UNIVERSIDADE PRESBITERIANA MACKENZIE

ALYNE PAULA DE SOUZA FERREIRA

REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO MERCADO DE COMPLIANCE

SÃO PAULO
2019

ALYNE PAULA DE SOUZA FERREIRA

REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO MERCADO DE COMPLIANCE

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como requisito parcial à obtenção doo título de Bacharel em Direito

ORIENTADOR: Prof. Diogo Rais Rodrigues Moreira

SÃO PAULO
2019

ALYNE PAULA DE SOUZA FERREIRA

REFLEXOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO MERCADO DE COMPLIANCE

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como requisito parcial à obtenção do título de Bacharel em Direito.

Aprovado em:

BANCA EXAMINADORA

_____

Universidade Presbiteriana Mackenzie

_____

Universidade Presbiteriana Mackenzie

_____

Universidade Presbiteriana Mackenzie

AGRADECIMENTOS

À minha mãe, Paula, a maior incentivadora nessa caminhada da vida, pelos ensinamentos, contação de histórias desde antes do nascimento, abraços, broncas e parceria. Obrigada por ter me feito enxergar o mundo muito além da caixa e apoiar todas as minhas vontades, desde uma aula de futebol, ou capoeira, a seis meses em outro país para estudar. Se eu estou aqui, é por sua luta.

Ao Fabio, pelas vezes que eu não tive visão e você me trouxe luz para enxergar. Obrigada por ter enxugado minhas lágrimas de desespero, angústia, alívio e tensão trazidas pelo último ano de graduação.

Aos meus avós, Daisy e João Roberto, por me ensinarem tanto sobre como não somos nada se não tivermos uma família que te apoie.

À minha irmã de coração, Larissa, por ter sido tão compreensiva nesse ano que passou e eu fiquei afastada. Você faz parte da minha história e agradeço sempre por nossa amizade.

Ao Victor, meu melhor amigo, por todo o amor e ódio nesses cinco anos. A graduação sem você teria, no mínimo, muito mais trabalhos para entregar.

À Giovana, que apareceu logo após o intercâmbio e que se tornou indispensável para minha vida. Obrigada por ser sempre a dupla dinâmica que tem até acessórios iguais. Sem você, não teria sobrevivido às aulas de trabalhista.

Às amigas que infelizmente chegaram tarde na graduação (e em todas as aulas do semestre), Carol e Marina. Vocês foram essenciais para que o núcleo de desenvolvimento fizesse sentido.

À Marisa, João, Flavia, Renato e Nana, por terem torcido por mim e comemorado comigo nesses dois anos. Obrigada por serem tão acolhedores e receptivos. Espero que, com esse agradecimento, uma nova garrafa de Cristal seja aberta (vale a tentativa) e possamos comemorar muito mais conquistas de todos nós no futuro.

À Joicy, por ser o presente inusitado que a Techint me trouxe e levo para a vida, até para agendar restaurantes. Quando eu crescer, quero ser que nem você. Túlio, o agradecimento também é para você, é um prazer chamá-lo de amigo.

Por fim, agradeço ao Diogo, pela amizade, parceria, paciência e ensinamentos. Obrigada por ter aceitado ser meu orientador antes mesmo de definirmos um tema, ou não ter desistido até quando eu pensei em falar sobre futebol. Você é uma inspiração para mim.

RESUMO

O presente artigo se destina a analisar, de forma crítica, os principais pontos da Lei Geral de Proteção de Dados, sob a ótica do Compliance. Posto que as repercussões da lei ainda são imensuráveis, dada a recente promulgação e tempo de estudo, propõe-se o presente trabalho a discutir os aspectos constitucionais dos princípios protegidos pela lei, bem como os impactos da Lei no cenário empresarial brasileiro e alguns casos recentes de vazamento de dados a fim de uma melhor compreensão do cenário atual enquanto não há a efetiva fiscalização da agência reguladora. Ainda, o artigo busca explicitar as diferenças entre dado pessoal, dado pessoal sensível e hipóteses de tratamento, bem como a importância do consentimento para a transparência do tratamento.

Palavras-Chave: Compliance; Dados Pessoais; Consentimento; Tratamento de Dados;

ABSTRACT

This article aims to critically analyze the main points of the Lei Geral de Proteção de Dados Pessoais, from the Compliance perspective. As that the repercussions of the law are still immeasurable, regarding the recent promulgation and time of study, this paper proposes to discuss the constitutional aspects of the principles protected by the law, as well as the impacts of the law on the Brazilian business scenario and some recent cases of data leakage, in order to understand more analytically the current scenario, while there is no effective oversight by the regulatory agency. Furthermore, the article seeks to explain the differences between personal data, sensitive personal data and treatment hypotheses, as well as the importance of consent for treatment transparency.

Keywords: Compliance; Personal Data; Consent; Data Treatment

SUMÁRIO

INTRODUÇÃO

A Lei 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais, LGPD, complementada e alterada parcialmente pela MP 869/2018, vem ao ordenamento brasileiro como uma resposta às preocupações internacionais frente aos escândalos de compra e venda de dados pessoais, como no Caso Cambridge Analytica, mais especialmente ao Regulamento 2016/679 (GDPR), da Comunidade Europeia.

