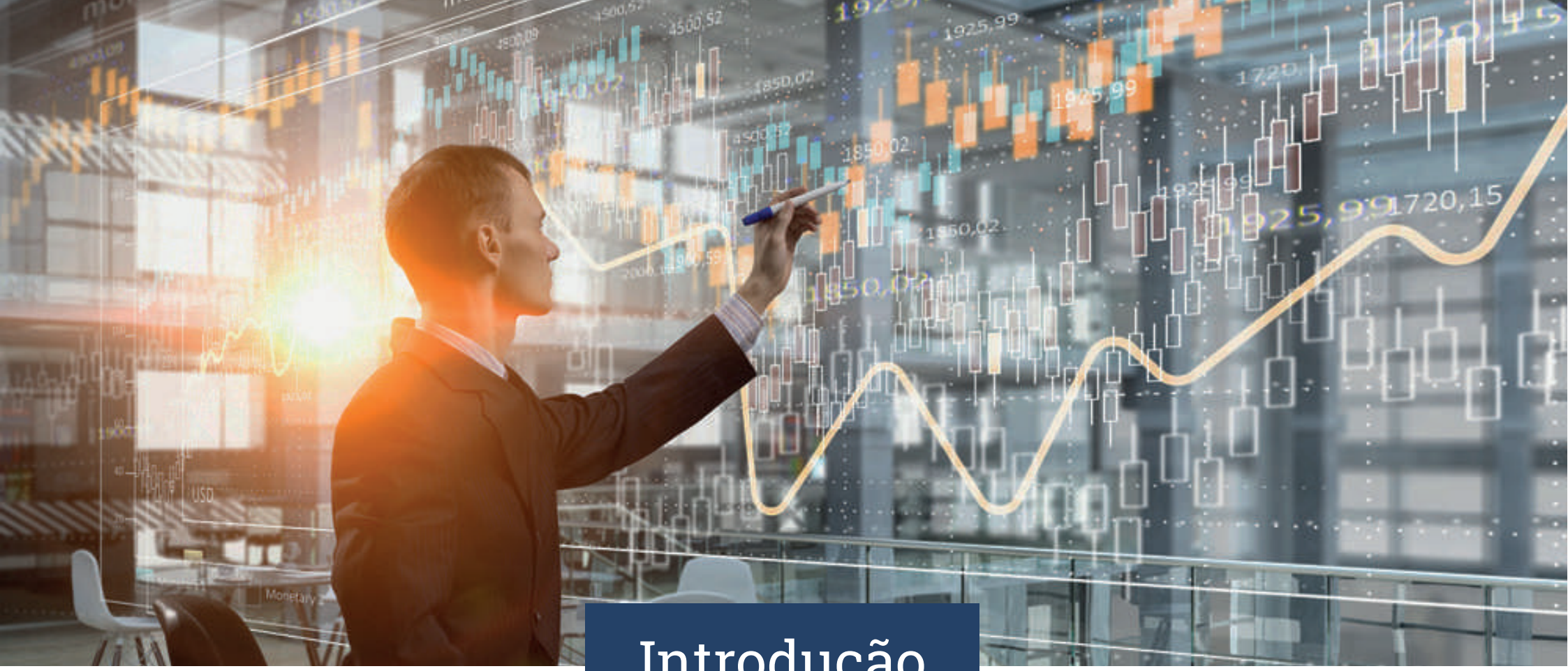
Resolução BACEN 4658 e a Lei Geral de Proteção de dados: O que muda no mercado financeiro?

ProMove



Introdução

O mercado financeiro é um dos mais regulamentados do país. Essa preocupação é evidente, visto que seu objetivo é a movimentação de dinheiro. A regulamentação e as leis têm o objetivo de proteger tanto os consumidores como as próprias instituições, e com este objetivo, duas alterações recentes trouxeram novidades para o setor. Estas mudanças são importantes para todos os profissionais, que precisam estar bem atentos a elas. Portanto, neste artigo, entenda tudo sobre a Resolução BACEN 4.658, a Lei Geral de Proteção de Dados e que mudanças elas trazem para o mercado financeiro.

Por que existem estas leis?

Antes de discutir o que são as leis e quais são os seus efeitos, é interessante trazer um pouco de contexto. Ambas abordam um tema muito interessante e cada vez mais presente no mundo moderno, a tecnologia.

