COMO FUNCIONA A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL E NO MUNDO?

Juliana Abrusio

A Lei nº 13.709/2018, conhecida por LGPD (Lei Geral de Proteção de Dados), entrou em vigor em 18 de setembro de 2020, com exceção de suas sanções administrativas que passaram a valer a partir de 1 de agosto de 2021. Até então, a privacidade e a proteção de dados pessoais, no Brasil, eram previstas em legislações esparsas, como o Código de Defesa do Consumidor, a Lei do Habeas Data, o Código Civil, o Marco Civil da Internet, a Lei de Acesso à Informação, a Lei do Cadastro Positivo, além da própria Constituição Federal. A regulação sobre o assunto era, portanto, pulverizada, genérica e não cobria todos os detalhes necessários quanto às operações de dados pessoais, fundamentais para garantir os direitos dos titulares, bem como eram insuficientes para criar um ambiente econômico com maior segurança jurídica, a fim de promover o desenvolvimento econômico, tecnológico e a inovação no país.

O Brasil se tornou o 127º país do mundo a ter um sistema legal próprio para a proteção de dados pessoais. Um lugar na fila um tanto discrepante comparado à efervescência de sua economia. Mas, apesar do atraso, fato é que o Brasil tem um longo caminho pela frente, uma vez que a existência de uma lei, por si só, não transforma imediatamente as pessoas, e tampouco muda, repentinamente, o comportamento dos agentes de tratamento de dados, sejam eles públicos ou privados (a lei aplica-se a ambos). É preciso desenvolver e fortalecer uma consciência de proteção de dados no país, o que demanda tempo e um árduo trabalho.

