Proteção de Dados e Direito Digital

Ana Carolina Cagnoni

A Proteção de Dados no Brasil: Uma Complexa Colcha de Retalhos

Keep Calm and Knit it on

Em meados de agosto do ano passado, o Congresso Nacional tomou um passo importante na criação de uma legislação geral de proteção de dados. Depois de muitos anos de debate e várias minutas, a Lei Geral de Proteção de Dados[1] finalmente foi sancionada. Claramente baseada nos dispositivos da GDPR, mas inovando também em alguns aspectos, a nova legislação cumpre um importante papel de harmonizar regras aplicadas ao setor público e privado, válidas para grandes e pequenas empresas, independentemente do setor e/ou atividade. Vemos, portanto, que o Brasil tomou uma decisão significativa no sentido de unificar princípios, direitos e obrigações relacionadas a proteção de dados pessoais. Essa nova realidade jurídica já entraria em vigor em fevereiro de 2020.

No entanto, como nem todas as coisas fluem suavemente como bossa nova no Brasil, o ex-presidente Michel Temer vetou alguns artigos da nova Lei, alegando serem formalmente inconstitucionais. Todos os artigos relacionados à criação da Agência Nacional de Proteção de Dados estavam incluídos nesse rol. Por uma série de razões que não serão discutidas aqui, em dezembro, uma medida provisória[2] foi promulgada para complementar pontos que foram vetados e para *prorrogar a data em que a Lei entraria em vigor por mais 6 meses*.

Hoje, no final do primeiro semestre de 2019, o cenário atual ainda é um pouco confuso. Isso porque a medida provisória deve ser discutida e ratificada pelo recém-eleito Congresso até junho, caso contrário, ela se tornará ineficaz e o texto original prevalecerá. Em suma, a atual situação da Lei Geral de Proteção de Dados no Brasil é incerta, já que ninguém sabe quando ela se tornará efetiva: fevereiro ou agosto de 2020.

[1] Lei 13.709/18.
[2] Medida Provisória 869/18.

Isso significa que não há regras efetivas sobre proteção de dados no Brasil hoje? Absolutamente não. Pelo contrário, o regime setorial anterior (e bastante complexo) de diferentes legislações permanece em vigor e efetivo. Isso também significa que, com base nesses textos legislativos, medidas coercitivas estão sendo tomadas, incluindo ações civis públicas sendo propostas por promotores e investigações sendo instauradas por órgãos de defesa do consumidor.

Entender como a Lei Geral de Proteção de Dados é aplicada atualmente é como costurar retalhos complexos de leis e regulamentos esparsos, além de legislações estaduais e municipais. Portanto, o objetivo deste artigo é fornecer uma visão geral das principais leis vigentes atualmente.

1) Constituição Federal (1988). Na lista de direitos fundamentais está a garantia de proteção à privacidade, intimidade e a imagem pessoal. Em termos gerais, esses direitos são considerados "invioláveis" e é garantida a indenização contra danos materiais e/ou morais resultantes dessa violação. Uma vez constituídos como direitos fundamentais, tais direitos não podem ser renunciados. Além disso, a Constituição Federal garante a confidencialidade das comunicações, que só podem ser acessadas no curso de um processo de investigação criminal e com a autorização prévia de um juiz. Uma lei federal específica estabelece critérios adicionais para interceptação de comunicações privadas. Por fim, vale destacar que a Constituição Federal também inseriu o *habeas data* no sistema jurídico brasileiro. Esse tipo específico de ação judicial pode ser interposto diretamente pelo titular dos dados interessado em solicitar acesso aos dados pessoais armazenados em qualquer banco de dados governamental.

2) Código Civil (2001). Em termos gerais, o Código Civil garante o direito de um indivíduo ter uma vida privada, constituindo um "direito pessoal". Sendo assim, o Código determina expressamente que esses direitos não podem ser cedidos ou renunciados sob nenhuma circunstância. Os direitos de imagem receberam um tratamento específico, uma vez que a imagem de um indivíduo só pode ser usada para fins comerciais se houver autorização. Além disso, embora não especificamente relacionado à proteção de dados, vale mencionar que a capacidade civil no Brasil é válida apenas para os maiores de 18 anos de idade. Indivíduos entre 16 e 18 anos são considerados relativamente capazes, o que significa que quaisquer atos civis realizados por eles (como dar consentimento) devem ser acompanhados por um adulto para ser considerado válido. Por fim, o Código Civil também fornece uma série de determinações gerais sobre indenizações, e vale destacar que é imposta a responsabilidade objetiva para aqueles que causam danos decorrentes de atividades conduzidas que tragam riscos iminentes aos direitos de terceiros.

3) Código de Defesa do Consumidor (1990). O Código de Defesa do Consumidor estabelece um amplo conjunto de obrigações aos prestadores de serviço/produto, assim como prevê uma série de direitos aos consumidores, que são considerados a parte vulnerável de tal relação. Dentre tais regras, o Código dispõe certos critérios para a coleta, processamento, transferência, divulgação e armazenamento de dados do consumidor e a necessidade das empresas em obter o consentimento do consumidor para realizar tais atividades, de preferência

de forma inequívoca. Ele também concede aos titulares dos dados o direito de acesso às informações obtidas sobre eles, bem como o direito de retificação desses dados.

