Importância da análise e gestão de riscos no tratamento de dados

As legislações de proteção de dados pessoais publicadas nos últimos anos podem ser vistas como respostas necessárias ao aumento exponencial do uso desses dados. Com efeito, a evolução tecnológica trouxe modificações nas relações pessoais e econômicas, na medida em que novas tecnologias da informação passaram a mediar comportamentos humanos, trazendo como uma de suas consequências o

Instrumentos normativos como o Regulamento Geral sobre Proteção de Dados (*General Data Protection Regulation* ou GDPR), a norma europeia em vigor desde maio de 2018, ou a Lei Geral de Proteção de Dados (LGPD), a norma brasileira em vigor desde setembro de 2020, representaram marcos importantes. Essas normas não têm como finalidade proibir o uso dos dados pessoais, mas deixam bem claro que, para o tratamento de dados é preciso obedecer a regras, sob pena de responsabilização.

Nesse sentido, as organizações de qualquer natureza — pública ou privada, unipessoal ou multinacional — que tinham o uso indiscriminado dos dados pessoais como *modus operandi* precisam, por força de lei, se adequar aos comandos trazidos pelo sistema normativo. Até então, prevalecia a ideia da coleta indiscriminada de dados pessoais com o objetivo de extrair o máximo de informações possíveis, para as mais diversas finalidades. As legislações de proteção de dados, ao estabelecer parâmetros de responsabilidade a serem cumpridos pelos agentes de tratamento, forçaram controladores e operadores a avaliar a vantagem real obtida pelo uso dos dados em face do esforço necessário para garantir sua efetiva segurança e a observância às normas de proteção de dados. Essa avaliação é necessária para que se resolva um *trade-off* inerente à sociedade de informação: de um lado, as vantagens obtidas com o tratamento de dados pessoais e, do outro, a necessidade de proteção da privacidade e demais direitos fundamentais dos titulares[2].

Evidentemente, não utilizar dados pessoais não é nem remotamente uma opção em uma sociedade cada vez mais dependente das informações deles extraídas. Contudo, é preciso que haja uma honesta autoavaliação das condições em que cada uma dessas instituições vem se beneficiando do uso dos dados. A verdade é que se, por um lado, o uso dos dados possibilita a extração de informações valiosas, por outro lado, cria uma grande responsabilidade muitas vezes custosas para quem os detém.

Assim, como a implementação da LGPD ocorre a partir de uma abordagem baseada em risco, quanto mais dados forem tratados, mais abrangentes precisam ser o controle e o programa de governança dos agentes de tratamento. É preciso aplicar a prática de uma *gestão de riscos*, com a adoção de um conjunto de ações coordenadas, com o objetivo de controlar os possíveis impactos que um determinado tratamento pode gerar.

Aderir a uma *gestão de riscos* com a sistematização e metodologia apropriadas é um elemento essencial em qualquer organização. Isso fica evidente a partir dos princípios da segurança (artigo 6º, VII), da prevenção (artigo 6º, VIII) e da responsabilização e prestação de contas (artigo 6º, X), bem como a partir da leitura da Seção III do Capítulo VI e do Capítulo VII da lei brasileira, que, respectivamente, dispõem sobre a responsabilidade e ressarcimento dos danos e sobre a segurança dos dados dos titulares.

A questão é que, para que tenhamos uma promoção efetiva dos direitos fundamentais tutelados pelas normas de proteção de dados, não basta que riscos sejam compensados. É preciso, em primeiro lugar, preveni-los[3]. Afinal, prevenir e avaliar danos são medidas necessárias em uma sociedade que se preocupa em alocar corretamente os custos dos riscos e danos causados por aqueles que ofertam bens e serviços[4]. E a prevenção se inicia com a avaliação da necessidade de tratamento dos dados. É essa a direção apontada pelo princípio da necessidade (art. 6º, III), o qual estabelece que o tratamento de dados deve limitar-se ao mínimo necessário para a realização de suas finalidades, abrangendo dados pertinentes e proporcionais, sem exceder ao limite da finalidade.

O GPDR, que inspirou a LGPD, traz passagens importantes nesse mesmo sentido em diversos Considerandos[5], e em destaque no artigo 5º, 1, "c", ao enunciar que os dados pessoais devem ser *adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados).* Ainda no mesmo artigo, enuncia que o responsável pelo tratamento deve cumprir os princípios e deve ser capaz de comprová-lo (responsabilidade ou *accountability*).

Ao determinar que os operadores e controladores devem usar os dados apenas na medida exata de sua necessidade e ao exigir que sejam capazes de demonstrar a adoção de medidas eficazes no cumprimento da norma, a LGPD — assim como o GDPR — condicionou o tratamento dos dados pessoais à capacidade de protegê-los. Sob o ponto de vista dos agentes de tratamento, o ganho obtido com as informações adquiridas através do uso dos dados deve ser sopesado com o custo necessário para seu tratamento seguro.

