PAGAMENTOS PIX, segurança de dados e os desafios de uma nova cultura da proteção

Angela Dias Mendes*

Recentemente foi noticiado que o aplicativo *WhatsApp* havia disponibilizado um novo recurso de pagamentos para seus usuários no Brasil. Logo em seguida, o Banco Central do Brasil (BCB) suspendeu o funcionamento desse serviço, justificando que tal sistema exigiria uma avaliação mais detalhada quanto à preservação da segurança e da transparência.

A suspensão também atingiu as bandeiras Visa e Mastercard para observância dos requisitos da Lei nº 12.865/2013, neste caso, com a finalidade de impedir danos ao Sistema de Pagamentos Brasileiro, especialmente em relação à competição e à privacidade de dados, embora, por razões diversas, a suspensão não tenha atingido outras bandeiras, como Nubank e Sicredi.

Para sanar as pendências, as operadoras Visa e Mastercard apresentaram uma proposta ao Banco Central contendo um conjunto de boas práticas, protocolos de segurança e interoperabilidade das soluções. Esse *accountability*[1] pôde ser traduzido como uma demonstração de consonância com as regras de *compliance*[2] corporativo, incluindo a responsabilidade e a transparência, requisitos exigidos pela legislação.

Em 3 de agosto recente, o Banco Central autorizou o funcionamento em caráter experimental de ambas as bandeiras, para transações de pequeno valor. Em comunicado à agência de notícias Reuters, a Mastercard disse que, num primeiro momento, *"somente um grupo restrito de cartões poderá realizar transações que sejam de valor baixo"*.

Para além das questões que envolvem o Sistema Financeiro Nacional, sua regulação e a operabilidade das

transações financeiras dedicamos este artigo, de forma sucinta, ao *arranjo de pagamentos Pix* e, nesse contexto, à relevância das políticas de segurança e à necessidade de uma nova cultura individual em favor da mitigação dos riscos de navegar em mares virtuais.

Sistema de pagamentos Pix

Na esteira da inovação, o BCB instituiu, por meio da Resolução nº1, de 12 de agosto de 2020, o *arranjo de pagamentos Pix*. O sistema é obrigatório para as instituições financeiras e para as instituições de pagamento por ele autorizadas, devendo todas atenderem ao disposto na resolução e demais regulações pertinentes. Para disponibilizar o serviço, as instituições deverão adotar procedimentos que incluam o *gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança, entre outros* assentados na Circular/BCB nº 3.681/2013.

No Brasil, Pix é o nome da marca instituída pelo BCB. A marca é um facilitador na identificação do serviço prestado. De acordo com a regulação, as instituições financeiras e de pagamento deverão incluir a marca Pix juntamente com as suas marcas individuais ao aderirem ao sistema.[3]

Uma característica marcante dessa modalidade de pagamento é a velocidade de transmissão. Ou seja, a transferência eletrônica da ordem de pagamento realizada pelo usuário pagador é instantaneamente disponibilizada na conta do usuário recebedor, permitindo que eventuais problemas sejam sanados no momento da prática do ato negocial.

Outras duas características consideradas fundamentais para o sucesso do serviço podem ser lidas em conjunto. A primeira é a disponibilidade, que ofertará o serviço 24 horas por dia, incluindo feriados e finais de semana. A segunda é a conveniência, que facilitará o acompanhamento e a confirmação da operação em tempo real.

Oportunamente, a resolução exigiu a conformidade e o adequado processamento e armazenamento dos dados pessoais. Desta forma, instituições não poderão prescindir da *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*, em alinhamento à Circular/BCB nº 3.909/2018.

A partir do dia 16 de novembro, o serviço ficará disponível e será fornecido gratuitamente para pessoas físicas.[4] O Banco Central divulgou que seu objetivo é apoiar a eletronização dos pagamentos e aumentar a eficiência no mercado de pagamentos de varejo, além de viabilizar o desenvolvimento de soluções focadas na experiência do cliente.

Sociedade tecnológica

Daniel Bell[5] cunhou o termo sociedade tecnológica sob a perspectiva das transformações ocorridas após a segunda fase da Revolução Industrial, essenciais para o desenvolvimento econômico e social.

No período subsequente à Segunda Guerra, a inovação tecnológica foi determinante, mormente pela domesticação da internet e pela automação de processos produtivos. A substituição da mão de obra por máquinas incrementou a escala produtiva, a distribuição e a comercialização de bens e serviços, tornando-os mais competitivos e menos onerosos. A internet, por sua vez, conectou pessoas e superou obstáculos geográficos, temporais etc. Com isso, ela produziu acervos multiculturais e novos modelos de negócios.

