Panorama da LGPD - Lei Geral de Proteção de Dados

Leonardo J. C. May[1], Luiz F. de Sá Joaquim[1], Tiago B. Boeing[1]

[1]Universidade do Sul de Santa Catarina, Tubarão, Brasil

leojcmay@gmail.com, luiz.sa.joaquim@gmail.com, contato@tiagoboeing.com

Abstract. *This meta-article analyzes the terms of the General Data Protection Law (LGPD), inspired by European data protection law (GDPR). They will be analyzed the implications and recommendations for companies that deal with personal data, mostly applicable to IT companies. The law has several features, the principle of confidentiality being one of the central points, which ensures that an individual is not identified in the middle of a mass of data through specific data, such as name, CPF, telephone, and others.*

Resumo. *Este meta-artigo faz uma análise sobre os termos da Lei Geral de Proteção de Dados (LGPD), inspirada na legislação de proteção de dados Europeia (GDPR). Serão analisadas as implicações e recomendações para empresas que lidam com dados sensíveis, aplicável em sua maioria às de tecnologia da informação. A lei possui diversas características, sendo o princípio da confidencialidade um dos pontos centrais, que visa garantir que um indivíduo não possa ser identificado em meio a uma massa de dados através de dados sensíveis, como como nome, CPF, telefone e outros.*

1. Introdução

A Lei Geral de Proteção de Dados (LGPD) tem como motivação os movimentos para criação de uma lei que garanta direitos aos cidadãos e deveres às empresas que lidam com estes dados na Europa, onde foi instituída como GDPR (General Data Protection Regulation). Na legislação brasileira, a LGPD está inscrita sob a lei nº 13.709 e foi aprovada pela Câmara em agosto de 2018. Em dezembro de 2018 o atual presidente Michel Temer editou a Medida Provisória nº 869, de 27 de dezembro de 2018 alterando o início da vigência da lei para agosto de 2020 <https://g1.globo.com/politica/noticia/2018/08/14/temer-sanciona-lei-de-protecao-de-dados-pessoais.ghtml>.

A criação de uma lei específica para proteção dos dados pessoais se fez necessária no Brasil pois embora existem leis que garantem o direito à intimidade e ao sigilo, as mesmas não contemplavam o cenário tecnológico atual. A LGPD preenche esta lacuna através de termos específicos aos dados no geral e como deve ser realizado o tratamento.

Um ponto importante da LGPD é que independente de onde for a sede e o centro de dados da empresa, sempre que houver processamento de dados de brasileiro ou estrangeiros em território nacional a legislação deverá ser cumprida. Outra determinação

é que é permitido compartilhar dados com organismos internacionais e com outros países, desde que isso ocorra à partir de protocolos seguros e/ou para cumprir exigências legais.

Embora os protocolos seguros não sejam especificados, um dos exemplos reais seria: uma empresa brasileira possui servidores em São Paulo, mas que operam replicação dos dados para outros servidores ao redor do mundo (este é o funcionamento de uma CDN - Content Delivery Network). Embora normalmente a comunicação ocorra internamente na infraestrutura, a exemplo de existir uma comunicação externa, a mesma deve utilizar protocolos como HTTPS ou SSH, que fornecem criptografia dos dados trafegados.

2. Contextualização

Um dos motivadores para a criação da lei foi a General Data Protection Regulation, GDPR (Regulamentação Geral de Proteção de Dados), a lei de proteção de dados da Europa, que foi considerada o maior avanço no direito à privacidade de dados dos últimos anos. A lei brasileira acaba utilizando diversos critérios estabelecidos pela legislação europeia, mas também é importante lembrar que algo similar já havia sido iniciado com a criação do Marco Civil da Internet em 2014.

A LGPD se baseia em princípios e regras de segurança da informação a qual o objetivo é a privacidade e garantia dos direitos dos cidadãos, estabelecendo regras relacionadas às operações e posse dos dados. Seja para entidades públicas ou privadas.

3. Desenvolvimento

3.1. Características

São vários termos que compõem a lei, cada um deles lida com diferentes responsabilidades conforme ilustração abaixo:

A LGPD em um giro [SERPRO]

3.1.1. Consentimento

Um dos pontos chaves da LGPD é a necessidade de consentimento do cidadão, isto é a base para tratamento dos dados pessoais. Existem exceções onde é possível tratar dados sem a necessidade de consentimento, como quando é indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa e outros <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>.

