/proteção de dados no setor financeiro

white-paper

BAPTISTA LUZ
ADVOGADOS

Última atualização em: 04.12.2017

Renato Leite
Pedro Ramos
Ana Paula Collet Camargo
Laura Felicíssimo

/ INTRODUÇÃO

Embora as normas de proteção de dados tenham aumentado no mundo durante os últimos anos, o Brasil não possui ainda uma Lei Geral de Proteção de Dados.

Em relação à proteção de dados no setor financeiro brasileiro, é a partir do segundo semestre de 2016 que algumas associações e agências reguladoras tomaram iniciativas específicas. Em agosto de 2016, a ANBIMA, associação brasileira de mercados de capital e financeiros, publicou uma diretriz de segurança cibernética[1], na qual se mostra a necessidade de procedimentos adequados de proteção de dados no setor financeiro devido a que os interesses financeiros motivam a maioria (80%) dos incidentes de segurança cibernética no Brasil.

Recentemente, em julho de 2017, a Autoridade Nacional de Valores Mobiliários (CVM), publicou um estudo sobre a "percepção dos riscos cibernéticos nas atividades de administradores e intermediários fiduciários"[2]. O Banco Central do Brasil (BACEN) abriu uma consulta[3] sobre uma resolução obrigatória para todo o setor financeiro em relação aos procedimentos e normas de segurança da informação. A consulta, aberta até 21 de novembro, abordou aspectos tais como a necessidade de nomear um diretor de segurança cibernética bem como as regras de localização de dados que determinem o armazenamento dos dados financeiros dentro do Brasil, medida que, se for promulgada, iria acarretar custos extras que atualmente não são suportados pelo armazenamento de dados na nuvem em locais com custos mais baixos.

[1] Disponível em: goo.gl/CFHsBT
[2] Disponível em: goo.gl/xNvBEn
[3] Disponível em: goo.gl/s7YvUU

No entanto, o setor financeiro brasileiro está sujeito a diversas normas setoriais que afetam a forma de processamento dos dados. Veja abaixo a lista de regulamentos relevantes que serão discutidos ao longo deste texto:

- Constituição Federal
- Código Penal (Lei nº 2,848/1940)
- Empresa Limitada (Lei nº 6,404/1974)
- Mercado de Valores Mobiliários (Lei nº 6,385/1976)
- Definição de crimes contra o Sistema Financeiro Nacional (Lei nº 7.492/1986)
- Código do Consumidor (Lei nº 8,078/1990)
- Lavagem de dinheiro (Lei nº 9,613/1998 conforme atualização de 2003 e 2012)
- Segredo bancário (Lei Complementar nº 105/2001)
- Código Civil (Lei nº 10,406/2002)
- Relatório de Credito e Histórico de Crédito (Lei nº 12,414/2011)
- Acesso à informação (Lei nº 12,527/2011)
- Crimes Cibernéticos (Lei nº 12,737/2012)
- Princípio de Garantias e Direitos para uso da Internet ("*Marco Civil da Internet*") (Law nº 12,965/2014)
- Regulação do Marco Civil da Internet (Decreto Federal 8.771/2016, sobre a proteção de dados pessoais na Internet)

/ GESTÃO DE DADOS PESSOAIS E FINANCEIROS

O Direito à Privacidade é protegido pela Constituição Brasileira (Artigo 5, X), bem como o Direito de não Intercepção da Comunicação, exceto no caso de investigações criminais em andamento (Artigo 5, XII). O Código Civil dá ênfase ao direito individual à privacidade e, por esse motivo, os tribunais, por solicitação de uma pessoa, podem adotar todos os remédios necessários para impedir atividades que possam afetar à privacidade individual.

O Código do Consumidor, Seção VI, pela sua vez, regula os registros e banco de dados dos consumidores, especialmente naquilo que se refere ao histórico de inadimplência de crédito. O artigo 43º regula que o consumidor deve ter direito ao acesso às informações relacionadas a elas disponíveis em registros e bases de dados. As provisões detalhadas são:

(i) estes registros devem ser de uso fácil e as informações negativas não podem continuar disponíveis após cinco anos;

(ii) o consumidor deve estar ciente de qualquer registro ou banco de dados usando seus dados;

(iii) o consumidor pode exigir a alteração imediata de dados incorretos;

(iv) uma vez que a prescrição da dívida de um consumidor for aplicada, os Sistemas de Proteção de Crédito não fornecerão qualquer informação que possa impedir o acesso a novos créditos.