Evolução dos meios de pagamento

Moedas de metal

Papel moeda

Cheque

Nesse cenário, lentamente, surgia no mercado um ativo importante: os dados pessoais. Hoje, a coleta de todo tipo de informação destina-se a formar bancos de dados de alto valor negocial. Por esta razão não é difícil ver ofertas gratuitas de serviços, com objetivo de coletar o maior número possível de informações dos usuários, transformando essa coleta em pacotes de produtos e serviços na medida do perfil consumerista e, portanto, mais atrativos. Por isso, vale a pena ficar atento às gratuidades, porque o produto pode ser você!

Hoje, tratamento de dados é sinônimo de lucro. Portanto, não foi sem razão a afirmação feita por Harari[6] que na atual sociedade *"há especialistas que transformam em decisões, os desejos e aptidões coletados."*

Cultura da proteção

A infinita capacidade humana de elaborar e reelaborar ideias ensejam as mais variadas ações, lícitas ou ilícitas. Por isso, entre tantas causas, Ulrick Beck utilizou a expressão Sociedade de Risco[7] ao denominar essa nova conformação social.

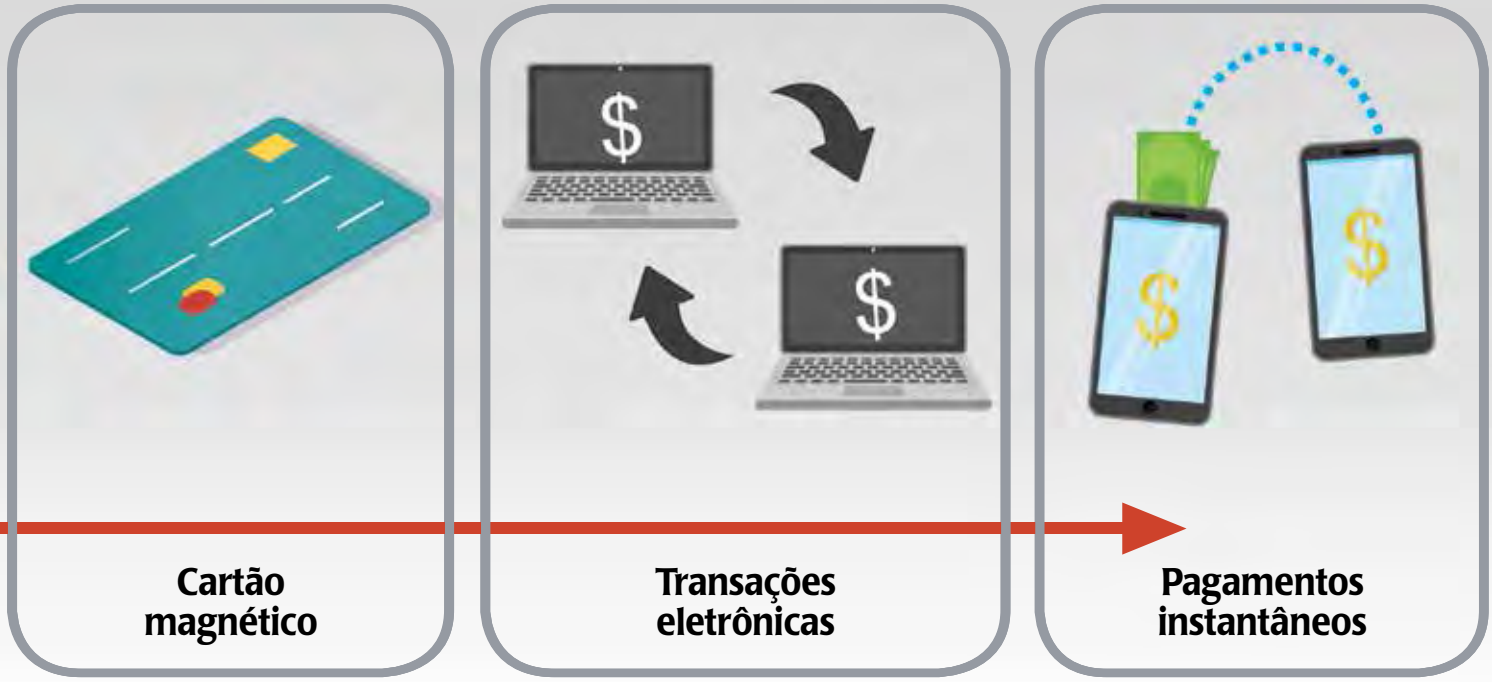
O Brasil vem seguindo a tendência internacional de legislar em proteção aos dados pessoais. Mas essa temática é um desafio para todos os atores envolvidos, sejam eles privados ou públicos, empresas ou clientes.