De acordo com Magalhães & Pereira,

> Após vários anos de utilização massiva da rede para comunicar, comprar, promover produtos e aproximar as pessoas e as empresas, fica o sentimento de insegurança que resulta destas relações virtuais, tendo se considerado essencial devolver às pessoas singulares o controlo da utilização que é feita dos seus dados pessoais, devendo ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.[1]

Embora positivamente recente, faz-se necessária a explicação de que a proteção dos dados pessoais, que podem ser equiparados a um direito fundamental, vem de tempos nos quais a sociedade não se preocupava com tratamentos referentes às mídias digitais, mas sim com os meios físicos de captação, tratamento e exposição destes dados pessoais.

Neste sentido, a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées* e a *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977 foram as pioneiras em trazer a discussão para o direito positivo. Mesmo assim, a falta de conhecimento técnico, aliado à uma tecnologia muito arcaica em relação a atual, tornou as mencionadas leis genéricas e abstratas, sem focar em desdobramentos específicos acerca do uso indiscriminado dos dados pessoais.

Neste sentido, o Ministro Ruy Rosado de Aguiar, em decisão de 1995, já trouxe a preocupação dos dados pessoais em relação aos bancos de dados:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das

[1] MAGALHÃES, F.; PEREIRA, M. **Regulamento Geral de Proteção de Dados**: Manual Prático. 2. ed. Porto: Vida Económica, 2018.

> diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.[2]

Ainda, mostra-se cada vez mais necessária a análise do impacto da Lei Geral de Proteção de Dados na sociedade, tanto para usuários – que são, consequentemente, os proprietários dos dados - quanto para as empresas – sejam elas grandes, médias, pequenas ou micro– que são, agora, alvos de um controle de fiscalização que ainda é desconhecido.

Como ainda não há, efetivamente, um parecer de como serão fiscalizadas as obrigatoriedades da lei, através da Agência Nacional de Proteção de Dados, grande parte dos preparativos de adequação acabam sendo uma prevenção baseada no que poderá ser feito.

Tal fato pode resultar em empresas extremamente cautelosas para o tratamento de dados, sem saberem ao certo qual o limite – e se há um – da aplicação da lei em seu negócio, este podendo ser grande ou apenas um comércio local, posto que não há distinção entre a complexidade da empresa e o tratamento devido na lei.

> Os dados pessoais, na sociedade contemporânea, assumem importância estratégica cada vez maior. Podem ser utilizados em inúmeras aplicações, como o direcionamento de propagandas e anúncios específicos para o perfil de determinado consumidor, a partir das páginas que este visita na internet, ou a identificação da preferência ideológica ou mesmo sexual mediante análise dos gastos realizados pelo cartão de crédito, ou a investigação de doenças com maior probabilidade de se manifestarem durante a vida de determinado indivíduo, por meio da análise de seu material genético. Os exemplos são praticamente inesgotáveis e, cada vez mais, presentes no cotidiano

[2] BRASIL. Superior Tribunal de Justiça. **Recurso Especial 22.337/RS**. Relator: Min. Ruy Rosado de Aguiar, 20 mar. 1995.

> – basta lembrar de seu smartphone, que sugere trajetos para o trabalho mesmo nos feriados[3]

Por consequência, caberá à Autoridade Nacional de Proteção de Dados (ANPD), criada através da Lei 13.853/19, em complemento à Lei Geral de Proteção de Dados Pessoais, a incumbência de acompanhar e fiscalizar a eficácia legislativa, como por exemplo, através da apresentação de um Relatório de Impacto à Proteção de Dados Pessoais, categorizado como

> documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.[4]

Este relatório poderá ser solicitado a qualquer momento pela ANPD e deverá conter, de maneira detalhada e extensiva, a descrição dos processos de tratamento de informações pessoais, bem como medidas e mecanismos elaborados para mitigar todo e qualquer risco que englobe as atividades referentes aos dados. Essa é mais uma forma da ANPD ter visibilidade de como as empresas utilizam dados pessoais para fins de "*big data* e *analytics*".

A coleta e o processamento de dados é permitida por lei, desde que clara e pública, visando que todos saibam seu conteúdo, devendo acorrer um ajuste de comportamento para estar de acordo com a regulação. Assim demonstra-se a importância da *General Data Protection Regulation* europeia e a Lei Geral de Proteção de Dados brasileira.

Juridicamente, qualquer exceção autorizada a um direito fundamental deve ser interpretada de forma restritiva, sem interpretações que expandam o conteúdo da permissão, sendo necessário objetivo legítimo e uma necessidade de interferência para atingir unicamente esse objetivo. [5] Neste sentido,

---

[3] ROQUE, André. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). **Revista Eletrônica de Direito Processual**. Rio de Janeiro, ano 13, v. 20, n. 2, maio/ago. 2019.

[4] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 jun. 2019.

[5] VIDOR, Daniel Martins. LGPD: origem e implicações. **Blog Mercury**. [*S.l.*], 19 mar. 2019. Disponível em: http://mercurylbc.com/lgpd-origem-e-implicacoes/. Acesso: 25 out. 2019.

> Sendo os direitos fundamentais concebidos como princípios – vale dizer, como comandos prima facie dirigidos ao legislador –, é possível que sejam restringidos em decorrência de razões antagônicas que, em determinadas situações, assumam maior peso. Dessa forma, há duas normas válidas que entram em conflito: a norma que estatui o direito *prima facie* e a norma que estabelece a restrição.[6]

Deste modo, deve ser questionada a real eficácia da fiscalização imposta pela lei no tocante ao controle da informação coletada e seu consentimento, posto que este não deve ser tido como exceção à aplicação estrita da norma e sim uma das alternativas jurídicas para poder continuar tratando os dados, desde que este consentimento seja claro e inequívoco.

[6] PEREIRA, Jane Reis Gonçalves. **Interpretação constitucional e direitos fundamentais**. São Paulo: Saraiva, 2018. [Minha Biblioteca].