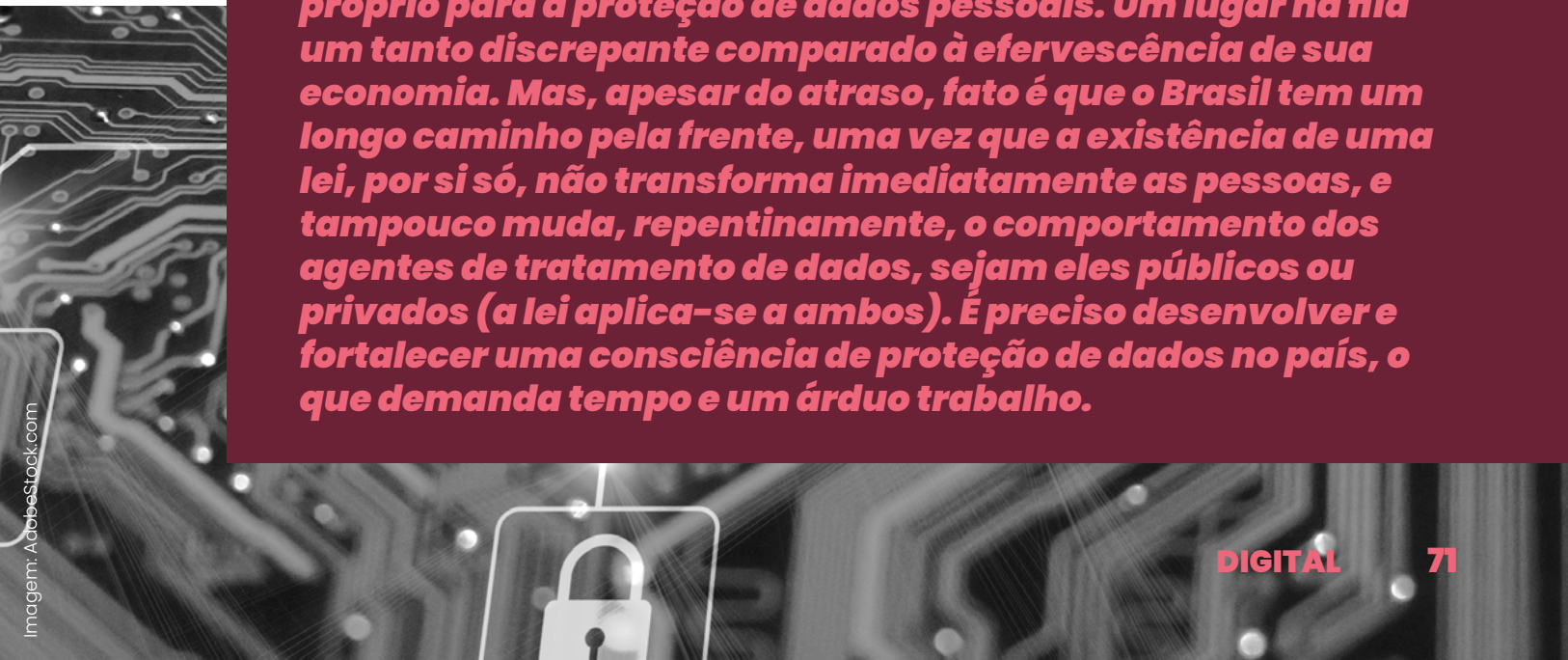


Imagem: AdobeStock.com

Nesse sentido, deposita-se grandes expectativas nos trabalhos da Autoridade Nacional de Proteção de Dados (ANPD), formalmente instituída em 6 de novembro de 2020, a qual, além das atribuições de fiscalizar e aplicar sanções, também tem como missão "promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança" (art. 55-J da LGPD).

A grande crítica, porém, diz respeito ao fato de a ANPD, em que pese dispor de autonomia técnica e decisória, ter sido criada como órgão da administração pública federal direta, integrante da Presidência da República.

O ideal e esperado – inclusive para maior respeito e credibilidade perante o mercado internacional – é que a ANPD seja transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial, gozando, portanto, da devida autonomia que uma autoridade como essa demanda. Não há, porém, previsão para essa mudança.

Vale lembrar, ainda, que a LGPD tem inspiração na legislação europeia e muitos paradigmas sobre o assunto, utilizados no Brasil, são oriundos do velho continente, o que pode ser uma perigosa armadilha. Isso porque não se pode esquecer que a União Europeia é um território regulado na matéria há mais de vinte e cinco anos, considerando a Diretiva 95/46, a qual foi substituída pelo Regulamento 679/2016, comumente conhecido por GDPR (*General Data Protection Regulation*), em vigor desde 2018.

Em outras palavras, o mercado do Brasil não pode ser inocentemente comparado com o europeu, o qual já tem uma regulação madura, acúmulo de várias decisões das autoridades sobre o assunto, e, principalmente, uma sociedade e mercado com uma cultura de proteção de dados muito mais desenvolvida.

