LGPD e Fintechs: um novo cenário para o compliance digital

BAPTISTA LUZ
ADVOGADOS

LGPD e Fintechs: um novo cenário para o compliance digital

A regulação de proteção de dados indica mudanças importantes sobre exposição e disponibilidade de informações pessoais. Quais são os cuidados que as fintechs e o mercado financeiro devem ter no contexto do novo compliance digital?

Autores

/ Davi Teófilo

/ Dennys Camara

/ Nathalia Dutra

/ Odélio Porto Júnior

/ Pamela Michelena De Marchi Gherini

Revisão

/ Gabriela Moribe

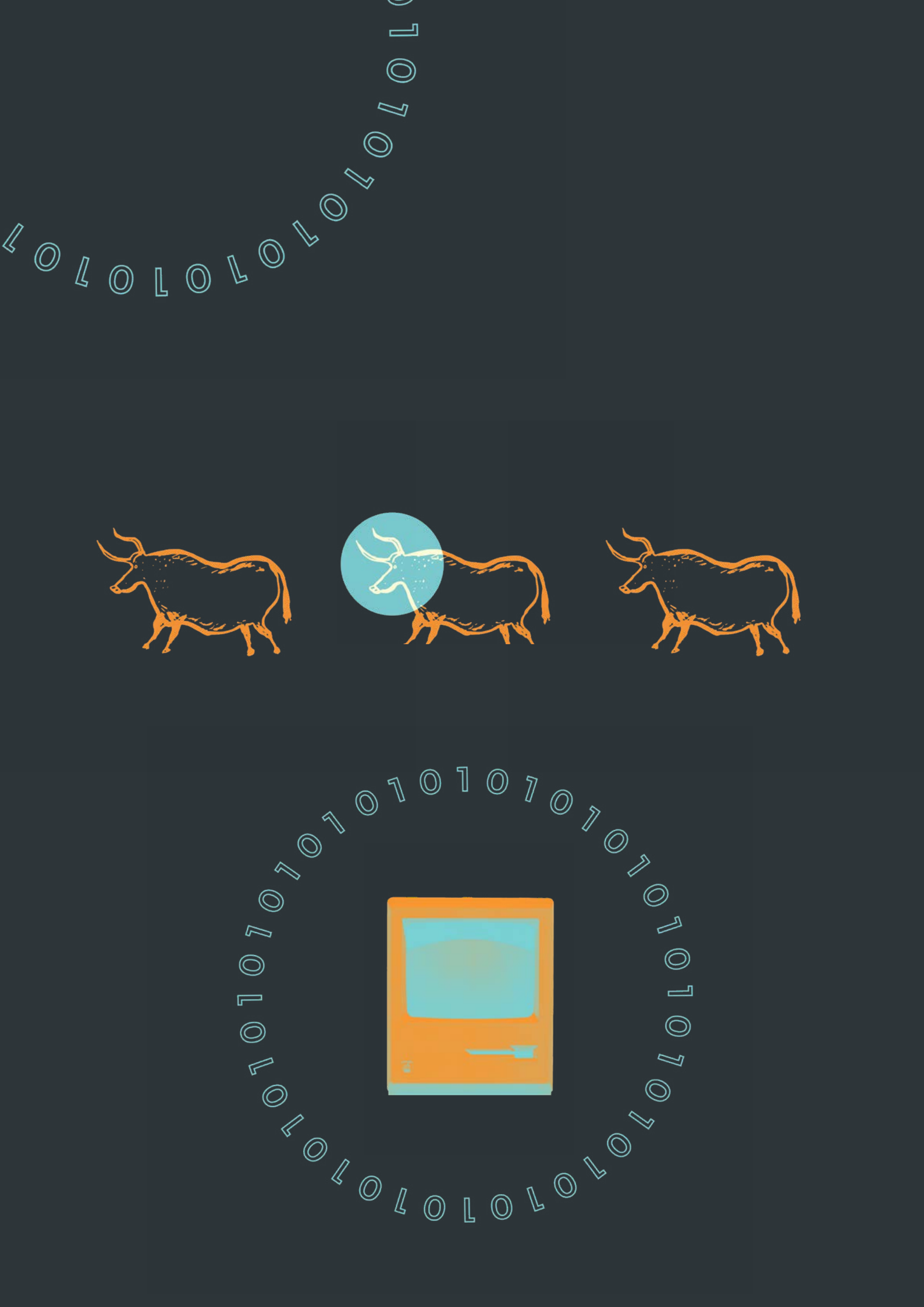
/ Luciana Simões Rebello Horta

/ Renato Leite

Projeto Gráfico

/ Laura Wolff Bandeira Klink

Sumário



1/ INTRODUÇÃO

Privacidade e proteção de dados são assuntos que vêm evoluindo bastante nos últimos anos, principalmente pela aplicação de novas tecnologias digitais. Essas inovações impactam setores como publicidade, medicina, advocacia e, inevitavelmente, o mercado financeiro e de capitais.

É preciso, no entanto, equilibrar a utilização dessas novas tecnologias. Nessa toada, surge a nova Lei Geral de Proteção de Dados ("LGPD")[1], buscando estabelecer um padrão para os mais diversos setores. Por ser o mercado financeiro e de capitais um setor extremamente regulado, o objetivo desse artigo é abordar a coexistência dos preceitos da LGPD ao arsenal regulatório do mercado já existente. De início, a LGPD, que entra em vigor em agosto de 2020, traz uma sistematização sobre o que já existe fragmentado em outras normas. Incluindo dispositivos sobre responsabilidade pelo uso indevido de informações e desrespeito à privacidade dos usuários.

Vale ressaltar que a nossa Constituição Federal estabelece o direito à privacidade[2]. Nosso Código Civil também pontua que a privacidade é um direito inviolável das pessoas naturais[3].

Sobre proteção de dados, mais especificamente, já existem diversas leis e normas administrativas fragmentadas em nosso ordenamento jurídico. Como exemplo, o Código de Defesa do Consumidor ("CDC"), a Lei de Sigilo Bancário, a Lei do Cadastro Positivo, as Resoluções e Circulares do Banco Central do Brasil ("BACEN"), dentre outras que abordaremos adiante.

[1] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 21.08.2019.

[2] BRASIL. Constituição da República Federativa do Brasil de 1988.. Artigo 5º, inciso X. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em 21.08.2019.

[3] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Artigo 21, caput. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 21.08.2019.

A LGPD impactará de maneira significativa o setor financeiro, levando em consideração que a sua aplicação se dá para agentes públicos e privados, estabelecendo um padrão que deverá ser integrado às relações específicas de cada setor.

Isso inclui fintechs, que devem estar atentas aos processos de conformidade das atividades às normas do sistema financeiro e de proteção de dados.

A intenção desse documento é muito mais no sentido de fornecer instrumentos para endereçar o tema do que, propriamente, apontar problemas e exposição ao risco.

Exploraremos, portanto, as principais leis e normas administrativas que tratam de privacidade e proteção de dados no setor financeiro, oferecendo uma visão geral da regulação nacional e o seu impacto sobre as responsabilidades dos agentes diante de incidentes (como vazamentos, utilização indevida de dados, armazenamento incorreto, etc). Seguir essas disposições faz parte do que, na nossa visão, poderá ser determinante para um novo modelo de "compliance digital" no mercado financeiro.

Assim, como diversas outras áreas do conhecimento, o Direito é dividido em subáreas que cuidam de relações jurídicas de naturezas diferentes. Pensando no mercado em que as fintechs se inserem e, principalmente, com o avanço do movimento de Open Banking (conforme discutiremos adiante), duas áreas do Direito acabam se comunicando de forma intensa, gerando obrigações e responsabilidades para o setor. Estas áreas são a do Direito Financeiro (incluindo Mercado de Capitais, a depender do caso) e a de Proteção de Dados.

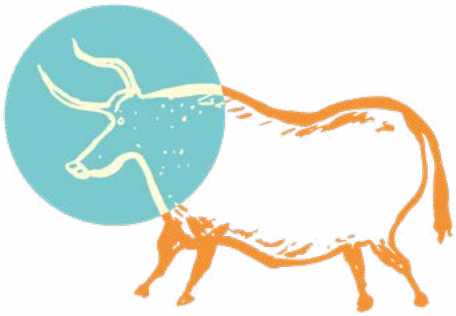
Isso significa que além da conformidade societária, tributária, trabalhista etc., fintechs precisam se atentar para aspectos legais intrínsecos às atividades exercidas por elas que, muitas vezes, envolvem fluxo de dados financeiros para que seus serviços e/ou produtos consigam ser prestados.

Portanto, este artigo abordará justamente as normas e obrigações decorrentes da intersecção entre a área do Direito que trata de Proteção de Dados e a que lida com o Mercado Financeiro.

É importante lembrar que, antes mesmo que o Brasil tivesse a LGPD, o Mercado Financeiro já reconhecia a importância de se proteger os dados financeiros das pessoas. Exemplos disso são a Lei de Sigilo Bancário, a Lei de Crimes Contra o Sistema Financeiro, dentre outras normas que também protegem informações que são utilizadas pelo Sistema Financeiro e pelas fintechs em suas atividades.

Estas informações representam conteúdo muitas vezes íntimo, podendo colocar em risco a segurança daqueles que têm suas informações compartilhadas de maneira irresponsável e, por vezes, criminosa.

É interessante perceber que o caráter privado dessas informações pode ser verificado no cotidiano como no cuidado com senhas bancárias (que justamente protegem os dados financeiros). Por exemplo, é considerado "indelicado" perguntar para alguém (que não se conhece) quanto a pessoa ganha de salário. Se estas informações não fossem delicadas de alguma forma ou não representassem algo ligado à privacidade da pessoa, talvez, o grau de proteção social conferida a elas não fosse tão intenso.



2/
UMA VISÃO GERAL DOS DADOS NO MERCADO FINANCEIRO

Antes de observarmos o que temos disposto nas normas, é preciso saber identificar o que exatamente cada uma delas visa proteger. Como veremos adiante, são utilizados os termos "dados sigilosos", "dados financeiros" e "dados pessoais". Saber diferenciá-los é imprescindível para a correta aplicação das leis, especialmente pelo fato destes dados poderem convergir em alguns casos, resultando na aplicação simultânea de mais de uma lei.

Dados Financeiros

São aqueles decorrentes de operações financeiras e serviços prestados por instituições financeiras. Essa definição advém da prática, não existe uma legislação específica definindo este termo. Dentre os três tipos de dados que comentaremos neste capítulo, este é o mais amplo, porque ele se caracteriza por um conjunto de mais de uma informação. Dados financeiros podem envolver informações sobre indivíduos específicos ou empresas, como também podem conter valores referentes às operações, datas de transação e assim por diante. A importância de entender a amplitude deste tipo de dado é justamente saber que ele nem sempre será um dado pessoal ou necessariamente um dado sigiloso, de forma que não precisará de tratamento diferenciado. Apenas a análise destes dados e o seu fluxo é o que poderá permitir uma conclusão sobre a forma adequada de tratá-los e quais procedimentos deverão ser adotados para entrar em conformidade com as normas.

Dados Sigilosos

Os "dados sigilosos" são aqueles que devem permanecer ocultos por determinação legal, judicial e, até mesmo, pessoal. A inviolabilidade do sigilo sobre dados é um direito constitucional, que pode ser excepcionado por uma ordem judicial para finalidade de investigação criminal[4]. Por isso, existem diversas razões pelas quais dados podem ser sigilosos. Existem dados sigilosos que não são financeiros, mas alguns dados financeiros são considerados sigilosos por determinação da lei, por exemplo. É o caso de dados bancários, conforme explicaremos mais adiante.

É importante lembrar que a solicitação de dados sigilosos realizada por parte de uma autoridade sem que haja determinação judicial pode ser considerada como quebra de sigilo. Por isso, se uma autoridade solicita que sejam cedidos dados sigilosos, muitas vezes é recomendado que um(a) advogado(a) seja acionado(a), antes de realizar esta liberação de informação. Isso, porque, em alguns casos, mesmo que o solicitante seja uma autoridade, pode ser que, ainda assim, esta necessite de decisão judicial para realizar tal solicitação.

Ao nos concentrarmos no mercado financeiro, a Lei Complementar nº 105, de 10 de janeiro de 2001 ("LC 105/2001") é a principal figura na regulação do sigilo das operações de instituições financeiras. De maneira geral, a norma afirma que as operações ativas, operações passivas e serviços prestados pelas instituições financeiras, enumeradas na lei[5], devem ser mantidas em sigilo[6].

[4] BRASIL. Constituição da República Federativa do Brasil de 1988. Artigo 5º, inciso XII. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso 21.08.2019.

[5] BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Artigo 1º, §1º, incisos I até XIII. Disponível em < http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm>. Acesso em 21.08.2019.

[6] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados Pessoais. Artigo 5º, inciso I. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 21.08.2019.

