EFEITOS E PROJEÇÕES SOBRE A VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O PAPEL DO ENCARREGADO DOS DADOS PESSOAIS

RESUMO

O cenário mundial vem mudando em relação a proteção de dados pessoais. Era comum, até pouco tempo atrás, empresas vendendo banco de dados, e outras trabalhando com as informações contidas nesses bancos para criação de perfis e gerando soluções que buscam ser atraentes para clientes vulneráveis à tecnologias como: Big Datas, inteligência artificial, dentre outras. Visando proteger a privacidade dos cidadãos através do mundo, foram criadas (e/ou ampliadas) leis que reforçam esta proteção. No Brasil, especificamente, criou-se Lei Geral de Proteção de Dados Pessoais (LGPD). Esta pesquisa visa analisar essa lei, bem como conhecer outras leis que "gravitam" em torno dela, com o objetivo de conhecer o impacto da aplicação da lei na rotina empresarial e, como objetivo específico, qual será o papel do encarregado de dados pessoais nas organizações. Utilizando uma pesquisa descritiva e aplicada, as análises apontam para uma necessidade de mudança cultural nas organizações que deverão criar uma equipe multidisciplinar visando gerenciar toda a segurança das informações da empresa. Equipe essa liderada pelo "encarregado de dados pessoais", função criada pela LGPD.

Palavras Chave: LGPD; Encarregado de Dados pessoais; Segurança da Informação

EFFECTS AND PROJECTIONS OF THE VALIDITY OF THE GENERAL DATA PROTECTION LAW (LGPD) AND THE ROLE OF THE DATA PROTECTION OFFICER

ABSTRACT

The world scenario is changing when we talk about personal data protection. Until a few time ago, it was common find companies that sold databases, and others companies worked with the information contained into these databases, aimed to create profiles and generate solutions, using technologies such as Big Datas, artificial intelligence, among others, looking to be attractive and get more customers. In order to protect the privacy of citizens across the world, laws have been created (and / or expanded) to reinforce this protection. In Brazil, specifically, was created the Lei de Proteção de Dados Pessoais (LGPD) . This research aims to analyze this law, as well as to know other laws that "gravitate" around it, with the objective of knowing the impact of law enforcement on business routine and, as a specific objective, what will be the role of the person in charge of personal data in organizations. Using descriptive and applied research, the analyzes point to a need for cultural change in organizations that should create a multidisciplinary team aiming to manage all the security of company information. This team is led by the DPO (Data Protection Officer), a function created by LGPD.

Keywords: LGPD; Data Protection Officer; Security Management

INTRODUÇÃO

É uma preocupação mundial nos dias de hoje a proteção de dados pessoais, principalmente após alguns incidentes como os acontecidos na empresa Cambridge Analytica, em que dados

pessoais foram utilizados para fomentar a eleição dos Estados Unidos da América no ano de 2016. Esta empresa demonstrou usar utilizar, técnica que vem se tornando comum, com os conceitos de Big Data e Mineração de dados, para analisar informações, criar perfis e alinhar estrategicamente estas informações aos interesses das organizações. Tudo isso visa elevar o faturamento e performance empresarial.

Essas tecnologias trouxeram consigo vários benefícios para as empresas. Porém, toda tecnologia, quando utilizada para outros fins podem ser prejudiciais. Nesse caso específico, como pode ser visto no *site Information is Beautiful*[1], vários são os incidentes de segurança que expõem dados de cidadãos ao redor do mundo, consequência da falta de planejamento de segurança, ou até mesmo do modo de utilização dos dados existentes.

Nesse contexto, pensando na proteção à privacidade, vários países promulgaram leis com o escopo de coibir este tipo de atitude por parte das empresas e pessoas mal intencionadas. No Brasil, em agosto de 2018, foi promulgada a Lei 13.709, chamada Lei Geral de Proteção de Dados Pessoais (LGPD), na qual foram descritas as "regras de conduta" que as pessoas, sejam naturais ou jurídicas, deverão seguir, caso não queiram sofrer sanções, que podem ser duras, caso a empresa não se adeque às suas exigências.

Implantar o *compliance* à esta lei deve ser um trabalho de uma equipe multidisciplinar, que leve em consideração as áreas de gestão, segurança da informação, tecnologia da informação e comunicações (TIC) e jurídica. Cada área terá uma contribuição importante para adequação, sendo difícil que apenas uma delas solucione as demandas das organizações.

Este trabalho faz um estudo da necessidade de haver uma conexão entre a áreas de gestão e segurança da informação com os efeitos e projeções sobre a vigência da LGPD no ordenamento jurídico brasileiro. A LGPD está diretamente conectada a diversas outras leis brasileiras e, somente conhecendo o impacto, será possível traçar um plano de ação visando mitigar os riscos existentes no negócio da organização.

O objetivo da pesquisa é conhecer as mudanças necessárias nas organizações para implantar o compliance à LGPD. Como objetivo específico, buscou-se analisar o papel do encarregados de dados pessoai (função criada pela lei) no momento e após a implantação do Compliance.

METODOLOGIA

[1] Disponível em https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Como metodologia de pesquisa, foi elaborada uma pesquisa aplicada, no intuito de conhecer o impacto nas organizações na adoção da LGPD e o papel dos encarregados neste momento. Através estudo descritivo, utilizou-se uma análise bibliográfica e documental na leitura de artigos, legislação pertinente a área, livros e sítios especializados.

