JOURNAL
AKEDIA
Versões, Negligências e Outros Mundos

IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO BRASIL: CONSIDERAÇÕES TECNOLÓGICAS

English title: *IMPLEMENTATION OF THE GENERAL DATA PROTECTION LAW (LGPD) IN BRAZIL: TECHNOLOGICAL CONSIDERATIONS*

10.33726/akdpapers2447-7656v11a72021p168-190

SANTOS, Juliano Gouveia dos[1]
ALMEIDA, Lohan Alves[2]
SOARES, Hélio Rubens[3]

RESUMO: Este artigo descreve as definições da atual Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei que lhe serviu de inspiração, a *General Data Protection Regulation* (GDPR). O objetivo do texto é o de demonstrar a relevância desses aparatos legislativos para a vida dos cidadãos numa atualidade, em que tudo gira em torno de informações digitais. Metodologicamente faz-se uma revisão da literatura sobre o tema, presente em acervos físicos e digitais, combinada com um estudo de caso. Como resultados do estudo, vimos que algumas considerações tecnológicas acerca da implementação de sistemas e sua adequação à nova Lei, exemplificam as formas de aplicação efetiva da segurança de dados pessoais.

PALAVRAS-CHAVE: Ciência da Computação, LGPD, Segurança de Dados

ABSTRACT: This article specifies the definition of the current General Law on Protection of Personal Data (LGPD) and the Law that served as inspiration, a General Regulation on Data Protection (GDPR). The purpose of the text is to demonstrate the relevance of these legislative devices to the lives of citizens today, when everything revolves around digital information. Methodologically, a literature review on the topic, present in physical and digital collections, is combined with a case study. As a result of the study, we saw that some technological considerations about the implementation of systems and their adequacy to the new Law, exemplify the ways of effectively applying the security of personal data.

KEYWORDS: Computer Science, LGPD, Data Security

[1] Estudantes de Ciência da Computação, no Centro Universitário do Triângulo – Uberlândia / MG. Contato: julianogouveia93@gmail.com.
[2] Estudantes de Ciência da Computação, no Centro Universitário do Triângulo – Uberlândia / MG. Contato: lohanalves@hotmail.com.
[3] Mestre em Ciência da Computação pela Universidade Estadual de Campinas (UNICAMP). Docente no Centro Universitário do Triângulo – Uberlândia / MG. Contato: helio.soares@asoec.com.br.

INTRODUÇÃO

Na Era da Informação, caracterizada pelo fluxo crescente de dados, se destaca a preocupação com a segurança e a integridade das pessoas que usufruem desse meio. Como consequência do desenvolvimento tecnológico, a tecnologia passa a ser utilizada com mais frequência, sobretudo na prática de crimes cibernéticos, como fraudes e acesso não autorizado a dados sigilosos (Figura 1).

Neste sentido, convém dizer, que os tipos mais comuns de crimes virtuais são: roubo e fraude de identidade; roubo de dados financeiros e dados corporativos; espionagem cibernética; jogos ilegais de azar; venda de itens ilegais *on-line*; e, produção ou posse de pornografia infantil:

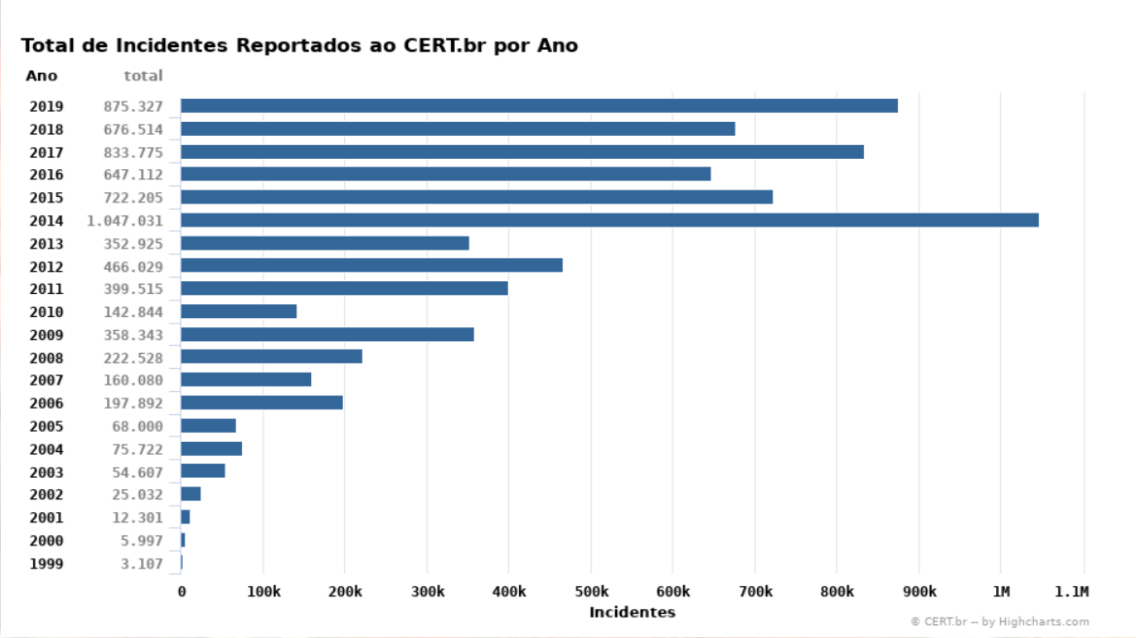

Figura 1. Gráfico de incidentes de crimes cibernéticos por ano

Diante disso, o presente artigo discorre sobre conceitos de segurança, com foco nos crimes cibernéticos, e particularmente aqueles que envolvem os dados de identidade. Serão, assim, elucidados conceitos sobre a nova Lei Geral de Proteção de Dados Pessoais – LGPD – Lei n. 13.709, de 14 de agosto de 2018 (BRASIL, 2018a) – e o seu funcionamento, além do processo de implementação de *softwares* (programas) de segurança em uma empresa.

Em vários âmbitos se destaca a segurança dos dados pessoais, devido à facilidade na sua obtenção por parte das empresas. A maioria dos estabelecimentos, como hotéis, lojas, farmácias e *sites* de vendas *on-line*, requerem informações básicas para cadastro que, por seu turno, possui diversos propósitos, como a divulgação de promoções e descontos, a obtenção de *feedback*, as pesquisas de mercado para saber o nicho de cada usuário e lançar produtos voltados para determinados grupos de pessoas, entre outros.

