Por Gustavo Artese (*)

Após anos de debates o Brasil conquistou no ano passado a Lei Geral de Proteção de Dados Pessoais (LGPD), que já começou a ser chamada de "O GDPR brasileiro", em referência à legislação europeia. A LGPD e o GDPR ficaram famosos nos últimos tempos e têm preocupado organizações que dependem do processamento de dados. Mas, afinal, qual o sentido dessas normas novas que vieram ocupar as preocupações (e o orçamento) das empresas? A pergunta começa a ser respondida nas conquistas de Alan Turing.

Turing foi um matemático britânico que dedicou sua vida ao estudo da computabilidade. Recentemente Alan Turing teve parte de sua vida retratada no filme "Jogo de Imitação", onde sua notória atuação na decodificação de mensagens alemãs durante a Segunda Guerra Mundial foi contada. Além de sua contribuição na decodificação dos enigmas alemães – e ao que nos interessa – o matemático inglês criou a chamada Máquina de Turing, que envolveu modelos lógicos que fundamentaram a computação tal qual conhecemos hoje. Alan Turing é considerado como pai da ciência da computação.

O trabalho de Alan Turing possibilitou o avanço da computação e de todas suas aplicações, incluindo o processamento de dados em grande volume. O fenômeno que se destaca nos dias de hoje é quando esse tipo de processamento envolve dados que dizem respeito a pessoas. Por vezes, o tratamento desses dados, ao passo que pode viabilizar uma infinidade de proveitos e avanços, também significa a criação de riscos às pessoas.

A ciência econômica define como externalidades os efeitos colaterais que uma decisão tem sobre aqueles que não participaram dela. Verifica-se uma externalidade quando há consequências para terceiros que não são levadas em conta por quem toma a decisão. A externalidade é negativa quando gera custos para os agentes externos. A poluição é o exemplo clássico de externalidade negativa.

De forma análoga, o tratamento de dados pessoais traz consigo riscos que são afeitos aos ônus da sociedade da informação. Tais riscos podem ocorrer, por exemplo, na forma de exposição indevida da intimidade de pessoais, na possibilidade de decisões arbitrárias, na discriminação para recebimento de serviços essenciais ou na falta de controle sobre o fluxo de dados que dizem respeito a uma pessoa.

A ideia central da existência da proteção de dados pessoais é buscar mitigar os riscos associados ao processamento de dados pessoais. As atuais normas sobre privacidade, são, em essência, respostas ao tratamento massivo de dados pessoais e os crescentes riscos a ele inerente. Ou seja, a criação da LGPD é uma resposta regulatória (risk regulation) ao veloz e inevitável avanço da computação e da sociedade da informação.

Não por outro motivo que as normas sobre proteção de dados pessoais partem do pressuposto de que o tratamento de dados dessa natureza somente pode ser realizado caso sejam atendidos uma série de obrigações, controles e requisitos. Para a LGPD o "não" é o *default* para o tratamento de dados pessoais. A conversão do "não normativo" à permissão para o tratamento de dados pessoais exige a adoção de medidas específicas, que dependem comprometimento e investimentos pelas organizações.

Superar o "não" da LGPD significa buscar atender a quatro conjuntos de medidas ou ações associados ao tratamento de dados pessoais, quais sejam: (i) observar os requisitos para tratamento (e.g. obtenção de consentimento, existência de interesses legítimos, tratamento para a tutela de saúde); (ii) tratar os dados pessoais de acordo com os princípios aplicáveis à gestão de dados (e.g. apenas para a finalidade objeto do consentimento; mínimo de dados necessários para atingir o propósito do tratamento); (iii) garantir aos titulares seus direitos quanto a seus dados (e.g. acesso, correção, portabilidade, eliminação e revogação); (iv) adotar de controles, processos,

boas práticas e governança (e.g. DPO, Privacy by Design, Accountability).

Advirta-se que as providências indicadas acima não deságuam em processo simples ou natural. Um programa de privacidade eficaz deverá estar inserido na estratégia, operação, processos e cultura da empresa. Somente assim será assegurado o sucesso e sustentabilidade dos negócios das data reliant companies (quase todas hoje em dia).

A par disso, as palavras de ordem, que devem permear qualquer esforço de compliance em proteção de dados são ética, confiança e comprometimento. Ética no sentido de que a organização deve pautar seu tratamento de dados com base na razoabilidade; confiança no sentido de que a conquista de confiança de todos os stakeholders (e.g. titulares, regulador e parceiros) deve ser perseguido; comprometimento na medida em que nenhum desses objetivos será atingido sem o compromisso da alta administração.

(*) **Gustavo Artese**, da **Viseu Advogados**.

Fonte: **TI Inside**, em 02.03.2019.