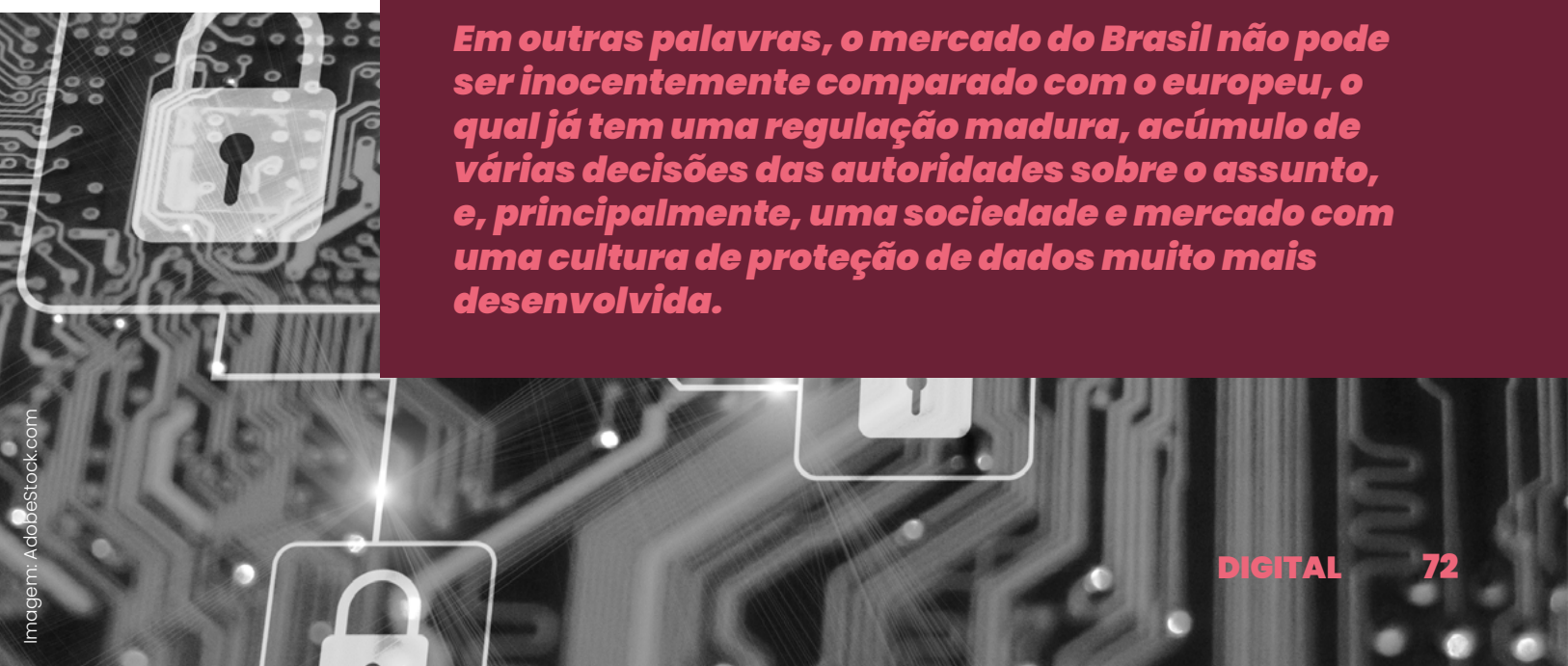


Imagem: AdobeStock.com

Além disso, em matéria de regulação de proteção de dados pessoais, seria um erro ignorar que a economia brasileira tem como importante pilar as micro e médias empresas, as quais desempenham um papel cada vez mais estratégico e respondem, atualmente, por mais de um terço do valor do PIB do país.

Não à toa, a LGPD dedica especial atenção a essa categoria ao determinar que a ANPD deve "editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, possam adequar-se a esta Lei" (Art. 55-J, inciso XVIII). Tudo isso somado ao fato do arrefecimento econômico advindo da crise sanitária que teve início em 2020 e que acabou por afetar ainda mais essa categoria das micro e médias empresas.

Aliás, não se pode imaginar que por estar em vigor desde 2018, a LGPD já teria sido devida e largamente implementada no mercado brasileiro. Tanto assim que às vésperas das sanções administrativas entrarem em vigor – cuja multa pode chegar a 2% do faturamento da empresa, limitada a 50 milhões de reais por ato de infração (art. 52, LGPD) – notícias com levantamentos realizados por consultorias circularam pelas mídias dando conta de que a grande maioria das empresas ainda não estava adequada à lei.

De outro lado, importante crítica que não pode deixar de ser mencionada diz respeito ao fato de muitas empresas e entidades terem implementado um sistema "para inglês ver", isto é, meros *templates* (modelos), encarregados pró-forma, etc, sem a adoção de um verdadeiro e adequado plano de governança de proteção de dados pessoais. Dito de outra forma, implementar de forma insuficiente pode significar não estar adequado à lei. Ressalte-se que a implementação da LGPD ocorre a partir de uma abordagem baseada em risco, de modo a ser essencial aplicar a prática de uma gestão de riscos, com a adoção de um conjunto de ações coordenadas, com o objetivo de controlar os possíveis impactos que um determinado tratamento pode gerar.

Dessa forma, aderir a uma gestão de riscos, por meio de um plano de governança de dados, com sistematização e metodologia apropriadas, é um elemento essencial em qualquer organização.

