O *PRIVACY BY DESIGN* COMO REQUISITO DOS SISTEMAS DE TRATAMENTO DE DADOS NA LGPD

Lucas Domakoski Cordeiro
Acadêmico de Direito da UFPR
Estagiário de Justen, Pereira, Oliveira e Talamini

Com orientação de ***Marina Kukiela***
Mestre em Direito Internacional Privado pela Université Panthéon-Assas
Advogada de Justen, Pereira, Oliveira e Talamini

1. Introdução

Na distopia totalitária orwelliana de *1984*, o controle, pelo Estado, dos mais diversos e sigilosos dados dos cidadãos se revelava irascível e cruel: a vigilância se encontrava por todos os lados, à espreita, e o próprio ato de manter um segredo tornava-se perigoso. Caso o indivíduo fosse incapaz de esconder profundamente seus pensamentos, inclusive de si mesmo, corria o risco de cometer um *crimepensar*, cujas consequências eram bastante claras – nas palavras de Winston Smith, protagonista do romance, *crime de pensamento não acarreta morte: crime de pensamento* ***é*** *morte*.

Na realidade, a despeito de não se ter alcançado o nível de opressão da distopia orwelliana (apesar de países como a China estarem se encaminhando nessa direção), a posse de dados e de informações sigilosas também tornou-se chave na era da revolução digital: no século XXI, os dados se transformaram em ouro, sendo cobiçados por seus potenciais quase ilimitados e ainda não completamente explorados.

Tanto por governos quanto por entidades privadas, a posse de dados dos indivíduos tornou-se questão controvertida, principalmente em vista dos numerosos escândalos envolvendo o tratamento de dados dos cidadãos em ambas as esferas, pública e privada: por um lado, os vazamentos do *Wikileaks* evidenciam o nível – antes inconcebível – de vigilância e acúmulo de dados que os atuais governos podem atingir; por outro, presenciou-se, nos últimos anos, os abusos cometidos pela *Big Tech*, como o escândalo da *Cambridge Analytica*, com a venda não-autorizada de dados de usuários pelo *Facebook* a empresas privadas, para fins político-eleitorais em vários países.

Em meio a esse cenário alarmante, e seguindo os passos da *General Data Protection Regulation* (GDPR) europeia, o Brasil se colocou na vanguarda da proteção das liberdades individuais ao aprovar a Lei Geral de Proteção de Dados (LGPD), enraizada fortemente no respeito à privacidade e à autodeterminação informativa. Dessa forma, busca se garantir ao indivíduo o controle do uso de seus dados.

No entanto, para que o governo e as entidades privadas se adequem a essa nova realidade, há um longo caminho pela frente até que as prescrições

trazidas pela Lei e as proteções que ela confere aos dados pessoais sejam de fato implementadas. Dessa forma, pretende-se analisar os requisitos para que a Lei se converta em proteção efetiva aos cidadãos, usuários e operadores dos sistemas de tratamento de dados.

2. Requisitos dos sistemas

O art. 49 da LGPD determina que "*os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares*".

O principal dever a ser observado quando da elaboração de sistemas de tratamento de dados, portanto, deve ser a segurança, ou seja, a preservação da privacidade dos dados, em consonância com o espírito geral da lei, que se constrói em torno da noção de proteção dos dados dos cidadãos.

Pode-se afirmar, portanto, que está imbuída na lei a noção de *privacy by design*, conceito criado por Ann Cavoukian, expert canadense em privacidade e *big data*. Este conceito estabelece que a privacidade deve ser levada em consideração *ao longo* do processo de engenharia de um sistema, não após a sua criação. Dessa forma, a privacidade deve ser elemento essencial e presente na própria concepção dos sistemas de tratamento de dados, devendo a sua construção se dar em torno dessa proteção.

Essa noção tornou-se basilar para os novos códigos legais de proteção à privacidade e para os sistemas de tratamento de dados, sendo amplamente aplicada, inclusive, pelas prescrições da GDPR europeia.

O *privacy by design* se baseia em sete princípios. O primeiro é o da proatividade, segundo o qual os sistemas têm que ser desenvolvidos prevendo a possibilidade de violações de privacidade antes que essas violações aconteçam, numa postura proativa e preventiva. Nesse sentido, busca-se evitar uma postura reativa, que seria aquela derivada da ausência de prevenção adequada aos problemas, surgida apenas após o aparecimento de violações.

O segundo princípio é o da privacidade como padrão. Pressupõe que os sistemas de tratamento de dados sejam construídos e planejados tendo, como padrão, os standards máximos de privacidade, de forma que o indivíduo não precise ativar, por si mesmo, configurações mais protetivas no sistema.

O terceiro princípio, da privacidade incorporada ao design, implica no desenvolvimento do sistema já tendo em mente a privacidade como característica primordial, não sendo um mero acréscimo posterior. A construção do sistema de tratamento de dados deve ser, aqui, holística, de forma a conciliar a usabilidade do sistema com a privacidade basilar do design.