Nesse âmbito, crimes como invasão de privacidade, roubo e fraude de identidade, extorsão por meio de dados sensíveis e compartilhamento de informações pessoais entre empresas, são os que favorecem e ou até interferem no funcionamento do livre mercado (HINTZBERGEN, 2018).

Para evitar crimes cibernéticos, a União Europeia – UE (2016) lançou o *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados, GDPR). Essa regulamentação indica maneiras corretas sobre o tratamento de informações, para não causar danos aos usuários. Inspirado pela UE, o Brasil criou a "Lei Geral de Proteção de Dados Pessoais" – LGPD (BRASIL, 2018a; BLUM, 2019).

Nesse contexto, o presente artigo investiga as bases teóricas da Lei supracitada e as formas de construção de sistemas que visam se adequar a tais conformidades. Na seção 02, serão mostrados os fundamentos da LGPD (BRASIL, 2018a) e do GDPR (UNIÃO EUROPEIA, 2016); na seção 03, as motivações para esse assunto e as possíveis vantagens e desvantagens acerca do tema; na seção 04, um estudo de caso sobre uma empresa fictícia, com foco em sistemas e ferramentas a serem utilizados para adequação à Lei; e, na seção 05, há a Conclusão versando sobre o assunto investigado.

2. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A LGPD – Lei n. 13.709, de 14 de agosto de 2018 (Brasil 2018a) – altera a "Lei do Marco Civil da Internet" – Lei n. 12.965, de 23 de abril de 2014 (BRASIL, 2014). Entre as mudanças, consta a criação da Autoridade Nacional de Proteção de Dados – ANPD, por meio da "Medida Provisória n. 869", de 27 de setembro de 2018 (Brasil 2018b); da "Lei n. 13.853, de 08 de julho de 2019"

(BRASIL, 2019a); e do “Veto n. 24, de 02 de outubro de 2019” (BRASIL, 2019b).

Prevista para entrar em vigor em outubro de 2019, ou seja, transcorridos 18 meses a partir da publicação, a LGPD (Brasil 2018a) foi impedida de tal ação devido à “Lei n. 13.853, de 08 de julho de 2019” (BRASIL, 2019a), que altera a data para 24 meses após a publicação da Lei original, que seria em abril de 2020, com vistas a proporcionar um prazo maior para a adequação das empresas. Contudo, em detrimento dos acontecimentos mundiais relativos à pandemia causada pelo Novo Coronavírus (COVID-19), houve mais um adiamento, com ratificação em 18 de agosto de 2020, data marcada como o início para a referida Lei.

Com o crescimento do mundo digital, dos comércios *on-line* e do fluxo de informações, constatou-se a necessidade de criarem-se medidas protetoras para assegurar a integridade das pessoas. Nos dias atuais, os que possuem maior quantidade de dados detêm um poder econômico mais elevado que os outros, o que ilustra a base do funcionamento da economia atual (MORELLI, 2020).

A LGPD (BRASIL, 2018a) foi criada com o intuito de resguardar os direitos fundamentais do cidadão que tem os dados coletados em todo o território brasileiro, para respeitar os direitos humanos no que tange à integridade, à privacidade, ao direito de imagem e à dignidade. Tal aparato legislativo visa proteger todas as informações, independentemente da forma como foram coletadas, seja por documento impresso ou formulários eletrônicos (DONDA, 2020).

Além de manter os dados protegidos, a LGPD (BRASIL, 2018a) se alinha aos objetivos da economia brasileira, ao evitar crimes virtuais e fraudes, além de estimular o livre-comércio e o desenvolvimento econômico e tecnológico (PINHEIRO, 2020). Ela é aplicável a qualquer pessoa, seja de natureza física ou jurídica, pública ou privada, com a possibilidade de ser não apenas um indivíduo, como também um grupo. Também é aplicável às duas partes, tanto àquele que oferece informações, quanto aos que as coletam de fato. No caso do indivíduo que dispõe seus dados pessoais, ao entregá-los, deve estar de acordo com os termos propostos pela outra parte que, por sua

vez, precisa se comprometer a guardar todos os dados daquela pessoa. Caso ocorra alguma alteração nos termos, é preciso avisar o cliente para ele ceder novamente seus dados (MALDONADO, 2019).

Nesse entremeio, a LGPD (BRASIL, 2018a) não é aplicável quando os dados forem usados exclusivamente para fins jornalísticos, artísticos ou acadêmicos; se aplicarem à segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais; e empregados na área da saúde, uma vez que, em alguns casos, faz-se necessário o compartilhamento de informações entre diferentes centros de atendimento, para garantir a vida do indivíduo (MALDONADO, 2019).

Em relação à territorialidade, a LGPD (BRASIL, 2018a) é aplicável em qualquer parte do país, além de ser permitida a coleta de dados por empresas de outros países. Sendo assim, tais organizações precisam estar de acordo com a Lei supra, para poder manipular as informações – isso poderá funcionar de maneira efetiva quando os dados forem enviados ao território brasileiro (LGPD, BRASIL, 2018). Para operacionalizar o sistema, existem três tipos de dados que podem ser coletados:

- Pessoais: dados sólidos, pelos quais é possível descobrir a identidade a quem pertencem tais informações, como o número do Cadastro de Pessoa Física (CPF), o Registro Geral (RG), a Carteira Nacional de Habilitação (CNH), e o nome do indivíduo, idade etc.;
- Pessoais sensíveis: de forma isolada, não permitem a identificação do sujeito, mas apresentam conteúdo expositivo que, caso seja divulgado, pode levar a situações de racismo, homofobia e outros crimes de ódio e falsificação. Por isso, é imprescindível a manipulação correta de informações como orientação sexual e religiosa, opinião política, filiação a algum grupo, origem étnica, dados genéticos e biométricos, entre outros; e,
- Anonimizados: informações que, de acordo com os meios técnicos e a manipulação correta, não permitem descobrir a identidade da pessoa, a exemplo da coleta de dados em investigações por meio de denúncias anônimas (POHLMANN, 2020).

