Um ensaio acerca dos três maiores desafios de adequação à LGPD enfrentados por empresas de pequeno porte, no Brasil.

Pode parecer um pouco tarde para falar em adequação à LGPD - Lei Geral de Proteção de Dados, ou lei 13.709/18. No entanto, a verdade é que, no apagar das luzes de 2021, há uma considerável quantidade de empresas, mormente pequenas, que ainda não começaram suas jornadas de adequação à LGPD - mesmo transcorridos mais de três anos da publicação desta novel legislação, em agosto de 2018.

Não seria demasiado lembrar, que a LGPD tutela aqueles dados entendidos como "pessoais", ou seja, uma informação relacionada a uma pessoa natural, identificada ou identificável - vide art. 5º, I, da LGPD. Além disso, aplica-se, como regra, salvo exceções previstas no art. 4º, da LGPD, a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio (físico ou digital) ou país (nacional ou estrangeiro). Por isso, todas as empresas que comercializam bens ou serviços no mercado, estão sujeitas à aplicação da LGPD, e precisam realizar o tema de casa de adequar suas estruturas às exigências da lei.

É compreensível a expectativa do mercado de que a ANPD (Autoridade Nacional de Proteção de Dados) possa, a qualquer momento, normatizar a aplicação da LGPD para pequenos negócios, flexibilizando muitas das disposições que, hoje, aplicam-se para todo e qualquer agente de tratamento de dados pessoais, controlador ou operador, independentemente do seu porte econômico (one-size-fit-all). No entanto, muito embora a ANPD tenha aberto, em agosto de 2021, consulta pública e inscrições para audiência pública sobre norma de aplicação da LGPD para microempresas e empresas de pequeno porte, até agora, essa deseja flexibilização ainda não se tornou realidade.

Para acalentar os anseios deste segmento, a ANPD até publicou, em outubro deste ano, um importante "Guia Orientativo" sobre "Segurança da Informação para Agentes de Tratamento de Pequeno Porte".1 No entanto, a desejada norma para flexibilizar a aplicação da LGPD para o segmento das pequenas empresas ainda não se tornou uma realidade. Neste contexto, o presente ensaio busca elencar os três maiores desafios identificados nos trabalhos de adequação à LGPD realizados por empresas deste porte, para servir de orientação para aquelas empresas que ainda não começaram a realizar o seu tema de casa.

Desafio 1: Mapeamento de Processos

O primeiro desafio enfrentado por pequenas empresas, em seus trabalhos de adequação, reside na necessária realização de um mapeamento de processos, para identificar todas as atividades e/ou operações em que há o tratamento de dados pessoais.

Tal mapeamento é uma exigência de diversas disposições da LGPD, a começar pelo ânimo dos artigos preliminares da Lei em empoderar o titular de dados com a gestão e controle acerca dos tratamentos realizados com seus dados pessoais, mas, também, pela necessidade de que todos esses processos sejam justificados por, ao menos, um dos autorizativos da Lei, constantes nos seus artigos 7º e 11.

Não bastasse, para o escorreito atendimento a diversos dos direitos dos titulares de dados, os agentes de tratamento não poderão furtar-se em dispor dos registros daquelas informações, devidamente mapeadas e justificadas. Isso, sem contar com a própria previsão do artigo 50 da Lei, acerca das boas práticas e da governança, na qual restam previstas as regras para construção de um Programa de Governança em Privacidade, que tem como elemento central um Mapeamento de Processos.

Ocorre que, por mais óbvio que possa parecer, um pré-requisito básico para a realização de um mapeamento de processos, é que a empresa disponha de processos claros e definidos. Neste ponto, não se pode confundir o "mapa" com o "território". O mapa consiste no desenho do território, para que as pessoas possam conhecer

o terreno e orientar sua trajetória. Agora, o território precede o mapa. Em outras palavras, se não existe território, nada há a ser mapeado.

Trazendo para a realidade de uma empresa de pequeno porte, forçoso reconhecer que, devido ao seu porte, muitos processos ainda não se encontram definidos na estrutura da empresa. Mesmo aqueles processos singelos e corriqueiros de qualquer empresa, como RH, financeiro e comercial, por exemplo, muitas vezes são realizados de forma personalíssima, por algum colaborador da empresa que acaba tendo bastante liberdade em definir os processos e fluxos, de forma ad hoc.