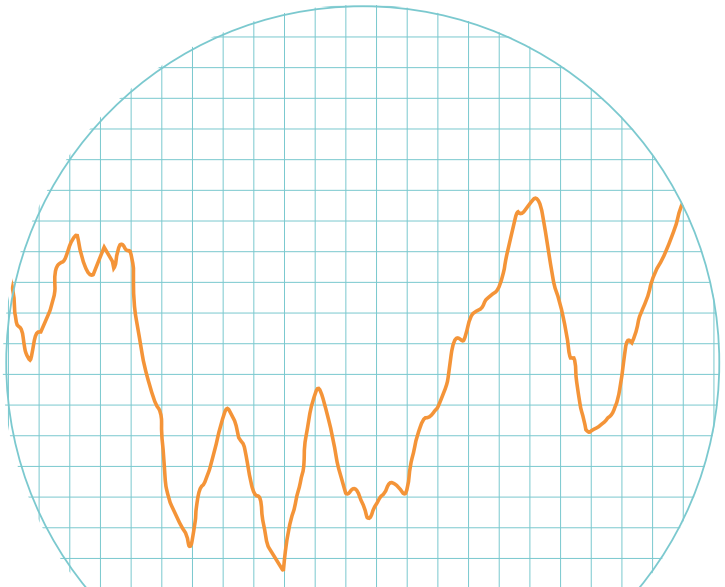
Portanto, alguns dados financeiros podem estar submetidos a sigilo em decorrência da lei. Existem diversos tipos de dados financeiros, uma parte deles está abarcada pela LC 105/2001.

Dados Pessoais

"Dados pessoais" estão definidos na LGPD como informações relacionadas a pessoa natural identificada ou identificável. Outra definição importante apresentada pela Lei é a de dados pessoais sensíveis, que são aqueles que versam "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Isso significa que dados financeiros ou até sigilosos não são por si só considerados sensíveis. A não ser que eles contenham informações ligadas à, como disposto na LGPD, origem racial ou étnica, convicção religiosa, opinião política e assim por diante.

Portanto, informações de pagamento do tratamento de quimioterapia de um paciente podem, a depender do caso, ser consideradas dados sensíveis, por trazer dados em relação à saúde daquele indivíduo que pode ser identificado ou identificável.



A identificação, direta ou indiretamente, é parte importante da classificação do dado como sendo pessoal ou sensível. Pensando em um financeiro relacionado ao pagamento de tratamento quimioterápico, que, contudo, não permite a identificação direta ou indireta de uma pessoa natural, então este dado não estaria sob o escopo da LGPD. Por outro lado, se o dado financeiro puder ser agregado a outras informações que permitam a identificação de uma pessoa natural, então as regras relativas à dados sensíveis se aplicariam ao caso. Existem diferenças práticas importantes para o tratamento de dados pessoais e de dados pessoais sensíveis, como veremos adiante.

Quando falamos em "tratamento de dados" estamos usando a linguagem estabelecida pelo artigo 5º, inciso X da LGPD, que define como:

> *"toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".*

Portanto, mesmo que a fintech não faça uso dos dados para nenhum propósito específico, a mera coleta, uso de informação obtida através de outra base de dados ou arquivamento dos dados já será considerado atividade de tratamento de dados, fazendo com que seja necessária a observância da LGPD. Explicaremos isso com mais cuidado adiante.

2.1/
RELAÇÃO ENTRE ESTES TIPOS DE DADOS

Tendo em mente estes tipos diferentes de dados é importante entender o cuidado que deve ser dado a cada um deles, sabendo identificar quando coincidem, acumulando, portanto, obrigações e responsabilidades, principalmente pensando na segurança da informação que deve ser garantida no tratamento destes dados.

Em outras palavras, é possível que exista um dado financeiro sem que este seja sigiloso ou pessoal (exemplo: uma pesquisa de mercado que apresente informações volumétricas sobre financiamento de apartamentos por jovens, na cidade de São Paulo). Por outro lado, se esta pesquisa contiver informações que permitam a identificação dos entrevistados, o que antes eram apenas dados financeiros se tornam não apenas sigilosos, sob proteção de leis penais como também terão proteção sob a óptica da LGPD.

Essa imagem representa as diferentes formas destes dados se relacionarem, conforme abordaremos a seguir.

Imagem 1: Relação entre dados financeiros, dados sigilosos e dados pessoais

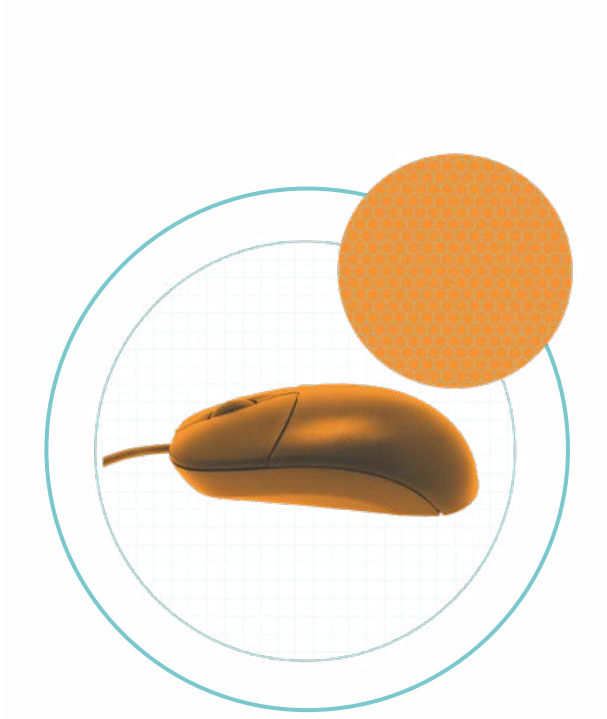
3/
LEGISLAÇÕES APLICÁVEIS ÀS FINTECHS E RESPONSABILIZAÇÃO EM CASO DE INCIDENTE

Diante do arsenal regulatório mencionado, como saber quais normas impactam as atividades das fintechs, levando em conta a intersecção entre mercado financeiro e proteção de dados?

Qual seria exatamente o impacto de incidentes de segurança da informação sobre a responsabilidade de agentes no mercado financeiro?

Quem são os atores envolvidos dentro do contexto de cada norma, quais são suas obrigações e que sanções são aplicadas caso ocorram incidentes, como vazamentos, utilização indevida, armazenamento incorreto de dados?

Vale mencionar que quando usamos o termo "incidentes" estamos considerando os eventos de forma ampla, aplicando-se a diversas hipóteses de infrações estipuladas por normais penais, cíveis e administrativas, se referindo ao uso inadequado, vazamento, quebra de sigilo dentre outras hipóteses, neste cenário de proteção de informações dentro do setor financeiro. Dentre estas normas, temos agora como grande referência para a proteção de dados pessoais, a LGPD.



3.1/
LEI DE CRIMES CONTRA O SISTEMA FINANCEIRO NACIONAL

A Lei nº 7.492 de 16 de junho de 1986 ("Lei de Crimes Contra o Sistema Financeiro Nacional") é um dos principais instrumentos de proteção ao mercado financeiro no Brasil. A Lei define "instituição financeira" como pessoa jurídica de direito público ou privado que exerça pelo menos as seguintes atividades: captação, intermediação ou aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira. O exercício de atividades como a custódia, emissão, distribuição, negociação, intermediação ou administração de valores mobiliários são englobados, também, no conceito de instituições financeiras[7].

Esta definição é relevante para compreendermos como funciona o regime de responsabilização na Lei de Crimes contra o Mercado Financeiro. Neste cenário, são penalmente responsáveis o *controlador* e os *administradores* de instituições financeiras, incluindo diretores e gerentes, por exemplo[8]. Ainda, a Lei determina que administradores de instituições financeiras se equiparam aos interventores, liquidantes ou síndicos.

Com base na definição ampla de "instituição financeira" trazida, é possível verificar que algumas fintechs estão submetidas à aplicação dos dispositivos desta lei, em razão da natureza das atividades que exercem diretamente[9].

[7] BRASIL. Lei nº 7.492, de 16 de junho de 1986. Define os crimes contra o mercado financeiro nacional. Artigo 1º. Disponível em: <http://www.planalto.gov.br/cciviL_03/LEIS/L7492.htm> Acesso em: 27.08.2019.

[8] Ibidem Artigo 25, caput e artigo 25, §1º.

[9] Ibidem. "Art. 1º Considera-se instituição financeira, para efeito desta lei, a pessoa jurídica de direito público ou privado, que tenha como atividade principal ou acessória, cumulativamente ou não, a captação, intermediação ou aplicação de recursos financeiros (Vetado) de terceiros, em moeda nacional ou estrangeira, ou a custódia, emissão, distribuição, negociação, intermediação ou administração de valores mobiliários. Parágrafo único. Equipara-se à instituição financeira:
I - a pessoa jurídica que capte ou administre seguros, câmbio, consórcio, capitalização ou qualquer tipo de poupança, ou recursos de terceiros;
II - a pessoa natural que exerça quaisquer das atividades referidas neste artigo, ainda que de forma eventual."

Isso quer dizer que esta lei deve ser observada em sua integridade, não apenas em relação à forma que os dados são tratados. As sanções, em caso de descumprimento, são altas, especialmente pelo fato de ser uma norma de teor penal.

O artigo 18 da Lei de Crimes contra o Sistema Financeiro dispõe o seguinte:

> *"Art. 18. Violar sigilo de operação ou de serviço prestado por instituição financeira ou integrante do sistema de distribuição de títulos mobiliários de que tenha conhecimento, em razão de ofício: Pena – reclusão, de 1(um) a 4 (quatro) anos, e multa."*
> Portanto, é crime violar o sigilo de dados de operação ou de serviços prestados por instituição financeira, tendo a pessoa o conhecimento destes dados com base nas informações que teve contato no seu ambiente de trabalho. Isso reforça o entendimento de que alguns dados financeiros também são dados sigilosos, conforme já abordado.

De acordo com o artigo 29 desta mesma lei:

> *"Ministério Público Federal, sempre que julgar necessário, poderá requisitar, a qualquer autoridade, informação, documento ou diligência, relativa à prova dos crimes previstos nesta lei (...) O sigilo dos serviços e operações financeiras não pode ser invocado como óbice ao atendimento da requisição prevista no caput deste artigo". (grifos nossos)*

Ou seja, o Ministério Público Federal pode requerer informações sigilosas para autoridades, quando se tratar de evidências ou indícios de crime, sendo que essas autoridades, diferente do que ocorre com a Lei de Sigilo Bancário, não poderão invocar a proteção constitucional do sigilo para negar a disponibilidade do conteúdo solicitado.

Essa prerrogativa conferida ao Ministério Público, contudo, não significa que ele tenha autorização legal para solicitar informações sigilosas sobre clientes, mesmo que sob suspeita de crime, para instituições que tenham dados sobre a pessoa suspeita, sem que haja uma decisão judicial autorizando esta liberação de informação.

3.2/ CÓDIGO PENAL

A LGPD não se aplica ao tratamento de dados relacionados à aplicação da lei, investigação ou repressão de infrações penais. Ela também não cria tipos penais novos. A criação de tipos penais que protejam dados de diversos tipos (não só dados pessoais) fica a cargo de algumas normas, dentre elas, o Código Penal Brasileiro (Decreto-Lei nº 2.848, de 7 de dezembro de 1940) e outras leis penais especiais.

O Código Penal possui uma seção dedicada aos Crimes Contra a Inviolabilidade dos Segredos (artigos 153 – 154-B). Esta seção foi modificada pela Lei nº 12.737, de 30 de novembro de 2012 que incluiu o crime de "invasão de dispositivo informático" que consiste em:

> *"Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".*

É importante mencionar este crime, pois os sistemas e dispositivos de fintechs podem ser vulneráveis a estes ataques. Isso pode resultar em incidentes de segurança, conforme abordaremos adiante.

Além disso, o Código Penal não determina medidas específicas em relação à proteção de dados, focando mais no sigilo e confidencialidade. Os outros crimes do Código Penal brasileiro (que tratam de sigilo e confidencialidade) são: **(i)** divulgação de segredo (art. 153); e **(ii)** violação de segredo profissional (artigo 154).

O primeiro é configurado por:

> *"Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:*
> *Pena - detenção, de um a seis meses, ou multa."*

O segundo se configura por:

> *"Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:*
> *Pena - detenção, de três meses a um ano, ou multa."*

É fácil de compreender como esses crimes podem acontecer num contexto em que diversos colaboradores tenham acesso aos sistemas tecnológicos contendo dados sigilosos. Dessa forma, as atividades das fintechs devem considerar formas de evitar a prática de condutas que possam configurar esses crimes. Por exemplo, oferecendo treinamentos aos funcionários que têm acesso aos dados, informando sobre a responsabilidade na manutenção de sigilo e prevenindo casos de violação de segredo profissional (artigo 154). Vale lembrar que o Código Penal e as leis penais especiais são aplicáveis a todos brasileiros maiores de 18 anos[10].

[10] Salvo aqueles classificados como inimputáveis: "agente que, por doença mental ou desenvolvimento mental incompleto ou retardado, era, ao tempo da ação ou da omissão, inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se de acordo com esse entendimento" BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Institui o Código Penal. Artigo 26.

3.3/
LEI DE LAVAGEM DE DINHEIRO

A Lei nº 9.613, de 3 de março de 1998 também conhecida como a Lei de Lavagem de Dinheiro, possui artigos que indiretamente impactam como os dados devem ser processados e enviados dentro do setor financeiro, especialmente em relação às inspeções do Conselho de Controle de Atividades Financeiras ("COAF"). Ela surgiu para afastar os riscos de utilização do mercado para ocultar origem irregular do dinheiro.

