condição *sine qua non* para a adequada proteção à privacidade, pois as leis não são autoimplementáveis e a cultura da privacidade não pode se estabelecer sem uma autoridade que a patrocine".

REFERÊNCIAS

Bennett, C. & Raab, C. (2006). *The Governance of Privacy*: Policy Instruments in Global Perspective. Cambridge: MIT.

Bennett, C. & Raab, C. (2018). *Revisiting 'The Governance of Privacy'*: Contemporary Policy Instruments in Global Perspective. Recuperado: 16 de maio de 2019, de ssrn.com/abstract=2972086.

Bioni, B. R. (2014). A produção normativa a respeito da privacidade na economia da informação e do livre fluxo informacional transfronteiriço. *Direitos e novas tecnologias*: XXIII Encontro Nacional do Conpedi, v. 1, pp. 59-82.

Hartmann, M. & Wimmer, J. (2011). Einleitung. In Hartmann, M. & Wimmer, J. (Eds.), *Digitale Medientechnologien*: Vergangenheit – Gegenwart – Zukunft (pp. 21). Wiesbaden: VS.

Manifesto pela aprovação da Lei de Proteção de Dados Pessoais. (2018). São Paulo. Recuperado de brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais.

Mattern, F. (2008). Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In Roßnagel, A. et al. *Digitale Visionen*: Zur Gestaltung allgegenwärtiger Informationstechnologien. Berlim: Springer.

Mendes, L. S. (2014). *Privacidade, proteção de dados pessoais e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva.

Mendes, L. S. & Doneda, D. (2016). Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, v. 9.

Entrevista I

P.S._ Na sua visão, quais são os principais atores e as dinâmicas que compõem o ecossistema de governança e regulação dos dados pessoais?

B.B._ Por um lado, há o titular, o próprio cidadão detentor daquela informação a ele vinculada, a ele correspondente – por isso, dados pessoais. Por outro lado, há os agentes de tratamento desses dados, que são as organizações que coletam e manejam as informações, como os setores privado e público. Existe uma subdivisão dentro desses agentes: o controlador, isto é, quem determina como os dados serão tratados. Em alguns cenários, ele terceiriza parte do tratamento dos dados. Nesses casos, entra em cena a figura do operador, cujo exemplo mais conhecido são as empresas contratadas para fazer o serviço de armazenamento dos dados, como as de computação em nuvem (*cloud computing*). Ainda para compor essa constelação de atores há os próprios órgãos reguladores. Nesse quesito, uma peça central da nova Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira é a criação de uma autoridade nacional de proteção de dados pessoais. O novo órgão terá como missão lidar com essa pauta e irá se juntar a outras agências reguladoras que têm essa responsabilidade dentro de seus respectivos setores, como a Secretaria Nacional do Consumidor. Um dos grandes desafios é promover a sinergia entre esses órgãos reguladores e, nesse sentido, o papel da futura autoridade nacional na coordenação da aplicação e fiscalização da LGPD com os demais atores será essencial. Por último, podemos citar as entidades de defesa de direitos difusos e coletivos. Em geral, o cidadão não tem no plano individual uma capacidade tão eficiente

Bruno Bioni
Consultor independente em privacidade e proteção de dados pessoais. Fundador do Data Privacy Brasil.

O Brasil já possui leis setoriais de proteção de dados pessoais, como no Código de Defesa do Consumidor, no Marco Civil da Internet, na Lei do Cadastro Positivo e na Lei de Acesso à Informação. Com a criação de uma lei geral, teremos um ordenamento jurídico regulatório mais completo, portanto, uma legislação de proteção de dados pessoais.

para a proteção de seus próprios direitos. Por isso, surgem organizações não governamentais que fazem a defesa de direitos em nome de grupos, além de outros órgãos, como a Defensoria Pública, o Ministério Público e os Procons. No cenário futuro, a tendência é que essas entidades lidem cada vez mais com uma agenda de proteção de dados pessoais.

P.S._ Na sua opinião, quais são os principais pontos da nova LGPD?

B.B._ O Brasil já possui leis setoriais de proteção de dados pessoais, como no Código de Defesa do Consumidor, no Marco Civil da Internet, na Lei do Cadastro Positivo e na Lei de Acesso à Informação. Com a criação de uma lei geral, teremos um ordenamento jurídico regulatório mais completo, portanto, uma legislação de proteção de dados pessoais. Por si só, a LGPD é importante porque, diferentemente dessas outras leis, ela é vocacionada para lidar somente com a proteção de dados pessoais. Assim, a LGPD elenca dez princípios que devem orientar qualquer tipo de tratamento de dados pessoais. Caso não haja o cumprimento de todos os dez princípios, o tratamento de dados pessoais será considerado ilegal.

Há agora um rol mais amplo de bases legais para o tratamento da proteção de dados pessoais, que são as autorizações e as hipóteses previstas pela LGPD que legitimam o tratamento dos dados. Essa lei é importante porque vai muito além do consentimento, a única base legal nas leis setoriais brasileiras. Com a LGPD, são adicionadas outras nove bases legais.