O Código do Consumidor foi interpretado pelo Ministério da Justiça para esclarecer que as cláusulas que permitem a transferência de dados para terceiros sem o devido consentimento podem ser inválidas. Além disso, o consentimento é necessário para coletar e usar os dados para outros fins que não sejam abrir o registro do consumidor em um banco de dados de clientes ou padrão de crédito.

De acordo com o regulamento supra, o Relatório de Crédito e a Lei de Pontuação de Crédito estabelecem a criação de banco de dados e a consultoria sobre o desempenho devido do cliente no histórico de crédito. Este tipo de banco de dados só pode manter os dados necessários para avaliar a situação econômica de uma pessoa; não pode reter dados excessivos (não relacionados/desnecessários) ou sensíveis. Além disso, o proprietário da informação deve autorizar a apertura do seu registro. No entanto, a pessoa que possui os dados pode pedir o cancelamento, para ter acesso a ele ou corrigir seus usos a qualquer momento.

Além disso, o "Marco Civil da Internet" (Lei no 12.965, artigo 7) define que qualquer organização que colete, use e trate dados pessoais por serviços prestados pela Internet deve ser autorizado pelos proprietários após ter fornecido informações claras e detalhadas sobre os procedimentos de processamento de dados. O objetivo da coleta de dados deve ser legítimo e não proibido por lei. Além disso, o Decreto Federal que complementa o "Marco Civil" definiu o que deve ser considerado como: i) "Dados pessoais" (os dados relacionados ao indivíduo identificado ou identificável,

incluindo números de identificação, dados de localização ou identificadores eletrônicos, considerando que se referem a uma pessoa); e ii) "tratamento de dados pessoais" (toda operação relacionada a dados pessoais, incluindo cobrança, produção, recebimento, qualificação, uso, acesso, reprodução, emissão, distribuição, processamento, arquivamento, armazenamento, exclusão, avaliação ou controle das informações, modificação, comunicação, transferência, difusão ou extração) conforme estabelecido no artigo 14, I e II; e iii) dados de registro, que abrange o nome, o endereço e a qualificação pessoal dos pais (incluindo nome completo, estado civil e profissão).

Além disso, o Decreto estabelece algumas regras de segurança da informação que devem ser seguidas pelas empresas que tratam dados pessoais, incluindo: i) a configuração de um controle rigoroso sobre o acesso aos dados, incluindo os deveres das pessoas que podem acessá-los; ii) o uso de sistemas de autenticação de dois fatores ou outro mecanismo para garantir a individualidade dos responsáveis pelo processamento do log; iii) a necessidade de um inventário detalhado dos acessos aos logs de conexão e logs de acesso aos aplicativos (incluindo tempo, duração, identidade dos responsáveis pelo acesso e do arquivo acessado); e iv) o uso de tecnologias de criptografia ou medidas de proteção análogas para garantir a integridade dos dados.

Algumas observações são necessárias no que diz respeito ao Código Penal brasileiro, o qual tem uma seção dedicada a crimes de violação do sigilo. A invasão ao dispositivo eletrônico de terceiros, por meio de acesso não autorizado e violação de sistemas de segurança para obter ou alterar dados, pode resultar em uma pena de prisão de três meses até um ano, incluindo o pagamento de uma multa. Essa penalidade pode aumentar se a invasão causar perdas econômicas.

As bases de dados de registros públicos estão sujeitas à Lei nº 12.527 / 2011, que permite o segredo de dados públicos somente quando uma divulgação tiver o potencial de arriscar a estabilidade financeira ou econômica, entre outras situações relativas à soberania.

/ LAVAGEM DE DINHEIRO

A Lei de Lavagem de Dinheiro especifica que o setor financeiro deve:

(i) identificar seus clientes e manter registros atualizados sobre eles;

(ii) manter um registro de todas as transações financeiras que ultrapassem o limite permitido;

(iii) responder corretamente a todas as solicitações feitas pelo COAF (o Conselho Brasileiro de Controle de Atividades Financeiras) ou um outro regulador adequado, de maneira que este conselho seja responsável por manter o sigilo sobre as respostas enviadas;

(iv) prestar atenção especial a qualquer transação que evidencie seriamente a constituição de crime, comunicando o fato, em segredo, ao COAF no prazo de 24 horas.

Instituições ou pessoas que não cooperem com os requisitos acima podem estar sujeitas às seguintes sanções: advertências; multas; proibição temporária de exercer cargos de administração de instituições financeiras; falta de poder para o exercício da atividade, operação ou função.

