A obrigação de registro das atividades de tratamento de dados

Série: Impactos operacionais e normativos da LGPD

Retomando esta coluna iniciada no que parece ser o distante ano de 2016 em termos de proteção de dados pessoais no Brasil, vamos concentrar esforços em análises teóricas e práticas com os olhos voltados para quem está com a "mão na massa" em processos de conformidade à LGPD[1]. Com isso, o objetivo desta série especial denominada "impactos operacionais e normativos da LGPD" será não só recortar os pontos mais importantes da legislação de proteção de dados pessoais no país, mas também, e em certa medida, apontar tendências das futuras disputas interpretativas em torno especialmente da principal peça do quebra-cabeça regulatório: a Lei 13.709/2019, nossa lei geral de proteção de dados pessoais.

O primeiro tema da série é a obrigação do registro das atividades de tratamento de dados[2].

O "livro contábil" dos dados

Antes de mais nada, é importante apontar que a previsão da criação de um inventário dos dados não é em si nova no Brasil. O decreto de regulamentação do Marco Civil da Internet (Decreto No 8.711/2016)[3] já obrigava provedores de conexão e aplicações a manterem certos registros das suas bases de dados, ainda que o objetivo fosse voltado à segurança da informação. Visava-se, sobretudo, a criação de uma estrutura de controle para gerenciar e auditar quem, quando e como era feito o acesso e a manipulação das bases de dados, a fim de se garantir a sua integridade.

---

[1] Em certa medida, esta série é inspirada em outra, que fez grande sucesso no ano anterior à entrada em vigência da GDPR, publicada pela International Association Privacy: Os 10 impactos operacionais da GDPR, disponível em: < https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/>

[2] Artigo 37 da LGPD: "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."

[3] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: (...) III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; (...)

A lei geral de proteção de dados extrapola essa obrigação para muito além da perspectiva da segurança da informação. Os agentes de tratamento de dados devem guardar registros de toda as suas operações de tratamento de dados pessoais. Levando-se em consideração que a definição do que é tratamento de dados engloba nada mais do que 20 (vinte) ações (*processing activities*[4]), ou seja, tudo o que é feito com dado: da coleta ao descarte. Definitivamente, é inédita a amplitude de tal obrigação de inventariança dos dados.

Por isso mesmo, poderia se pensar, em um primeiro momento, que organizações deveriam criar uma espécie de diário dos dados onde se anotaria literalmente tudo a seu respeito. No entanto, não nos parece ser esse o sentido normativo da obrigação em questão. Levando-se em consideração que a lógica por trás dessa obrigação legal é incultar nos agentes de tratamento de dados reflexão sobre um uso responsável dos dados, tal documentação deveria conter somente as informações pertinentes para tal juízo de valor. Caso contrário, quem faria tal catalogação e quem teria o poder-dever (órgãos reguladores) de requisitá-la despenderia uma energia desnecessária em meio a uma papelada infindável.

Por essa razão, o Regulamento Europeu de Proteção de Dados Pessoais (artigo 30) não só previu a obrigação de manter os registros das atividades de tratamento de dados, como, também, a calibrou. Há uma listagem das informações que deveriam compor um inventário de dados, a qual é, aliás, distinta para as figuras do controlador e processador. Destacamos o seguinte:

a. a finalidade do tratamento;
b. descrição das categorias dos dados e dos titulares;
c. o fluxo dos dados para fora da organização;
d. as medidas de segurança;
e. informações de identificação e contato do controlador;
f. os períodos para a exclusão das diferentes categorias de dados.

[4] Artigo 5º da LGPD: "Art. 5º Para os fins desta Lei, considera-se: (...) X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (...)".

Portanto, ao invés de um diário dos dados onde se registraria todos os seus movimentos, tal instrumento deveria ser mais uma espécie de "ficha corrida" com os eventos mais importantes. Abusando do didatismo e da analogia, faria as vezes de um livro contábil com a descrição do fluxo e a gestão dos dados. Como dito, o objetivo é que agentes econômicos reflitam sobre os aspectos mais importantes das suas atividades de tratamento de dados, gerando uma documentação que, ao final, permita aos órgãos reguladores "puxar a capivara"[5] dos dados.