Um destaque é o legítimo interesse, passível de ser tomado como base por organizações em situações em que não seria possível obter consentimento, seja porque não há ponto de contato com o titular do dado, seja porque não seria recomendável buscar tal autorização. Isso poderia ocorrer, por exemplo, em atividades para a prevenção de fraude bancária. Está dentro do legítimo interesse de um banco evitar fraudes; ao mesmo tempo, como titular correntista do banco, é de meu benefício e está sob minha legítima expectativa que a instituição financeira trate meus dados pessoais sem o meu consentimento para gerar um perfil comportamental que sirva de critério para identificar operações financeiras possivelmente fraudulentas e, com isso, criar um sistema que previna fraudes. Esse é um típico caso de aplicação do legítimo interesse no qual há mais flexibilidade para autorizar o tratamento de dados pessoais.

Vale salientar ainda a aproximação da lei com ferramentas importantes de *compliance*, promovendo a existência de uma documentação por meio da qual organizações dos setores público e privado demonstram a sua conformidade com a LGPD. Hoje em dia, a principal ferramenta é o relatório de impacto da produção de dados pessoais, que indica o fluxo de dados tratados pela organização e aponta as respectivas bases legais, assim como as ações tomadas para atender à lei. É importante olhar para essa ferramenta de *compliance* como um documento por meio do qual as organizações

prestam contas sobre a sua conformidade com a lei, o que dialoga com um dos dez princípios da LGPD. Não adianta a organização dizer que faz um uso responsável dos dados pessoais; é preciso que ela documente esse processo de modo que, no futuro, possa demonstrar seu estado de conformidade com a LGPD.

P.S._ Qual é o impacto da General Data Protection Regulation (GDPR)[6] na América Latina?

B.B._ De maneira geral – e isso não é privilégio da GDPR –, ela tem aplicação extraterritorial, ou seja, a lei segue o dado, independentemente de onde esteja situado quem trata aquele dado. Para uma organização na América Latina que queira acessar o mercado europeu por meio da venda de produtos ou serviços, caso isso envolva tratamento de dados pessoais, a GDPR se aplica. Isso impacta a América Latina e o próprio cenário brasileiro de forma significativa, pois muitas das organizações locais têm, em menor ou maior medida, interface com o mercado da União Europeia.
Outro impacto diz respeito ao livre fluxo informacional, que está ligado a de que maneira os países trocam dados pessoais. Isso serve para os dois lados, ou seja, como as empresas brasileiras conseguem trazer dados coletados de pessoas situadas na União Europeia e como as empresas europeias conseguem transferir dados coletados de pessoas no Brasil. Por isso denominou-se de movimento bilateral. Na maioria das leis de proteção de dados pessoais – incluindo a GDPR e a LGPD –, há o livre fluxo informacional quando um país reconhece que o outro possui um nível adequado de proteção de dados pessoais. No futuro, algo que será tema de grande discussão no Brasil é a convergência entre a regulamentação brasileira e a europeia para que haja essa troca livre de dados. É por esse motivo que as leis de proteção de dados pessoais têm relação direta com a agenda de comércio exterior: em um cenário em que uma série de produtos e serviços depende do tratamento de dados pessoais e de sua transferência para viabilizar operações em um sentido global, essas leis têm um impacto importante.

P.S._ Na sua opinião, as legislações nacionais são suficientes para garantir o respeito à privacidade e a proteção dos dados pessoais? Existem outros mecanismos necessários?

B.B._ O código da lei, por si só, não é garantia de que aquilo que está previsto terá aderência na realidade. Na perspectiva de se pensar uma caixa de ferramentas para modular comportamentos na sociedade, o direito e

Não adianta a organização dizer que faz um uso responsável dos dados pessoais; é preciso que ela documente esse processo de modo que, no futuro, possa demonstrar seu estado de conformidade com a LGPD.

[6] General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados) é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais aplicável a todos os indivíduos na União Europeia (UE) e no Espaço Econômico Europeu (EEE). Regulamenta também a exportação de dados pessoais para fora da UE e EEE.

(...) a lei é apenas uma das ferramentas e, sozinha, não é suficiente para garantir o respeito à privacidade e a proteção dos dados pessoais. É preciso que ela seja articulada ao interesse econômico – o mercado –, ao aspecto cultural – as normas sociais – e à tecnologia. Aí, sim, será possível falar de uma proteção eficiente de dados pessoais.

as leis são apenas uma delas. Há outras ferramentas possíveis, como o próprio mercado, uma vez que ele pauta uma série de comportamentos sociais. Nesse sentido, uma grande mudança é as organizações enxergarem na privacidade e na proteção de dados pessoais uma vantagem competitiva, uma questão reputacional. Quando passa a existir um grupo de organizações que vocaliza como diferencial a proteção efetiva das informações de seus consumidores, o mercado emerge como um instrumento de modulação dos comportamentos.