Abaixo, fizemos uma lista resumida de disposições importantes desta lei sobre o uso de dados por membros do setor financeiro.

(i) Identificação dos seus clientes e manutenção de registros atualizados sobre eles;

(ii) registro de todas as transações financeiras que ultrapassem os limites permitidos pela lei;

(iii) responder adequadamente a todos os pedidos feitos pelo COAF ou outro regulador, sabendo que o destinatário de tal informação será responsável por manter sigilo das respostas enviadas;

(iv) prestar especial atenção a qualquer transação que demonstre evidências sérias de provável crime, comunicando o fato, em sigilo, ao COAF no prazo de 24 horas; e

(v) as instituições ou pessoas que não cooperarem com os requisitos acima podem estar sujeitas às seguintes sanções: advertências; multas; inabilitação temporária de exercer cargos de gestão de instituições financeiras; cassação e suspensão da atividade, operação ou função.

As penalidades previstas na Lei[11] são:

(i) Advertência, caso haja irregularidade no cumprimento das obrigações previstas em Lei;

(ii) multa pecuniária variável, com valor não superior:

ii.1. ao dobro do valor da operação;

ii.2. ao dobro do lucro real obtido ou que presumivelmente seria obtido pela realização; ou

ii.3. à vinte milhões de reais.

(iii) inabilitação temporária por até dez anos, para o exercício do cargo de administrador das pessoas jurídicas referidas no artigo 9º;

(iv) cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento.

É importante destacar, no contexto dessa Lei, que o COAF (atualmente denominado UIF) [12] , diferente das autoridades reguladoras, foi criado com a finalidade de ser uma Unidade de Inteligência Financeira, que captura informações de operações consideradas suspeitas pelo comunicante ou realizadas em dinheiro "vivo" em valores superiores aos limites fixados em normativos (R$ 30.000,00). O BACEN, A Comissão de Valores Mobiliários ("CVM") e, muito menos a Receita Federal tem autorização para acessar o bando de dados do COAF. Esses órgãos somente têm acesso às informações do COAF quanto este inclui a informação em Relatórios de Inteligência Financeira que são disparados para os demais órgãos, caso sejam identificados indícios consistentes de irregularidade.

Ao lidar com dados pessoais no contexto dessa norma, é preciso, também, considerar os pontos elencados pela LGPD e outras normas sobre proteção de dados na interpretação da Lei de Lavagem de Dinheiro. Grande parte das normas do mercado financeiro é anterior à LGPD, de forma que é preciso revisitá-las, aplicando-as conjuntamente.

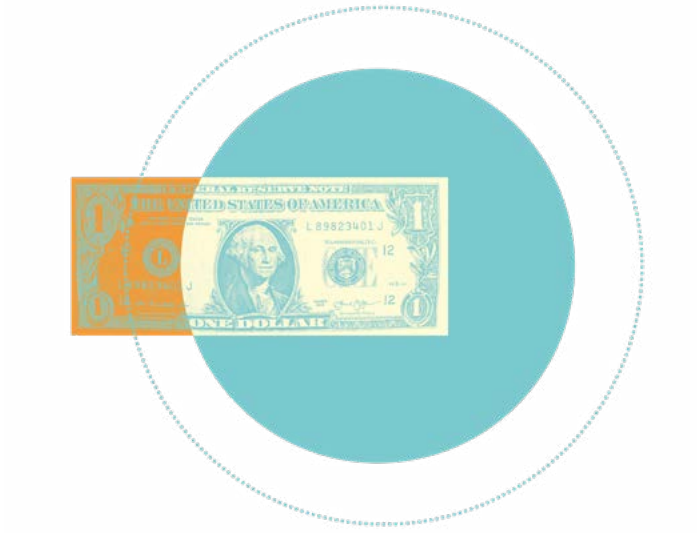
[11] BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e dá outras providências. Artigo 12, incisos I a IV. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9613.htm>. Acesso em: 27.08.2019.

[12] De acordo com a Medida Provisória nº 893, de 19 de agosto de 2019, o COAF passa a se chamar Unidade de Inteligência Financeira , conservando as competências originárias do COAF, porém passando a ficar vinculada administrativamente ao Banco Central do Brasil, e não mais ao Ministério da Economia. Disponível em <https://www.fazenda.gov.br/orgaos/coaf/banners-rotativos/o_que_faz.pdf>. Acesso em 02.09.2019.

3.4/
LEI DO SIGILO BANCÁRIO

A Lei Complementar nº 105, de 10 de janeiro de 2001 também conhecida como Lei do Sigilo Bancário exige confidencialidade das instituições financeiras e outras empresas, em razão da natureza de suas operações e dos dados financeiros com as quais lidam. Isso significa que fintechs podem estar legalmente vinculadas à Lei do Sigilo Bancário, mesmo que algumas delas não sejam necessariamente instituições financeiras de acordo com a legislação brasileira.

Algumas fintechs podem ser entendidas como instituições financeiras, porque se enquadram nos requisitos legais; por outro lado, nem todas as fintechs são instituições financeiras como, por exemplo, aquelas que podem operar, com alguns limites, sem autorização prévia do BACEN. A conformidade destas empresas com a Lei do Sigilo Bancário, portanto, ocorrerá com base nas informações a que tenham acesso para oferecer serviços ou produtos aos clientes.



Os atores previstos na Lei de Sigilo Bancário

A Lei Complementar nº 105/2001 elenca uma série de atores considerados instituições financeiras. Eles devem se submeter ao dever de sigilo em suas operações ativas e passivas, bem como em serviços prestados. Para fins de definição, a Lei enumera já em seu artigo 1º, §1º uma série de agentes englobados na definição de "instituições financeiras"[13].

Essa Lei também destaca outros agentes que devem obedecer ao dever de sigilo, como empresas de fomento comercial ou factorings. Este dever se estende também às autoridades administrativas, como o BACEN e a CVM, sendo afastado somente nos casos em que desempenharem suas funções de fiscalização e investigatórias, em suas respectivas competências[14].

Nesses casos investigativos em que a autoridade administrativa verifica a existência de algum indício de irregularidade, e somente nesses casos, os dados sigilosos podem ser compartilhados com outras autoridades competentes. Ou seja, é importante que fique claro que, inclusive os órgãos administrativos não podem divulgar informações sigilosas ou permitir o acesso direto a essas informações para outros órgãos como o Ministério Público, a Polícia Federal, autoridades estrangeiras ou quem quer que seja.

[13] São eles: (1) Bancos de qualquer espécie; (2) Distribuidoras de Valores Mobiliários; (3) Corretoras de Câmbio e de Valores Mobiliários; (4) Sociedades de Crédito, Financiamento e Investimento; (5) Sociedades de Crédito Imobiliário; (6) Administradoras de Cartões de Crédito; (7) Sociedades de Arrendamento Mercantil; (8) Administradoras de Mercado de Galpão organizado; (9) Cooperativas de Crédito; (10) Associações de Poupança e Empréstimo; (11) Bolsas de Valores e de Mercadorias e futuros; (12) Entidades de Liquidação e Compensação; e (13) Outras sociedades que, em razão da natureza de suas obrigações, assim venham a ser consideradas pelo Conselho Monetário Nacional.

[14] BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Artigo 2º, §1º a §6º.

As obrigações previstas na Lei de Sigilo Bancário

O **dever de sigilo** é a principal obrigação instituída pela Lei de Sigilo Bancário às instituições financeiras. São instituídas também algumas obrigações para entidades públicas (como a CVM e o BACEN) que devem, sempre que se fizer necessário, prestar informações ao COAF, à Advocacia-Geral da União, ao Poder Legislativo Federal e à administração tributária da União[15]. Além disso, a CVM e o BACEN têm a obrigação de comunicar ao Ministério Público a ocorrência de um crime[16].

Vale ressaltar que a Lei do Sigilo Bancário é tão enfática em relação à compulsoriedade no cumprimento dessa obrigação, que nos mostra o que não seria considerado violação do dever de sigilo[17], ou seja, traz como exceção as hipóteses em que o dever de sigilo não se aplica. São elas:

(i) Troca de informações entre instituições financeiras para propósitos de fins cadastrais;

(ii) fornecimento de informações de cadastro de devedores para entidades de proteção de crédito;

(iii) fornecimento de informações sobre identificação dos contribuintes e valores globais de suas operações à Secretaria da Receita Federal;

(iv) comunicação às autoridades competentes da prática de infrações, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa;

(v) revelação de informações sigilosas com o consentimento expresso dos interessados;

(vi) prestação de informações entre entidades públicas; e

(vii) fornecimento de dados financeiros e pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento, de pessoas naturais ou jurídicas, para gestores de bancos de dados, para formação do histórico de crédito.

Um ponto importante diz respeito ao consentimento expresso dos interessados com relação ao compartilhamento das suas informações pessoais. Na hipótese de haver consentimento expresso do titular da informação para a divulgação de informações sigilosas, não haverá cometimento de crime.

A relevância dos dados obtidos por instituições financeiras e outros do mesmo mercado não requerem apenas níveis adequados de segurança cibernética, como também torna necessário que essas empresas repensem os procedimentos internos para que o tratamento de dados seja realizado de acordo com a LGPD e as outras normas complementares que também prevejam sigilo[17] e confidencialidade.

[15] Ibidem. Artigo 2°, §6°; Artigo 3°, §3°; Artigo 4°; e Artigo 5°.
[16] Ibidem. Artigo 9°.
[17] Ibidem. Artigo 1°, §3°, incisos I a VII.

3.5/
RESOLUÇÃO CMN Nº 4.658/2018 SOBRE CIBERSEGURANÇA

O Conselho Monetário Nacional ("CMN"), por meio da Resolução CMN nº 4.658 de 26 de abril de 2018, ("Resolução CMN nº 4.658/2018") trouxe novo regramento 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 a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN.

Estas organizações devem implementar e manter Política de Segurança Cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, conforme dispõe o artigo 2º. Ainda, deve ser instituído também um Plano de Ação e de Respostas a Incidentes.

Essas instituições do setor financeiro precisam indicar um Diretor de Segurança Cibernética e só podem contratar prestadores de serviços estabelecidos em países que tenham um acordo com o BACEN.

Tendo em mente o escopo da Resolução CMN nº 4.658/2018, analisaremos agora os seguintes aspectos:

(i) como se dá a implementação de Políticas de Segurança Cibernética;

(ii) quais são os pontos centrais previstos para o Plano de Ação e Respostas a Incidentes;

(iii) obrigações presentes no regime de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem; e

(iv) questões pertinentes ao BACEN.

A implementação de uma Política de Segurança Cibernética.

Segundo a Resolução CMN nº 4.658/2018, a implementação de uma Política de Segurança Cibernética deve ser aprovada pelo Conselho de Administração ou, na sua inexistência, pela Diretoria da instituição.

Esta Política de Segurança Cibernética deve conter, pelo menos:

(i) objetivos de segurança cibernética da instituição, que devem contemplar a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;

(ii) procedimentos e controles adotados para redução de vulnerabilidade da instituição a incidentes e atender os demais objetivos de segurança cibernética. Eles devem abranger, pelo menos: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações. Devem também ser aplicados inclusive no desenvolvimento de sistemas de informações seguros e na adoção de novas tecnologias empregadas nas atividades da instituição;

(iii) controles específicos, incluindo aqueles de rastreabilidade da informação, para garantir a segurança das informações sensíveis;

(iv) registro, análise da causa e do impacto e o controle dos efeitos de incidentes relevantes para as atividades da instituição;

(v) diretrizes para:

a. elaboração de cenários de incidentes, considerados nos testes de continuidade de negócios;

b. definição de procedimentos e de controles para prevenção de incidentes no tratamento de dados sensíveis ou relevantes para as atividades operacionais da instituição, devendo contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os usados pela própria instituição;

c. classificação dos dados e das informações quanto à relevância;

d. definição dos parâmetros a serem utilizados na avaliação de relevância dos incidentes.

(vi) mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a. implementação de programas de capacitação e de avaliação periódica de pessoal;

b. prestação de informações a clientes e usuários sobre precauções na utilização dos produtos; e

c. demonstração de comprometimento da alta administração da instituição com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

(vii) iniciativas para compartilhamento de informações com as demais instituições financeiras, ou instituições com funcionamento autorizado pelo BACEN, sobre os incidentes relevantes.

Além disso, a Política de Segurança Cibernética deve ser compatível com alguns fatores. O primeiro deles é a compatibilização da Política de Segurança com o porte, perfil de risco e o modelo de negócio da instituição. O segundo, refere-se a natureza das operações e a complexibilidade dos produtos, serviços, atividades e processos da instituição. O terceiro fator relaciona-se com a sensibilidade dos dados e informações sob responsabilidade da instituição.

As instituições podem adotar uma Política de Segurança Cibernética única por conglomerado prudencial e sistema cooperativo de crédito[18]. Ou seja, caso instituições estejam em um mesmo conglomerado prudencial, ou integrem um conjunto sistema cooperativo de crédito, podem formular e implementar a mesma Política de Segurança Cibernética.