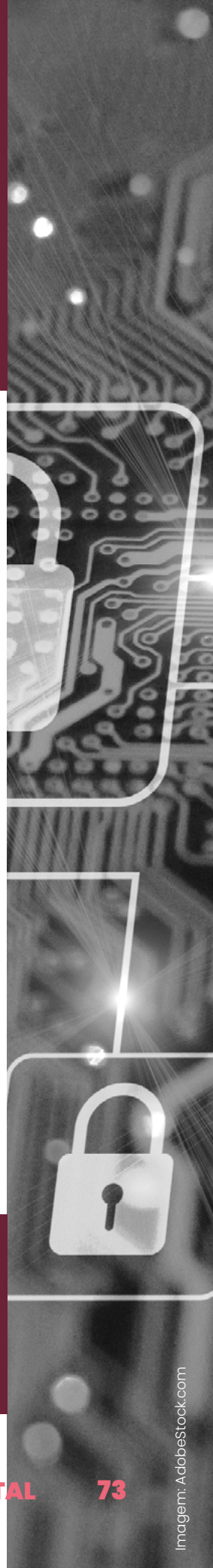


Imagem: Adobestock.com

Outro equívoco, que não é incomum, é o falso entendimento de que o tratamento de dados pessoais depende sempre de autorização de seu titular. Se assim o fosse, haveria, sem dúvida, um engessamento nas operações e negócios, especialmente naqueles do tipo digital, quando na verdade a LGPD – é bom sempre lembrar disso – não veio para travar o mercado, mas para impulsioná-lo a partir do delineamento das regras do jogo, bem a partir do empoderamento conferido ao cidadão, enquanto titular de seus dados pessoais. É um ganha-ganha: tanto para o cidadão quanto ao mercado.

Retomando, vale aqui uma pausa para explicar uma das regras basilares trazidas pela LGPD, qual seja: o tratamento de dados pessoais somente poderá ser realizado nas hipóteses previstas em lei. Por *tratamento* de dados pessoais entenda-se "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" (art. 5º, inciso X da LGPD)". Mas existem dez bases legais, como regra geral (exemplos: dados necessários para execução de contrato, proteção da vida, tutela da saúde, legítimo interesse, proteção do crédito, dentre outras), sendo que apenas uma das dez previstas em lei é a do consentimento. As demais não dependem de autorização do titular dos dados pessoais. Não está correto, portanto, qualquer afirmação no sentido de que uma determinada base legal prevaleça como mais importante do que a outra. Uma vez que determinado tratamento esteja compatível com as suas finalidades, a base legal pode ser considerada como adequada, segundo as regras dos arts. 7º e 11 da LGPD.

Consequência do referido equívoco pode ser vista, por exemplo, na ampla utilização de pedidos de autorização de uso de *cookies* nos sites brasileiros, quando, na verdade, essa prática não é exigida pela LGPD, porquanto a hipótese legal mais indicada para a coleta de dados via *cookies* seria o legítimo interesse. Some-se ao *mito do coringa do consentimento* o fato de a Europa dispor de uma Diretiva Específica (*ePrivacy Directive*) que obriga a aposição das barras de *cookies* em seus sites. Contudo, repise-se, essa determinação não é exigida pela LGPD, em que pese grande parte dos sites brasileiros a estarem adotando (possivelmente por desconhecimento).

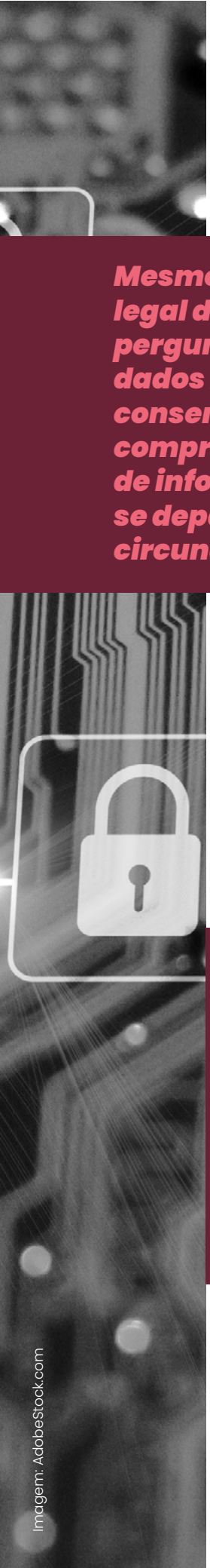


Imagem: AdobeStock.com

Ainda sobre a base legal do consentimento, é importante observar e trazer outra importante crítica ao assunto, essa de caráter mais complexo e que apresenta maiores desafios dogmáticos: a *fadiga do consentimento.*