Torna-se necessário ressaltar nomenclaturas como “titular”, “controlador”, “operador”, “encarregado” e “tratamento” (PINHEIRO, 2020). O primeiro se refere ao proprietário dos dados; o segundo é responsável por criar os termos de consentimento e por atuar em alguma ocorrência com as informações do titular – os profissionais dessa área documentam os dados

pessoais do cliente e garantem o cumprimento de todos os itens delimitados nos termos de uso (RAPÔSO *et al*. 2019); o terceiro manipula tais informações e garante o tratamento correto; já o encarregado associa controlador e titular, além de zelar pela integridade da empresa e fidelidade por meio da Lei e encaminhar as mudanças aos demais, se não houver algo em conformidade ao processo; e o tratamento se refere à manipulação dos dados, que envolve a operação de coleta e a movimentação das informações do cliente.

No tocante à manipulação de dados, há uma diferenciação no tratamento, de acordo com a faixa etária. Quando se é criança ou adolescente, os responsáveis legais fornecem as informações; já no caso dos adultos, a pessoa se responsabiliza pelos próprios dados; e em relação ao idoso, podem ocorrer ambas as situações – pode ser responsável por ele mesmo ou, caso alguma doença o impossibilite de tomar decisões, a responsabilidade recai ao cuidador (POHLMANN, 2020).

Diante disso, o usuário final tem o completo controle sobre todos os aspectos relativos a ele. Assim, pode solicitar a retirada das informações dos bancos de dados da companhia e alterações nos termos, caso seja favorável. Essa empresa, caso ocorra qualquer problema com os dados coletados, tem até 72 horas para comunicar ao cliente a situação e, transcorrido esse tempo, ficará passível da aplicação de multas (DONDA, 2020).

O descumprimento da Lei resultará em penalidades, a depender do grau da infração, desde uma simples advertência até a aplicação de multas com valores elevados, que podem chegar a 2% do faturamento total da empresa, grupo ou conglomerado brasileiro no seu último exercício, podendo custar até R$ 50.000.000,00 (cinquenta milhões de reais) (DONDA, 2020).

2.1 *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados, GDPR)

O GDPR consta na “Lei n. 679, de 27 de abril de 2016” (UNIÃO EUROPEIA, 2016), mas entrou em vigor a 25 de maio de 2018 em toda a UE. Ela tem como objetivo dar mais privacidade e segurança aos dados de todos os cidadãos europeus (BLUM, 2019).

Essa regulamentação se direciona às pessoas que disponibilizam os próprios dados na Internet, ou seja, para protegerem os cidadãos contra qualquer tipo de crime que pode ocorrer com tais informações que, nesse caso, precisam do consentimento da pessoa para serem coletadas. A transparência é primordial, uma vez que o usuário precisa saber exatamente como os dados são manipulados/compartilhados, além de ter o direito ao esquecimento/apagamento das informações do sistema, algo obrigatório para as empresas da área (POHLMANN, 2020).

Juntamente ao GDPR (UNIÃO EUROPEIA, 2016), foi criado o cargo público de *Data Protection Officer* (Oficial de Proteção de Dados, DPO), responsável por fiscalizar e controlar as organizações quanto à manipulação dos dados das pessoas. No que concerne ao descumprimento da Lei, as companhias podem sofrer sanções que podem ser de 4% do faturamento anual ou de € 20.000.000,00 (vinte milhões de Euros) (POHLMANN, 2020).

Essa Lei é válida para todos os serviços *on-line* que processam dados de pessoas europeias, mesmo se não estiverem sediados na Europa. Por isso, as empresas estrangeiras devem estar de acordo com tal legislação, se pretenderem fazer negócios com algum cidadão daquele continente (BLUM, 2019).

2.2 Exemplos de aplicação do GDPR e da LGPD

Apesar de as leis possuírem diferenças quanto ao tratamento, o funcionamento delas é similar. Nesta seção, serão apresentados dois exemplos de adoção de tais legislações na prática e, na seção subsequente, haverá as diferenças entre elas.

Em um primeiro contato, quando são disponibilizados formulários para cadastro é preciso informar, claramente aos usuários, quais dados são solicitados, o que será feito com eles, onde irão passar e como serão armazenados, mesmo que as informações, por vezes, sejam autoexplicativas. Podem ser utilizados em uma campanha ou repassados a uma empresa parceira e, independentemente disso, a finalidade deve ser documentada e comunicada ao cliente.

Quando uma cláusula é alterada no termo, um novo documento deve ser enviado para o cliente ter ciência e decidir se irá (ou não) aceitá-lo novamente, uma vez que possui direitos sobre todas as suas informações. Caso o titular não queira participar dos termos, a empresa, obrigatoriamente, deve apagar todas as informações dele constantes nos bancos de dados.

2.3 Diferenças entre a LGPD e o GDPR

Existem outros países com leis voltadas ao uso da Internet e afins, a exemplo dos Estados Unidos, com foco na proteção dos dados. Já, a inspiração da LGPD (BRASIL, 2018a) pelo GDPR (UNIÃO EUROPEIA, 2016), em detrimento das outras, se deu pelo fato de tratar o usuário e o que lhe pertence em ambiente *on-line*, com vistas à segurança da informação e à integridade desse indivíduo. Apesar da semelhança, há algumas particularidades a serem abordadas.

A primeira diferença é que, no Brasil não existiam leis para proteger os dados das pessoas no meio virtual, em contraposição à Europa. Com a criação da LGPD (BRASIL, 2018a), o país iniciou uma cultura que já estava em curso naquele continente (BLUM, 2020).

Outra diferença diz respeito à segurança dos dados. Enquanto que, na Europa, a Lei especifica itens de segurança, tais como o uso de criptografia, aqui não existe tal descrição. No Brasil, foi criada a Agência Nacional de Proteção de Dados (ANPD), responsável unicamente por supervisionar a segurança dos dados nas empresas, contudo, não há um órgão específico para a fiscalização em solo europeu (PINHEIRO, 2020).

Quanto ao *marketing* direto, que compreende o tratamento de dados pessoais para fins de criação de perfis e da mercadologia, a Lei europeia tem definições específicas, com requisitos e etapas a serem seguidos e que permitem aos titulares se opor em qualquer momento. Como a Lei brasileira não aborda o assunto de forma direta pode-se gerar problemas de autorização implícita – nesse contexto, são citadas apenas as regras gerais aplicáveis de objeção, segurança e consentimento dos titulares dos dados pessoais (OLIVEIRA, 2020).