Ademais, em termos mais gerais, o CDC impõe que todas as comunicações dirigidas a consumidores (tais como os termos de uso) deve estar em português e em uma linguagem simples e clara, facilmente compreendida. Por ser aplicável a todas as relações de consumo, apesar de ser uma lei setorial, os princípios e regras do Código são também aplicáveis à maioria das atividades empresariais no Brasil, incluindo serviços gratuitos ou que são remunerados indiretamente (como serviços baseados em publicidade). Além disso, o Código adota o regime de responsabilidade objetiva, o que significa que fornecedores (e todas as empresas da cadeia de fornecimento) podem ser considerados responsáveis por danos sofridos pelos consumidores, independentemente da sua culpa. No que tange o *enforcement*, o direito do consumidor no Brasil é vigilantemente fiscalizado por órgãos de proteção ao consumidor em todos os níveis da administração (municipal, estadual e federal), bem como por setores específicos do Ministério Público, o que significa que este Código é a base legal utilizada na maioria das reclamações e ações judiciais sobre a proteção de dados existentes hoje.

4) Marco Civil da Internet (2014). Esse mais recente componente da legislação brasileira contém regras e princípios fundamentais de proteção de dados e pode ser amplamente aplicável, pois estabelece os direitos e obrigações relacionados ao uso da internet no Brasil. Existem disposições expressas determinando o alcance extraterritorial ao impor a aplicação das leis brasileiras em qualquer ato de coleta, armazenamento ou processamento de dados pessoais, se as comunicações ocorrerem no Brasil ou um ponto final de processamento é no Brasil. Empresas estrangeiras devem também estar vinculadas a essas regras, se eles tem pelo menos uma pessoa jurídica estabelecida no país ou se os serviços oferecidos são destinados aos brasileiros.

Além de reafirmar a inviolabilidade da privacidade, esta lei determina de forma clara e específica que a coleta, uso, processamento ou transferência de dados pessoais para terceiros não pode ser feita sem o consentimento livre, expresso e informal dos titulares dos dados. Ademais, a linguagem do consentimento deve ser destacada de outras cláusulas contratuais, ou seja, deve ser visivelmente diferente para chamar a atenção do indivíduo. Disposições adicionais que impõem o dever de transparência e minimização de dados também estão incluídas nesta Lei, bem como medidas de segurança a serem adotadas. Em relação às sanções, o Marco Civil da Internet permite penalidades graduais, desde notificações, multas e suspensão ou mesmo a proibição da atividade de processamento de dados são opções disponíveis para as autoridades. Deve ser salientado, contudo, que tais sanções são mais duras do que as da lei recém-promulgada: a multa atual pode chegar a até 10% do faturamento anual no Brasil, enquanto a nova Lei Geral de Proteção de Dados limita multas em até 2% e não dá espaço para suspensão da proibição de atividades de processamento de dados. Não se sabe, porém, como os dois dispositivos legais serão compatibilizados assim que a Lei Geral de Proteção de Dados entrar em vigor.

Além destas mencionadas aqui, outras leis setoriais específicas estabelecem regras de proteção de dados e disposições mais gerais de privacidade. Dentre elas, podemos mencionar (a) a Lei de Geral de Telecomunicações aplicável as empresas de telecomunicações, (b) a Lei do Sigilo de Operações Financeiras aplicável aos bancos e outras instituições financeiras, e (c) a Lei do Cadastro Positivo.

Cumpre ressaltar que determinados setores são regulados por agências federais específicas, que podem instaurar procedimentos administrativos para investigar e impor sanções em resposta a violações de tais leis. Esses órgãos administrativos também podem aprovar regulamentações sobre atividades de processamento de dados a serem adotadas por empresas por eles regulamentadas, assim como o Banco Central do Brasil ao determinar padrões de segurança para instituições financeiras que contratam serviços de processamento de dados em nuvem.

Por fim, é preciso mencionar que o Código Penal também estabelece certas proibições criminais relacionadas à violação da lei de proteção de dados. Por exemplo, a violação de sigilo profissional é um crime no Código Penal Brasileiro. Ademais, certas profissões têm o dever de sigilo imposto por leis federais (como o Estatuto da Ordem dos Advogados) ou pelo Regulamento dos Conselhos (como o Conselho Federal de Medicina).

Diante deste resumo sobre a atual legislação brasileira, é impossível dizer que nenhuma proteção é dada aos dados pessoais no país. Mesmo assim, é visível que a nova Lei Geral de Proteção de Dados trará mais certeza e detalhes sobre como os dados pessoais devem ser tratados, apesar da existência de alguns pontos de conflito com a legislação vigente, que deverão ser resolvidas por meio de decisões judiciais futuras. Até lá, esperamos que este artigo traga alguma luz aos profissionais estrangeiros ao avaliar como conduzir seus negócios enquanto a nova Lei Geral de Proteção de Dados do Brasil ainda não entrou em vigor.

Ana Carolina Cagnoni – CIPP/E e CIPP/US. Advogada de Propriedade Intelectual, Direito Digital e Proteção de Dados - Sócia em Grinberg Cordovil Advogados

Artigo inicialmente publicado em inglês no site da International Association of Privacy Professionals – IAPP em 10 de abril de 2019.