1 UM RAIO-X DA LGPD

A Lei Geral de Proteção de Dados Pessoais traz para o ordenamento brasileiro os mesmos princípios, objetivos, especificações e consequências trazidos à União Europeia pela GDPR, ainda que, no cenário brasileiro, estes ainda pareçam confusos e mal adaptados à realidade político-jurídica do país.

Isto porque a Lei não realiza uma distinção de direitos, deveres e consequências entre o volume de dados processados, sendo igual sua validade e aplicação tanto para multinacionais de consumo, com gigantescos bancos de dados, quanto para comércios locais que possuem um cadastro de clientes limitado e reduzido.

Talvez, seja por essa questão que sua *vacatio legis,* inicialmente de 18 meses, foi alterada através da MP 869/2018, prorrogado para 24 meses após a sanção da lei. Logo, em agosto de 2019, as empresas já deverão estar adequadas às obrigações da lei, prazo que cada vez fica mais próximo, de acordo com as análises mais populares. Por sua vez, há um debate acerca da *vacatio legis*, com ênfase na LINDB.

> Pois bem, como determina o citado § 3º, contados os vinte e quatro meses, a partir de 28 de dezembro de 2018 (data de publicação da MP nº 869/2018, que deu nova redação ao artigo 65 da LGDP), conclui-se que a LGPD entrará em vigor em 29 de dezembro de 2020 e não em 16 de agosto, tal como ocorreria se o prazo pudesse ser contado a partir da data original da publicação da lei.[7]

Entretanto, seja para agosto ou dezembro de 2020, poucas são as empresas que já começaram a se mobilizar em prol da adequação: em pesquisa realizada pela Serasa Experian, em março deste ano, das 508 companhias entrevistadas, de diferentes portes e segmentos em todas as regiões do país, 85% declararam não estarem prontas para a adequação à LGPD[8].

---

[7] BRUNA, Sérgio Varella. A LINDB e a entrada em vigor da Lei de Proteção de Dados. **Jota**, 10 jan. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lindb-e-a-entrada-em-vigor-da-lei-de-protecao-de-dados-10012019. Acesso em: 25 out. 2019.

[8] SERASA EXPERIAN. 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais, mostra pesquisa da Serasa Experian. 08 ago. 2019. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian. Acesso em: 25 out. 2019.

Em um país com tantas outras questões marcantes, como reforma previdenciária, desemprego e variação cambial, a preocupação da alta direção e dos setores mais influentes na tomada de decisões não é focada em uma nova lei ainda muito incerta, mas sim nos problemas mais urgentes. Assim, as discussões ficam escassas e evitam compromissos efetivos com a proposta legislada, enquanto esta não estiver efetivamente em vigor

As empresas, sejam nacionais ou estrangeiras, se encontram em um cenário focado na proteção de dados, como a portabilidade, descarte seguro e o direito do titular à exclusão/alteração dos dados pessoais. Entretanto, tal fato acarretará muito provavelmente em alterações de políticas, códigos e manuais internos, o que acaba complicando em muito a adequação de grandes empresas ao texto normativo.

Para se adequarem propriamente, as empresas deverão estabelecer, em sua hierarquia, quem serão os responsáveis que assumirão os postos de controlador (a quem compete as decisões sobre o tratamento das informações) operador - que realiza o tratamento dos dados em nome do controlador, denominados Agentes de Tratamento - e de encarregado, o será responsável pela comunicação entre o controlador, o titular dos dados e a Autoridade Nacional de Proteção de Dados. Sendo assim, surgem as dúvidas referentes à estruturação de cargos em uma possível designação de novas atribuições, ou a pesquisa no mercado por profissionais capacitados para tal, mesmo com ninguém possuindo experiência, no contexto legislativo brasileiro, de como será a função.

Por sua vez, a alteração legislativa feita pela MP 869/18, que traz a desnecessidade da figura do Encarregado vir a possuir algum vínculo empregatício ou societário com a empresa acaba trazendo um certo alívio quando se tratar da escolha e da responsabilidade que tal cargo possui, trazendo as empresas a necessidade de avaliação referente ao risco de incluir terceiros em seu sistema de dados e informações, com um acesso quase irrestrito a todo e qualquer processo da Empresa.

Ainda a Lei Geral de Proteção de Dados Pessoais acabou trazendo para o cenário brasileiro um âmbito único de aplicação: não somente as grandes empresas, detentoras de diversos cadastros, fichas de funcionários e informações, mas também as micro e pequenas empresas, como um cabeleireiro de bairro que possui uma lista de seus clientes, estão inclusos nas mesmas obrigações legais, não havendo a

aplicação de discriminações positivas para favorecer um grupo de pequenos empresários que, por muitas vezes chegam até a desconhecer da existência da lei.

A Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por acompanhar e aplicar as sanções da LGPD, será composta por um Conselho Diretor, um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio, unidades administrativas e unidades especializadas.

Entretanto, embora apresente características de agência reguladora, a agência ainda será submetida ao vínculo com a presidência da República, e, ao contrário das agências setoriais, será responsável pela fiscalização de todo e qualquer mercado e atividade relacionado à tratamento de dados pessoais, o que nos leva a refletir, frente ao cenário instável político do país nos últimos anos, de que talvez essa pauta acabe ou sendo deixada de lado ou sendo utilizada como articulação política, o que demonstra mais ainda a incerteza quanto à aplicabilidade desta lei.

Em relação à competência a lei estabelece um rol de atividades, como elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis, entre outros.