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD) foi aprovada mas sua vigência, até a presente data, carece da sanção presidencial. Sua efetividade vincula-se, especialmente, a dois aspectos importantes. O primeiro, relacionado aos efeitos sancionatórios (Capítulo VIII) que foram postergados para maio de 2021 pela Medida Provisória nº 959/2020. O segundo, referente à competência da Autoridade Nacional de Proteção de Dados (ANPD) cuja atribuição inclui a *regulamentação das sanções administrativas e a fundamentação da gravidade e da extensão do dano em caso de infração* (Art. 53 e 54, LGPD), sem os quais a lei é inócua.

O Decreto nº 10.474, publicado em 26 de agosto último, chegou em boa hora e estabeleceu a estrutura da Autoridade, o que sinaliza bons ventos para a Política Nacional de Proteção de Dados Pessoais e Privacidade, assim como a segurança jurídica dos negócios.

Outra medida em consonância com a proteção de dados foi a citada Resolução dos pagamentos Pix. Seu conteúdo não deixou dúvidas quanto à obrigação das

pix
powered by Banco Central



instituições financeiras adotarem políticas de segurança e adequação legal na adesão ao sistema. As exigências de conformação e os planos de ações de segurança cibernética são claras e taxativas para que o serviço seja disponibilizado ao público.

Atualmente, as empresas e instituições públicas devem investir em segurança cibernética, sem esquecer do alicerce da estratégia, que são as políticas de segurança e os usuários. Essa é uma afirmação do Prof. Lourival Moreira,[8] utilizando-se da *metáfora do cubo multifacetado*, para reforçar a ideia multidisciplinar da arquitetura de segurança.

O fascinante mundo digital e suas ferramentas não deixam escapar o elemento psicológico para atrair ou distrair a atenção das pessoas. Por isso, o usuário deve ter cautela durante o acesso virtual. A prática estelionatária é comum nesse ambiente. Ela se utiliza de meio ardiloso para enganar e obter vantagem para si ou para outrem. Com isso, o estelionatário frauda o mecanismo, enganando o usuário para que ele, distraidamente, acredite numa verdade inexistente e realize o ato por vontade própria.

Assim, é necessário buscar segurança desde o simples ato de navegar na rede. Isto pode ser feito, por exemplo, atentando para o *domínio, que serve à localização e identificação da instituição acessada*. É também valioso identificar a hospedagem desse domínio que deve estar em sites estáveis, de boa reputação e *qualidade, o que resulta em maior segurança ao proprietário e, também, ao usuário*[9].

Além disso, antes de qualquer aceite, é importante ler as políticas de privacidade, porque elas contêm as principais informações para salvaguarda do usuário. Durante a utilização de um serviço (preencher um formulário, abrir mensagem de e-mail ou SMS etc.), se houver algo suspeito, a atitude coerente é estancar o processo, certificar-se do modo seguro de acesso da fonte confiável e denunciar, se for o caso. Nesse cenário, vitais para a segurança. Estudos recentes demonstram que boa parte dos usuários repetem a mesma senha (*password*) na maioria dos acessos. Em qualquer qualidade, todos os que acessam dados sensíveis devem possuir uma senha especial, criteriosa quanto à formação e que não guarde relação com sua vida privada, nem reproduza informações de fácil verificação, como datas de aniversários.

um dos crimes mais comuns é a engenharia social [10] que é a *manipulação de pessoas para obter uma informação*, muitas vezes explorando sua boa-fé e curiosidade.

Vale acrescentar que a engenharia social é composta de vários tipos de ataques, entre eles o *pretexting*, quando o invasor cria uma mentira utilizando-se de informações verdadeiras ou falsas, para obter dados pessoais, e o *phishing*, quando o invasor envia uma mensagem por um destinatário com aparência de legitimidade, fazendo a vítima acreditar que é verdadeira. A vítima fornece o que foi solicitado pelo engenheiro social ou acaba instalando *malwares* (*software* nocivo, vírus) ao clicar em um link como doc., pdf etc. Também é comum o *rainbow table* (tabela colorida), que é um método utilizado para descobrir senhas a partir de uma sequência de informações do usuário.