As inovações e a transformação digital mudaram a forma como as pessoas e empresas operam. Existe uma grande relação de dependência entre o ser humano e a tecnologia, que evidentemente traz muitos benefícios. Porém, também trazem alguns riscos.

Estes riscos não envolvem necessariamente os hackers e outras formas de ataque cibernético com o objetivo de roubar informações, apesar de eles existirem, mas sim, ações mais subjetivas, como práticas abusivas de empresas que se aproveitam de uma posição mais frágil do consumidor.

E é este o objetivo da Lei e da Resolução. Proteger a parte mais fraca desta interação, que é o consumidor, e se adaptar à nova tecnologia para atualizar as normas para um cenário mais moderno, e muito diferente de como o mundo era quando as leis anteriores foram concebidas.

O que é a resolução BACEN 4.658?

Não existe melhor exemplo da necessidade de se adaptar às novas tecnologias do que a Resolução BACEN 4.685. Ela foi estabelecida pelo Banco Central em abril de 2018, por meio de um calendário de ações que devem ser tomadas pelas instituições financeiras e de pagamentos em todos os serviços de nuvem que oferecem.

O calendário terminou no meio do ano de 2019, quando as empresas deveriam ter comprovado que estão adaptadas às exigências da resolução.

Já quanto ao objetivo, a Resolução existe para criar normas de cibersegurança, proteção de dados pessoais, além de estabelecer condutas e diretrizes de resposta caso ocorra algum incidente em um servidor de nuvem terceirizado.

Trazendo um pouco mais de contexto, e fazendo uma explicação bem rápida e básica, a computação em nuvem envolve o uso de servidores digitais em que são armazenadas as informações e, até mesmo, são feitos certos processos. Os servidores não ficam mais fisicamente nas empresas, e sim, existe a contratação do espaço virtual com parceiros terceirizados.

Para que esta estrutura funcione, ela precisa ser confiável, rápida e, mais importante, segura. Evidentemente, que ela apresenta uma vulnerabilidade, assim como qualquer ambiente virtual.

Porém, ao contratar um serviço terceirizado, esta proteção tende a ser maior, pois a empresa tem mais conhecimento sobre o assunto e foca todos os seus esforços em criar uma rede segura. É uma opção mais vantajosa, desde que sejam cumpridos certos pré-requisitos. E é esta prática que a Resolução 4.658 busca regulamentar.

O que diz a Resolução BACEN 4.658?

Esta resolução é uma resposta a 4.557, de 2017, que já trazia algumas informações sobre as potenciais ameaças. Mas, como a resolução antiga era muito rasa e não abordava todas as ameaças e práticas necessárias para revertê-las, foi necessário criar a 4.658.

O primeiro ponto que a resolução aborda é que qualquer empresa do setor deve implementar e ter uma política de segurança cibernética. É dito também que esta política deve ser construída com o objetivo de garantir a confidencialidade, integridade e disponibilidade tanto das informações como dos próprios sistemas que as mantém.

Enquanto este é o objetivo principal, existem diversas diretrizes que precisam ser identificadas. As principais são:

• Procedimentos que visam reduzir a exposição de risco e garantir os objetivos de segurança cibernética da empresa;

• Registro, análise e um relatório de efeitos de quaisquer incidentes que tenha ocorrido e que possa ter relação com a segurança da informação;

• Formas de disseminar a cultura de segurança dentro da própria empresa;

• Classificação de dados de acordo com a sua importância;

• Implementação de programas de capacitação e de avaliação da equipe, no quesito da segurança;

• Definição clara de todos os procedimentos que devem ser adotados por prestadores de serviço terceirizados;

• Formas de controlar os procedimentos, internos e externos, que visam garantir a segurança dos dados;

• Rastreabilidade da informação, para determinar o caminho exato que ela percorre dentro e fora da empresa.

• Objetivos estratégicos da segurança da empresa.

É claro que implementar estes pré-requisitos é um enorme desafio, especialmente tendo em vista que eles devem considerar o nível de complexidade e o tamanho de cada instituição.