Assim, o escopo da agência torna-se extenso e desafiador: são diversas as atividades que deverão ser realizadas e implementadas pela ANPD, e pouco se sabe como será feita a gestão da autonomia da Autoridade, posto que o Conselho Nacional será composto por 23 representantes, titulares e suplentes, designados pelo presidente da República.

De acordo com um levantamento feito pela comissão mista da medida provisória nº 870, de 2019, dos 120 países que aprovaram uma lei de proteção de dados, aproximadamente 80% possuem uma autoridade de proteção em formato de agência reguladora, sendo totalmente independentes. Há também o grupo representando 12 países que não possui positivada a figura da autoridade e, enfim, o grupo que possui a autoridade, mas sem atribuição de independência administrativa,

que representa os últimos 10% dos países, fato que nos leva a refletir sobre tal dependência da agência frente ao chefe do executivo.[9]

Quanto à especificidade dos dados, uma categoria especial foi positivada na lei para dados pessoais que abrangem registros sobre raça, opiniões políticas, crenças, dados de saúde e características genéticas e biométricas – denominados como sensíveis. Tal separação foi criada para buscar o atendimento do princípio da não discriminação, posto que os dados possuem potencial discriminatório, requerendo uma atenção especial do Estado frente ao tratamento destes.

A lei estabelece condições específicas para tratamento dessa categoria de dados, como a obtenção de consentimento do titular antes do tratamento, bem como uma real justificativa para tal tratamento existir.

> A Lei previu uma série de obrigações, como a garantia da segurança dessas informações e a notificação do titular em caso de um incidente de segurança. A norma permite a reutilização dos dados por empresas ou órgãos públicos, em caso de "legítimo interesse" desses, embora essa hipótese não tenha sido detalhada, um dos pontos em aberto da norma.[10]

Já em relação à aplicabilidade, a LGPD engloba qualquer operação de tratamento de dados pessoais realizada por pessoa natural ou por pessoa jurídica, seja de direito público ou de direito privado, independentemente do meio, do país sede da pessoa física ou jurídica, ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; ou a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.[11]

Via de regra, a lei estabelece que a obtenção do consentimento, a comunicação de alterações, ou novos processamentos, a necessidade de anonimização dos dados,

---

[9] BRASIL. **Medida Provisória n° 870, de 2019**. Organização da Presidência e dos Ministérios. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135064. Acesso em: 25 out. 2019.

[10] VALENTE, Jonas. Lei de Proteção de dados traz desafios a empresas, cidadãos e governo. **Agência Brasil**, 25 ago. 2019. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo. Acesso em: 01 out. 2019.

[11] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 jun. 2019.

entre outros, são esforços do controlador dos dados. Ou seja, o sujeito ativo é quem quer usar os dados, enquanto o sujeito passivo é o titular dos dados. A ele não cabem obrigações, nesse sentido.

Neste sentido, cabe a nossa reflexão em olhar para o contexto do país em relação a ataques cibernéticos nos últimos anos.

> O site “Não Me Perturbe” começou a funcionar hoje (16) e permite o cadastro de números para bloquear chamadas de telemarketing das empresas Algar, Claro, Oi, Nextel, Sercomtel, Sky, TIM e Vivo. A iniciativa é fruto de um acordo entre operadoras e a Anatel para “padronizar o uso deste mecanismo [telemarketing], em alinhamento com o crescente debate do tema pela sociedade e em respeito ao cidadão”, informa o site. Na noite desta terça-feira (16), o “Não Me Perturbe” acabou vazando a chave do SendGrid (...) serviço de email baseado em nuvem que fornece uma entrega de email transacional, escalabilidade e análise em tempo real confiáveis com APIs flexíveis que facilitam a integração personalizada”[12]

Como descrito, um site criado para os usuários pararem de receber ligações indesejadas das operadoras de telefonia, que coleta dados como nome, endereço eletrônico e CPF, se mostrou vulnerável para ataques de hackers.

Ainda mais recente, em 8 de outubro de 2019, mais de 70 milhões de brasileiros tiveram seus dados vazados pelo Departamento Estadual de Trânsito do Rio Grande do Norte (Detran-RN).

> Um pesquisador de segurança, que anonimamente denunciou o vazamento ao site Olhar Digital, descobriu que era só inserir diferentes números de CPFs gerados aleatoriamente para causar um erro no site.
> Esse erro em questão dava acesso ao banco de dados de todas as unidades do Detran do Brasil, já que o órgão possui seus sistemas estaduais integrados. De acordo com a reportagem do site, todos os brasileiros que possuem CNH tiveram os dados pessoais expostos no site do Detran-RN.
> Ao ter acesso ao sistema do órgão, era possível obter vários dados sensíveis, como endereço residencial, telefone, operadora e dados da CNH – como categoria, validade, emissão, restrição, registro. Personalidades públicas também foram afetadas pela brecha, com os

[12] PAYÃO, Felipe. Site ‘Não Me Perturbe’ vaza chave de email que permite ataque hacker. **Tecmundo**, 16 jul. 2019. Disponível em https://www.tecmundo.com.br/seguranca/143865-site-nao-me-perturbe-vaza-chave-email-permite-ataque-hacker.htm. Acesso em: 25 out. 2019.

> dados do presidente Jair Bolsonaro e do seu filho Flávio, além do jogador Neymar, sendo vazados, por exemplo.[13]

Neste sentido, cabe a indagação de como será feita a fiscalização e real aplicação da Lei pela Agência criada pelo Governo Federal, uma vez que o Estado, responsável pela fiscalização, também é alvo de ataques e vulnerável a eventuais falhas em sistema, não atuando como um exemplo de aplicação da Lei criada.