Não é demais lembrar que as senhas fortes são

Considerações finais

A comunidade internacional segue na esteira da regulação, conferindo mecanismos de controle em todo o ciclo de vida dos dados. Atualmente, o Brasil segue essa tendência mundial com uma regulação nativa propulsora da inovação. Percebemos que, paulatinamente, a legislação brasileira tenta convergir diferentes interesses para alcançar a estabilidade social. Nesse caso, a segurança dos dados pessoais alinha-se ao desenvolvimento econômico, em conclusão da leitura do art. 4º da LGPD, que elenca as exceções legais com objetivos diversos, entre eles, o de não engessar o mercado.

Embora a lei pudesse ter evitado alguns conceitos abertos, os quais, naturalmente, geram dúvidas na interpretação, ela revela tendências de resultados satisfatórios ao longo do tempo. Vale ressaltar a leitura

sob o prisma das boas práticas na governança, engendrando o alinhamento entre a garantia dos direitos fundamentais e o desenvolvimento econômico.

A história demonstra que a vida em sociedade minimamente equilibrada, somente foi possível a partir do momento que o homem passou a estabelecer regras de convivência social. A nova sociedade digital, apesar de inovadora, não demonstra distância da necessidade de regras para harmonização do convívio em ambiente virtual.

Entretanto, de nada valem as classificações, as políticas de segurança ou mesmo o rigor das leis, se cada pessoa não absorve a proteção em sua prática cotidiana. Isto se chama cultura da proteção. Trata-se de um novo agir para minimizar os riscos oriundos da exposição indevida de dados sensíveis, do descuido com a guarda de informações reservadas e do vazamento resultante da inabilidade no uso das ferramentas digitais e acesso à rede. São medidas simples de segurança que, se utilizadas diariamente, podem tornar-se um estilo de vida, imperioso e crucial nesses novos tempos em que os negócios virtuais serão uma constante em nossas vidas. ■

Notas:

(1) O termo *accountability* foi incorporado em nosso idioma com significado de prestação de contas. Assim, ele reflete um compromisso com a legalidade, a ética e a transparência nas ações que envolvem setores governamentais.

(2) Regras de *compliance* são regras de adequação às normas, às leis, aos regulamentos exigidos nas mais diversas negociações e no cotidiano institucional. Mas a palavra *compliance* tem um significado que vai além da adequação legal e alcança as boas práticas, objetivando combater a corrupção e os desvios de conduta nos setores público e privado.

(3) Para consultar a imagem da marca basta acessar o site do Banco Central do Brasil disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pagamentosinstantaneos

(4) A afirmação da gratuidade é do diretor da Organização do Sistema Financeiro do Banco Central, João Manoel de Mello.

(5) BELL, Daniel. O advento da sociedade pós-industrial. São Paulo: Cultrix, 1973.

(6) HARARI, Yuval Noah. Homo Deus. Uma breve história do amanhã. Trad. Paulo Geiger. São Paulo: Companhia das Letras, 1ª. Ed., p. 373, 2016.

(7) Ulrich Beck, sociólogo alemão, desenvolveu estudo intitulado Risikogesellschaft. Auf dem Weg in eine andere Moderne, em Frankfurt no ano de 1986. No Brasil a obra foi traduzida, em 2010, por Sebastião Nascimento como o título Sociedade de Risco - rumo a uma outra Modernidade.

(8) Prof. Lourival José Passos Moreira é Doutor em Política e Estratégia, Expert em TSIoT, Membro do Grupo de Interesse CTEMI/Clube Naval. Em palestra ministrada no Clube Naval sobre Cibersegurança ele utiliza a metáfora do cubo multifacetado para apresentar a arquitetura de segurança, demonstrando seus contornos multidisciplinar e multiprofissional. Disponível em: https://www.clubenaval.org.br/novo/?=v%C3%ADdeos-das-palestras, acesso em 31 ago 2020.

(9) Prof. Fabio Bittencourt Quirino, Membro do Grupo de Interesse CTEMI/Clube Naval. Disponível em: https://www.clubenaval.org.br/novo/?=v%C3%ADdeos-das-palestras, acesso em 31 ago 2020.

(10) Pesquisa realizada no Repositório Scielo, onde poderão ser encontradas outras informações, especialmente em SILVA, Clayton Silvestre da et all. Engenharia social: o elo mais frágil da segurança nas empresas.

**Doutoranda PPGD/UNESA, Mestre em Direito, Membro do Grupo de Interesse CTEMI/Clube Naval.*