No que tange aos dados sensíveis, o Brasil confere proteção especial no "Artigo 5º, inciso II", em que podem ser tratados apenas nas hipóteses previstas em Lei (BRASIL, 2018a). Há duas exceções no consentimento do titular em relação a esse tipo de informação: se houver a necessidade de se investigar algum crime e quando há riscos à saúde. Já, na Europa, é proibida a manipulação dos dados sensíveis por qualquer empresa, com apenas três tipos de exceções referentes à saúde, aos dados biométricos e aos genéticos, respectivamente (PINHEIRO, 2020).

Existe uma discrepância também na relação entre controlador e operador. Enquanto que, na LGPD (BRASIL, 2018a), o primeiro deve instruir o segundo sobre o tratamento dos dados, podendo ser de modo informal, quase totalmente técnico, no GDPR (UNIÃO EUROPEIA, 2016), o controlador deve formalizar essa instrução para o operador em um contrato ou outro tipo de ato jurídico para vinculá-los. Caso haja alguma ocorrência, o GDPR (UNIÃO EUROPEIA, 2016) determina a responsabilidade a ambos que firmaram o contrato, no que tange à ocorrência. Por sua vez, no Brasil, os responsáveis são aqueles que estão em exercício no momento da queixa (BIONI, 2019).

Por fim, com relação aos relatórios de impacto, a Lei brasileira não apresenta regras específicas sobre as situações nas quais o controlador deve fazer os relatórios. Por outro lado, a Lei europeia prevê que os relatórios de impacto devem ser feitos se o tratamento dos dados pessoais resultar em elevado risco para a integridade, ao direito e à liberdade dos indivíduos (BIONI, 2019).

3. IMPACTOS DA LGPD

A LGPD (BRASIL, 2018a) causa diversos impactos, como em cidadãos e empresas, sob o ponto de vista geral, e em cada setor da organização. Diante disso, nesta seção serão abordados os aspectos mais relevantes do tópico estudado.

Evidentemente, os cidadãos serão os mais beneficiados com a entrada da Lei em vigor, pois toda informação pessoal está protegida por legislação, ou seja, há mais segurança à integridade do indivíduo. Ela permite a eles o total controle sobre as informações: por exemplo, se um indivíduo requisitar a

retirada de suas informações da base de dados de uma empresa, esta precisará atender de maneira rápida à solicitação. O usuário também pode pedir a alteração dos dados ou cancelar o recebimento de *e-mails* automáticos, caso haja necessidade. Nada aconteçendo como previsto no negócio, a companhia tem 72 horas para avisar ao cliente sobre o ocorrido e apresentar a solução, sob pena de multa equivalente a até 2% do faturamento mensal (MALDONADO, 2019).

Várias organizações foram penalizadas com os impactos do advento da LGPD (BRASIL, 2018a). Antes, as empresas coletavam os dados das pessoas e os usavam livremente, mas, após a Lei, os clientes passaram a ter o direito de solicitar a remoção completa de seus dados, como dito anteriormente. Isso ocasiona mudanças logísticas de funcionamento das companhias, como a criação de cargos para manipulação de informações pessoais ou a forma de elaboração e fechamento de acordos, pois o compartilhamento dos dados se torna realizável apenas com algum tipo de supervisão (OLIVEIRA, 2020).

Em documentos de consentimento elaborados para os usuários estarem cientes sobre o uso de seus dados, necessita-se de uma revisão para esclarecer as formas de emprego dessas informações. Como estas são repassadas em vários setores da mesma empresa, há grandes chances de se perderem ou serem corrompidas. Logo, a estruturação é essencial para evitar eventualidades, como criar um setor especializado em manipulação de dados ou até mesmo designar quais áreas têm acesso a eles.

Além de demandar tempo e dinheiro, as organizações precisam se adequar às normas da Lei, caso contrário, estarão sujeitas às medidas jurídicas, como multas, advertências e, em casos mais graves, a imobilização total, até que seja feito algo a respeito da situação.

Houve também impactos em relação à competitividade entre as empresas. Em curto prazo, há uma perda de liderança daquelas organizações que se adequaram à Lei, pois já investiram valores consideráveis enquanto outras não realizaram aquisições. Porém, no médio e longo prazos, as que se adaptaram ganham uma vantagem competitiva, uma vez que não terão problemas com a justiça quanto ao cumprimento das normas e, tampouco, serão multadas ou advertidas.

Companhias que estão em conformidade às diretrizes contarão com termos de usuários atualizados de acordo com a LGPD (BRASIL, 2018a), o que pode ser um fator decisivo na hora de o cliente aceitar os termos e enviar os dados. Após a Lei, a garantia de segurança das informações pessoais é maior, e o cliente preferirá comprar produtos de uma empresa que garanta sua segurança, em detrimento às que não tomaram as devidas precauções (MALDONADO, 2019).

A área de Recursos Humanos – RH foi afetada, uma vez que trabalha com um grande fluxo de informações pessoais, tanto de colaboradores quanto de candidatos a uma vaga na empresa ou ex-funcionários. Esse setor precisa estar atento e em conformidade com a LGPD (BRASIL, 2018a), pois manipula dados de indivíduos que interagem com organizações, e não somente de clientes. Para se adaptar à Lei, é necessário atualizar os termos de contratação e repassá-los para os atuais funcionários, para eles verificarem se estão de acordo ou não com a documentação, o que também se aplica às propostas de emprego (MARTINI e BERGSTEIN, 2019).

O *marketing* também é uma das áreas que mais foram impactadas pela LGPD (BRASIL, 2018a), por se basear em dados pessoais adquiridos por meio de pesquisas de mercado que permitem traçar perfis mercadológicos para cada indivíduo ou grupo de pessoas. Com os resultados desses estudos, planejam-se ações para direcionar a propaganda a um nicho específico do negócio. Para realizar as ações mercadológicas, são necessárias as informações dos consumidores, o que influencia diretamente o setor; e, para se adequar à Lei, a equipe de *marketing* precisa construir um termo de forma concisa e clara, em que o cliente fica ciente e livre para aceitar (ou não) o uso de seus dados para pesquisas futuras (CANHADAS FILHO, 2019).

Enquanto isso, a área de comércio engloba as negociações da empresa, desde a compra e venda dos produtos até os serviços terceirizados, para melhor gerenciamento com parceiros de vendas. Esse setor é afetado de várias formas, como, por exemplo, nas parcerias com outras organizações para aumentar a lucratividade de ambas, mas, para isso, é preciso o cruzamento de dados sobre os usuários para verificar a parte em que há mais lucro.