[13] GAVIOLI, Allan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. **Infomoney**, 10 out. 2019. Disponível em: https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/. Acesso em: 25 out. 2019.

2 O CONSENTIMENTO NA LGPD

A principal base legal para o tratamento de dados pessoais é o consentimento, que acaba possuindo natureza contratual por, de um lado, existir a manifestação de vontade de uma das partes em se apropriar dos dados para tratá-los para sua finalidade pré-determinada e, de outro, alguém que concorde com esta manifestação.

Assim, tal como em um contrato regulamentado pelo Código Civil, o titular dos dados somente deve consentir com o tratamento de seus dados pessoais se essa manifestação vier a ser livre, informada e inequívoca, sabendo a finalidade para qual seus dados serão utilizados.

Neste sentido, o consentimento apenas será válido se a pessoa puder exercer uma verdadeira escolha, não abrindo margens para longas e extensas cláusulas de "termos e condições de uso" feitas especialmente para evitar a leitura do detentor dos dados, não podendo existir nenhum tratamento distinto caso o tratamento não vier a ser aceito. Desta forma, se o tratamento vier a ser motivo para violar o direito de liberdade de escolha da pessoa, não há o que se falar em verdadeira escolha.

> A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais. Ele está em uma situação de *vulnerabilidade específica* em meio a uma *relação assimétrica* que salta aos olhos, havendo uma série de evidências empíricas a esse respeito.[14]

De acordo com a lei, o consentimento deve se dar por escrito ou por qualquer outro meio que demonstre que houve manifestação de vontade do titular, não admitindo o consentimento tácito. Independentemente do meio pelo qual o titular expressou seu consentimento, este deve ser preservado para que se prove que houve inequívoca manifestação de vontade do titular dos dados, conseguindo ser comprovado caso necessário às autoridades judiciais, em caso de questionamento, e adequado aos termos do tratamento de dados proposto.

Nesta mesma linha de raciocínio, a cláusula sobre o consentimento, quando inserida em uma política ou contrato, deverá ser devidamente destacada, dentro do texto do contrato celebrado com o detentor dos dados, com sublinhados, caixa alta,

---

[14] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – a função e os limites do consentimento**. Rio de Janeiro: Grupo GEN, 2019.

itálico, negrito, etc., ou através de capítulo ou seção específico para tal. Caso não seja observada a forma prescrita na lei para coleta do consentimento, o negócio jurídico será nulo.

Ainda, o consentimento deverá ser específico e determinado, detalhando como os dados do titular serão utilizados e qual a finalidade de sua coleta, não admitindo a utilização de finalidades genéricas ou expressões vagas.

Ainda, se o consentimento for a justificativa para a coleta, e houver mudança nessa finalidade específica após a coleta, ou na forma, duração ou compartilhamento dos dados, o titular dos dados deverá ser novamente informado para que declare novamente seu consentimento, podendo revogá-lo a qualquer instante.

Portanto, percebe-se que a redação da cláusula de consentimento traz uma importância extrema para a validade do tratamento, sendo qualquer omissão capaz de anular o consentimento previamente obtido.

> Na lógica da economia digital, os dados pessoais são a moeda de troca pelo bem de consumo. Em um contexto de agregação de dados e de complexidade do fluxo informacional (subcapítulo 4.1.2), o consumidor não sabe, ao certo, os custos efetivos de tal transação econômica, já que é incerto o alcance do fluxo de seus dados pessoais e, por conseguinte, o que deles se pode extrair.
> O consumidor “compra agora para pagar depois”. Esse quadro de incertezas é a *eloquência* de uma *nova vulnerabilidade*, na medida em que o titular dos dados pessoais pode ser “machucado” pela má utilização de seus dados pessoais, cuja potência da “ferida” não pode ser nem mesmo antevista.[15]

Quanto à revogação do consentimento, a LGPD explicita que esta poderá ocorrer a qualquer momento, desde que seja da vontade do titular. É o que consta no artigo 8º da lei, abaixo transcrito.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular
> §1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

[15] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – a função e os limites do consentimento**. Rio de Janeiro: Grupo GEN, 2019.

> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.[16]

Sendo assim, a retirada de consentimento deverá ser tão fácil quanto seu fornecimento, ou seja, por manifestação expressa do titular, através de procedimento gratuito e desburocratizado e, uma vez retirado, a organização responsável pelo tratamento de dados, além de finalizar o processo de tratamento de dados, deverá garantir a eliminação dos dados, caso requerido. É o que assegura o art. 18, VII:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;[17]

Em síntese, todas essas informações deverão constar de forma clara e objetiva nas políticas de privacidade daqueles que coletam os dados para posterior tratamento de dados, sendo necessário destinar uma parte específica à revogação de consentimento, esclarecendo-se ao titular o modo pelo qual poderá solicitá-lo, seja online, por e-mail, formulário digital ou até mesmo formulário físico, desde que assinado por ambas as partes.

Mesmo assim, de acordo com uma pesquisa do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, apenas 12% das plataformas preveem em seus termos de uso a possibilidade que, após o cancelamento da conta, os dados pessoais gerados pelos usuários ou coletados de outra forma serem excluídos. Ainda, 60% das plataformas sequer fornece informações sobre o assunto, ao passo que 10%

---

[16] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 jun. 2019.