Mesmo nos casos em que a base legal do consentimento for exigida, pergunta-se: o quanto o titular dos dados realmente está apto para consentir, na medida de sua real compreensão diante de um tsunami de informações e textos com os quais se depara durante sua rotina diária, circundada de devices, sites e apps?

Consentimento vem de *co-sentire*. Existe um envolvimento para conhecer e concordar com as bases as quais se consente. Na toada da vida de hoje, no compasso apressado dos dias, de imediatismo e tempo escasso, parece não haver espaço e disponibilidade, de tempo e mente, para refletir e consentir sobre os inúmeros instrumentos com os quais é necessário consentir.

Tudo isso deve, ainda, ser sopesado com o fato de vivermos sob a *algocracia,* pela qual são utilizados algoritmos que processam diversos dados pessoais para a tomada de decisões automatizadas que afetam, juridicamente, os interesses de seu titular de dados.

Assim, a questão que ora se amplia é o quanto o titular dos dados realmente está apto para consentir, na medida de sua real compreensão do que consiste e no que pode implicar o uso dos algoritmos em uma decisão automatizada que afete, juridicamente, os seus interesses.

Diante de tantas opacidades, torna-se um desafio encontrar um meio de conferir ao titular o conhecimento e controle sobre o fluxo de seus dados pessoais.

Existe importante risco de o indivíduo ser expropriado do direito à autodeterminação informacional tão almejada e comemorada. Daí dizer que o consentimento está perdendo a importância e confiança que outrora lhe foram confiadas.

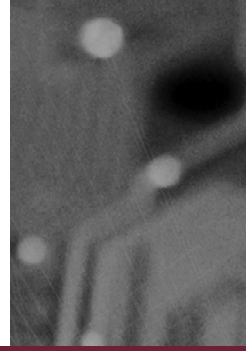
No palco praticamente ilimitado da ubiquidade computacional e algorítmica, o tempo é finito. Nesse sentido, verifica-se que, na maioria dos casos, o usuário quer passar o mais rápido possível por todas as telas que pedem seu "de acordo" para chegar ao destino, sem se importar *com o que* está consentindo. As pessoas são rápidas, estão com pressa e sem paciência, para não dizer exaustas. Nesse contexto, há aqueles que pregam a morte das políticas de privacidade (de *sites* e aplicativos), pois entendem que de nada servem, uma vez que praticamente ninguém as lê.

Ao que parece, o modelo do consentimento informado foi útil há duas décadas, mas hoje pode se revelar em uma fantasia. Em um fluxo constante de interações *online*, especialmente nas telas pequenas de celulares, que agora são responsáveis pela maior parte do uso, não é realista, tampouco factível, confiar que as pessoas estejam sequer lendo as políticas de privacidade.

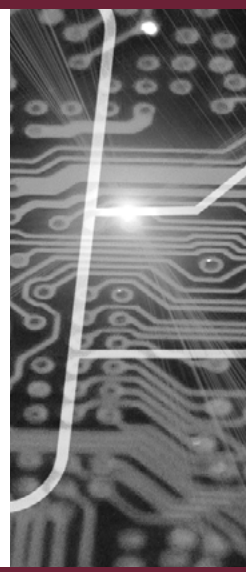
Por isso que, para maior efetividade das cláusulas que tratam da proteção de dados, é essencial trabalhar na questão do design de interface e, especialmente, capacitar usuários com controles de privacidade, de modo a aumentar a transparência, bem como a confiança e poder de controle sobre seus dados pessoais.