[18] BRASIL. Resolução nº 4.658, de 26 de abril de 2018. 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 a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Artigo 2º, §2º. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf> Acesso em 21.08.2019.

Vale ressaltar também a obrigação de documentação e revisão desta Política de Segurança Cibernética, no mínimo, anualmente[19].

Por fim, é importante destacar a **necessidade de divulgação da Política de Segurança Cibernética**. Ela deve ser divulgada aos funcionários da instituição e às empresas prestadoras de serviços à terceiros. Esta divulgação deve ter linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações[20]. Ainda, ressalta-se que as instituições **devem divulgar ao público** um resumo contendo linhas gerais da Política de Segurança Cibernética[21].

O Plano de Ação e de Resposta a Incidentes.

Na prática, é importante saber quais devem ser as medidas adotadas em resposta a ocorrência de incidentes. Caso ocorram vazamentos de informações, ou armazenamento incorreto de dados, entre outras possibilidades de uso indevido de dados, como proceder?

Surge então, através da Resolução CMN nº 4.658/2018, o chamado "Plano de Ação e de Resposta a Incidentes". A existência deste plano também depende da aprovação pelo Conselho de Administração ou, na sua inexistência, pela Diretoria da instituição.

Este plano deve abranger, pelo menos[22]:

(i) as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

(ii) as rotinas, procedimentos, controles e as tecnologias a serem utilizadas na prevenção e na resposta a incidentes, conforme as diretrizes da Política de Segurança Cibernética; e

(iii) qual a área responsável pelo registro e

[19] Ibidem. Artigo 10.

[20] Ibidem Artigo 4º. Acesso em 21.08.2019.

[21] Ibidem. Artigo 5º. Acesso em 21.08.2019

[22] Ibidem. Artigo 6º, incisos I a III. Acesso em 21.08.2019

controle dos efeitos de incidentes relevantes.

Ainda, as instituições têm a obrigação de apontar um Diretor responsável tanto pela Política de Segurança Cibernética, quanto pela implementação do Plano de Ação e Respostas a Incidentes.

Neste âmbito, há também a obrigação de elaboração, pelas instituições, de um **relatório anual** sobre a implementação do Plano de Ação e de Respostas a Incidentes[23], com data-base em 31 de dezembro.

Este relatório deve conter, no mínimo, informações sobre:

(i) a efetividade da implementação das ações do Plano de Ação e Respostas a Incidentes;

(ii) um resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizadas na prevenção e na resposta de incidentes;

(iii) quais incidentes relevantes relacionados com o ambiente cibernético ocorreram no período; e

(iv) quais são os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

É importante lembrar que, segundo a Resolução CMN nº 4.658/2018, o Relatório Anual deve ser submetido ao Comitê de Risco da instituição, quando ele existir, e ao Conselho de Administração ou, quando inexistente, à Diretoria da instituição até 31 de março do ano seguinte ao da data-base.

Assim como a Política de Segurança Cibernética, o Plano de Ação e de Resposta a Incidentes deve ser documentado e revisado pelo menos uma vez por ano[24].

[23] Ibidem. Artigo 8º. Acesso em 21.08.2019.

[24] Ibidem. Artigo 10. Acesso em 21.08.2019.

O regime de Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em nuvem, nos moldes da Resolução CMN nº 4.658/2018.

A Resolução CMN nº 4.658/2018 tem diversas disposições acerca dos procedimentos de contratação, pelas instituições, de serviços de processamento e armazenamento de dados e de computação em nuvem, já que se faz necessário que estas contratações de terceirização de serviços contemplem as políticas, estratégias e estruturas para gerenciamento de riscos[25].

Assim, para que este tipo de contratação possa ocorrer, são estabelecidas algumas obrigações anteriores, inclusive, à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem. É preciso que as instituições adotem e documentem procedimentos como[26]:

(i) adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;

(ii) verificação da capacidade do potencial prestador de serviço de assegurar:

a. cumprimento da legislação e da regulamentação em vigor, sendo que a instituição deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo terceiro, prestador de serviço;

b. acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c. confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d. aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

e. acesso da instituição aos relatórios elaborados por empresa de auditoria especializada independente, contratada pelo prestador de serviço, em relação aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f. provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g. identificação e segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

h. qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Em seguida, a Resolução do CMN nº 4.658/2018 determina que serviços de computação em nuvem abranjam, sob demanda e de maneira virtual da instituição contratante, serviços como:

> *"o processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos".*[27]

[25] Ibidem. Artigo 11. Acesso em 21.08.2019.
[26] Ibidem. Artigo 12, incisos I, II e alíneas *a* a *h*. Acesso em 21.08.2019.
[27] Ibidem Artigo 13, *caput*, e artigo 13, inciso I. Acesso em 21.08.2019.

Outros serviços enquadrados na definição de serviços de computação em nuvem seriam **(i)** a implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços[28]; e **(ii)** a execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços[29].

Vale dizer que ainda persiste a responsabilidade da instituição de que os serviços prestados por terceiro obedeçam a confiabilidade, integridade, disponibilidade, segurança e sigilo, além do cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada pelas instituições ao BACEN. Esta comunicação deve ser feita pelo menos 60 dias antes da contratação do serviço, ou, havendo alterações contratuais, a comunicação deve ser feita pelo menos 60 dias antes da alteração contratual. [30] [31]

Caso os serviços contratados de processamento, armazenamento de dados e de computação em nuvem ocorram no exterior, eles devem observar requisitos dispostos no artigo 16, da Resolução do CMN nº 4.658/2018[32].

Como podemos perceber, a Resolução CMN nº 4.658/2018 é extensa, e delimita inclusive, em seu artigo 17, quais são as cláusulas contratuais essenciais para os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem.

Por fim, outro fator fundamental a ter em mente é a obrigação das instituições de instituir mecanismos de acompanhamento e controle, como forma de assegurar a implementação e a efetividade da Política de Segurança Cibernética, do Plano de Ação e de Resposta a Incidentes e dos Requisitos de Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em nuvem, incluindo[33]:

(i) definição de processos, testes e trilhas de auditoria;

(ii) definição de métricas e indicadores adequados; e

(iii) identificação e a correção de eventuais deficiências.

[28] Ibidem. Artigo 13, inciso II. Acesso em 21.08.2019.

[29] Ibidem. Artigo 13, inciso III. Acesso em 21.08.2019.

[30] E o que está comunicação ao BACEN deve informar? As informações necessárias são referentes a (i) denominação da empresa a ser contratada; (ii) os serviços relevantes a serem contratados; e (iii) a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados. Ibidem. Artigo 15, caput e artigo 15, §2°e §3°. Acesso em 21.08.2019

[31] Ibidem. Artigo 15, §1°, incisos I a III. Acesso em 21.08.2019

[32] Ibidem. Art. 16. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior deve observar os seguintes requisitos: I - a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados; II - a instituição contratante deve assegurar que a prestação dos serviços referidos no caput não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil; III - a instituição contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e IV - a instituição contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços. § 1° No caso de inexistência de convênio nos termos do inciso I do caput, a instituição contratante deverá solicitar autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações requeridas nos termos do art. 15 desta Resolução. § 2° Para atendimento aos incisos II e III do caput, as instituições deverão assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil aos dados e às informações. § 3° A comprovação do atendimento aos requisitos de que tratam os incisos I a IV do caput e o cumprimento da exigência de que trata o § 2° devem ser documentados.

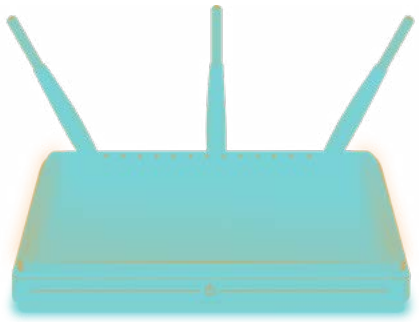
[33] Ibidem. Artigo 21, caput, incisos I a III. Acesso em 21.08.2019

Questões pertinentes ao BACEN, segundo a Resolução CMN nº 4.658/2018.

Finalmente, a Resolução CMN nº 4.658/2018 determina, em suas disposições finais, que alguns documentos devem permanecer à disposição do BACEN pelo prazo de cinco anos[34].

Ainda, o BACEN pode adotar as medidas que julgar necessárias e estabelecer **(i)** os requisitos e procedimentos para o compartilhamento de informações; **(ii)** exigir certificações e outros requisitos técnicos a serem requeridos das empresas contratadas pelas instituições; **(iii)** prazos máximos para reinício ou normalização das atividades ou dos serviços relevantes interrompidos; **(iv)** os requisitos técnicos e procedimentos operacionais a serem observados pelas instituições para cumprimento da Resolução.

Adicionalmente, o BACEN é o órgão competente para vetar ou impor restrições para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, descumprimento ou inobservância da Resolução CMN nº 4.658/2018. O BACEN poderá, assim, estabelecer prazo para adequação dos referidos serviços[35].



[34]Estes documentos são: (1) Documento relativo à Política de Segurança Cibernética; (2) Ata de Reunião do Conselho de Administração ou, na sua inexistência, da Diretoria da instituição, caso seja adotada uma Política de Segurança Cibernética única; (3) Documento relativo ao Plano de Ação e de Resposta a Incidentes; (4) Relatório Anual; (5) Documentação sobre contratação de serviços relevantes de processamento e armazenamento de dados e de computação nuvem; (6) Documentação relevante caso sejam contratados serviços relevantes de processamento e armazenamento de dados e de computação nuvem no exterior; (7) Contratos de prestação de serviços relevantes de processamento e armazenamento de dados e de computação nuvem; (8) Dados, registros e as informações relativas aos mecanismos de acompanhamento e de controle, contando o prazo a partir de sua implementação. BRASIL. Ibidem. Artigo 23, caput, incisos I a VIII. Acesso em 21.08.2019

[35]Ibidem. Artigo 27. Acesso em 21.08.2019

3.6/
CIRCULAR BACEN Nº 3.909/2018 SOBRE CIBERSEGURANÇA

Seguindo a mesma lógica da Resolução CMN nº 4.658/2018 a Circular do BACEN nº 3.909 de 16 de agosto de 2018 ("Circular BACEN nº 3.909/2018") prevê especificidades relativas à Política de Segurança Cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, só que desta vez, a serem observados pelas instituições de pagamento autorizadas a funcionar pelo BACEN.

Conforme analisado, a estrutura e as obrigações previstas na Resolução CMN nº 4.658/2018 e na Circular BACEN nº 3.909/2018 são extremamente similares. Isto porque, no que concerne a regulação de Políticas de Segurança Cibernética, a implementação de Planos de Ação e de Resposta a Incidentes, e até mesmo em relação ao regime de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o órgão regulador praticamente replicou o disposto na Resolução CMN nº 4.658/2018 sobre a Circular BACEN nº 3.909/2018, alterando apenas os alvos da regulação, que passaram a ser as **instituições de pagamento.**

Por serem normas tão similares, focaremos em seus pontos de diferença, que, já adiantando, são poucos.

Diferentemente da Resolução CMN nº 4.658/2018, a Circular BACEN nº 3.909/2018 refere-se às instituições de pagamento com funcionamento autorizado pelo Banco Central do Brasil. O próprio BACEN define instituição de pagamento como sendo:

> *"pessoa jurídica que viabiliza serviços de compra e venda e de movimentação de recursos, no âmbito de um arranjo de pagamento, sem a possibilidade de conceder empréstimos e financiamentos a seus clientes*[36]*".*

A primeira diferença identificada entre estas normas refere-se ao escopo de suas Políticas de Segurança Cibernética. A Resolução CMN nº 4.658/2018 requer, para a sua implementação, iniciativas para compartilhamento de informações sobre incidentes relevantes entre instituições financeiras e outras instituições com funcionamento autorizado pelo BACEN.

Por sua vez, a Circular BACEN nº 3.909/2018 não restringe o compartilhamento de informações sobre incidentes relevantes apenas entre outras instituições de pagamento. Ao contrário: ela prevê que informações desta natureza sejam compartilhadas por instituições de pagamento com outras instituições de pagamento, com instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN[37].

A segunda diferença refere-se à comunicação ao BACEN sobre a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem. Além do rol de informações que devem ser comunicadas ao BACEN e seus prazos, previstos no artigo 15 da Resolução CMN nº 4.658/2018, a Circular BACEN adicionou uma provisão que dispõe que a comunicação destas informações podem ser realizadas em prazos inferiores a 60 dias em casos excepcionais, como forma de garantir o funcionamento regular da instituição de pagamento, desde que acompanhada de justificativa fundamentada[38].

[36] BRASIL. Banco Central do Brasil. O que é instituição de pagamento? Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/instituicaopagamento>. Acesso em: 21.08.2019.

[37] BRASIL. Circular nº 3.909, de 16 de agosto de 2018. 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 a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil. Artigo 3º, inciso VII. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50645/Circ_3909_v1_O.pdf> Acesso em 27.08.2019.

[38] Ibidem. Artigo 15, §4º.

A terceira diferença identificada concerne aos prazos que as instituições de pagamento têm, em comparação com instituições financeiras ou outras instituições com funcionamento autorizado pelo BACEN, para enviar ao BACEN seus cronogramas de adequação às normas regulatórias.