Diante disso, repita-se, tão importante quanto a previsão da obrigação do registro das atividades de tratamento de dados é a definição de quais deveriam ser seus componentes. Na medida em que a LGPD não chegou a tal nível de detalhes, do ponto de vista prático resta:

a. aguardar futura regulamentação da Autoridade Nacional de Proteção de Dados/ANPD, a qual deveria:
    i. precisar quais são os componentes de um inventário de dados, levando-se em consideração as particularidades entre controladores e processadores que podem resultar numa documentação igualmente distinta[6];
    ii. considerar eventual exceção a tal obrigação legal, considerando-se o porte da organização e se a sua atividade de tratamento de dados seria de alto risco de acordo com as suas competências e de forma similar ao que fez o Regulamento Europeu[7];

---

5 "Puxar a capivara" é sinônimo da consulta aos antecedentes criminais de uma pessoa.

6 Artigo 55-J da LGPD: "Art. 55-J da LGPD: "Art. 55-J. Compete à ANPD: (...) XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (...) XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; (...)".

7 De acordo com o art. 30 (5) do Regulamento Europeu, estarão desobrigadas de realizar esses registros as instituições que (i) empregam menos de 250 pessoas, (ii) não realizam processamento de alto risco (iii) nem de categorias especiais de dados e antecedentes criminais, e (iv) realizam processamento ocasional. Os critérios são, portanto, cumulativos: "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

b. na ausência de regulamentação da ANPD, socorrer-se de boas práticas e exemplos de outras jurisdições, como, por exemplo, da própria GDPR enquanto um patamar mínimo do que deve conter um inventário de dados.
    1. isso caso a organização não esteja sujeita à aplicação de ambas legislações, caso em que, por consequência, considerar a GDPR seria uma questão de *compliance* em sentido *strictu sensu*;
c. considerar tal obrigação enquanto um dos pilares de qualquer programa de conformidade, atentando-se para:
    1. o auxílio preferencialmente de uma consultoria técnica, a qual pode combinar métodos e soluções tecnológicas parcialmente automatizadas para a catalogação de bases estruturadas e não estruturadas;
    2. no cenário de organizações de médio ou pequeno porte, no qual o orçamento é enxuto e tal inventariança tende a ser feita internamente, considerar que o exercício de inventariança é muito próximo ao chamado mapeamento de dados (discutiremos esse ponto em outro artigo desta coluna). Diante disso, deve-se pensar em uma metodologia pela qual se evite a duplicação de esforços.
    3. Considerar que será um exercício contínuo, uma vez que o inventário deve retratar o organismo vivo que é uma organização em termos de tratamento de dados.

A obrigação de registro das atividades de tratamento de dados é a base de qualquer programa de governança de dados. Sem essa fotografia em série é impossível compreender o fluxo da informação, esboçar o que precisa ser modificado e o que pode ser mantido para estar em conformidade com a legislação de proteção de dados. Ao mesmo tempo, contudo, a amplitude dessa obrigação legal pode e deve ser melhor calibrada pela futura Autoridade Nacional de Proteção de Dados/ANPD para fins de segurança jurídica e equilíbrio econômico-regulatório, disciplinando especialmente o que deve compor um inventário de dados e, eventualmente, quais situações não atrairiam tal ônus. Até isso acontecer, resta seguir boas práticas e lembrar do exemplo corriqueiro no campo tributário: por mais que todos os tributos estejam devidamente recolhidos, ainda

assim uma organização pode ser atuada caso não tenha sua escrituração contábil. É o mesmo racional com a LGPD.

Bruno Ricardo Bioni. Doutorando em Direito Comercial e Mestre em Direito Civil pela Faculdade de Direito da USP. trainee do *European Data Protection Board* e do Departamento de Proteção de Dados do Conselho da Europa. Fundador-professor do Data Privacy Brasil e consultor na área de direito e tecnologia com ênfase em proteção de dados pessoais (www.brunobioni.com.br)