Enquanto estas são as principais diretrizes, existem alguns pontos em que a Resolução é mais específica. Por exemplo, nos quesitos técnicos da resolução, é preciso garantir algumas práticas básicas da segurança cibernética, como:

• Criptografia;
• Detecção e prevenção de invasões;
• Autenticação, de preferência com múltiplos passos;
• Prevenção de vazamento de informações;
• Criação de cópias de segurança dos dados;
• Mecanismos de rastreabilidade;
• Controle de acesso e segmentação de redes;
• Testes periódicos de vulnerabilidade;
• Proteção contra softwares maliciosos;
• E diversos outros.

Outro ponto abordado pela 4658 é a necessidade de uma política de transparência, em que a empresa vai divulgá-la com colaboradores, empresas que prestem serviços a ela e os próprios clientes que quiserem ter acesso. Além disso, também é preciso enviar as informações ao próprio Banco Central.

O que a resolução BACEN 4.658 muda para o mercado financeiro?

Com essa nova resolução, as instituições do mercado financeiro precisam se adequar a todos os pré-requisitos estabelecidos na 4658. A resolução completa pode ser encontrada no site do **Banco Central**.

Na prática, a resolução indica que qualquer serviço de nuvem que for ser contratado precisa cumprir as políticas estabelecidas nas normas acima. Logo, também é uma boa prática adotar políticas de compliance e governança, antes mesmos de contratar um serviço terceirizado, para garantir que o trabalho vai cumprir as exigências.

Outro ponto fundamental é que as instituições devem ter respostas prontas para possíveis incidentes. Nelas, estão incluídas ações que vão adequar a instituições às políticas de segurança e rotinas para **prevenir e responder** a determinados acidentes.

Uma boa prática, é estabelecer um profissional que será focado em implementar e controlar a política e as atividades de segurança cibernética que precisam ser adotadas pela instituição.

Também é necessário fazer relatórios sobre a implementação do plano e sobre possíveis incidentes. Uma prática interessante que a resolução estabelece é o compartilhamento de incidentes e problemas que possam ser encontrados, para outras instituições financeiras. É uma forma de trazer confiabilidade para todo o mercado e garantir uma evolução conjunta do setor.

O que é a LGPD?

A Lei Geral de Proteção de Dados tem o objetivo básico idêntico ao da resolução anterior, ou seja, regulamentar práticas de segurança em relação ao uso das novas tecnologias. Porém, mais especificamente, como o nome indica, seu foco é nos dados pessoais dos usuários.

A existência da LGPD também acaba sendo uma resposta clara a forma como tanto as empresas quanto as pessoas usam os dados pessoais atualmente. Esta é uma fonte de informação extremamente valiosa, cujo mercado movimenta bilhões. É por meio dos dados dos usuários que empresas conseguem criar estratégias e mecanismos de venda mais eficientes e segmentados.

Durante muito tempo, não houve muito controle sobre este tipo de prática. Afinal, o tratamento de dados acabou de nascer e levou um certo tempo até as leis se adaptarem a ele. A GDPR é um exemplo de um novo modelo de regulamentação geral usado na Europa, e foi nele que a LGPD se baseou. Ou seja, fica claro que esta preocupação é por todo o mundo. Até a nova lei, a Constituição brasileira, e nenhuma outra do mundo, estava preparada para a enxurrada de dados pessoais e o tratamento que as empresas fariam a ele. Esta prática fez a LGPD se tornar uma grande necessidade.

Basicamente, a LGPD envolve dois pilares principais: o direito à privacidade e o tratamento dos dados pessoais.

No caso das instituições financeiras sua posição é interessante em relação à nova lei. Evidentemente, este tipo de serviço usa alguns dados extremamente sensíveis e pessoais, como o nome, o CPF, o perfil de crédito e a movimentação financeira do cliente. Porém, como estes dados são tão importantes, já existe uma certa estrutura de proteção para eles.

A CVM é um exemplo de instituição que já existe para garantir que o mercado financeiro irá manter sigilo e proteger os dados de seus clientes. Porém, a LGPD traz um foco maior na tecnologia, o que significa que é preciso conhecê-la.

Qual a abrangência da LGPD?