Sob outro enfoque, um dos problemas do antiquado modelo de notificação prévia e escolha individual é que esse formato desloca o ônus da proteção da privacidade e da proteção de dados sobre o indivíduo titular destes dados, o que pode ser questionado como uma barganha desigual.

Diante da impotência, é necessário adicionar outros meios, para além das formas tradicionais. Não se pode mais pensar e agir com os meios herdados das antigas ordens.



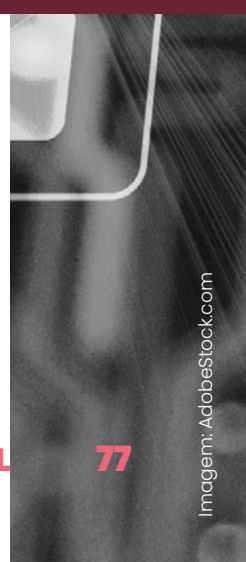
O direito, por si só, é limitado para dar amparo às necessidades atuais, de maneira que é necessário recorrer, outrossim, à própria tecnologia.



Há caminhos que buscam equalizar melhor a proteção de dados pessoais, cujo socorro não é delegado à lei propriamente dita, mas sim à tecnologia. São as assim chamadas *Privacy Enhancing Technologies* (PETs), de cujo espectro deriva o conceito do *privacy by design*, expressão cunhada na década 1990, por Ann Cavoukian, ex-comissária de Informação e Privacidade da Província de Ontário-Canadá.

Trata-se da regulação pela própria tecnologia. Para além de se basear tão somente em soluções trazidas unicamente pelos instrumentos jurídicos, verifica-se a necessidade de delegar às ferramentas padrões que elevem a proteção de dados do indivíduo.

Em outras palavras, conceitos do direito à privacidade e proteção de dados pessoais são incorporados, desde a concepção da arquitetura dos sistemas (by design), e por padrões de configuração padrão (by default), de modo a garantir condições para que o usuário tenha possibilidade de controlar sua privacidade e o tratamento de seus dados pessoais.