Nessa mesma toada, existe outra diferença de prazo, quando comparamos instituições financeiras e outras instituições com as instituições de pagamento. Estas últimas têm até 90 dias, contados a partir da entrada em vigor da Circular, para aprovarem suas Políticas de Segurança Cibernética e Planos de Ação e de Resposta a Incidentes[39]. Enquanto instituições financeiras e outras instituições autorizadas a funcionar pelo BACEN poderiam aprovar estes documentos até 6 de maio de 2019.

A diferença final entre estes documentos refere-se às competências atribuídas ao BACEN. A Resolução CMN nº 4.658/2018 determinava que o BACEN pode vetar ou impor restrições para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, descumprimento ou inobservância da Resolução CMN nº 4.658/2018. O BACEN poderá, assim, estabelecer prazo para adequação dos referidos serviços.

Na Circular BACEN nº 3.909/2018 também existe esta previsão. Contudo, ela é expandida, já que compete ao BACEN também impor às instituições de pagamento o prazo de adequação não só para os serviços de processamento e armazenamento de dados e de computação em nuvem, como também o prazo de adequação para os contratos correspondentes[40].

[39] Ibidem. Artigo 25.

[40] Ibidem. Artigo 26.

3.7/
LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD é uma lei de uso geral, que busca regular qualquer tipo de tratamento[41] de dados pessoais, similar à *General Data Protection Rule* ("GDPR")[42]. Vale lembrar que a LGPD só entra em vigor no dia 20 de agosto de 2020. Isso significa que as instituições que lidam com dados pessoais têm até esta data para entrarem em conformidade.

Como não é uma norma direcionada especificamente ao sistema financeiro ela não traz dispositivos focados para esse setor, uma vez que o interesse dela é regular a forma que dados são usados nos mais diversos setores da sociedade.

Contudo, diversas obrigações previstas na LGPD já são exigíveis atualmente por meio de outros diplomas como o Código de Defesa do Consumidor e o Marco Civil da Internet, que possuem obrigações coincidentes em alguns casos. Por isso, pensando em segurança jurídica, quanto antes forem adotados os dispositivos da LGPD, melhor será para a organização que busca conformidade.

A LGPD se aplica para quaisquer tratamentos de dados realizados em território brasileiro e/ou tratamento de dados de pessoas naturais que estejam em nosso território, seja de forma digital ou analógica. Essa regra não leva em consideração as diferentes formas de tratamento ou a localização da empresa.

Em resumo, ela se aplica para:

- tratamento de dados de pessoas localizadas em território nacional;
- tratamento de dados realizados em território nacional;
- tratamento de dados com o objetivo de comercializar produtos e serviços para o público brasileiro.

[41] Explicamos o conceito de tratamento de dados pessoais conforme a LGPD no capítulo "Uma visão geral dos dados no mercado financeiro". Trata-se de um conceito importante para compreender as diferentes formas de utilização de dados pessoais.

[42] UNIÃO EUROPEIA. Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. General Data protection Regulation.

Os atores da Lei Geral de Proteção de Dados Pessoais

Na LGPD, são considerados agentes responsáveis pelo tratamento de dados o controlador e o operador. Outro importante agente nesta matéria é também o encarregado. O controlador é definido na Lei como: *"uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"*.[43] Por sua vez, entende-se como operador a pessoa que realiza o tratamento de dados pessoais em nome do controlador, seja ela uma pessoa jurídica ou natural, de direito público ou privado.[44]

As obrigações definidas na LGPD

A LGPD dispõe de um extenso rol de obrigações para os controladores, e serão analisadas aqui aquelas mais pertinentes para as atividades exercidas no mercado financeiro.

A primeira refere-se à necessidade de o controlador realizar um relatório de impacto à proteção de dados pessoais, que pode ser solicitado por autoridade nacional[45]. Este documento deverá conter a descrição dos processos de tratamento de dados pessoais que possam arriscar as liberdades civis e direitos fundamentais, além de incluir medidas, salvaguardas e mecanismos de mitigação de risco de incidentes[46].

Ainda, caso o titular tenha dado seu consentimento para o tratamento de seus dados pessoais, cabe ao controlador o ônus da prova do consentimento obtido[47]. Além disso, o controlador também é obrigado a sempre deixar explícito ao titular dos dados caso a finalidade do tratamento dos dados pessoais seja alterada. Isso permite que este titular possa fazer uma decisão informada sobre manter o seu consentimento, mesmo nesta hipótese, ou revogá-lo[48].

Uma vez expostas algumas obrigações próprias da figura do controlador, a LGPD dispõe sobre uma obrigação comum tanto para o controlador quanto para o operador: manter registradas as operações de tratamento de dados pessoais que realizarem, em especial quando elas estiverem fundamentadas por legítimo interesse (uma das 10 bases legais, que explicamos adiante)[49].

O encarregado, nos ditames da LGPD, é a pessoa física ou jurídica, indicada pelo controlador e pelo operador dos dados pessoais para estabelecer a comunicação entre o controlador, os titulares dos dados e a ANPD. Essa atuação é similar à figura do Data Protection Officer (DPO), prevista na GDPR, por isso o termo DPO é muito usado no Brasil também, mesmo que não seja este o nome previsto na LGPD.

É muito importante que o contato do encarregado seja acessível, tendo em vista sua obrigação de receber manifestações dos titulares dos dados pessoais e da ANPD, de ajudar os funcionários do controlador dos dados a atuarem nos ditames da LGPD etc. Por fim, é ressaltamos que o encarregado deve estar sempre atento, pois a ANDP poderá emitir normas administrativas específicas que devem ser observadas por ele.

As obrigações dos agentes de tratamento de dados também decorrem de fatores como medidas de segurança[50], ditadas pela LGPD.

É muito importante que o contato do encarregado seja acessível, tendo em vista sua obrigação de receber manifestações dos titulares dos dados pessoais e da ANPD, de ajudar os funcionários do controlador dos dados a atuarem nos ditames da LGPD etc. Por fim, é ressaltamos que o encarregado deve estar sempre atento, pois a ANDP poderá emitir normas administrativas específicas que devem ser observadas por ele.

As obrigações dos agentes de tratamento de dados também decorrem de fatores como medidas de segurança[50], ditadas pela LGPD.

[43] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Artigo 5º, inciso VI.
[44] Ibidem. Artigo 5º, inciso VII.
[45] Este relatório deve conter, no mínimo, a descrição dos tipos de dados coletados, qual a metodologia utilizada para coleta e para garantia da segurança das informações e análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados, nos termos do § único do art. 38 da LGPD. Ibidem. Art. 38.
[46] Ibidem. Artigo 5º, inciso XVII.
[47] Ibidem. Artigo 8º, §2º.
[48] Ibidem. Artigo 9º, §2º.
[49] Ibidem. Artigo 37.
[50] Segurança da informação refere-se ao conjunto de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. Em contrapartida, Proteção de Dados refere-se ao conjunto normativo que prevê direitos e obrigações durante o tratamento de dados, além de definir os principais conceitos no que se refere aos titulares de dados, quem são os agentes responsáveis por este procedimento, entre outros importantes aspectos.

Obrigações de Segurança dos Controladores e Operadores segundo a LGPD

A LGPD determina que controladores e operadores têm o dever de adotar medidas de segurança, técnicas e administrativas. Estas medidas devem proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito[51].

Estas medidas de segurança poderão obedecer, inclusive, padrões técnicos dispostos pela Autoridade Nacional (ANPD)[52]. A sanção pela não observância destes padrões é, novamente, a responsabilização do controlador ou operador por danos decorrentes de violação da segurança dos dados.

Ainda no âmbito da segurança, o controlador é também responsável por comunicar à ANPD e ao titular dos dados sobre incidente de segurança que possa gerar risco ou dano relevante aos titulares[53]. Essa comunicação precisa ser feita de acordo com um prazo razoável (a ser definido pela ANPD), mencionando, pelo menos[54]:

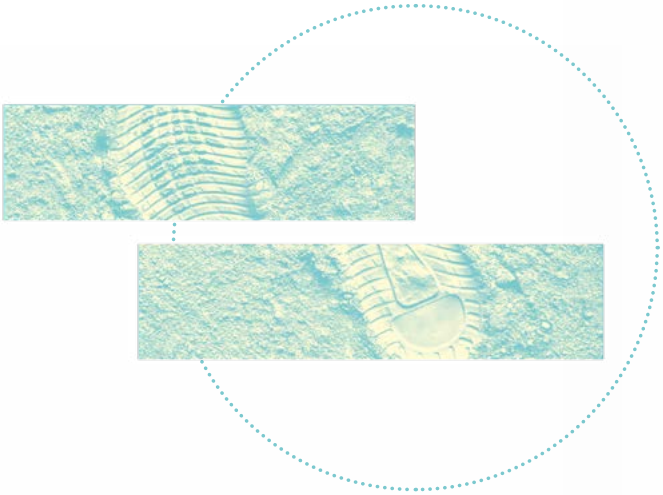
- uma descrição da natureza dos dados pessoais afetados;
- informações sobre os titulares de dados envolvidos;
- quais medidas técnicas e de segurança foram utilizadas para proteção de dados (tendo em vista segredos comercial e industrial);
- riscos relacionados ao incidente;
- motivos da demora, caso a comunicação à ANPD e ao titular de dados não tenha sido imediata; e
- que medidas foram ou serão adotadas para mitigar ou reverter os efeitos do prejuízo gerado.

Uma vez, avaliada a gravidade do incidente no tratamento de dados, a ANPD poderá impor ainda sobre o controlador a adoção de medidas, como uma ampla divulgação do fato em meios de comunicação, por exemplo, em jornais de grande circulação; ou então medidas sancionatórias para reversão e mitigação dos efeitos do incidente.

Direitos dos titulares

A LGPD confere diversos direitos aos titulares dos dados, como forma de equilibrar as práticas de tratamento. Nessa toada, os direitos dos titulares dos dados pessoais são:

(i) confirmação da existência de tratamento do dado pessoal;
(ii) acesso aos dados pessoais coletados;
(iii) retificar dados incompletos, incorretos ou desatualizadas;
(iv) anonimizar, bloquear ou exclusão do dado pessoal;
(v) direito de portabilidade;
(vi) exclusão de dados tratados, mesmo que tenham sido coletados com o consentimento do titular;
(vii) obter informações sobre a transferência dos dados pessoais entre entes públicos e privados;
(viii) ser informado das consequências pelo não fornecimento dos dados pessoais;
(ix) revogar o consentimento dado para o tratamento; e
(x) solicitar revisão de decisões tomadas com base em tratamento automatizado de dados pessoais que afetem seus interesses.



[51] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Artigo 46, caput. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 27.08.2019.
[52] Ibidem. Artigo 46, §1º.
[53] Ibidem. Artigo 48, caput.
[54] Ibidem. Artigo 48, §1º, incisos I a VI.

Tratamento automatizado

É importante fazer algumas considerações sobre o tratamento automatizado, tendo em vista a sua aplicação para atividades como perfilhamento de consumidor, aspectos profissionais, *credit scoring* etc.

O controlador dos dados, ou seja, a pessoa física/jurídica a quem compete as decisões referentes aos dados pessoais, deve informar com clareza os critérios e procedimentos utilizados no sistema de decisão automatizada. Esse dever é limitado pelas questões de propriedade intelectual. A ideia é informar aos titulares dos dados sobre os critérios e procedimentos utilizados e não, necessariamente, abertura do código fonte.

Se esses esclarecimentos não forem fornecidos aos titulares dos dados pessoais, a ANPD poderá solicitar uma auditoria para verificar a utilização de critérios discriminatórios no sistema de decisão automatizada.

Bases Legais

Voltando aos aspectos gerais da LGPD, outro ponto relevante é que o tratamento de dados pessoais (não sensíveis) deve atender à, pelos menos, uma das bases legais previstas na Lei. Bases legais funcionam como requisitos autorizativos de tratamento de dados. Se a instituição que realiza alguma atividade de tratamento não tiver muito claro pelo menos uma base legal de tratamento esse tratamento está sendo feito de forma irregular. Essa estrutura normativa também é derivada da legislação europeia (GDPR). Entretanto, de maneira diversa, a LGPD apresenta 10 bases legais diferentes, sendo 6 delas as mais relevantes para o mercado financeiro (as que estão grifadas):

(i) consentimento do titular dos dados pessoais;

(ii) cumprimento de obrigação legal ou regulatória pelo controlador dos dados;

(iii) execução de políticas públicas;

(iv) realização de estudos por órgãos de pesquisa;

(v) relação contratual com o titular dos dados;

(vi) para o exercício de direitos em processos judiciais, administrativos ou arbitrais;

(vii) proteção à vida;

(viii) tutela da saúde;

(ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular; e

(x) para proteger crédito, inclusive nos termos de legislações que tratem do tema.

Com relação à proteção do crédito, esse aspecto pode parecer bastante abrangente; no entanto, vale ressaltar que é preciso observar, além da LGPD, as regras dispostas em outras leis que tratam dos dados financeiros utilizados para análise do perfil do investidor e do limite de crédito a ser considerado, especialmente porque o cruzamento das informações que dizem respeito aos tomadores podem vir das mais variadas bases de dados, cujas regras de proteção precisam ser conhecidas e alinhadas às regras aplicadas pela fintechs.