A LGPD tem uma abrangência enorme. Ela pega alguns conceitos do Código de Defesa do Consumidor, do Marco Civil da Internet, da própria Constituição Federal e de diversos outros. A Lei completa pode ser consultada no site do **Planalto Federal.**

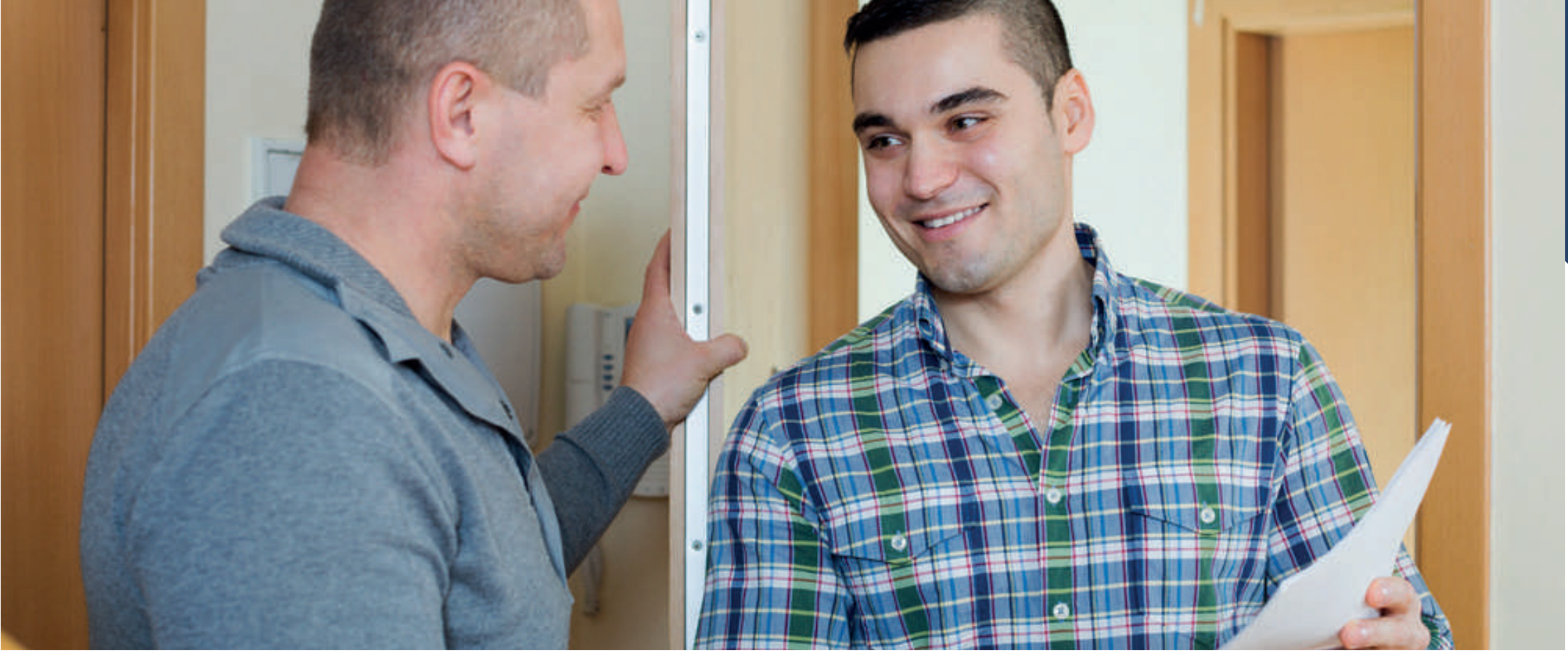
Porém, antes mesmo de conhecer a lei é preciso fazer uma pergunta interessante, que não é tão óbvia quanto parece.

O que é um dado pessoal?

Evidentemente, este é um conceito extremamente abrangente. Segundo a LGPD, um dado pessoal é qualquer informação que torne a pessoa identificável ou identificada. Ou seja, dados como CPF, nome completo, RG, CNH e outros destes são exemplos que permitem quase imediatamente, identificar uma pessoa.

Uma subcategoria dos dados são os dados sensíveis que, de acordo com a lei, abordam temas que se referem à origem racial ou étnica de uma pessoa, além de informações sobre a sua convicção religiosa, opinião pública, ou algum dado de caráter de saúde, ou da vida sexual do indivíduo. Prontuários médicos, por exemplo, são dados sensíveis.

Existe, ainda, uma terceira categoria de dados, que são os dados anonimizados. Este é um dos conceitos mais importantes da LGPD e que ainda irá permitir que as empresas usem essas informações.



Por exemplo, se eu disser que uma pessoa é loira, este dado não é o suficiente para torná-la identificável, o que significa que é um dado anonimizado. Estes sim, podem ser usados.