[17] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 jun. 2019.

afirmam expressamente que não permitem a exclusão total dos dados, e, por fim, 18% fornece informações contraditórias nesse aspecto. Outro exemplo é o fato de que somente 62% das empresas possuem cláusulas exigindo consentimento dos usuários para o compartilhamento dos dados com fins comerciais.[18]

Tais dados refletem efetivamente como o setor de *Compliance* deverá ser extremamente ativo na aplicação da Lei, seguindo seus preceitos de zeladoria do cumprimento assertivo das Leis e procedimentos. Sem a devida fiscalização do setor e investimento na reformulação das minutas contratuais, processos e procedimentos, as empresas ficarão fadadas à uma crescente fiscalização e sanção por parte da Agência Nacional.

Se analisarmos bem, o atual modelo de consentimento se explicita pelos dados pessoais tornaram-se uma moeda que pode ser utilizada pelos indivíduos para acessar conteúdo online. Em outras palavras, para desfrutar de um serviço e não ser excluído de seu uso, o indivíduo consente que seus dados pessoais sejam acessados, processados e divulgados[19]. Em uma máxima popular, quando você não paga pelo uso do produto, o produto é você.

[18] BELLI, Luca; CAVALLI, Olga (org.). **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2019.

[19] BELLI, Luca; SCHWARTZ, Molly; LOUZADA, Luiza. Selling your soul while negotiating the conditions: from notice and consent to data control by design. **Health and Technology**, v. 7, p. 453-467, 2017. Disponível em: https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0185-3.pdf. Acesso em: 25 out. 2019.

3 COMPLIANCE E LGPD

Com as altas demandas de um setor de *compliance* nas empresas, seja por exigência dos órgãos públicos, como por exemplo o Ministério da Agricultura[20], seja pelo mercado, hoje poucas são as empresas que não possuem uma área destinada à conformidade em plena função.

Fugindo das premissas jurídicas, o setor acaba por englobar diversos assuntos, como responsabilidade social, contratação de fornecedores, ética, governança corporativa e até mesmo, sistemas da informação.

> A existência de um programa de compliance criará uma cultura em que essas práticas serão evitadas e, se ocorrerem, vão ser detectadas e corrigidas, com sanções que, em casos mais graves, podem significar, inclusive, pedido de abertura de um inquérito policial. Prevenindo, detectando e respondendo esses tipos de ocorrência, ficará mitigada a perda de receitas com tais pagamentos.[21]

Neste sentido, tão logo a LGPD foi promulgada, diversos foram os convites para grupos de trabalho, reuniões, palestras, workshops e discussões sobre o impacto desta no contexto empresarial, lideradas pelos principais nomes de direito digital do país, porém frequentados, em maioria, por empregados de *compliance* das empresas.

> Assim, ao ser criada uma nova legislação que acaba por afetar o tratamento de dados e a segurança das informações, compartilhadas entre as empresas e nela própria, a política de compliance precisa se adaptar às demandas que desta decorrem. Compliance constitui-se de um conjunto de práticas administrativas que objetivam assegurar a adesão da empresa à legislação em geral, a um código de conduta, políticas e princípios. Acontece não somente com medidas preventivas, mas implica também a atividade de detectar as violações e posteriormente responder, aplicando sanções às eventuais violações. Vale reiterar que compliance implica prevenir, detectar e responder.[22]

Será necessária a reflexão, e consequentemente a adaptação, das empresas no tocante à necessidade de um profissional focado no tema da lei para atuar junto

---

[20] PIRONTI, Rodrigo. O resgate da credibilidade pelo compliance e a exigência do Ministério da Agricultura. **Conjur**, 14 jun. 2018. Disponível em: https://www.conjur.com.br/2018-jun-14/pironti-exigencia-compliance-ministerio-agricultura. Acesso em: 30 jun. 2019.

[21] NEVES, Edmo Colnaghi. **Compliance Empresarial - o tom da liderança**. São Paulo: Trevisan Editora, 2018. [Minha Biblioteca].

[22] NEVES, Edmo Colnaghi. **Compliance Empresarial - o tom da liderança**. São Paulo: Trevisan Editora, 2018. [Minha Biblioteca].

ao Comitê de *Compliance*, se tornando o responsável por cuidar dos procedimentos internos relacionados ao tratamento de dados e segurança das informações, internas e externas, de que a empresa venha a lidar, sendo imprescindível uma ação multidisciplinar de *compliance*, com gestores, advogados e analistas de sistemas. Somente assim será possível começar a analisar os impactos efetivos da Lei no cotidiano das empresas.

Entretanto, a elaboração de um plano de governança de dados e a adoção de medidas de *compliance* deveriam estar sendo elaborados desde agora, para evitar consequências jurídicas negativas num futuro próximo, principalmente devido ao fator econômico estratégico.

O alinhamento das empresas frente às obrigações da lei, além de todo o impacto jurídico, também deve ser considerado como um investimento de ganho imediato, uma vez que se torna destaque na realização de novos modelos de negócios.

O estudo global Future Focus de 2019, realizado pela Iprospect, no qual foram entrevistados mais de 300 profissionais de marketing e líderes globais em um amplo espectro de marcas, denota que a busca pela confiança deve ser o principal objetivo das marcas, pois somente 26% acreditam que as empresas são transparentes no uso de seus dados pessoais; 88% dos gestores de marketing entrevistados tem a confiança de marca como sua prioridade para 2019; e 76% afirmam também que a confiança é importante para manter seus clientes consumindo sua marca.[23]

O aumento do nível de privacidade, segurança e tratamento de dados será encarado inicialmente como um diferencial competitivo, junto à um impacto mercadológico, posto que, no fundo, se torna uma estratégia de marketing, já que uma empresa pioneira no desenvolvimento de políticas e procedimentos atualizados, acabam por ter uma representatividade maior e sua reputação cresce no mercado.