O consentimento pode ser obtido através de contratos, sejam eles físicos ou assinados digitalmente por termos de aceite. Estes termos devem conter detalhes sobre o procedimento de revogação do consentimento, que é outra característica da lei onde o usuário pode a qualquer momento revogar o direito a utilização de seus dados. Obviamente isto é aplicável nos cenários em que o consentimento se faz necessário, não às exceções para garantias legais.

3.1.2. Automatização com autorização

O cidadão pode solicitar que dados sejam deletados, revogar um consentimento, transferir dados para outro fornecedor de serviços, entre outras ações. E o tratamento

dos dados deve ser feito levando em conta alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão. O indivíduo deve ser informado que pode intervir, pedindo revisão deste procedimento feito por máquinas <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>.

3.1.3. ANPD e agentes de tratamento

O país contará com a Autoridade Nacional de Proteção de Dados Pessoais, a ANPD. A instituição vai fiscalizar e, se a LGPD for descumprida, penalizar. Além disso, a ANPD terá, é claro, as tarefas de regular e de orientar, preventivamente, sobre como aplicar a lei. Cidadãos e organizações poderão colaborar com a autoridade <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>.

3.1.4. Gestão em foco

A gestão em foco se resume a gerir riscos e falhas. Significa que quem gere base de dados pessoais terá que criar normas de governança; adotar medidas preventivas de segurança; replicar boas práticas e certificações existentes no mercado. Terá ainda que elaborar planos de contingência; fazer auditorias e resolver incidentes com agilidade. Se ocorrer, por exemplo, um vazamento de dados, a ANPD e os indivíduos afetados devem ser imediatamente avisados.

3.2. Termos da lei

3.2.1. Dados pessoais

Qualquer informação que permita identificar um indivíduo, ou seja, qualquer dado com o qual seja possível encontrá-lo em meio à uma “massa de dados”, como nome, RG, CPF, número de telefone e outros.

3.2.2. Dados sensíveis

Aqueles que dizem respeito aos valores e convicções de cada um, como orientação sexual, etnia, opinião política, convicção religiosa, crenças filosóficas e informações de saúde. Todas essas informações podem originar discriminação e preconceito, por isso, são consideradas sensíveis.

3.2.3. Tratamento de dados

Os dados podem ser usados de várias maneiras. É possível apenas armazená-los na coleta, mas podem ser compartilhados, classificados, acessados, reproduzidos, avaliados, processados e transformados em novos dados a partir dos antigos. Qualquer operação que envolva esses dados é considerada um tratamento.

3.2.4. Titular dos dados

O titular dos dados nada mais é do que a pessoa física dona das informações coletadas.

3.2.5. Anonimização e pseudo anônimos

A pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

3.2.6. Controlador e processador

O controlador é a pessoa ou empresa que se responsabiliza e decide o que será feito com as informações coletadas de um consumidor, enquanto o processador é quem faz o tratamento dos dados.

3.3. Impactos na área de TI

A LGPD lida principalmente com o armazenamento, tratamento e segurança de dados de usuários. As exigências de tratamento e segurança de informações pessoais vão se tornar mais rígidas, sendo uma forma de garantir a confiabilidade das empresas, elevando a segurança dos usuários, estabelecendo critérios e regras para isso. As empresas de TI terão de aumentar o investimento em segurança e também deverão ter maior atenção ao modo como as informações e dados serão armazenados, elas terão que atuar como líderes dessa transformação, auxiliando os seus clientes a ficarem em acordo com a nova lei.

Outro princípio importante é a necessidade de transparência que a lei estabelece. As empresas devem ter formas de demonstrar como os dados são coletados, manipulados, armazenados e protegidos para eventuais auditorias externas que buscam garantir o cumprimento da lei. Nesse sentido é importante que as empresas renovem os contratos com clientes e parceiros buscando inserir essas novas regras da LGPD nos termos. Contratos e acordo de uso desatualizados poderão gerar consequências legais bastante severas para as operadoras de dados.

4. **Estudo de caso**

ICO fines British Airways £20m for data breach affecting more than 400,000 customers [ico.]

Tradução: A ICO multa a British Airways £ 20 milhões por violação de dados que afeta mais de 400.000 clientes

O fato ocorreu em setembro de 2018, uma falha de segurança no site da British Airways resultou no vazamento de dados pessoais e financeiros de 400 mil clientes. A empresa foi multada em 20 milhões de libras esterlinas, ou aproximadamente R$ 145 milhões, pelo Information Commissioner's Office (ICO), órgão do Reino Unido que trata da privacidade dos usuários. O incidente, em parte, envolveu o tráfego de usuários do site da British Airways sendo desviado para uma outra página fraudulenta. Acredita-se que o servidor falso tenha iniciado a coleta dos dados em junho de 2018, três meses antes de o caso vir a público <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/>.