Diante dessa sistemática de bases legais, vale reforçar que, quando falamos em mercado financeiro, não podemos esquecer que se trata de um setor extremamente regulado e que diversas normas já incidem sobre os dados coletados, nesse contexto.

Transferência Internacional

Transferências internacionais de dados pessoais podem ocorrer desde que o país ou organização de destino desses dados forneçam nível de proteção similar ou maior do que a LGPD. A ANPD será responsável por analisar a transferência pretendida pelo controlador dos dados, este deverá conformar a transferência de acordo com as regras da LGPD por meio de cláusulas contratuais, códigos de conduta, certificações etc.

Para que a transferência internacional dos dados ocorra de maneira adequada, segundo a LGPD, é preciso que os titulares dos dados tenham informações claras da transferência, destacadas das demais informações sobre o tratamento. Vale também lembrar que é necessário o consentimento específico do usuário para a transferência.

Segurança da Informação

A LGPD demanda que controladores e operadores dos dados pessoais adotem medidas técnicas e/ou organizacionais de segurança da informação. Apesar da LGPD não ser mais específica sobre o assunto, a ANPD poderá criar padrões mínimos de segurança de informação que deverão ser observados. Como a ANPD ainda está sendo criada, não temos esses parâmetros ainda, apenas os que foram adotados pelas autoridades europeias que podem ser usadas como base.

Caso ocorra algum incidente de segurança de informação, como um vazamento de dados pessoais, o controlador deve informar à ANPD e aos titulares dos dados pessoais sobre a ocorrência.

O regime de responsabilidade por incidentes previsto na LGPD

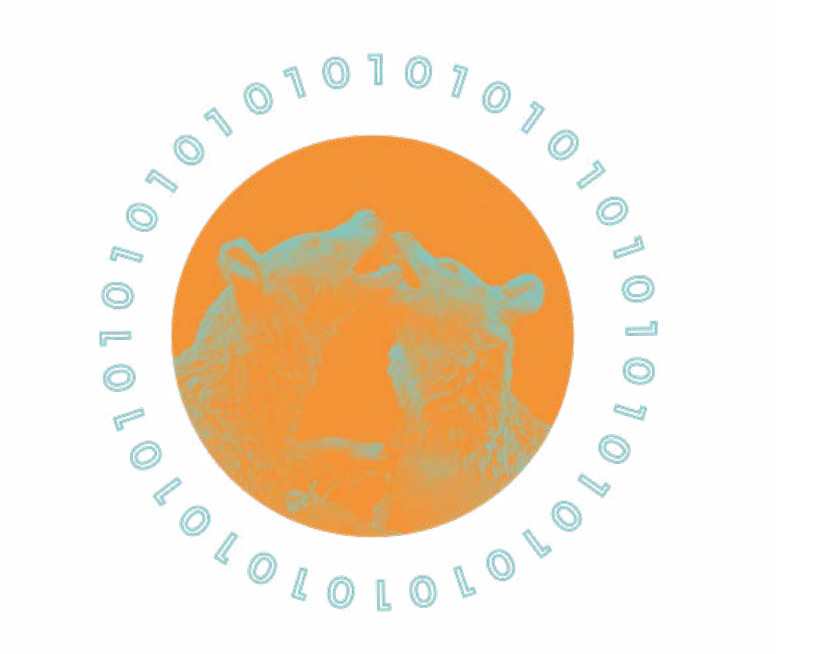
Segundo esta Lei, a responsabilidade por incidente no tratamento de dados seria do controlador ou do operador que, pelo exercício de sua atividade, causou dano patrimonial, moral, individual ou coletivo a alguém, sendo obrigatória a reparação deste dano.

Como forma de assegurar a efetiva indenização ao titular dos danos, observa-se que o operador responde solidariamente pelos danos causados pelo tratamento quando não tiver obedecido as instruções lícitas do controlador, ou quando descumprir as obrigações da legislação de proteção de dados[55].

No âmbito da LGPD, fica ainda um questionamento: quais os limites da responsabilidade dos agentes de tratamento de dados?

A única forma de não haver esta responsabilização será quando os agentes provarem **(i)** que não realizaram o tratamento de dados que lhes é atribuído pelos titulares; **(ii)** que não houve violação à legislação de proteção de dados, embora tenham realizado o tratamento de dados que lhes é atribuído pelos titulares; e **(iii)** que o dano é de culpa exclusiva do titular de dados ou de um terceiro[56].

[55] Ibidem. Art. 42, §1°, I.
[56] Ibidem. Artigo 43, incisos I, II e III.



Sanções Previstas na LGPD

Os controladores, operadores e encarregados que não se adequarem às obrigações e responsabilidades que lhes foram atribuídas pela LGPD poderão sofrer algumas sanções administrativas, aplicáveis pela ANPD[57].

São seis as sanções que podem ser aplicadas pela Autoridade Nacional, previstas pela LGPD[58]:

(i) advertência, com indicação de prazo para adoção de medidas corretivas;
(ii) multa simples, de até 2% do faturamento de empresa ou grupo empresarial no Brasil em seu último exercício, excluídos os tributos, com limitação de até R$50 milhões de reais por infração;
(iii) multa diária, com valor limitado a R$50 milhões de reais;
(iv) uma vez apurada e confirmada a ocorrência de infração, torná-la pública;
(v) bloqueio dos dados pessoais referentes à infração até a sua regularização; e
(vi) eliminação dos dados pessoais relacionados à infração.

Para aplicação destas sanções, foram elencados alguns critérios, como:

· a gravidade e a natureza das infrações e dos direitos pessoais afetados;
· a boa-fé do infrator;
· a vantagem auferida ou pretendida pelo infrator;
· a condição econômica do infrator;
· a reincidência;
· o grau do dano;
· a cooperação do infrator;
· a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;
· a adoção de políticas de boas práticas e governança;
· a pronta adoção de medidas corretivas; e
· a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

[57] Ibidem. Artigo 52, caput.
[58] Ibidem. Artigo 52, incisos I a VI.

3.8/
MARCO CIVIL DA INTERNET E O SEU DECRETO REGULAMENTADOR

Os princípios, direitos e obrigações envolvendo provedores de internet, incluindo os de conteúdos e os de infraestrutura, estão previstos na Lei nº 12.965, de 23 de abril de 2014, mais conhecida como Marco Civil da Internet ("MCI"). Essa Lei apresenta algumas considerações sobre tratamento de dados pessoais no ambiente online, enquanto a LGPD também se aplica para dados offline. É importante lembrar que o MCI veio antes da LGPD e, por isso, existem matérias que ambas as normas abordam.

O MCI prevê uma série de direitos para os usurários da internet, visando proteger sua privacidade e suas comunicações privadas, seus dados pessoais, o direito de acesso e coleta de informações, de excluir dados, entre outros.

Uma das previsões do MCI que destacamos é a de que empresas que oferecerem serviços online para consumidores devem armazenar alguns dados (como logs e endereços de IP) quando os usuários acessam os serviços. Fintechs que funcionam como aplicativos e sites de bancos, fundos de investimento e empresas de scoring são exemplos de empresas que devem observar essa obrigação.

Além das regras do MCI, é também importante estar atento aos dispositivos do Decreto nº 8.771, de 11 de maio de 2016 ("Decreto Regulamentador"). Especificamente sobre proteção de dados pessoais, é preciso adotar medidas de segurança de informação, como a adoção de controle de acesso ao banco de dados da empresa pelos seus funcionários. Outro ponto relevante é a necessidade de estabelecer que o uso de dados deve ser limitado e adequado, observando o propósito de seu fornecimento. Inclusive, o dado pessoal deve ser excluído quando ele atinge a sua finalidade.

Os agentes previstos no MCI e suas obrigações
Agentes importantes neste âmbito são os provedores de aplicações da internet, que devem obrigatoriamente respeitar a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros[59].

É dever deles, segundo o artigo 11, §3° do MCI, prestar informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

Além disso, o MCI dispõe sobre o regime de responsabilidade por danos decorrentes de conteúdo gerado por terceiros. Neste âmbito, vale ressaltar que provedores de conexão à internet não serão responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros. Em contrapartida, o provedor de aplicações de internet poderá ser responsabilizado civilmente por danos desta natureza se não tomar providências, após expedição de norma judicial específica, nos limites técnicos do seu serviço e dentro de prazo assinalado para tornar indisponível o conteúdo apontado como infringente.

Nesse contexto, os provedores de conexão são aqueles que disponibilizam acesso à internet do ponto de vista da conectividade e infraestrutura (como empresas telefônicas, por exemplo). Por outro lado, provedores de aplicações são aqueles que prestam serviços na internet, como é o caso de sites e aplicativos, e como muito provavelmente, se classificariam as fintechs.

Das sanções previstas no MCI

O próprio MCI prevê, inclusive, algumas sanções caso os provedores de conexão e os de aplicações na internet descumpram suas obrigações. São exemplos de penalidades aplicáveis:

(i) advertência, com indicação de prazo para adoção de medidas corretivas;
(ii) multa de até 10% do faturamento do grupo econômico no Brasil, em seu último exercício, excluídos os tributos e considerando a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e intensidade da sanção;
(iii) suspensão temporária de atividades como coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicação na internet; ou
(iv) proibição de exercício de atividades como coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicação na internet.

[59] BRASIL. Lei n° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Artigo 11. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 21.08.2019.

3.9/
LEI DO CADASTRO POSITIVO

A Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011) está em vigor desde 2011, mas foi significativamente alterada pela Lei Complementar nº 166, de 8 de abril de 2019 ("LC nº 166/2019"). Estas leis estabelecem as condições para a criação de bancos de dados sobre o adimplemento de pessoas físicas e jurídicas para a formação de histórico de crédito (informações sobre operações de crédito e pagamento adimplidas ou em andamento).

Falamos mais sobre o impacto dessas leis para as fintechs no texto "Fintechs, Atenção: Mudanças na Lei do Cadastro Positivo!" no nosso blog Espaço Startup. Traremos no presente texto alguns dos principais pontos para o setor.

Esse histórico de crédito é, no fundo, uma espécie de elaboração de "perfil" de crédito referente a uma pessoa física ou empresa, fenômeno conhecido no exterior como *credit scoring*.

Este conceito foi definido, em debates acadêmicos, como sendo a realização de uma espécie de resumo, contendo informações sobre a credibilidade do crédito de clientes. Estas informações variam, abordando, por exemplo, se há uma boa projeção sobre esse cliente e seus pagamentos, ou não. Logo, *credit scoring* é utilizado para permitir que certos clientes obtenham alguns financiamentos ou possam usar alguns serviços financeiros, por exemplo, e para analisar as chances de descumprimento destes clientes em relação a seus créditos[60].

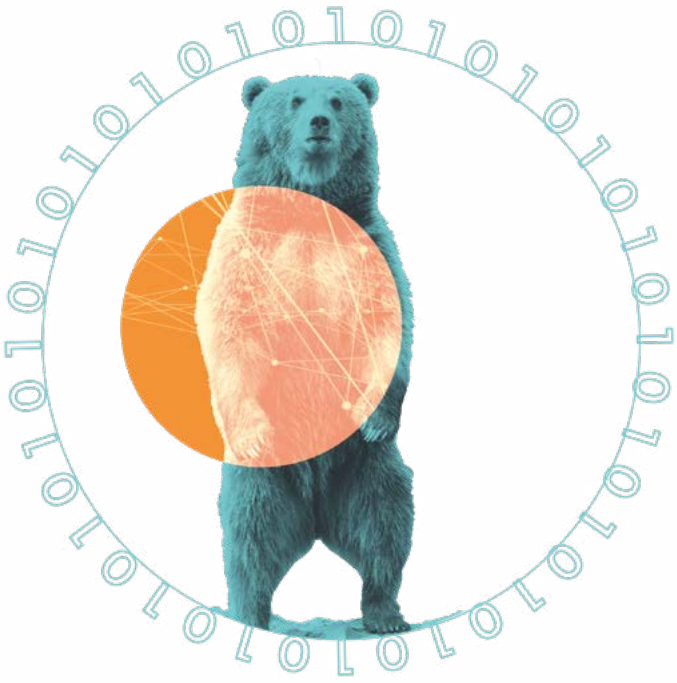
Os efeitos de *credit scoring* são importantes não só porque definem a pontuação de crédito de pessoas e empresas, facilitando ou dificultando suas transações financeiras, como também porque se trata de uma pontuação referência até para a obtenção de trabalhos, já que muitos empregadores utilizariam esta métrica ao determinarem quem seriam seus futuros colegas de trabalho.

[60] HURLEY, Mikella; ADEBAYO, Julius. *Credit Scoring* in the Era of Big Data. Publicado no Yale Journal of Law and Technology. 2017. Disponível em: <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt>. Acesso em 27.08.2019.

Sendo a Lei de Cadastro Positivo a norma regulatória da prática de *credit scoring* em terras brasileiras, vale ressaltar novamente que esta Lei regula justamente como empresas (pessoas jurídicas) poderão gerenciar dados de pessoas naturais ou jurídicas ou naturais em bancos de dados.