Outra rotina corporativa influenciada é a terceirização, situação em que uma companhia contrata determinada prestadora de serviços com foco em gerenciar o armazenamento das informações em banco de dados. Para se enquadrar na Lei, esse setor deve propor termos para os usuários saberem que os conteúdos estarão sob a tutela da terceirizada. Ademais, uma empresa pode se unir com outra e utilizar os dados dos clientes para esse vínculo funcionar de fato. Em ambos os casos, os clientes deverão estar cientes e ter a oportunidade de aceitarem ou não os termos (CANHADAS FILHO, 2019).

Nesse ínterim, a área jurídica é responsável pela parte burocrática da adequação, com a montagem dos termos de consentimento do usuário, em que deve levar em consideração as ponderações dos outros setores para elaborar essas documentações. Se os dados pessoais forem utilizados de maneira indevida, divulgados ou compartilhados com terceiros sem consentimento, tal setor deverá representar a empresa e responder legalmente sobre o ocorrido (MARTINI e BERGSTEIN, 2019).

O Departamento Financeiro é outro setor afetado pela LGPD (BRASIL, 2018a), pois a adequação com a Lei irá demandar gastos. Por conseguinte, precisa estar ciente sobre o que as outras áreas pretendem fazer para adotar as novas medidas e apresentar os custos da operação. Com isso, a parte financeira é responsável por coordenar as despesas e os investimentos, com vistas a se adaptar aos recursos disponíveis (CANHADAS FILHO, 2019).

A área de Tecnologia da Informação (TI) se responsabiliza pela implementação e execução da LGPD (BRASIL, 2018a), ao garantir a segurança das informações dos usuários. Os funcionários desse setor irão tratar e/ou criar os *softwares* de terceiros que manuseiam os dados. Logo, é necessário criar sistemas seguros, por meio de boas práticas de segurança da informação, como criptografia, controles de *firewall* (sistema de segurança) e dispositivos de armazenamento mais rápidos e seguros, a exemplo das *Solid-State Drives* (Unidades de Estado Sólido, SSDs).

Geralmente, as empresas precisam realizar três ações: ajustar a logística para assegurar a integridade dos dados pessoais; criar termos de consentimento condizentes; e, programar os sistemas para cumprir os termos. Não há descrição sobre tais aspectos em Lei, mas se sugere a criação de um

comitê voltado à LGPD (BRASIL, 2018a), composta por funcionários de vários setores que, juntos, podem ajustar os procedimentos adotados. Nesse grupo, o controlador (funcionário de qualquer setor) fica responsável por guiar o operador (colaborador de TI) – sugere-se, ainda, contratar consultorias especializadas em LGPD (BRASIL, 2018a) para auxiliá-los.

Junto aos impactos e efeitos da LGPD (BRASIL, 2018a), destacam-se pontos positivos e negativos acerca do funcionamento da legislação, dentre as quais será mostrado a seguir.

Obviamente, houve vários benefícios com a implementação da LGPD (BRASIL, 2018a), mas ainda há desvantagens, como o custo e o tempo para a adequação à Lei. Devido à desinformação, muitas empresas sequer sabem da existência de tal aparato legislativo, o que pode levar a penalidades decisivas nos resultados dessas organizações, pois, se não houver os ajustes, podem ser multadas em até 2% do faturamento relativo ao ano anterior, com limite de R$ 50 milhões.

Ademais, quanto mais burocrático for o negócio entre empresa e cliente, mais esforço será necessário na manipulação dos dados, o que pode acarretar na desmotivação das organizações nos acordos. Isso se aplica, sobretudo, a companhias internacionais, pois, como a maioria dos países possui regulamentação própria, a imposição a novas regras como a LGPD (BRASIL, 2018a) dificulta a adaptação e a realização de negócios com cidadãos brasileiros (SALOMÃO, 2019).

Dentre as vantagens, a principal delas é a segurança. De acordo com a LGPD (BRASIL, 2018a), todo cidadão tem os dados protegidos e pode decidir sobre a destinação das informações. Como dito anteriormente, as empresas não podem mais usar os dados sem nenhum tipo de consentimento e, se um cliente pretende remover suas informações dessas companhias, elas são obrigadas a apagá-las, por serem de propriedade exclusiva do cidadão. Esse ponto implica na confiabilidade do usuário, pois, ao concordar com os termos de uso, ele percebe que a empresa assegura a integridade dos dados. Caso o consumidor adquira outro produto ou serviço em outra organização e os termos são inadequados, ele preferirá continuar com a empresa que já conhece (SALOMÃO, 2019).

Outro ponto positivo é o avanço tecnológico, principalmente na área de segurança da informação. Como a prioridade é assegurar os dados pessoais, novas tecnologias começarão a surgir para melhorar e facilitar a elaboração de medidas protetivas, não apenas em relação a esse tipo de informação, visto que as tecnologias podem ser expandidas para outros campos que necessitam de segurança e possam vir a ser beneficiados (DLA PIPER, 2020).

A introdução da LGPD (BRASIL, 2018a) e do GDPR (UNIÃO EUROPEIA, 2016) pode levar outros países a criarem as próprias regulamentações e, com o tempo, ter uma cultura de garantir a integridade dos cidadãos na Internet. Posteriormente, isso pode acarretar em leis que objetivem proteger qualquer tipo de informação que circula na rede, e não apenas das informações pessoais (SALOMÃO, 2019).

4. ESTUDO DE CASO

Adotamos uma organização fictícia que ainda não possui produtos ou serviços prontos para serem comercializados e precisa passar pela burocracia de abertura de empresas, incluindo a adequação à LGPD (Brasil 2018a). Este estudo de caso servirá de base para as considerações tecnológicas voltadas à criação de sistemas a serem adequados à referida Lei, desde o início até o lançamento de produtos ou serviços no mercado. Para tal, considera-se uma Microempresa (ME) hipotética, com Sociedade Limitada (LTDA), onde os três sócios são os fundadores; possuem, igualitariamente, um terço das cotas; e são funcionários da entidade.

A empresa é um *e-commerce* (*electronic commerce* | comércio eletrônico) com foco em vendas de calçados. No *website* (sítio da Internet), lojas que comercializam esse item poderão fazer cadastros, divulgar e vender os produtos, enquanto os clientes poderão fazer cadastro, realizar buscas, aplicar filtros para refiná-las e selecionar as peças de acordo com a própria preferência. Como resposta, o *website* fornece as opções de lojas para o usuário encontrar o produto desejado.