/ SEGURANÇA BANCÁRIA E CONFIDENCIALIDADE

Existe uma lei específica no Brasil que exige confidencialidade das instituições financeiras. O quadro regulamentar é complementado por vários regulamentos fornecidos por reguladores, como o Banco Central do Brasil e a Autoridade de Valores Mobiliários. A Lei Complementar nº 105 de 2001, segundo a qual apenas as seguintes situações não violam as obrigações de confidencialidade:

- intercâmbio de informações entre instituições financeiras para fins de base de dados;
- informações de inadimplentes de crédito exigidas pelas entidades de proteção de crédito;
- comunicação de atividades ilícitas a reguladores adequados (e.g. CVM, COAF);
- divulgação de informações com o consentimento expresso de todas as pessoas envolvidas e proprietários da informação;

- a violação da confidencialidade também pode ser necessária como parte de uma investigação judicial, especialmente se for nos seguintes crimes: terrorismo; tráfico de drogas ou armas; extorsão por sequestro; contra o sistema financeiro nacional; contra a administração pública; contra o direito tributário e a segurança social; lavagem de dinheiro; praticado por organizações criminosas.

É possível perceber semelhanças entre a Lei de Lavagem de Dinheiro e a Lei Complementar do Segredo Bancário quando se trata de proteção de dados. O cumprimento do sigilo bancário e a conformidade com a proteção de dados permitem o intercâmbio de dados privados, se forem solicitados por entidades públicas específicas associadas ao setor financeiro ou para suporte de investigação legal.

A Lei nº 7.492/1986 define os crimes contra o sistema financeiro nacional. Neste regulamento, a violação do segredo em uma operação ou serviço oferecido por uma instituição financeira pode resultar em uma pena de prisão de um a quatro anos mais o pagamento de uma multa, exceto se as informações forem exigidas pelas autoridades.

/ NOTIFICAÇÃO DE VIOLACAO DE DADOS

O Brasil não tem um regulamento para instruir notificações de violação de dados em qualquer setor. No entanto, existem dois projetos de lei de proteção de dados relacionados à proteção de dados pessoais. Ambas propostas devem aplicar instruções sobre notificações de violação de dados para todos os setores da sociedade brasileira, independentemente da sua natureza.

O artigo 47 da Lei nº 5,276/2016, proposto pela Câmara de Deputados, estabelece procedimentos em caso de qualquer incidente de segurança. As medidas propostas são muito semelhantes às do artigo 24 do projeto de lei n°. 330/2013, do Senado Federal. Em resumo, o processador de dados deverá:

(i) comunicar o incidente dentro de um prazo razoável à Autoridade de Proteção de Dados (que deverá ser criada);

(ii) oferecer informações detalhadas sobre a natureza dos dados danificados, as informações pessoais envolvidas, os procedimentos utilizados para proteger os dados, os riscos relacionados com o incidente, as medidas adotadas para lidar com elas e, se for o caso, os motivos pelos quais o processador de dados demora em comunicar o fato.

Dependendo do dano causado aos dados, a Autoridade de Proteção de Dados pode solicitar outras medidas, tais como informar o incidente ao proprietário da informação, promover o incidente na mídia ou tomar mais ações para reverter o incidente (artigo 48 do projeto de lei no 5.276/2016).

/ MARKETING, NOVA MÍDIA E COMUNICAÇÕES

O Marco Civil estipula que o relacionamento da mídia com seus usuários é um "relacionamento de consumidor", portanto, ela está sujeita ao Código do Consumidor, que já foi analisado no tópico dois.

No entanto, não existe uma relação específica quanto ao uso de dados para fins de marketing.

Ambos projetos de lei de proteção de dados mencionados são orientados à regulação do uso de dados para práticas comerciais, portanto, também serão aplicados para fins de marketing. Ambas propostas exigem o consentimento do proprietário da informação, quem deverá entender muito claramente os propósitos para a validez da sua autorização. Além disso, as empresas devem ser responsáveis pela proteção de dados, mantendo-os estritamente dentro daquilo para o que foi autorizado.

/ SEGUROS

Em primeiro lugar, é importante ter em mente que as regras de proteção de dados do Código do Consumidor aplicam-se às companhias de seguros. Além disso, as companhias de seguros também são consideradas instituições financeiras pela supracitada Lei nº 7.492/1986, que define os crimes contra o sistema financeiro nacional. Nessa regulamentação, a violação do segredo em uma operação ou serviço oferecido por uma instituição financeira poderá resultar em uma pena de prisão de um a quatro anos mais o

pagamento de uma multa, exceto quando as informações forem exigidas pelas autoridades.

