais exigências dessa lei é justamente que as cooperativas informem, de forma clara e acessível, para quais finalidades utilizam os dados pessoais de seus cooperados.

Informações específicas sobre quais as formas de tratamento de dados relacionadas a ações de divulgação e marketing de novos produtos devem constar na Política de Privacidade, a qual deve ser disponibilizada no site e no aplicativo, em locais de fácil acesso. Recomenda-se, sempre que possível, obter o aceite nesta Política. O uso de notinhas de privacidade simplificadas que direcionem à Política também é uma boa prática recomendada.

Para além da divulgação na interface do próprio aplicativo, conforme exemplificado acima, também é comum que o associado seja convidado a conhecer novos serviços por e-mail. A divulgação por esse canal pode ser realizada com base no legítimo interesse, desde que devidamente informada e sendo mantida a possibilidade do cooperado sinalizar caso não deseje receber esse tipo de comunicação. Por essa razão, é importante manter uma opção de “descadastrar” ou “opt-out” em todos os contatos com finalidades de marketing e divulgação enviados por e-mail aos cooperados.

Impera também o princípio da minimização. Com o objetivo de evitar o tratamento excessivo ou desnecessário de dados pessoais, o qual constitui uma violação da LGPD, é recomendado alinhar com os responsáveis por marketing quais os dados pessoais essenciais à realização da atividade.

Como as atividades de marketing e divulgação são realizadas com base no legítimo interesse da cooperativa, também é recomendado elaborar um Teste de Balanceamento de Legítimo Interesse. Embora a ANPD ainda não tenha regulamentado detalhes sobre o conteúdo desse teste, trata-se de uma importante documentação de conformidade, capaz de evidenciar que a cooperativa sopesou os interesses para resguardar a privacidade do cooperado.

Recomenda-se incluir, ao mínimo, uma análise sobre quais dados serão utilizados para aquela finalidade, a forma e o período de coleta desses dados, a maneira pela qual o associado será contatado e demais questões práticas sobre a atividade de divulgação e marketing. Está disponível no site da ANPD um estudo preliminar que possui um modelo de teste de balanceamento que pode ser utilizado pelas cooperativas.

A LGPD impactou significativamente as áreas de marketing e comunicação de todos os ramos empresariais cujo público-alvo são pessoas físicas. É necessário compreender, porém, que boas práticas de privacidade não vêm para inviabilizar as ações com os cooperados. Pelo contrário, são grandes aliada na medida que permitem à cooperativa construir uma relação baseada no respeito aos associados e ao se demonstrar preocupada com sua privacidade e a proteção de seus dados pessoais.

Esses valores não são somente compatíveis com a proposta das cooperativas de manter um relacionamento ativo e personalizado com seus associados: são essenciais para a consecução desse objetivo.

ARTIGOS DE AUTORIA DE

BRENDA BELTRAMIN

Advogada e especialista em Direito
Digital e Proteção de Dados

O que não pode faltar para a

SEGURANÇA DA INFORMAÇÃO?

Neste material, exploramos como as cooperativas de crédito podem atender às diretrizes e requisitos estabelecidos pela LGPD e pela Resolução nº 4.658 do Banco Central do Brasil. Discutimos as melhores práticas e os desafios legais na aplicação de decisões automatizadas e inteligência artificial, bem como as restrições que as estratégias de marketing das cooperativas devem observar.

No entanto, mesmo com todos esses cuidados, o trabalho da cooperativa de crédito em proteger os dados sensíveis de seus cooperados contra-ataques cibernéticos está longe de terminar, pois a implementação de medidas de segurança da informação é crucial.

Desde políticas de acesso até protocolos de criptografia, a criação de regulamentações que definem os parâmetros de coleta e tratamento dos dados aos quais têm acesso, incluindo informações sobre os tipos de dados e o período de retenção, é vital para as cooperativas.

Para saber mais sobre as práticas essenciais de segurança da informação e como proteger os dados confidenciais de sua empresa e de seus clientes contra roubo, perda e uso indevido,

OUÇA O EPISÓDIO #104 DO CHENUTCAST.

Neste episódio, a nossa sócia de Direito Digital, **Iara Peixoto Melo**, conversa com o Sócio-Diretor da Proxys Soluções, **Everton Alves**, sobre o assunto.

Acessar episódio

O CHENUT

Experiência e reconhecimento conquistados no mercado

Chenut é sinônimo de contemporaneidade. E ser contemporâneo é viver a atualidade em sua plenitude.

É ASSIM QUE ATUAMOS, SEM MEDO DO NOVO.

Nossa advocacia empresarial alia conhecimento e experiência à criatividade. Respondemos com agilidade às mudanças e estamos sempre buscando aprimoramento. Qualidade é premissa.

Saiba mais sobre o nosso escritório

Conheça nosso código de ética

HÁ 15 ANOS ATUAMOS CONECTANDO DISTÂNCIAS, COM FORTE PRESENÇA INTERNACIONAL QUE SEGUE EM EXPANSÃO.

Nossa equipe multicultural transita em todas as áreas do Direito empresarial visando a prosperidade e segurança dos negócios dos nossos clientes

Veja as áreas e os segmentos em que atuamos

E conheça o nosso time de especialistas

Chenut