Depois da contextualização da empresa e ao considerá-la em conformidade aos trâmites legais judiciais possíveis para a abertura, deve-se criar completamente o sistema. O *website*, já em processo de finalização,

necessita da implementação de elementos de segurança, com o intuito de assegurar a integridade dos dados das lojas de calçados e dos consumidores.

Para isso, é preciso citar os tipos de dados a serem manipulados pela companhia e elaborar os termos de consentimento aos fornecedores e clientes, como um levantamento de requisitos para auxiliar no funcionamento do sistema de segurança. Por ser uma organização recém-chegada ao mercado e de pequeno porte, cada sócio usa apenas um computador, totalizando três unidades, e têm à sua disposição um servidor dedicado somente para guardar as informações de fornecedores e consumidores. Nesse caso, os cargos de operador e controlador já foram definidos.

Quanto aos clientes, os termos de consentimento postulam que os dados solicitados são usados para pesquisas de mercado e direcionamento de *marketing*. Ou seja, quando os usuários entrarem no *site*, serão mostradas propagandas personalizadas com sugestões de calçados do interesse deles. A escolha do produto divulgado a cada consumidor se baseia nos dados coletados das compras e em pesquisas feitas por cliente. Além disso, as informações são repassadas para as lojas cadastradas no *site*, para elas verificarem a validade (ou não) da venda. Quando os dados são repassados aos parceiros cadastrados, eles passam a ser responsáveis pela gestão das informações.

No *website*, quando as lojas fazem o cadastro e começam a divulgá-los, há uma área específica em que cada uma poderá anexar os próprios termos de consentimento, para os clientes ficarem cientes sobre as formas de manipulação das informações. Esses documentos são exibidos antes de o consumidor finalizar o pedido e, para realizar as compras, ele precisa cadastrar dados como *e-mail*, nome completo, CPF, Código de Endereçamento Postal (CEP), endereço, bairro, cidade, estado e telefone. Para o processamento da compra, o cliente deve indicar os dados bancários para pagamento, como número de cartão, nome impresso na frente (conforme as abreviações), data de vencimento e código de segurança.

As únicas informações repassadas aos fornecedores são os dados pessoais do primeiro cadastro e os de compras realizadas pelo usuário que correspondem somente à loja em questão. Por exemplo, o cliente adquiriu um

tênis na loja ***x***; depois, outro sapato na loja ***x*** novamente; e, por último, comprou um chinelo na loja ***y*** – nesse caso, a loja ***x*** só terá acesso às informações das próprias vendas (tênis e sapato), e a ***y***, à comercialização do chinelo. Após a compra, uma porcentagem do dinheiro fica com a ME responsável pela conexão entre cliente e fornecedor.

Para os fornecedores, os termos de consentimento mostram que os dados obtidos podem ser utilizados em validações e pesquisas de mercado. Estas últimas visam mostrar aos fornecedores o setor de calçados mais lucrativo e o público-alvo de cada área. Assim, as lojas conseguem divulgar produtos voltados a determinadas pessoas, aumentar a lucratividade e proporcionar propagandas personalizadas, de acordo com as preferências do consumidor.

Além disso, precisa haver uma política de segurança para as informações dos usuários e informá-los, por meio do termo de consentimento, como elas são manipuladas. Para o cadastramento das lojas na plataforma, os dados solicitados são: nome, nome fantasia, Cadastro Nacional da Pessoa Jurídica (CNPJ), CEP, endereço, bairro, cidade, estado, telefone, *e-mail* e termo de consentimento do usuário. Caso a fornecedora não disponibilize esse último documento, não será possível finalizar o cadastro. Ao final desse processo, solicita-se uma pequena porcentagem dos lucros obtidos pelas parceiras em cada venda realizada.

Após definir o funcionamento e os métodos de tratamento e manipulação dos dados na nova empresa, a próxima etapa consiste na arquitetura de segurança do sistema, para garantir a integridade das informações de consumidores e fornecedores. Consideram-se quatro ferramentas para garantir a segurança dos dados: um *framework* (quadro) LGPD Ninja (2018), os *firewalls*, a criptografia e um antivírus corporativo.

A LGPD Ninja (2018) possui um *framework* gratuito, com várias normas e formas de adequação à LGPD (BRASIL, 2018a) para uma empresa, ao definir os processos de dados, onde e quando ocorrerão os processos. Outra funcionalidade importante dessa ferramenta é a catalogação/separação dos dados por setor, para saber como são tratados. O *framework* também recomenda fazer auditorias de *compliance*, que correspondem ao cumprimento

de regulamentos legais para obter um melhor funcionamento; e da *compliance* com a LGPD (BRASIL, 2018a) e os riscos na continuidade do negócio – tais medidas visam certificar que os dados são tratados de forma correta e não há danos para a empresa.

Também é pontuada a necessidade de detalhar os tratamentos e procedimentos realizados com os dados, algo relevante para corrigir os problemas encontrados. Ainda existe um programa pago que funciona na *web* (rede) e pode ser integrado ao *software* desenvolvido, em que todas as informações passarão para a LGPD Ninja (2018) as tratar e repassar para os clientes somente em relatórios.

Para a empresa analisada neste estudo de caso, é utilizada a modalidade paga disponibilizada no *website* da LGPD Ninja (2018), para quem são acreditadas todas as questões acerca da Lei em si. É disponibilizado um relatório, para acompanhamento da auditoria, que contempla o catálogo de dados, a consultoria, a análise de fontes e o impacto às informações pessoais – tal documento é solicitado pelo governo para checar se a empresa manipula os dados de forma correta.

Foi usado também o *firewall*, que gera uma camada extra de segurança, ao controlar todas as solicitações de acesso feitas por fornecedores (divulgação de produtos) e consumidores (aquisição). Nesse caso, é necessário fazer o registro inicial, mas sem ser de maneira anônima, até mesmo para consultas simples ao *website*, o que indica mais proteção nas navegações dos usuários na plataforma.

Por exemplo, em um *website* livre de proteções, caso ocorra alguma infração sobre a movimentação de dados pessoais e/ou sensíveis, tomar-se-ia certo prazo até identificar os responsáveis pelo crime. Porém, com o controle de *firewall*, esse processo seria simplificado, uma vez que qualquer entrada é reconhecida pelos gerenciadores. Cumpre ressaltar que, ao acessar o *website*, haverá um aviso sobre as políticas e os termos de consentimentos de usuário, seja para consumidores ou fornecedores.