O Conselho Nacional de Seguros Privados emitiu a Resolução CNSP no 297/2013 que regula as operações das companhias de seguros. Esta resolução determina que as companhias de seguros são responsáveis pela integridade, segurança e segredo de suas operações. Por outro lado, eles devem fornecer aos clientes informações claras, precisas e adequadas sobre os direitos e obrigações relacionados aos produtos de seguros oferecidos.

Em relação ao seguro médico, é importante mencionar a regulamentação dos registros médicos. Os registros médicos eletrônicos são regulados pela Resolução Nº 1.821 / 07 do Conselho Federal de Medicina ("a Resolução") (disponível apenas em português aqui). No entanto, a Resolução concentra-se na digitalização de registros médicos físicos e não fornece salvaguardas apropriadas para dados pessoais sensíveis, como dados de saúde. Não há nenhuma lei que obrigue aos provedores de serviços de registro médico a solicitarem a autorização dos pacientes para processar seus dados, com base no fato de que a autorização já foi dada ao médico. No entanto, as práticas de mercado indicam que a autorização deve ser dada. Existem políticas internas que lidam com este assunto, que podem ser impugnadas em um tribunal de justiça, como nos casos em que a autorização não pode ser outorgada, por exemplo, em caso de emergência ou quando o paciente estiver incapacitado. No entanto, os registros médicos de um indivíduo não podem ser transferidos para terceiros, por eles serem considerados parte de um documento confidencial entre o médico e o paciente. Este requisito é regulado pelo Código Penal, pelas regras de confidencialidade profissional e pelos regulamentos da profissão médica.

/ OUTRAS ÁREAS DE INTERESSE

A relação entre profissionais do setor financeiro e segurança de dados é regulada pelo Código Penal brasileiro e as regras específicas apresentadas pela legislação setorial.

O Código Penal, na seção dedicada a crimes de violação do segredo, impõe que a violação do segredo profissional pode causar uma pena de prisão de um mês a um ano ou ao pagamento de uma multa.

No mesmo sentido, a Lei das Sociedades por Ações impõe o dever de lealdade aos administradores deste tipo de empresa. Os administradores não podem usar para seu próprio benefício, mesmo sem prejuízo da empresa, oportunidades comerciais descobertas como resultado da sua função. Eles também não podem omitir as boas oportunidades comerciais da empresa quando estas tiverem benefícios a eles próprios ou a uma outra pessoa.

Também é necessário manter o sigilo de informações que ainda não foram promovidas fora da empresa, especialmente se influenciar a bolsa de valores. Os gerentes também devem envidar esforços para que os empregadores sob sua responsabilidade ou pessoas de sua confiança não atuem contra esta regra.

Se alguma pessoa for danificada devido a uma falha nesta obrigação, ela terá o direito de ser indenizada pelo malfeitor.

A Lei do Mercado de Valores Mobiliários considera um crime contra este mercado o uso de informações relevantes ainda não fornecidas ao mercado. A penalidade, neste caso, é maior do que a prevista no Código Penal, combinando de um a cinco anos de reclusão com multas de até três vezes o valor do benefício obtido.

Para reforçar a importância deste assunto, a Comissão de Valores Mobiliários (CVM), autoridade responsável pela regulamentação do mercado de valores mobiliários e seus interesses no Brasil, emitiu a

Instrução 31 de 1984. Esta Instrução enfatiza a necessidade de informar ao mercado sobre dados relevantes que possam afetar a todos os investidores de uma empresa com ações no mercado de ações. Caso a empresa optar por manter alguma informação em segredo, tal decisão deverá ser submetida à CVM devendo todos os administradores e acionistas respeitar tal segredo.

/ CONCLUSÃO

Embora o Brasil ainda esteja desenvolvendo requisitos legais específicos para proteger dados, o setor financeiro já está muito preocupado com a proteção de dados e já possui regulamentos e diretrizes específicos para proteger informações importantes. A regra geral é que os dados financeiros devem ser mantidos em sigilo. Mas (i) as informações que possam afetar o mercado devem ser divulgadas; (ii) em alguns casos, uma empresa pode manter um fato confidencial se tal fato não afetar a operação do mercado, no entanto todas as pessoas envolvidas deverão manter o sigilo não tirando proveito dela.