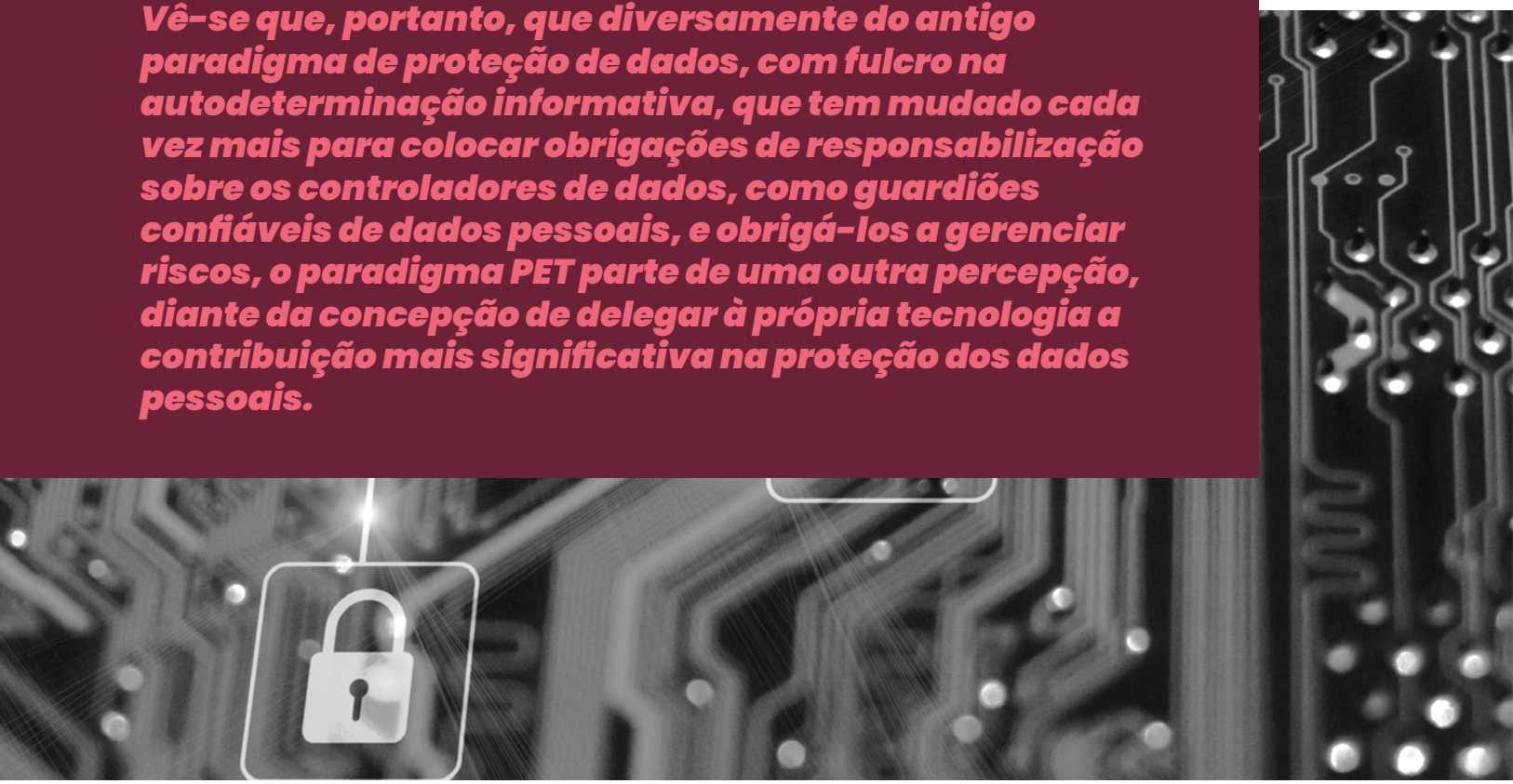


Esses conceitos não estão expressamente previstos na LGPD, porém o art. 46, § 2º prevê que as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações incidentais, deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Além disso, pelo §1º do mesmo artigo citado, a lei prevê que a ANPD poderá "dispor sobre padrões técnicos mínimos para tornar aplicável as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, considerando a natureza das informações

Imagem: AdobeStock.com

tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis". E, ainda, pela redação do artigo 55-J, inciso VIII da LGPD, compete à ANPD "estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle e proteção dos titulares sobre seus dados pessoais, consideradas as especificidades das atividades e o porte dos controladores", em clara adesão indireta ao conceito de *privacy by design* e *by default*. Ademais, na LGPD os conceitos *privacy by design* e *by default* são derivados da previsão dos princípios da transparência, segurança e prevenção, transcritos no artigo 6º da lei. De toda forma, perdeu o legislador brasileiro a oportunidade de inserir, de forma geral e expressa, um importante mecanismo de proteção de dados.

Vê-se que, portanto, que diversamente do antigo paradigma de proteção de dados, com fulcro na autodeterminação informativa, que tem mudado cada vez mais para colocar obrigações de responsabilização sobre os controladores de dados, como guardiões confiáveis de dados pessoais, e obrigá-los a gerenciar riscos, o paradigma PET parte de uma outra percepção, diante da concepção de delegar à própria tecnologia a contribuição mais significativa na proteção dos dados pessoais.



Não se pode deixar de verificar, por fim, o fato de que os controladores de dados encontram dificuldades para aplicação concomitante de várias leis, em seus serviços oferecidos ao mercado global de dados. E não menos importante, encontram-se os reguladores e governos com suas dificuldades (questões políticas, falta de recursos, etc.) de *enforcement.* E daqui deriva um cenário desigual que, por muitas vezes, direciona o regulador a se concentrar nos casos que tiveram mais repercussão na mídia, deixando outros *a latere* que mereceriam igual, ou até maior, atenção.

Juliana Abrusio

Advogada atuante há vinte anos em Direito e Tecnologia. Doutora em Direito pela PUC-SP. Mestre em Direito pela Universidade de Roma. Professora Permanente do Programa Stricto Sensu em Direito Político e Econômico da Universidade Presbiteriana Mackenzie.

Imagem: AdobeStock.com