Ainda segundo o ICO, uma série de informações foram comprometidas pela falta de medidas de segurança da empresa, incluindo login, cartões de pagamentos e detalhes das reservas de viagens, além de informações tais como nomes e endereços.

Com o vazamento, a British Airways infringiu o Regulamento Geral sobre a Proteção de Dados (GDPR), que protege os dados dos cidadãos da União Europeia. "Os dados pessoais das pessoas são apenas isso: pessoais. Quando uma organização falha em protegê-los contra perda, dano ou roubo, isso é mais do que uma inconveniência. Por isso que a lei é clara: quando você recebe dados pessoais, precisa cuidar deles", diz a comissária de informação, Elizabeth Denham <https://tecnoblog.net/297840/british-airways-multa-recorde-vazamento-dados/>.

Segundo o Information Commissioner's Office (ICO), órgão do Reino Unido que trata da privacidade dos usuários, poderia ter sido evitada se houvesse melhor gerenciamento dos sistemas de proteção contra ciberataques. Dados de consumidores

são ativos valiosos sob custódia das empresas, e devem ser protegidos com constante atenção e investimento, definiu o ICO, em sua conclusão.

O relatório completo pode ser lido no site oficial da ICO em <https://ico.org.uk/action-weve-taken/enforcement/british-airways/>.

5. **Conclusão**

A LGPD traz um novo panorama para a forma com que empresas coletam, manipulam, armazenam e garantem as seguranças dos dados dos indivíduos, sendo uma lei voltada a proteger os direitos civis na internet. A mesma visa garantir que entidades, sejam públicas ou privadas, se adequem e priorizem a segurança em suas operações digitais, além de instituir penalização caso os termos sejam violados, garantindo o direito à privacidade do cidadão e ressarcimento dos danos causados devido a vazamentos.

Durante a produção deste artigo novas penalidades foram aplicadas pela ICO, como à Marriott International Inc em 30 de outubro de 2020. A empresa foi multada em £18.4 M, pelo vazamento de 339 milhões de registros de hóspedes em todo o mundo, após um ataque cibernético em 2014. O ataque permaneceu sem ser identificado até setembro de 2018.
<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/>

Em contrapartida, é importante analisar outro ponto de vista. O SERPRO, empresa pública de tecnologia e responsável por acompanhar os procedimentos relacionados à LGPD em 2018 foi alvo de investigações relacionadas à venda de dados pessoais de brasileiros <https://tecnoblog.net/247511/serpro-nega-venda-dados>, situações como estas trazem à tona questionamentos relacionadas ao gerenciamento dos dados com responsabilidade e gestões de boa índole nestas organizações. Os dados pessoais a adequação, boa índole e cuidado com os dados pessoais deve se estender também a entidades governamentais e não se limitar apenas às empresas privadas de tecnologia, sendo uma enorme fração de dados sensíveis se encontram em mãos de órgãos públicos.

6. **Referências**

Higa, P., João and Johndoe1981 (8 jul 2019). British Airways recebe multa recorde de R$ 900 milhões por vazar dados: Legislação. https://tecnoblog.net/297840/british-airways-multa-recorde-vazamento-dados/.

ICO fines British Airways £20m for data breach affecting more than 400,000 customers ([S.d.]). https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fine

s-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

Lunden, I. (8 jul 2019). UK's ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users. https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/.

Mendes, J. ([S.d.]). Vazamento de dados de clientes leva empresa aérea a pagar multa milionária. https://www.correiobraziliense.com.br/app/noticia/economia/2019/07/09/internas_economia,769255/vazamento-de-dados-de-clientes-leva-empresa-aerea-a-pagar-multa.shtml.

Serpro - Serviço Federal de Processamento de Dados ([S.d.]). O que muda com a LGPD. https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd.

Alecrim, E., Mt-09, Y., Spaki, E., et al. (15 jun 2018). Serpro reafirma que não vende dados pessoais de brasileiros: Antivírus e Segurança. https://tecnoblog.net/247511/serpro-nega-venda-dados/.

Temer sanciona com vetos lei de proteção de dados pessoais ([S.d.]). https://g1.globo.com/politica/noticia/2018/08/14/temer-sanciona-lei-de-protecao-de-dados-pessoais.ghtml.

ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure ([S.d.]). https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/.