Notícias sobre grandes vazamentos de dados pessoais ocorridos no Brasil[6] deveriam acender o alerta para a gravidade das consequências que incidentes como esses podem trazer aos titulares de dados, e para as organizações.

Independentemente das circunstâncias dos incidentes citados, o que deve servir de alerta para todas as instituições que tratam dados pessoais é a possibilidade de vazamentos acontecerem, ainda que todos os cuidados necessários tenham sido tomados. Quando incidentes como esses acontecem, ainda que em proporções menores, a organização envolvida terá que demonstrar que tinha feito tudo o que estava ao seu alcance e que, mesmo assim, não foi possível evitar o evento.

Em junho de 2021, a Agência Espanhola de Proteção de Dados publicou um Guia para a gestão dos direitos e liberdades dos interessados aplicável a qualquer tratamento, independente do seu nível de risco. O documento intitulado *Gestión del Riesgo y Evaluación de Impacto en Tratamientos de Datos Personales* destaca que em qualquer nova atividade, levar a efeito uma reflexão prévia com vista a identificar problemas, bem como antecipar-se a futuras dificuldades, permite a tomada de decisões racionais e agir com maiores garantias de êxito.

A gestão de risco é obrigatória ao controlador e ao operador. Nesse processo é importante ter visibilidade sobre todas as atividades da organização que envolvam tratamento de dados pessoais, o que pode ser feito por meio do "registro das operações de tratamento de dados pessoais" (artigo 37, LGPD). A lei brasileira, tal qual o regulamento europeu que a inspirou, exige, em algumas situações, que o controlador elabore o relatório de impacto de proteção de dados, como no caso de tratamento de dados tendo como hipótese legal o legítimo interesse (artigo 10, § 3º) ou envolvendo o uso de dados sensíveis (artigo 38).

O relatório deve conter a descrição dos processos de tratamento de dados pessoais e que podem gerar riscos às liberdades civis e aos direitos fundamentais, além de medidas de segurança e formas de mitigar os riscos (artigo 5 º, XVII). No entanto, ainda que o tratamento de dados não seja feito com base no legítimo interesse ou não envolva o uso de dados sensíveis, o controlador pode utilizar a elaboração de relatórios de impacto à proteção de dados como uma ferramenta de apoio para avaliar o risco da realização de determinados tratamentos.

Tanto os registros como o relatório são importantes para avaliar e gerir os riscos envolvidos do tratamento, e também para demostrar a efetividade das medidas técnicas adotadas em busca da conformidade com a LGPD. Trata-se de uma abordagem que busca primeiramente prevenir os danos, em vez de remediá-los[7] Casos como os citados vazamentos de dados demonstram que, muito embora os cuidados tenham sido adotados, incidentes podem acontecer. E as organizações devem estar preparadas para mitigar os danos, evitando os prejuízos que podem derivar desses incidentes.

Se todo tratamento envolve risco, não faz qualquer sentido uma organização ter sob sua responsabilidade dados pessoais que não sejam realmente necessários para atingir a finalidade desejada. Na verdade, a prática de coletar o máximo de dados possíveis para depois definir seu uso está mais do que descartada pela LGPD ou GPDR, já que ambos diplomas condicionam o tratamento à existência de uma hipótese legal e prévia finalidade. No entanto, ainda que exista base legal ou finalidade determinada, é recomendável que o dado pessoal em questão seja realmente necessário para obtenção do objetivo desejado para que valha a pena dispender o esforço necessário para garantir seu tratamento seguro e a demonstração clara dessa conformidade.

A implementação de uma análise e gestão de riscos efetiva na organização, ademais, integra o próprio princípio que lhes impõe a adoção de práticas de responsabilidade proativa (*accountability)* por parte dos agentes de tratamento.

[1] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*. Cambridge,2015. p. 69.

[2] PALMEIRA, Mariana de Moraes. A segurança e as boas práticas no tratamento de dados pessoais. In: MULHOLLAND, Caitlin (Org.). *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020.

[3] BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. *civilistica.com* , v. 9, n. 3, p. 1-23, 22 dez. 2020

[4] COSTA, Luiz. Privacy and the precautionary principle. *Computer Law & Security Review,* vol. 28, 2012, 14-24.

[5] Considerandas 39, 78, 156.

[6] Cf.: "Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava". Disponível em**:** https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Acesso em: 14 fev, 2021. .

[7] COSTA, Luiz. Privacy and the precautionary principle. *Computer Law & Security Review,* vol. 28, 2012, 14-24.

Date Created
13/07/2021