Criptografia é outra tecnologia embarcada no sistema para garantir a segurança dos dados pessoais de todos os usuários. Dentre os mais usados atualmente, o tipo DES e suas variantes (3DES, DESX e AES) têm sido

empregados como padrão em governos como os dos Estados Unidos. Há também o Camellia, o RSA, o SAFER e o IDEA – os dois últimos são os mais complexos e, ao mesmo tempo, os que demonstram maior segurança.

Porém, para a empresa em questão, foi estudado o método de criptografia *Blowfish* e suas variantes *Twofish* e *Threefish*, em que consiste basicamente em algoritmos com uma chave simétrica/privada relativa a um código no qual emissor e receptor da mensagem possuem a mesma chave para descriptografá-la.

Nessa conjuntura, é possível criar um canal privado para apenas os usuários conhecerem o conteúdo da mensagem, e a criptografia de chave simétrica possui a cifra da criptografia em si, em que a mensagem é embaralhada em cifras de fluxo ou de blocos. O *Blowfish* usa as cifras de bloco, ao criar um conjunto de *bytes* (conjunto de oito *bits*) de tamanho fixo, no qual a mensagem também é embaralhada – caso a mensagem seja maior que um bloco, ela é dividida para criar dois blocos e, se ela for menor, o bloco é completado com dados desnecessários para ter um tamanho fixo. São utilizados blocos fixos de 64 *bits* (códigos binários) de tamanho, enquanto a única diferença das variantes é o tamanho dos blocos fixos.

Para o estudo de caso, escolheu-se o *Blowfish* básico gratuito, por apresentar código de fonte aberta, o que possibilita obter uma cópia e manipular o código de forma a melhor se encaixar no sistema. Embora ofereça uma segurança maior do que as criptografias do tipo DES ou RSA, ainda proporciona menos proteção do que o SAFER e o IDEA. O *Blowfish* é bastante utilizado no ramo de *e-commerce* para garantir a segurança, principalmente na hora do pagamento; proteger as senhas dos usuários; ter uma velocidade relativamente rápida; e não requerer um poder computacional mais elevado.

Outro motivo dessa opção, diz respeito ao tamanho dos blocos das cifras (quanto maiores, mais lentos são os processos); assim, o sistema selecionado consegue atender uma empresa nova, com poucos clientes no lançamento, uma vez que apresenta um fluxo baixo de processos. Porém, à medida que ela crescer, será preciso considerar as variantes.

Há também a necessidade de um antivírus corporativo, para garantir uma camada extra de proteção. Consideraram-se programas como *Avast*,

Kaspersky, *McAfee* e o *Norton*. Este último foi escolhido com a versão *Deluxe*, que oferece o melhor custo-benefício em relação aos outros e protege cinco dispositivos – na empresa, há três computadores e um servidor.

Entre os benefícios oferecidos está a proteção contra vírus, *malwares* (programas maliciosos), *spywares* (*softwares* espiões) e *ransomwares* (programas de bloqueio de dados) por meio de uma *Artificial Intelligence* (Inteligência Artificial, AI) – se algo duvidoso começar a aparecer nas máquinas da empresa, o antivírus irá bloquear grande parte das tentativas de ataque.

Outro benefício se refere a *firewalls* e criptografias próprios, reforçados com o antivírus. O *Norton* apresenta ainda uma segurança de *Virtual Private Network* (Rede Privada Virtual, VPN), que ajuda a esconder as máquinas quando estão conectadas a uma rede – essa é uma ótima opção para a empresa, por ser segura o bastante para um fluxo pequeno de processos, com um custo menor.

Convém salientar que os equipamentos e acessórios foram adquiridos conforme o custo-benefício, isto é, com preços acessíveis, mas que garantem a segurança (Figura 2).

COMPUTADORES	
PRODUTO	PREÇO (R$)
Processadores Intel Core i5 8400	1500
Placa mãe Asus TUF B360M - Chipset Z370	700
SSD - 1TB	750
Memória RAM (8GB)	300

SERVIDOR	
PRODUTO	PREÇO (R$)
Processadores Intel Core i7 9700K	2000
Placa Mãe Aorus B460M Aorus Pro - Chipset Z370M	950
SSD - 4TB (4 SSDs de 1T)	3000
Memória RAM (12GB)	550

Figura 2. Tabela de precificação do ambiente empresarial

Por ser uma pequena empresa, os métodos foram levados em consideração quanto aos valores, a exemplo da criptografia gratuita. Os maiores gastos se referem à montagem das máquinas, em torno de R$

4.000,00 (quatro mil reais), e ao servidor, de R$ 7.000,00 (sete mil reais) – o antivírus custa apenas R$ 80,00 (oitenta reais) por ano. Então, o gasto total para montar um ambiente seguro para os clientes, que demanda um investimento baixo, ficará em aproximadamente R$ 20.000,00 (vinte mil reais).

Considerando o que foi demonstrado no estudo de caso, foram observados métodos para a implantação de segurança no *software*, como VPNs, chaves públicas, criptografias, *frameworks*, auditorias do serviço e de arquivos, sistemas de detecção de intrusão, ambientes de execução isolada, *firewalls*, *hardwares* (equipamentos físicos) mais recentes e antivírus.

Para a empresa em questão, as melhores opções para implantar mecanismos de segurança apropriados se referem a *hardwares* recentes, *framework* LGPD Ninja (2018), *firewall*, criptografia e antivírus corporativo Norton.

Como a empresa está no início das atividades e ainda não possui clientes, não é necessário um sistema robusto para conseguir lidar com um elevado fluxo de dados, e sim apenas alguns métodos para se adequar à LGPD (BRASIL, 2018a). Todavia, a estrutura de segurança foi idealizada com o intuito de evitar problemas futuros. Neste estudo de caso, foram elencadas as melhores formas de implementação de elementos seguros, e não apenas o mínimo possível para uma organização em fase de inauguração.

CONCLUSÃO

Neste artigo, foram mostrados aspectos concernentes à LGPD (BRASIL, 2018a), desde os fundamentos e as definições até os cenários demonstrativos relativos ao impacto ocasionado em empresas e cidadãos. Relataram-se vantagens, desvantagens, similaridades e diferenças entre LGPD (BRASIL, 2018a) e GDPR (UNIÃO EUROPEIA, 2016), além de ter sido apresentado um estudo de caso prático acerca da implementação de um sistema de segurança com as melhores práticas na área de TI em uma empresa, em consonância com a legislação vigente.