Assim, os preceitos de ética e boa-fé, primordiais no funcionamento e manutenção de um programa de compliance efetivo e operante, se mostram essenciais na aplicação da LGPD, e, por consequência, na conduta quanto às obrigações decorrentes da Lei.

---

[23] NA ECONOMIA digital, confiança de marca se torna prioridade para os negócios, revela estudo da iProspect. **Crypto ID**, 14 mar. 2019. Disponível em: https://cryptoid.com.br/e-commerce-e-varejo/na-economia-digital-confianca-de-marca-se-torna-prioridade-para-os-negocios-revela-estudo-da-iprospect/. Acesso em: 01 out. 2019.

> Falar de ética implica falar de integridade, nome adotado para o programa de *Compliance* pela legislação nacional. Integridade é qualidade daquele que é íntegro, vale dizer, inteiro, que não se divide, que não adota uma postura em público e outra na esfera privada, que tem a mesma atitude, independentemente se está sendo observado ou não.[24]

Partindo do pressuposto de que, ao coletar um dado, as empresas deverão informar a finalidade e que somente se o usuário aceitar repassar suas informações, como ao concordar com termos e condições de um aplicativo, as companhias passam a ter o direito de tratar os dados respeitada a finalidade específica, há toda uma prerrogativa ética que terá de ser revista quanto ao cuidado com os dados recebidos, sejam eles de funcionários ou de terceiros.

No senso comum, não raro pode-se observar sendo formado o entendimento errôneo de ética como fosse esta uma tabela onde estivessem presentes todas as respostas de regimento das condutas humanas e indicado em colunas lado a lado o que se deve ou não fazer. E assim, a análise ética das condutas estaria condenada à simples classificação de cada conduta de acordo com a coluna na qual esta se enquadra. No entanto, a ética está longe de ser uma tabela pronta, uma vez que estamos a todo momento diante de novos desafios

> A existência de autoridades com alta expertise técnica, como os Data Protection Authorities (DPA) e o grupo de trabalho Article 29 Data Protection Working Party, seria outra evidência de uma racionalidade regulatória de risco, fundada no conhecimento técnico e na criação de obrigações de produção de informação sobre riscos ao setor privado (SUNSTEIN, 2002), como os “estudos de impacto à privacidade” (GELLERT, 2015, p. 11-12).20 Alessandro Spina, em ensaio recente para o European Journal of Risk Regulation, defende uma agenda de pesquisas capaz de unir “regulação do risco e governança dos dados”. Em argumento semelhante ao de Gellert (2015), Spina alega que, ao menos na União Europeia, está se testemunhando uma espécie de “risquificação” do direito de proteção de dados pessoais[25]

Assim como as organizações serão responsáveis no caso de incidentes no tratamento dos dados, estas também deverão aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação das informações.

---

[24] NEVES, Edmo Colnaghi. **Compliance Empresarial - o tom da liderança**. São Paulo: Trevisan Editora, 2018. [Minha Biblioteca].

[25] ZANATTA, Rafael. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. Encontro da Rede de Pesquisa em Governança da Internet, 1, 2017, Rio de Janeiro. **Anais [...]**. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2017. p. 175-193.

Desta forma, então, buscando o constante aprimoramento e manutenção das boas práticas, as empresas deverão se atentar aos limites do consentimento e dar a este seu real valor, evitando o uso descompensado desta alternativa jurídica que a LGPD trouxe e buscando outra base legal para amparar seu tratamento.

> Dependendo do ramo do negócio, da empresa e da maturidade da governança dos dados pessoais, é fundamental criar um programa de compliance digital, com risk assessment, planos de respostas a incidentes, treinamentos e comunicação, due diligence de terceiros em um contexto multissetorial dentro do negócio e com visão holística para a legislação nacional e internacional.[26]

Em tese, para uma empresa efetivamente se adequar às premissas da lei, deverá haver uma força tarefa dos mais diversos setores, visando a revisão e atualização da política de privacidade da companhia, estabelecendo a conformidade com as novas demandas jurídicas de proteção de dados pessoais; a atualização das cláusulas de contratos, destacando-se as cláusulas de contratos com os parceiros e fornecedores que realizam algum tipo de tratamento de dados; o mapeamento do fluxo de dados para mapear, junto a TI, os controles de consentimento e seus possíveis desdobramentos; o modelo de resposta para a ANPD, a respeito do nível de *Compliance* da empresa para prevenção contra multas e fiscalizações e uma listagem modelo para novos fornecedores e parceiros.

Assim, o setor de *compliance* mostra-se indispensável para assegurar tal adequação de maneira uníssona entre as diversas áreas de uma empresa, cabendo a ele o poder de auditar, zelar e monitorar o cumprimento das obrigações legais e extralegais.

---

[26] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD.** São Paulo: Saraiva, 2018. [Minha Biblioteca].

4 CONSIDERAÇÕES FINAIS

Demonstrada a importância da proteção dos dados pessoais no cenário atual, são diversas as implicações de que a Lei Geral de Proteção de Dados Pessoais trará para diversos setores da empresa.

Desta forma, as empresas terão que disponibilizar não somente recursos financeiros, mas também empregados para buscar a adequação a lei, antes que esta seja efetivamente válida no território brasileiro.

Neste sentido, a área de *compliance* se evidencia essencial para o bom funcionamento e gerenciamento da interdisciplinaridade tratada na lei, através de seus principais pilares: ética, integridade, gestão e comprometimento.

> Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de compliance digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura.[27]

Nos vemos diante de um cenário de avanço desenfreado da tecnologia e com um tráfego de informações pessoais aumentando cada dia mais. Prefere-se um aplicativo gratuito, que acabe tendo acesso à contatos, microfone, câmera, atividades, do que se pagar noventa e nove centavos para um aplicativo que não consumirá tais dados, não se perguntando como tais dados serão utilizados pelas empresas.

Agora a indagação se norteia em como as empresas poderão utilizar-se legalmente das informações recebidas, sem violar a intimidade de seus clientes, consumidores e usuários, e concomitantemente, como resguardar tais informações de acessos indevidos, sejam estes hackers ou funcionários sem a devida autorização para tratamento dos dados.

Assim, as empresas terão que se preocupar não somente como serão utilizadas as informações pessoais que recebem e tratam, mas também com a proteção de tais informações frente à má-fé de outros.

Desta forma, tal qual ocorrido na União Europeia, que cada vez mais se mostra exemplo – em sanções e aplicação da GDPR – todas as empresas brasileiras que

---

[27] PINHEIRO, Patrícia Peck. **Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD.** São Paulo: Saraiva, 2018. [Minha Biblioteca]. PINHEIRO, Patrícia Peck. *Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD*. [Minha Biblioteca].

tratem dados assumem uma responsabilidade para estarem aptas ao princípio da transparência, ética e integridade tão defendido no setor de *compliance*. Mais do que nunca, o *compliance* deixa de ser uma área acessória da empresa para uma área chave para o desenvolvimento de ações mitigatórias de combate a exposições desnecessárias e possível perda de capital no cenário empresarial brasileiro.

REFERÊNCIAS

BELLI, Luca; CAVALLI, Olga (org.). **Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2019.

BELLI, Luca; SCHWARTZ, Molly; LOUZADA, Luiza. Selling your soul while negotiating the conditions: from notice and consent to data control by design. **Health and Technology**, v. 7, p. 453-467, 2017. Disponível em: https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0185-3.pdf. Acesso em: 25 out. 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – a função e os limites do consentimento**. Rio de Janeiro: Grupo GEN, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 27 jun. 2019.

BRASIL. **Medida Provisória n° 870, de 2019**. Organização da Presidência e dos Ministérios. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135064. Acesso em: 25 out. 2019.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 22.337/RS**. Relator: Min. Ruy Rosado de Aguiar, 20 mar. 1995.

BRUNA, Sérgio Varella. A LINDB e a entrada em vigor da Lei de Proteção de Dados. **Jota**, 10 jan. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lindb-e-a-entrada-em-vigor-da-lei-de-protecao-de-dados-10012019. Acesso em: 25 out. 2019.

GAVIOLI, Allan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. **Infomoney**, 10 out. 2019. Disponível em: https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/. Acesso em: 25 out. 2019.

MAGALHÃES, F.; PEREIRA, M. **Regulamento Geral de Proteção de Dados**: Manual Prático. 2. ed. Porto: Vida Económica, 2018.

NA ECONOMIA digital, confiança de marca se torna prioridade para os negócios, revela estudo da iProspect. **Crypto ID**, 14 mar. 2019. Disponível em: https://cryptoid.com.br/e-commerce-e-varejo/na-economia-digital-confianca-de-marca-se-torna-prioridade-para-os-negocios-revela-estudo-da-iprospect/. Acesso em: 01 out. 2019.

NEVES, Edmo Colnaghi. **Compliance Empresarial - o tom da liderança**. São Paulo: Trevisan Editora, 2018. [Minha Biblioteca].

PAYÃO, Felipe. Site 'Não Me Perturbe' vaza chave de email que permite ataque hacker. **Tecmundo**, 16 jul. 2019. Disponível em https://www.tecmundo.com.br/seguranca/143865-site-nao-me-perturbe-vaza-chave-email-permite-ataque-hacker.htm. Acesso em: 25 out. 2019.

PEREIRA, Jane Reis Gonçalves. **Interpretação constitucional e direitos fundamentais**. São Paulo: Saraiva, 2018. [Minha Biblioteca].

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD.** São Paulo: Saraiva, 2018. [Minha Biblioteca].

PIRONTI, Rodrigo. O resgate da credibilidade pelo compliance e a exigência do Ministério da Agricultura. **Conjur**, 14 jun. 2018. Disponível em: https://www.conjur.com.br/2018-jun-14/pironti-exigencia-compliance-ministerio-agricultura. Acesso em: 30 jun. 2019.

ROQUE, André. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). **Revista Eletrônica de Direito Processual**. Rio de Janeiro, ano 13, v. 20, n. 2, maio/ago. 2019.

SERASA EXPERIAN. 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais, mostra pesquisa da Serasa Experian. 08 ago. 2019. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian. Acesso em: 25 out. 2019.

VALENTE, Jonas. Lei de Proteção de dados traz desafios a empresas, cidadãos e governo. **Agência Brasil**, 25 ago. 2019. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo. Acesso em: 01 out. 2019.

VIDOR, Daniel Martins. LGPD: origem e implicações. **Blog Mercury.** [*S.l.*], 19 mar. 2019. Disponível em: http://mercurylbc.com/lgpd-origem-e-implicacoes/. Acesso: 25 out. 2019.

ZANATTA, Rafael. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. Encontro da Rede de Pesquisa em Governança da Internet, 1, 2017, Rio de Janeiro. **Anais [...]**. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2017. p. 175-193.