Segundo a Lei de Cadastro Positivo *"banco de dados"* são:

> *"um 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*[61]*"*.



Os agentes previstos na Lei de Cadastro Positivo

A Lei de Cadastro Positivo apresenta algumas figuras importantes para sua aplicação, definidas já nos incisos de seu artigo segundo. São elas:

· **o gestor,** pessoa jurídica responsável pela administração de um banco de dados e pela coleta, pelo armazenamento, pela análise e pelo acesso de terceiros aos dados armazenados. Assemelha-se a figura de operador, prevista na LGPD.

· **a fonte,** pessoa jurídica ou natural que conceda crédito, administre operações de autofinanciamento ou realize venda a prazo ou outras transações comerciais e empresariais que lhe impliquem risco financeiro. Isto se assemelha a alguns tipos de instituições financeiras. Também são consideradas fontes instituições autorizadas a funcionar pelo Banco Central do Brasil e os prestadores dos seguintes serviços continuados: água, esgoto, eletricidade, gás, telecomunicações e assemelhados.

· **o consulente**, pessoa natural ou jurídica que acesse informações em bancos de dados para qualquer finalidade permitida pela Lei de Cadastro Positivo.

· **o cadastrado**, pessoa natural ou jurídica cujas informações tenham sido incluídas em banco de dados. Assemelha-se ao Titular de Dados, previsto na LGPD.

[61] BRASIL. Lei nº 12.414, de 9 de junho de 2011. 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. Artigo 2º, inciso I. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em 27.08.2019.

As obrigações previstas na Lei de Cadastro Positivo

Em primeiro lugar, os gestores só poderão armazenar em banco de dados informações objetivas, claras, verdadeiras e de fácil compreensão[62].

Os gestores de banco de dados nesta modalidade devem estar atentos a um segundo ponto importante: é proibido armazenar informações excessivas (não vinculadas à análise de risco de crédito ao consumidor). É igualmente proibido o armazenamento de informações sensíveis (aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas[63]).

Outra obrigação imputada aos gestores refere-se à comunicação aos cadastrados. Essa comunicação deve ocorrer em até 30 dias, após a abertura do cadastro no banco de dados, e deve ser sem custo para o cadastrado. A comunicação deve ser feita pelos gestores diretamente, podendo ser realizada por intermédio das fontes, e, em seu conteúdo, a comunicação deve informar ao cadastrado quais são os canais disponíveis para o cancelamento do cadastro no banco de dados[64].

Os gestores também são obrigados a manter procedimentos adequados para comprovar a autenticidade e a validade da autorização do cadastrado, que viabilize apresentação a consulentes de seu histórico de crédito[65].

Há, também, o dever do gestor de manter sistemas seguros de consulta às informações de cadastrados[66]. Isto é relevante para assegurar o direito do cadastrado de acessar as informações sobre ele existentes no banco de dados, incluindo seu histórico e nota ou pontuação de crédito. O gestor deverá, inclusive, disponibilizar estas informações e quais são os principais elementos considerados para análise de risco ao cadastrado em até dez dias[67].

Ressaltam-se, por fim, outras relevantes obrigações do gestor:

- disponibilizar, em até 2 dias úteis, o cancelamento e a reabertura de cadastro ao cadastrado[68];
- cancelar automaticamente pessoa natural ou jurídica que tenha manifestado previamente, por meio telefônico, físico, ou eletrônico, a vontade de não ter aberto seu cadastro[69];
- fornecer ao cadastrado[70]:
  - todas as informações constantes de seus arquivos, no momento da solicitação;
  - indicação de todas as fontes relativas às informações dos arquivos do cadastrado, incluindo endereço e telefone para contato;
  - indicação dos gestores de bancos de dados com os quais as informações foram compartilhadas;
  - indicação de todos os consulentes que tiveram acesso a qualquer informação sobre ele nos seis meses anteriores à solicitação;
  - cópia do texto com o sumário dos direitos do cadastrado, definidos em lei ou em normas infralegais pertinentes à sua relação com gestores, bem como a lista dos órgãos governamentais aos quais ele poderá recorrer, caso considere que estes direitos foram infringidos; e
  - confirmação de cancelamento do cadastro.

Destacarmos também que as obrigações das fontes estão previstas no artigo 8º da Lei nº 12.414/2011.

[62] Ibidem. Artigo 3º, §1º.
[63] Ibidem. Artigo 3º, §3º.
[64] Ibidem. Artigo 4º, §4º, incisos I a III.
[65] Ibidem. Artigo 4º, §8º.
[66] Ibidem. Artigo 5º, II.
[67] Ibidem. Artigo 5º, §3º
[68] Ibidem. Artigo 5º, §6º.
[69] Ibidem. Artigo 5º, §7º
[70] Ibidem. Artigo 6º, incisos I a VI.

As sanções previstas na LCP

Já elencamos os deveres atribuídos tanto aos gestores de banco de dados, quanto às fontes, nos moldes da Lei nº 12.414/2011. Agora, vale ressaltar quais são as penalidades previstas na LCP, caso estes agentes sejam infratores:

(i) cancelamento de registro de agente responsável pela administração de banco de dados e pelo tratamento de dados (também conhecido como "gestor") no BACEN, caso este agente não adote medidas do Conselho Monetário Nacional (CMN) relacionadas às operações com características de concessão de crédito. Nessa hipótese, também poderão ser aplicadas como penalidades normas de proteção do consumidor;

(ii) aplicação das sanções e penas do Código de Defesa do Consumidor (CDC), quando a pessoa (física ou jurídica) que teve suas informações incluídas em banco de dados (conhecida como "cadastrado") for consumidora;

(iii) exclusão, feita por bancos de dados, do cadastro de informações incorretas no prazo de 10 dias e o cancelamento dos cadastros de pessoas que assim o solicitaram. Também poderão ser aplicadas medidas corretivas por órgãos de proteção e defesa do consumidor;

(iv) pena de reclusão de 1 a 4 anos e multa imposta aos responsáveis por quebra de sigilo, omissão, retardamento injustificado ou prestação falsa de informações requeridas. Aplica-se também o Código Penal e o Código de Proteção e Defesa do Consumidor; e

(v) aplicação subsidiária da LGPD e futuros direcionamentos sancionatórios a serem feitos pelo Executivo e aplicados aos gestores de banco de dados, na hipótese de vazamento de informações de cadastrados.

A alteração da Lei do Cadastro Positivo eliminou o modelo prévio de "*opt-in*", permitindo com que os gestores de bancos de dados de análise de crédito possam abrir cadastros sem a necessidade de obtenção do consentimento prévio do cadastrado. Entretanto, ainda é possível que a pessoa natural possa requisitar sua exclusão do cadastro, sendo, portanto, adotado o modelo de "*opt-out*" (pedido de saída). O cadastrado deve ser informado pelo gestor da abertura do cadastro em até 30 dias, inclusive com informações claras sobre como pode requisitar o cancelamento dele.

Os gestores dos bancos de dados ficam autorizados a compartilhar as informações cadastrais e de adimplemento entre si. Esta alteração, em conjunto com a previsão da lei original de que as fontes não podem discriminar quanto a quais gestores elas irão oferecer os dados de crédito, facilita, de forma expressiva, o fluxo de dados nesse mercado.

Alguns dos direitos do cadastrado são: obter o cancelamento do cadastro; acessar gratuitamente as informações sobre ele; solicitar a impugnação de informações errôneas; ser informado dos critérios utilizados na análise de risco; ser informado previamente pelo gestor de que seus dados estão sendo tratados; o direito de revisão de decisões exclusivamente automatizadas; e ter seus dados utilizados somente de acordo com a finalidade com que foram coletados.

Como se percebe, grande parte desses direitos também são previstos na LGPD para qualquer tratamento de dados pessoais. É curioso notar que os direitos previstos na Lei do Cadastro Positivo são extensíveis às pessoas jurídicas, ao contrário da LGPD que só se aplica a pessoas naturais. Também é interessante destacar que o cadastrado tem o direito de requisitar do gestor quem foram os terceiros (consulentes) que requisitaram seus dados de crédito nos 6 meses anteriores ao pedido.

3.10/
CÓDIGO DO CONSUMIDOR

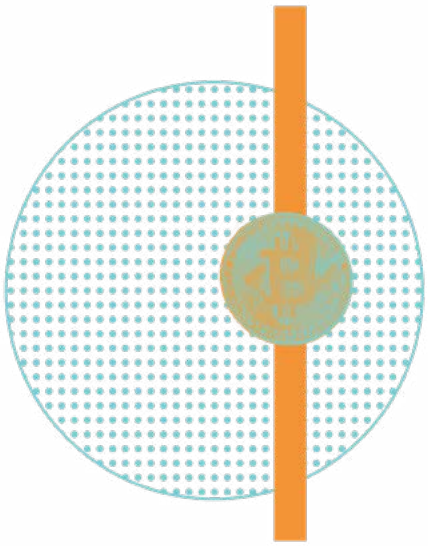
O Código de Defesa do Consumidor ("CDC"), ou Lei nº 8.078, de 11 de setembro de 1990, tem a finalidade de proteger consumidores que são, legalmente, considerados uma parte vulnerável na relação com os fornecedores de produtos e serviços.

Essa condição de vulnerabilidade confere ao consumidor uma série de direitos, como o de retificar informações sobre si, proteção contra publicidade enganosa ou abusiva, proteção contra cláusulas abusivas, o ônus da prova sobre a irregularidade por ele apontada recair sobre o fornecedor do produto ou serviço, entre outros.

É importante ressaltar que o Supremo Tribunal Federal ("STF")[71] e o Superior Tribunal de Justiça ("STJ")[72] já afirmaram que o CDC se aplica para atividades bancárias, financeiras, creditícias, seguradoras dentre outras. Em alguns casos, até mesmo investidores individuais de fundos de investimento podem ser considerados consumidores.

Além disso, o CDC fornece regras específicas sobre bancos de dados de consumidores e dados de crédito negativos. Nestes casos, o consumidor tem o direito de acessar qualquer informação armazenada sobre ele e corrigir qualquer informação errada. Informações negativas sobre consumidores não podem ser mantidas por mais de 5 anos, de acordo com a lei.

Os direitos dos consumidores podem ser exercidos de forma individual ou coletiva. Considerando o último, organizações da sociedade civil e o Ministério Público podem representar os consumidores coletivamente. Por exemplo, há casos de violação de dados nos quais uma empresa foi multada porque o Ministério Público representou os consumidores afetados, mesmo antes da entrada em vigor da LGPD (o que só acontecerá em agosto de 2020) embasando a acusação no CDC[73].



[71] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 2.591-1. Relator: Ministro Eros Grau. Sessão de 07/06/2006. Diário Oficial da União, Brasília, DF, 29.09.2006. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=266855> Acesso em 27.08.2019.

[72] BRASIL. Superior Tribunal de Justiça. Súmula Vinculante nº 297. Disponível em: <https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2011_23_capSumula297.pdf> Acesso em 27.08.2019.

[73] BRASIL. Ministério Público do Estado de Minas Gerais. Processo Administrativo – PROCON nº 0024.18.002027-3. Mais informações disponíveis em nota de imprensa do MPMG: "Drogaria Araújo deverá pagar multa de R$ 7 milhões por capturar CPF dos consumidores". Disponível em: <https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm>. Acesso em 28.08.2019.

[73] BRASIL. Ministério Público do Distrito Federal e Territórios. Nota de imprensa "MPDFT e NETSHOES firmam acordo para pagamento de dados morais após vazamento de dados". Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>. Acesso em 28.08.2019; BRASIL. Ministério Público do Distrito Federal e Territórios. Termo de Ajustamento de Conduta nº 01/2019. Disponível em: <http://www.mpdft.mp.br/portal/pdf/tacs/espec/TAC_Espec_2019_001.pdf>. Acesso em 28.08.2019.

As sanções previstas no CDC

As sanções nesta esfera dividem-se em duas categorias: as sanções administrativas e sanções decorrentes de infrações penais.

Dentre as sanções administrativas[74], destacamos como relevantes para o mercado financeiro as seguintes penalidades:

(i) multa;

(ii) suspensão temporária de atividade;

(iii) cassação de licença do estabelecimento ou de atividade; e

(iv) interdição, total ou parcial, de estabelecimento, de obra ou de atividade.

Já no universo das infrações e sanções penais[75], são exemplos relevantes de crime, considerando o contexto de mercado financeiro e tratamento de dados:

(i) detenção de três meses a um ano, e multa, quando for feita uma afirmação falsa ou enganosa, ou omissão de informação relevante sobre a natureza, qualidade, quantidade, segurança, desempenho, durabilidade, preço ou garantia da atividade prestada;

(ii) detenção de seis meses a um ano ou multa, caso um agente impeça ou dificulte o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros; e

(iii) detenção de um a seis meses ou multa, caso uma informação sobre consumidor em cadastro, banco de dados, fichas ou registros não seja corrigida imediatamente, sendo que um agente sabe ou deveria saber que a informação estaria inexata.

Vale ressaltar que existem algumas circunstâncias agravantes para o cálculo das sanções na esfera de crimes tipificados no CDC. Por exemplo, quando os crimes são cometidos em época de grave crise econômica, ou por ocasião de calamidade; quando ocasionarem grave dano individual ou coletivo ou dissimularem a natureza ilícita do procedimento.