O quarto princípio deriva do terceiro: funcionalidade total, de forma que o usuário não precise optar entre usabilidade e privacidade – ambos devem estar integrados de forma sinérgica na plataforma.

O quinto princípio, por sua vez, trata da segurança de ponta-a-ponta, significando que a informação ou o dado tratado no sistema deve estar seguro e protegido ao longo de todo o processo, desde sua entrada, passando pelo seu tratamento e encerrando com sua destruição ao cabo do procedimento.

A transparência é o sexto princípio, pois o sistema deve permitir que o usuário saiba como a informação é processada, de forma clara e verificável. Dessa forma, evita-se a obscuridade de sistemas herméticos, que os indivíduos não consigam compreender – os dados devem ser tratados de forma clara, transparente e disponível.

Por fim, o sétimo princípio é o respeito à privacidade do usuário: o sistema de tratamento de dados deve ser todo voltado a este princípio, de forma a tornar central a preocupação com a privacidade do indivíduo.

A observação desses princípios na elaboração de sistemas de dados permitirá um tratamento transparente e seguro, visto que a LGPD servirá para frear o uso incorreto e irresponsável de informações pessoais, tendo a segurança do indivíduo como seu ponto focal.

3. Boas práticas e governança

Para operacionalizar as prescrições da Lei e projetar/operar os sistemas de tratamento de dados de acordo com o *privacy by design*, se faz necessário garantir que haja engajamento e sinergia entre todos os setores envolvidos com os sistemas – público e privado.

É nesse sentido, inclusive, que o art. 50 da LGPD prevê que "*os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais"*.

O necessário foco na proteção da privacidade do usuário também fica claro no § 1º do art. 50, que estabelece que o operador e o controlador dos sistemas precisam levar em consideração todos os riscos e benefícios que podem decorrer do tratamento de dados, de forma a preservar o usuário.

Dessa forma, os processos de governança corporativa devem sofrer alterações profundas, que passam pela implementação de métodos de *compliance* digitais e mais modernos. Há também necessidade de uma mudança de cultura, para que os encarregados da proteção dos dados tenham

meios técnicos e intelectuais aptos a garantir a substituição de velhas práticas e a adequada proteção dos dados dos cidadãos.[1]

4. A *Internet das Coisas* (*IoT*) e os sistemas de tratamento de dados

Internet das Coisas (*IoT*) é o conceito segundo o qual todos os aparelhos (domésticos ou não) em um ambiente podem estar conectados não apenas entre si, mas também à Internet. Dessa forma, todos os *gadgets*, eletrodomésticos e eletroeletrônicos em um mesmo recinto poderiam trabalhar em sinergia, trazendo definitivamente o mundo digital ao mundo físico e facilitando as tarefas do dia-a-dia.

No entanto, o maior problema da *Internet das Coisas,* no que tange à proteção de dados, é que cada dispositivo inteligente que se conecta à internet tende a coletar padrões de comportamento e perfis de usuário, e pode acabar enviando dados sigilosos para a rede ou para os bancos de dados de governos e companhias. Sendo assim, se faz necessário adaptar, também, estas tecnologias às prescrições da LGPD.

Nesse sentido, podem ser adotadas medidas de Segurança da Informação[2] para implementar as demandas da LGPD, através, por exemplo, do mapeamento de todos os processos desenvolvidos com o uso de IoT. As etapas de coleta, transmissão e armazenamento de dados de cada dispositivo passam, portanto, a sofrer um nível maior de controle pelo usuário, que terá visão da totalidade dos processos.

Dessa forma, possibilita-se a análise e classificação das vulnerabilidades de cada processo e permite-se a sua reformulação, tendo a segurança como ponto focal da interconexão dos aparelhos e dos processos nos quais eles são utilizados.

5. Conclusão

A LGPD surgiu, justificadamente, após os diversos escândalos de mau uso de dados pelo mundo, tanto por parte de governos quanto por parte de entidades privadas. Nasceu em bom momento, fruto de positivos debates em prol do cidadão, como comprovam as exigências para os sistemas de tratamento de dados: se colocados em prática, estes requisitos tornarão o tráfego de dados muito mais transparente e acessível, colocando o poder de escolha, ao cabo, novamente nas mãos do indivíduo.

Informação bibliográfica do texto:

---

[1] PINHEIRO, Patricia Peck. *Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)*. São Paulo: Saraiva, 2019, p. 43.

[2] OLIVEIRA, Nairobi Spiecker de. *Segurança da informação para internet das coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD)*. In: Revista Eletrônica de Iniciação Científica em Computação, v.17, nº 4, 2019, p. 8.

CORDEIRO, Lucas Domakoski; KUKIELA, Marina. O *privacy by design* como requisito dos sistemas de tratamento de dados na LGPD. Informativo Justen, Pereira, Oliveira e Talamini, Curitiba, nº 163, setembro de 2020, disponível em **http://www.justen.com.br**, acesso em [data].