Mesmo dados sensíveis podem ser anonimizados. Por exemplo, quando uma empresa como o IBOPE vai às ruas fazer uma pesquisa de intenção de voto, ela pergunta um dado sensível, mas se não identificar quem vota em quem, esta informação pode ser divulgada. O mais importante é como os dados são tratados e assim, voltamos à LGPD.

Quais são os princípios da LGPD?

Os princípios básicos da LGPD envolvem 5 atividades em relação aos dados de usuários:

• Tratamento;
• Transmissão;
• Reprodução;
• Utilização;
• Arquivamento.

A lei demanda que qualquer empresa que irá "tratar" estas informações, precisa instituir um regime de **proteção de dados,** de modo a segurar os dois princípios mencionados acima: o direito à privacidade e o tratamento adequado destes.

Este tratamento quer dizer que a empresa só pode manipular os dados de usuários mediante a um consentimento claro do mesmo.

A lei também estimula que o consentimento deve obedecer a certas exigências, de modo a eliminar políticas de permissão "escondidas". Por exemplo, ele deve ser dado de forma voluntária pelo usuário, manifestando a sua ação de concordância. Esta prática quer dizer que é contra a lei trazer opções em que o consentimento seja dado como padrão. O usuário precisa de fato tomar uma ação.

Outro ponto fundamental é que o usuário tem total direito de saber para que as suas informações são usadas. Ou seja, a empresa deve informar exatamente o que vai fazer com os dados dos usuários, também de forma clara e direta, com um recurso que garante que esta informação foi vista. Entre estas informações incluem:

• Finalidade do tratamento;
• Duração do tratamento;
• Identificação e contato de quem será o responsável por estes dados;
• Informações se os dados forem compartilhados, com uma agência, por exemplo;
• Todos os direitos do usuário.

O usuário também tem o direito de revogar este consentimento, na hora que quiser e sem a neces-

sidade de apresentar nenhum motivo. Já a empresa, deve informá-lo também de forma clara que houve uma mudança na forma com que os seus dados são tratados.

Porém, existe um caso de consentimento específico que afeta diretamente os bancos. Quando um dado é inerentemente necessário para a função que o usuário contrata, o consentimento é implícito. Ou seja, dados como CPF e o nome completo são essenciais para o banco fazer a sua atividade, o que significa que não é necessário pedir consentimento, desde que sejam mantidos apenas as informações necessárias.

Por fim, o usuário também tem o direito de exigir que os dados sejam deletados ou atualizados sempre que desejar.

Anonimização

A anonimização já foi mencionada um pouco acima, mas também é um dos pontos cruciais da lei e que permite que as empresas continuem usar os dados de usuários para os mais diversos objetivos.

Pela lei, anonimizar é usar algum meio técnico para permitir que um dado não possa mais ser associado diretamente a uma pessoa, quebrando assim a possibilidade dele a identificar. É preciso também que esta forma de anonimizar seja razoável, ou seja, não seja muito custosa para a empresa, mas que representa a impossibilidade, ou pelo menos a necessidade de um enorme esforço, para reverter o processo e torná-lo identificável novamente.

Outro ponto crucial que a LGPD traz é que as empresas têm total responsabilidade sobre os danos causados aos usuários, cuja origem seja o tratamento destas informações. Sejam danos morais, patrimoniais, individuais ou coletivos, as empresas têm a obrigação de repará-los.

Os únicos casos em que não é necessário reparar os dados é se comprovarem que não realizaram o tratamento que foi atribuído, ou que se mantiveram de acordo com todas as premissas da LGPD. Se o dano for culpa do usuário, a empresa evidentemente também não precisa repará-lo.

Nesse caso, a empresa tem até 72 horas para notificar tanto a autoridade nacional quanto o usuário, ou usuários, que foram vítimas do vazamento ou de qualquer erro que tenha ocorrido com os seus dados.

Além disso, é importante destacar que existem as multas que podem ser aplicadas às empresas que não se adequarem às normas explícitas pela LGPD, e seu valor pode ser bem alto. Ela pode chegar até 2% do faturamento anual, ou R$ 50 milhões.

Para evitar este problema é preciso tomar certas medidas, e neste ponto, a LGPD tem algumas semelhanças com a Resolução 4658.