Outra ferramenta são as próprias normas sociais, ou seja, como a sociedade constrange determinados comportamentos por si mesma, independentemente do Legislativo e do mercado. Isso está ligado a um aspecto cultural: nos países ou ambientes em que há uma cultura de proteção de dados pessoais, a própria sociedade exige do setor público – enquanto regulador ou grande interessado em tratar os dados – e do setor privado boas práticas para a proteção dos dados.

Por último, há a tecnologia, ou seja, como ela pode reforçar ou neutralizar a nossa capacidade de controlar as informações que nos dizem respeito. Um exemplo clássico é a criptografia, que reforçou o controle sobre nossos dados, sobretudo ao manter sigilo sobre o conteúdo das comunicações entre remetente e destinatário, onde se encontra uma série de dados pessoais. Existem também tecnologias que vão no sentido contrário, como as de reconhecimento facial, que permitem não só identificar uma determinada pessoa no meio de uma multidão, mas também reconhecer emoções e aspectos comportamentais por meio das expressões faciais. Portanto, a lei é apenas uma das ferramentas e, sozinha, não é suficiente para garantir o respeito à privacidade e a proteção dos dados pessoais. É preciso que ela seja articulada ao interesse econômico – o mercado –, ao aspecto cultural – as normas sociais – e à tecnologia. Aí, sim, será possível falar de uma proteção eficiente de dados pessoais.

P.S._ Muito se discute sobre o uso de dados pessoais por grandes empresas como Facebook e Google. De maneira geral, como o setor privado coleta e utiliza nossos dados?

B.B._ Uma primeira colocação é que a LGPD e, de modo geral, as regras de proteção de dados pessoais vão muito além do ecossistema da Internet, principalmente quando consideramos as organizações cujos modelos de negócios são baseados no uso de dados pessoais para o direcionamento de publicidade, conteúdo, entre outros. Setores tradicionais da economia, como a indústria automobilística, o setor de saúde e o de energia elétrica, têm cada vez mais apostado no uso dos dados de sua audiência,

consumidores e público-alvo para otimizar a prestação de serviços e fazer uma modelagem mais precisa dos produtos antes de seu lançamento no mercado. Então, em termos gerais, podemos dizer que boa parte do setor privado coleta e utiliza nossos dados pessoais para gerar competitividade e mais eficiência em suas atividades econômicas.
Algo que aparenta ser uma tendência é o entendimento pelo próprio setor privado da proteção de dados pessoais como valor, sobretudo, de ordem reputacional. Uma das questões que a LGPD traz é o direito de portabilidade, que permite ao titular migrar junto com seus dados para um serviço concorrente. Dentro dessa possibilidade, começamos a olhar para um cenário em que a proteção de dados pessoais aparece como um diferencial competitivo, o que é uma grande janela de oportunidade para o setor privado reconhecer o valor dessa mensagem de proteção e uso responsável dos dados enquanto uma estratégia de negócios.

P.S._ E o que acontece no âmbito dos provedores de serviço de Internet?

B.B._ A maioria dos modelos de negócios que existem hoje na Internet se baseia na publicidade comportamental. O consumidor ou usuário do serviço não paga por ele em dinheiro, mas faz uma "troca" de seus dados para que esse modelo de negócios seja monetizado pela entrada de publicidade comportamental em uma rede social ou um mecanismo de busca, por exemplo. Esse é um ecossistema bastante impactado por qualquer lei de proteção de dados pessoais. No Brasil não será diferente. Daqui para frente, precisamos observar o comportamento desses atores. Nesse cenário, tal como aconteceu na União Europeia, temos o papel das associações de classe em convocar todos esses atores a pensar boas práticas para que a própria reputação do setor seja responsiva às normas de proteção de dados pessoais. Isso significa, por exemplo, pensar como as tecnologias podem gerar padrões interoperáveis nessa multidão de atores para que, uma vez assinalada a opção do que você quer que seja ou não feito com seus dados, essa decisão seja alcançável e gere uma trilha auditável ao longo de todo o ecossistema de mídia *on-line*. O grande dilema, especificamente no âmbito da Internet, é que quando você utiliza essas plataformas, diversos atores estão acompanhando, monitorando e colecionando uma série de informações sobre seus hábitos para formar um perfil comportamental bastante preciso sobre você. Não é por acaso que uma determinada publicidade passa a te acompanhar em vários ambientes que você frequenta na Internet. Dessa forma, a questão que se coloca é conseguir desenvolver tecnologias capazes de escalar a capacidade do titular de ter mais controle e visão da maneira como seus dados são trafegados nesses ambientes, como isso se volta para eles, seja enquanto direcionamento de conteúdo ou de publicidade.

O consumidor ou usuário do serviço não paga por ele em dinheiro, mas faz uma "troca" de seus dados para que esse modelo de negócios seja monetizado pela entrada de publicidade comportamental em uma rede social ou um mecanismo de busca, por exemplo.