[74] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Artigos 56 e seguintes. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em 27.08.2019.

[75] Ibidem. Artigo nº 61 e seguintes.

4/
COMPLIANCE DIGITAL NO CONTEXTO DE OPEN BANKING

Open Banking é um movimento acompanhado por regulamentações no mundo todo para transformar o funcionamento tradicional do sistema financeiro. Ele permite que tecnologias seguras possam acessar dados financeiros dos consumidores, tornando o mercado mais competitivo e consequentemente, beneficiando os consumidores com novos produtos e serviços de maior eficiência tecnológica e operacional. Falamos mais detalhadamente sobre este assunto em nosso artigo "O que é *Open Banking?*".

Algumas premissas basilares do Open Banking são: (1) dados têm valor, principalmente na sociedade contemporânea; (2) o consumidor é titular de seus próprios dados e, por isso, detém o poder de decisão quanto ao que ocorre com eles; (3) dados referentes a operações financeiras de consumidores são privados e sigilosos, nos termos da Lei Complementar nº 105/2001 ou Lei do Sigilo Bancário, conforme já discutimos; (4) possuir dados sigilosos significa, além de responsabilidade, uma enorme oportunidade de entender o perfil dos consumidores e poder ofertar produtos e serviços com base em padrões identificados; e (5) o setor financeiro sempre foi severamente regulado e restrito, o que determinou a concentração desse mercado por poucas e grandes instituições financeiras que por muito tempo foram os únicos a terem acesso aos dados bancários dos consumidores.

É bem verdade que o Open Banking inaugura uma nova fase em termos de concorrência, pois abre espaço para um mercado inovador, além de munir os consumidores de maiores informações, permitindo que tenham opções e possam escolher de maneira mais informada.

Além disso, também abre espaço para desenvolvimento de novas tecnologias, não só como forma de oferecer produtos e serviços inovadores, mas como meio de lidar com o outro lado do Open Banking que também gera preocupações. Estamos falando de questões ligadas à manutenção da segurança da informação e prevenção de incidentes de segurança.

É visível que as fintechs estão fortemente inseridas neste cenário, e por isso, ficarão no centro das principais normas que regulamentarão as atividades de Open Banking, no Brasil.

Apesar de ainda não haver regulamentação específica sobre o tema, algumas leis e resoluções brasileiras servem como bom ponto de partida para pensar o desenvolvimento e a aplicação segura da tecnologia. É o caso, por exemplo, da Lei do Sigilo Bancário (sobre a qual já discutimos) e da Resolução nº 3.401 de 2006, do BACEN[76].

A Lei do Sigilo é importante nesta dinâmica para conferir a devida proteção aos dados financeiros que estão protegidos sob sigilo. Sobre o fornecimento de informações cadastrais de uma instituição para outra, a Resolução nº 3.401, de 2006, do BACEN, traz em seu artigo 3º:

> *"Art. 3º As instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil devem fornecer a terceiros, quando formalmente autorizados por seus clientes, as informações cadastrais a eles relativas, de que trata a Resolução 2.835, de 30 de maio de 2001."* *(grifos nossos)*

[76] O fato de termos citado estas duas normas como exemplo das que são aplicáveis à dinâmica do Open Banking não significa que outras não sejam também aplicadas, como o Código Civil, o Código do Consumidor dentre tantas outras.

Ou seja, já existe no ordenamento brasileiro a previsão legal do dever de troca de informações entre instituições financeiras e de revelação de informações sigilosas a terceiros, desde que com o consentimento do usuário. No entanto, essas normas foram pensadas em um momento anterior ao surgimento do Open Banking e, mesmo que possam ser aplicadas ao cotidiano de algumas fintechs, elas não são suficientes para regulamentar o ecossistema de maneira completa.

Além disso, podemos citar o Comunicado n° 33.455, de 24 de abril de 2019 do BACEN em que divulgaram *"os requisitos fundamentais para a implementação, no Brasil, do Sistema Financeiro Aberto (Open Banking)"*. Apesar de não ser uma norma impositiva o Comunicado pode ser visto como uma declaração oficial do BACEN que informa ao mercado seus entendimentos e inclinações regulatórias.

É uma forma do Conselho do BACEN demonstrar o caminho de como o Open Banking será brevemente regulado no Brasil, ressaltando a importância deste movimento internacional; por outro lado, com desafios em relação ao cumprimento da LGPD e a segurança para o setor financeiro. O BACEN reforça a importância do consentimento quando se trata de compartilhar dados do cliente e como isso é fundamental para o Open Banking.

Em relação a uma definição para o termo, o Comunicado traz o seu entendimento:

"O Open Banking, na ótica do Banco Central do Brasil, é considerado o compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação, de forma segura, ágil e conveniente."

Além de anunciar uma possível consulta pública neste tema, ainda em 2019, o BACEN avisa que a "expectativa é de que o modelo de Open Banking descrito seja implementado a partir do segundo semestre de 2020".

Em outros termos, instituições financeiras e fintechs necessariamente precisarão estar preparadas para esse processo de interação operacional, de modo que, todos os fluxos de procedimentos, seja de controles internos, cadastro, compliance, gestão de riscos, invariavelmente, seguirão para um modelo digital. Nele, a tecnologia utilizada deve atender às necessidades de privacidade e segurança da informação, mantendo a integridade dos serviços desde o primeiro ponto de contato digital realizado pelos clientes/consumidores/usuários.

A entrada de fintechs como novos agentes aptos a garantir a eficiência dos serviços e, mais do que isso, a interoperabilidade entre as instituições certamente é o início de uma nova era, especialmente em termos de oferta no mercado financeiro.

Para as fintechs e demais confiantes na eficiência e integridade da tecnologia que está por trás dos seus serviços, é imprescindível pensar que toda a dinâmica de operações representa necessariamente uma cadeia de relações jurídicas e que, portanto, prescindem de contratos digitais formalizando a interface do usuário com a plataforma de serviço.

Afinal, se as relações jurídicas, daqui por diante, acontecerão cada vez mais no ambiente digital, esse ambiente deve estar preparado para produzir a materialização das relações digitais, o que significa dizer que toda a interação do usuário com as plataformas digitais, como as fintechs, deve ser juridicamente pensada e produzida como meios de prova, sobre quem deu causa à sequência dos eventos cursados.

Trata-se de responsabilidade desafiadora e de constante atualização também para os profissionais do direito que, muito mais do que elaborar documentos, precisará entender a inteligência operacional do seu cliente, para imprimir integridade jurídica ao seu compliance digital.

5/ CONCLUSÃO

Muito mudou nos últimos anos em relação ao mercado financeiro, principalmente ao que se refere à proteção de dados no Brasil. A principal inovação foi a promulgação da LGPD, que basicamente é o primeiro instrumento coeso e robusto sobre proteção de dados, no Brasil. Antes disso, existiam apenas leis setoriais esparsas que lidavam pontualmente com o assunto.

Muitas dessas normas ainda estão em vigor, com a diferença de que devem ser interpretadas e aplicadas considerando um novo sistema de proteção que foi estabelecido pela LGPD. O processo pelo qual o Brasil está passando é semelhante à internalização europeia da GDPR, uma vez que a LGPD só entrará em vigor em agosto de 2020, dando às instituições tempo para se adequarem e a ANPD para estabelecer suas atividades.

Também temos algumas outras normas no sistema brasileiro que protegem o direito à privacidade através da preservação da confidencialidade e sigilo, como também analisamos neste artigo. Elas são principalmente normas do sistema financeiro como a Lei do Sigilo Bancário, Lei de Lavagem de Dinheiro, normas administrativas do CMN, BACEN, CVM etc. Além destas, temos também o Código do Consumidor e o Código Penal que representam instrumentos importantes de proteção neste cenário.

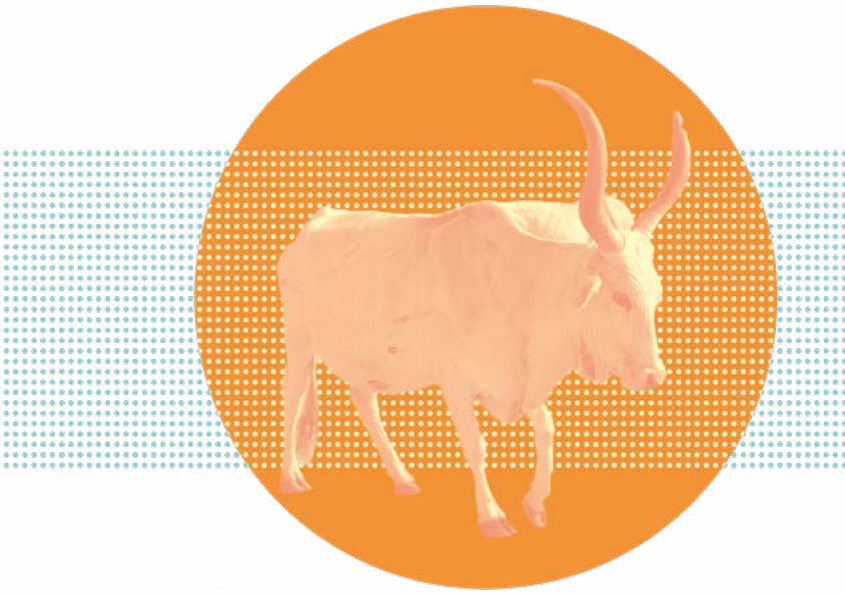
A proteção de dados, a confidencialidade e o sigilo não devem ser confundidos entre si, embora sejam normalmente usados para proteger o direito à privacidade. É por essa razão que pontuamos a diferença de dados financeiros, sigilosos e dados pessoais. Isso é especialmente importante levando em consideração a ampla definição de dados pessoais determinada no LGDP.

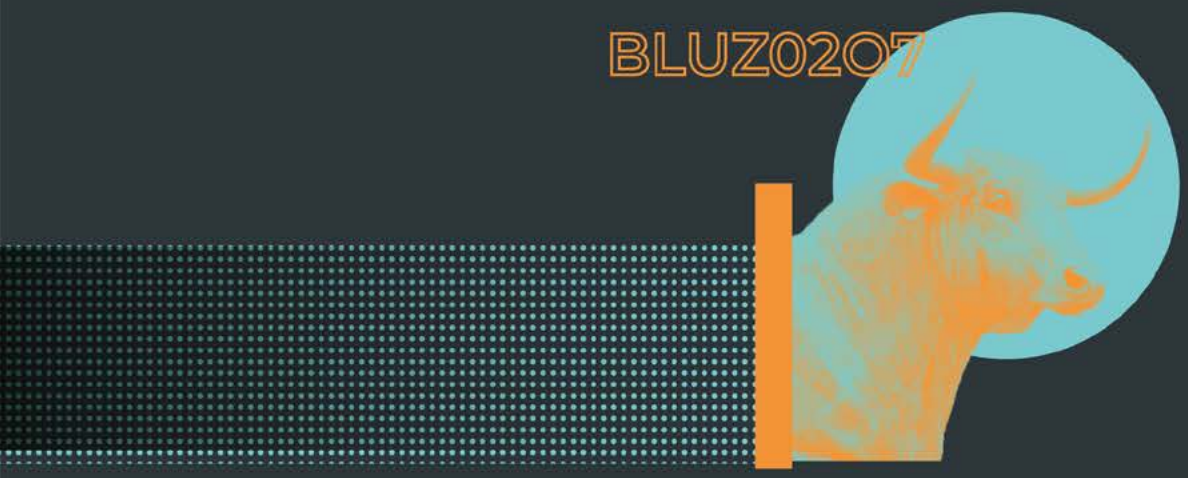
A depender da atividade exercida pela fintech, o seu processo de adequação pode ser bastante trabalhoso, e conforme pontuamos ao longo deste material, as sanções são diversas variando de responsabilização administrativa e civil com multas e indenizações até responsabilização penal com pena de reclusão, a depender do ilícito cometido.

A natureza dos dados tratados necessariamente tem efeitos em como o processo de adequação deverá ocorrer, por isso, é muito importante que um(a) advogado(a) especialista seja chamado para fazer essa avaliação, para compreender quais dessas normas seriam aplicáveis ao caso concreto da fintech.

Não se trata de um cenário alarmante, porém estamos diante de processos que precisam ser implementados, se forem concomitantemente ao nascimento da fintechs, melhor. Quanto antes as empresas começarem a se preocupar com esse assunto maiores as chances de estarem regulares na entrada em vigor da LGPD, lembrando que todas as outras normas mencionadas neste artigo já são exigíveis, portanto, a maior parte das sanções já poderão ser aplicadas em caso de descumprimento.

É verdade que o mercado tem se mostrado excessivamente preocupado com a chegada da LGPD, pensando nos impactos devastadores que essa norma pode provocar nos diversos setores. Contudo, já temos diversas outras leis que protegem direitos e preveem sanções para condutas previstas na LGPD. Isso significa que responsabilizações podem ocorrer mesmo antes da entrada em vigor dessa Lei e que um compliance digital deve ser observado, invariavelmente.





BAPTISTA LUZ
ADVOGADOS

WWW.BAPTISTALUZ.COM.BR