Também é importante que as instituições financeiras usem todos os seus recursos para criar uma estrutura segura que irá impedir o vazamento de dados. Logo, é necessário ter um programa de proteção de dados que traga as seguintes medidas:

- Análise de cenários e riscos;
- Programa de governança e compliance;
- Elaboração de Termos de Uso e Política de Privacidade;
- Estrutura técnica preparada para suprir a demanda e garantir a segurança;
- Escolha de um Data Protection Officer, um funcionário que será a interseção entre usuários, empresa e governo;
- E diversas outras.

O que a LGPD e a Resolução BACEN 4658 mudam no mercado financeiro?

Ao entender melhor o que as duas novas normas determinam, fica claro que elas têm as suas especificações, mas que também têm certos pontos em comum. Por exemplo, ambos demandam um maior sigilo e medidas de segurança. Como os bancos precisam usar os dados para trabalhar, a proteção destes acaba sendo o ponto principal.

Logo, as instituições financeiras precisam se focar nas medidas de segurança estabelecidas por ambas as leis, para garantir o cumprimento de ambas e evitar maiores problemas.

O roteiro para implementar as medidas e resolver os problemas começa por um diagnóstico. A maioria das instituições financeiras já têm algumas **medidas de segurança**, mas é preciso fazer uma análise completa de todas as possíveis vulnerabilidades e encontrar formas de contorná-las.

Como vimos acima, as multas podem ser bem pesadas, sem falar na perda de credibilidade que a empresa sofre ao ter os dados de clientes vazados. Ao se tratar de dados extremamente sensíveis como os bancários, qualquer problema pode ser muito prejudicial para a empresa.

Em seguida, é importante elaborar um plano para implementação de soluções que irão resolver estes problemas e eliminar as vulnerabilidades. Durante este planejamento, também é importante pensar nas ações de contingência, planos B, backups e diversas outras medidas de compliance que irão garantir a proteção de dados, mesmo caso ocorra alguma falha.

Já quanto a implementação, fazer testes para garantir que a estrutura está apta a atender a demanda é fundamental para assegurar a proteção contra determinados riscos. É importante neste tempo, também fazer um treinamento para que a equipe esteja preparada a lidar com as novas demandas.

O setor bancário, como qualquer outro, precisa se adaptar às novas Leis, o que significa que o ideal é contar com um acompanhamento que ajude a sua empresa se adaptar à nova realidade.

A LGPD entra em vigor em 2020, o que significa que o tempo para se adequar está acabando. Muitas empresas já estão se antecipando a lei e implementando as soluções antes mesmo que ela seja exigida de fato, não somente para avaliar a capacidade da empresa de cumpri-la, mas também para garantir mais aprovação dos clientes.

Como dito acima, o setor financeiro já tem uma vantagem nessa corrida por possuir medidas semelhantes. A CVM, por exemplo, tem um artigo na sua Instrução que diz que é preciso manter os dados que possam afetar os investidores em sigilo. O COAF, faz um serviço de fiscalização muito forte, identificando e analisando qualquer possível atividade suspeita.

Já a ANBIMA, tem um guia que orienta as empresas a implementar um programa de cibersegurança. O documento busca ajudar as diversas instituições do mercado, para consolidar as práticas e garantir a confiabilidade de todo o sistema financeiro.

O mercado financeiro tem uma enorme necessidade de se autorregular, de modo a garantir o melhor desempenho e a segurança de todos os envolvidos. Essa preocupação significa que diversas instituições já deram alguns grandes passos para o objetivo da segurança cibernética.

Mas, mesmo assim, se a sua empresa ainda não começou a se movimentar para se adequar às especificações da 4658 e da LGPD, o ideal é se ajustar às leis o mais rápido possível. Evite deixar este processo para a última hora e garanta que ele é o mais eficiente e tranquilo para a sua empresa.

Sobre a ProMove

Entre em **contato** com a ProMove para saber como podemos ajudar na implementação dos requisitos da LGPD e da Resolução BACEN 4658!

Somos uma empresa de consultoria em melhoria de processos em TI e temos como objetivo conectar e automatizar equipes por meio de serviços exclusivos, como consultorias em gamification, certificações CMMI, ISO, MPS e automação com DevOps.

Visite nossos canais e descubra como a tecnologia pode transformar a produtividade do seu negócio!