A implantação de uma nova Lei no Brasil constitui um avanço, tanto para a tecnologia, principalmente no que tange à segurança da informação, quanto à economia, posto que as empresas terão uma base mais estável e poderão criar

um vínculo maior entre elas e os consumidores. A implantação de ambos os aparatos legislativos – LGPD (BRASIL, 2018a) e GDPR (UNIÃO EUROPEIA, 2016) – pode incentivar outros países a consolidar as próprias políticas e levar ao avanço das tecnologias nessa área.

Ao considerar o exemplo mostrado, há bastantes recursos tecnológicos para implantar um sistema voltado a assegurar a integridade dos dados pessoais, sobretudo para as empresas que irão iniciar suas atividades com a Lei em vigência, como destacado na seção 04 deste trabalho. É algo plausível de ser feito e, com o tempo, passará a ser um item básico nas organizações.

Nesse contexto, as considerações tecnológicas acerca do tema demonstram que a LGPD (Brasil 2018a), juntamente com o GDPR (União Europeia 2016), iniciaram a expansão de tecnologias de segurança da informação, com a intenção de garantir a integridade de dados pessoais. No futuro, estudos sobre essa temática poderão gerar novas tecnologias em sistemas e mais segurança para as pessoas poderem usufruir as ferramentas da Internet.

Destarte, o estudo de caso apresentado neste Artigo é uma metodologia que pode ser usada em vários ramos. Pode-se aplicar a metodologia em empresas parecidas com o *e-commerce* ou em outras áreas das organizações, apesar de serem necessários novos estudos para adequar a segurança dos dados aos interesses de cada setor. Há também a possibilidade de estudar outras melhorias estratégicas, como os métodos para implantação da segurança e a redução de custos.

REFERÊNCIAS

BIONI, B. R. *Proteção de dados pessoais* – a função e os limites do consentimento. São Paulo: Forense, 2ª ed., 2019.

BLUM, R. O. Comentários ao GDPR. *Revista dos Tribunais*, 1ª ed., 2019.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24/04/2021, às 19h03min.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018(a)*. "Lei Geral de Proteção de Dados Pessoais". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 24/04/2021, às 19h05min.

BRASIL. *Medida Provisória n. 869, de 27 de dezembro de 2018(b)*. "Altera a Lei n. 13.709, de 14 de agosto de 2018". Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/57220361/do1-2018-12-28-medida-provisoria-n-869-de-27-de-dezembro-de-2018-57219992. Acesso em: 24/04/2021, às 19h04min.

BRASIL. *Lei n. 13.853 de 08 de julho de 2019(a)*. "Altera a Lei n. 13.709, de 14 de agosto de 2018". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 24/04/2021, às 19h10min.

BRASIL. *Veto n. 24, de 09 de julho de 2019(b)*. "Altera a Lei n. 13.709, de 14 de agosto de 2018". Disponível em: https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445. Acesso em: 24/04/2021, às 19h11min.

CANHADAS FILHO, G. *Implicações legislativas da nova economia digital*. Portal Migalhas, 2019. Disponível em: https://www.migalhas.com.br/depeso/315962/implicacoes-legislativas-da-nova-economia-digital. Acesso em: 24/04/2021, às 19h14min.

DLA PIPER. *Data protection laws in the world*, 2020. Disponível em: https://www.dlapiperdataprotection.com/. Acesso em: 24/04/2021, às 19h15min.

DONDA, D. *Guia prático de implementação da LGPD*. São Paulo: Labrador, 1ª ed., 2020.

HINTZBERGEN, J. *Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002*. Rio de Janeiro: Brasport, 1ª ed., 2018.

LGPD BRASIL. *"Homepage"*, 2018. Disponível em: https://www.lgpdbrasil.com.br/. Acesso em: 24/04/2021, às 19h21min.

LGPD NINJA. *"Página inicial"*, 2018. Disponível em: https://www.lgpd.ninja/. Acesso em: 24/04/2021, às 19h23min.

MALDONADO, V. N. Lei Geral de Proteção de Dados Pessoais – manual de implementação. *Revista dos Tribunais*, 2ª ed., 2019.

MARTINI, S. R. e BERGSTEIN, L. "Aproximações entre o direito ao esquecimento e a Lei Geral de Proteção de Dados Pessoais (LGPD)". *Revista Científica Disruptiva*, v. 1, n. 1, jan-jun de 2019, p. 160-176. Disponível em: http://revista.cers.com.br/ojs/index.php/revista/article/view/14/13. Acesso em: 24/04/2021, às 19h27min.

MORELLI, E. *"LGPD – Lei Geral de Proteção de Dados Pessoais"*, 2020. Disponível em: https://www.udemy.com/course/cursolgpd/. Acesso em: 24/04/2021, às 19h28min.

OLIVEIRA, R. O legítimo interesse e a LGPD. *Revista dos Tribunais*, 1ª ed., 2020.

PINHEIRO, P. P. *Proteção de dados pessoais*: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2ª ed., 2020.

POHLMANN, S. A. *LGPD Ninja*: entendendo e implementando a Lei Geral de Proteção de Dados nas empresas. Rio de Janeiro: Fross, 1ª ed., 2019.

RAPÔSO, C. F. L.; LIMA, H. M.; OLIVEIRA JUNIOR, W. F. O.; SILVA, P. A. F. e BARROS, E. S. "LGPD – Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação: revisão sistemática". *Revista de Administração*, 2019, v. 4, p. 58-67. Disponível em: https://revistas.cesmac.edu.br/index.php/administracao/article/view/1035/802. Acesso em: 24/04/2021, às 19h37min.

RODRIGUES, Fabrizio. *Como iniciar o processo de implantação da LGPD?*, 2020. Disponível em: https://fabriziorodriguesr.jusbrasil.com.br/artigos/878114156/como-iniciar-o-processo-de-implantacao-da-lgpd?ref=serp. Acesso em: 24/04/2021, às 19h39min.

SALOMÃO, L. F. *"Debater a Lei Geral de Proteção de Dados é refletir sobre o futuro"*, 2019. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Debater-a-Lei-Geral-de-Protecao-de-Dados-e-refletir-sobre-o-futuro--afirma-ministro-Salomao.aspx. Acesso em: 24/04/2021, às 19h41min.

UNIÃO EUROPEIA. *Regulamento (UE) n. 679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. "Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)". Disponível em: https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf. Acesso em: 24/04/2021, às 19h43min.