Por **Marco Aurélio Souza Mendes**[1]

O mês de agosto inaugurou um momento até então esperado e, ao mesmo tempo, temido pelo mercado brasileiro. Isso porque o período marca o início da vigência das sanções administrativas da Lei Geral de Proteção de Dados (LGPD), ou seja, da atuação verdadeira e legítima da autoridade pública sobre o assunto.

Neste contexto, é necessário que os experts de prateleira deixem de comprar a ideia fast-food de que a LGPD é uma legislação de inúmeras proibições e com ausência de instrumentos práticos para resolução de problemas. Outra ideia do setor dos enlatados é a percepção de que a Autoridade Nacional de Proteção de Dados (ANPD) atuará com extrema paciência, esperando inerte que as empresas adotem práticas de conformidade.

Os extremos são produtos vencidos e que precisam ser prontamente descartados. A urgente necessidade deste momento é a de desconstruir mitos sobre a LGPD e a proteção de dados que foram até então amplamente propagados.

A digitalização de cadeias de abastecimento, a transição das operações do meio físico para o virtual e a intensa percepção do uso de tecnologias orientadas à ótica Data Driven fez com que o uso e a importância dos dados nas operações de negócio tomassem proporções de necessidade e velocidade até então inimagináveis.

Assim, a LGPD segue o exemplo e a estrutura da maior parte das legislações de privacidade ao trazer suas regras com o sentido de garantir a adoção de novas práticas de governança, segurança cibernética e organização do sistema de interceptação e coleta massiva de dados. A postura do operador de compliance desta Lei deve ser a de interpretar seus preceitos sob a égide da neutralidade tecnológica e um sistema global de boas práticas.

Com esse fundamento, não se deve pensar na proibição em si quando há a oportunidade de entender as novas tecnologias e ferramentas que podem ser aplicadas ao negócio para que aquilo que já se realiza possa ser feito com mais segurança e eficiência. As atuações do CISO (Chief Information Security Officer), do CIO (Chief Information Officer) e do DPO (Data Protection Officer) se encontram justamente neste trabalho.

O diálogo interoperacional entre estes gerenciadores da Segurança da Informação e de Privacidade da empresa deve sempre possuir o objetivo de construir soluções e processos novos que sejam capazes de continuar gerando receitas, ao mesmo tempo que analisa o ambiente em que a atividade está inserida para minimizar riscos, mitigar vulnerabilidades e adotar os recursos tecnológicos e procedimentos que garantirão a segurança.

Sob o aspecto da privacidade, neste campo, a preocupação deve ser adequar o processo para que ele colete o mínimo possível de dados e atinja com maior eficiência os objetivos pretendidos pela finalidade desenvolvida na análise de riscos. A Lei deve, portanto, ser um motor de criatividade e possíveis inovações no modelo de como a atividade é desenvolvida.

A organização do suitability pelas instituições financeiras segue modelo de abordagem criativa apresentado. O processo para verificar a adequação de um cliente ao portfólio de investimentos coleta um agrupamento de dados que irá gerar novas informações com relação ao perfil, apetite de risco e tolerância de perdas. A atividade é altamente regulamentada e necessária para minimizar as perdas e melhorar o nível de personalização da relação entre cliente e instituição financeira.

Outro exemplo interessante é a atividade que alguns varejistas utilizam de coleta de dados pessoais para obtenção de perfil individualizado de consumo. Com essa personalização, o titular receberia as comunicações de ofertas com base no seu potencial interesse individual.

O trade-off, neste caso, é extremamente positivo para as duas partes, pois dentre os inúmeros benefícios que podemos citar está a realização de uma relação comercial com maior pessoalidade e ganho de potencial de compra. Novamente, a preocupação para esta atividade deve ser sempre com aspectos dos meios de segurança da informação aplicados e das condutas de minimização e aderência de finalidade na coleta.

Para levantar as fragilidades e riscos das atividades da empresa, é imprescindível que o grupo "DPO, CIO e CISO" possua como principal roadmap de atuação o trabalho conjunto em criar um planejamento de governança para promover uma cultura de segurança em que a proibição e a punição deem lugar ao espaço de flexibilidade, criatividade e adesão às novas tecnologias. Tudo para garantir o equilíbrio proposto entre segurança, privacidade e geração de receitas.

Estimativas da Verizon, em seu Relatório Data Breah Investigations Report, de 2020, apontam que 17% de todas as violações de dados que ocorreram em 2020 foram causadas por conta de erro humano ou comportamentos inadequados, como a utilização de dados reais em ambientes de desenvolvimento ou o armazenamento acidental de dados confidenciais em ambientes públicos ou abertos. Esse cenário pode chegar a custar bilhões para uma empresa, pois a estimativa média de 2020 da IBM sobre o custo médio de um vazamento de dados foi de 4,24 milhões de dólares por incidente, um aumento significativo de 10% com relação à estimativa do ano anterior.

O mesmo raciocínio pode e deve ser aplicado para a atuação fiscalizatória da ANPD. O projeto de resolução da atuação de monitoramento da Autoridade apresenta a fórmula de fiscalização por ciclos e classificação de faixas indicativas, mecanismo parecido ao que já ocorre na atuação regulatória do mercado financeiro.

A orientação pedagógica não retirará o caráter de possibilidade sancionatória, tendo em vista que o trabalho dentro de um Ciclo de Monitoramento será individualizar a percepção do nível de conformidade em privacidade da empresa com o máximo possível de elementos específicos sobre a estrutura do negócio.

O projeto normativo do Regulamento de Fiscalização da ANPD traz a imagem mencionada de uma atuação por partes. A Autoridade, baseando-se na experiência de outras entidades fiscalizatórias e de processo coletivo, como na atuação do CADE, Mercado Financeiro e os ajustamentos de conduta na Tutela Coletiva, apresentará de início medidas de conformidade e regularização para posteriormente avançar no processo administrativo sancionatório.

O gestor precisará entender que a Autoridade utilizará como premissa para a atividade fiscalizatória a gestão de riscos e o estímulo à cultura de proteção de dados visando o equilíbrio entre a geração de receitas e a autorregulação no tema da privacidade.

A Minuta da Resolução mencionada traz em sua norma a menção explícita de que a aplicação da sanção será precedida por uma fase de regularização ou um plano de conformidade e que o não cumprimento das medidas indicadas neste planejamento levará ao escalonamento da atuação do órgão regulatório e à adoção dos instrumentos repressivos como a multa ou a proibição de realizar a atividade de tratamento.

Dessa forma, analisar a lei como uma carta somente de proibições individuais lhe fará correr dois riscos de alta sensibilidade e ambos com relevante perda financeira: o impacto na perda de agilidade e tomada de decisões nas atividades de seu negócio ou a não conformidade com os aspectos globais de privacidade e proteção de dados citados que culminará, em algum momento, na aplicação de multa pela Autoridade.

O conselho fundamental para os próximos meses é a contínua adaptação. Da mesma maneira que na natureza uma mudança no ecossistema força que espécies se adaptem entre hábitos e comportamentos para sobreviverem, a empresa necessita replicar essa flexibilidade para não incorrer na extinção de seu negócio.

_____

[1] Marco Aurélio Souza Mendes é consultor de Data Privacy da ICTS Protiviti, empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação e proteção e privacidade de dados.