Essa liberdade excessiva que pequenas empresas dispõem em moldar seus processos internos de negócio, sem maiores definições e formalizações de processos ou rotinas, acaba por dificultar, quiçá inviabilizar, um mapeamento efetivo de processos de tratamento de dados. Mesmo que realizado, descrevendo o território possível, esse mapeamento não disporá de mínima perenidade e acuracidade - eis que os processos são sempre mutáveis e temporários neste tipo de estrutura - não satisfazendo, portanto, as necessidades da LGPD.

Por isso, aqui reside o primeiro grande desafio de uma jornada de adequação à LGPD para pequenas empresas: o Mapeamento de Processos.

Desafio 2: Segurança da Informação

Muitas vezes tratados como temas idênticos, "proteção de dados" e "segurança da informação", na verdade, são temáticas autônomas que se intersecionam. Ao passo em que "proteção de dados" preocupa-se, exclusivamente, com o tratamento de dados pessoais (excluindo-se dados de pessoas jurídicas), "segurança da informação" pode ser compreendida, em um conceito livre, como um conjunto de medidas físicas, técnicas e organizacionais aptas a garantir a confidencialidade, integridade e disponibilidade da informação. Por isso, uma vez que os dados pessoais representam prismas de uma informação, a segurança da informação serve como uma das medidas protetivas previstas na LGPD para o escorreito tratamento de dados pessoais.

Avançando nas disposições legais, essas intersecções podem ser identificadas, por exemplo, no âmbito dos princípios da LGPD. Consoante comando do seu artigo 6º, as atividades de tratamento de dados pessoais deverão observar a "segurança" e a "prevenção", entendidos, respectivamente, como: (i) a utilização de medidas 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 difusão; e (ii) adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Indo além, no artigo 47, da LGPD, em seção que trata do "da Segurança e do Sigilo de Dados", resta prevista a disposição de que "os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término". Com efeito, essa temática é tão relevante, na perspectiva da LGPD, que em pouco mais de seis dezenas de artigos, a palavra "segurança" é grafada vinte e cinco vezes!

Em que pese esse ânimo legislativo, estudos apontam que as práticas de segurança da informação em pequenas empresas ainda são bastante incipientes. A esse respeito, vale trazer à lume pesquisa realizada pelo Núcleo de Informação e Coordenação do Ponto BR, denominada "TIC Empresas 2019" (NIC.br, 2019), que revelou "a presença incipiente de políticas ou práticas de segurança digital entre as empresas brasileiras de todos os portes, sobretudo nas pequenas empresas". Mais precisamente, identificou-se que mais de 60% (sessenta por cento) das empresas com até 49 (quarenta e nove) funcionários não dispõe de uma Política de Segurança, sendo que, neste mesmo segmento, mais de 80% (oitenta por cento) ainda não promoveram treinamentos sobre segurança digital.2

Os números são alarmantes, e refletem, via de consequência, o segundo grande desafio de um processo de adequação à LGPD, mormente para a realidade de pequenas empresas: "Segurança da Informação". Certamente, ciente desta carência especial, a ANPD lançou o

já mencionado "Guia Orientativo" sobre "Segurança da Informação para Agentes de Tratamento de Pequeno Porte". Trata-se de importante ferramenta para guiar empresas deste porte em suas jornadas de adequação.

Desafio 3: Cultura de Proteção de Dados

Por fim, o terceiro grande desafio pode ser denominado: Cultura de Proteção de Dados. Esse desafio reflete uma necessidade de que a temática se torne um tema institucional na estrutura empresarial, e não apenas um projeto, com início e fim, que, após o seu término, não será mais desenvolvido. Com efeito, é crucial que o projeto de adequação à LGPD migre para um status de Programa de Governança em Privacidade, em constante progresso e atualização.

Nesse sentido, empreender esforços para a expansão de uma cultura da proteção de dados na empresa é fundamental para o efetivo sucesso de um Programa de Governança em Privacidade. Além da criação de canais, procedimentos e políticas para orientar colaboradores e parceiros de negócios sobre as novas "regras do jogo", é crucial a criação de estratégicas de comunicação interna e treinamentos, voltados para a fixação de conceitos e procedimentos internos.

No quesito da "cultura", paciência é fundamental. Fazendo alusão a uma corrida, pode-se afirmar, com tranquilidade, que a gestão de um Programa de Governança em Privacidade pode ser comparada a uma maratona: cadência e ritmo são fundamentais para que se possa chegar ao fim da empreitada. A única diferença da maratona para a realidade da proteção de dados é que aquela tem fim, após quarenta e dois quilômetros. Já um programa de governança em privacidade, será uma constante daqui para frente.