Optou-se pela pesquisa qualitativa pois, segundo Gerhardte e Silveira (2009, pg. 31), "não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, etc". Segundo os autores, ao se utilizar a metodologia qualitativa, o pesquisador será ao mesmo tempo sujeito e objeto de suas pesquisas. Para eles o objetivo da amostra é produzir informações aprofundada e ilustrativas, sendo importante que nessa interação ela gera novas informações.

Assim foi possível na análise realizada, conhecer as leis que "gravitam" em torno da LGPD e o impacto que este arcabouço legal trará para as organizações. Alinhada a esta análise, realizou-se uma pesquisa bibliográfico no intuito de conhecer as melhores práticas de segurança, bem como entender o papel do encarregado de dados pessoais no momento da implantação e na rotina empresarial.

EVOLUÇÃO REGULATÓRIA: ASPECTOS DAS CONTRIBUIÇÃO DA GENERAL DATA PROTECTION REGULATION (GDPR) PARO MARCO DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

Entre os anos de 1973 e 1974 a União Europeia já se ocupava em estabelecer parâmetros para a proteção de dados, haja vista as resoluções 22 e 29. Avançando um pouco mais, em 1995 a diretiva 95/46/EC concernente ao processamento de dados foi aprovada, e exigia que cada país membro da União Europeia tivesse

> uma agência ou comissão de proteção de dados, este último um agente estatal que supervisione a aplicação dos princípios e leis de proteção à privacidade individual, Ela também exige que cada uma deles edite leis sobre o processamento de dados pessoais. (REINALDO FILHO, Demócrito, 2013

Durante 20 anos a diretiva 95/46/EC foi um dos documentos mais importantes no tocante aos avanços voltados à proteção de dados, entretanto, diante disso e de novas necessidades em um universo cada vez mais digital em que a demanda é crescente por atualizações, abriu-se o cenário ideal para que uma lei mais atualizada e abrangente figurasse no panorama europeu.

> O primeiro instrumento internacional disciplinado especificamente essa temática com força legal, aberto a membros e não membros da Comunidade Europeia. - 1995: Diretiva 95/46/CE. (...) Essa diretiva foi por mais de 20 anos, o principal documento internacional sobre o assunto (VAINZOF, Rony, 2019, p. 21)

Foi então que no ano de 2016 a General Data Protection Regulation foi legislada, entrando em vigor dois anos depois, em maio do ano de 2018. Segundo VAINZOF (2019) a regulação 2016/679 (UE) entrou em vigor no dia 25/5/2018, substituindo a diretiva 95/46/CE, bem como as leis e regulações nacionais nela baseadas. Para GOMES (2018) a GDPR é o "maior conjunto de proteção à privacidade online já criado desde o início da internet".

No âmbito empresarial, MOREIRA (2017) destacou que a resolução europeia oferece um rico substrato para que as entidades/empresas afetadas possam pautar sua atuação com considerável segurança jurídica.

A evolução regulatória no Brasil até o marco da LGPD sofreu muitos percalços e foi inspirada na general data protection regulation (GDPR). Segundo REINADO FILHO (2013)

> "a partir das décadas de 60 e 70, com o advento das tecnologias da informação. O grande poder de processamento de dados pelos computadores foi o fator responsável pela germinação da moderna legislação nessa área. O aumento do poder de controle e processamento de dados prontamente desencadeou a demanda por uma legislação específica para regular a coleta e manuseio de informações pessoais." (REINALDO FILHO, 2013)

Desde então, a crescente necessidade por uma legislação mais específica e que fosse ao encontro das legislações internacionais como a GDPR favoreceram o desenvolvimento da mencionada lei. No Brasil havia até o marco da LGPD algumas normas que tratavam sobre a proteção de dados, entretanto a sua promulgação significou um avanço histórico para o país.

> "A promulgação da lei é um marco para o Brasil já que anteriormente não existia legislação específica sobre proteção de dados. O que existiam eram algumas normativas esparsas, como o Código de Defesa do Consumidor, a lei do Cadastro Positivo e a lei 12.965/14 que ficou conhecida popularmente como o Marco Civil da Internet e que foi parcialmente alterada pela LGPD". (SANTIAGO & TAMBA, 2018)

Pensar em uma lei de proteção de dados que esteja em conformidade com o cenário mundial é uma ferramenta que contribui para o avanço da economia, favorecendo o diálogo com outros países.

> "Seguindo o modelo do GDPR, a LGPD busca criar um quadro normativo moderno, incluindo o Brasil no rol de países e organismos internacionais aptos a proporcionar um grau de proteção de dados pessoais considerado adequado pelos padrões internacionais". (BENTO, 2018)

> "tendo se inspirado em muitos aspectos no regulamento europeu General Data Protection Regulation, ou GDPR, que entrou em vigor em maio de 2018. Esta influência decorre, entre outros motivos, da intenção de incluir o Brasil no rol de países que proporcionam um grau de proteção de dados pessoais adequado conforme parâmetros internacionais". (SANTIAGO & TAMBA, 2018).

Sabe-se que a LGPD atingirá todos os setores que atuam com o tratamento de dados pessoais, e que a necessidade de compreender e adequar a realidade das empresas à nova legislação possui caráter imediato, visto que, embora tenha, como a GDPR proporcionado um período de

adequação de 24 meses, está prevista para entrar em vigor no mês de agosto de 2020 mudando drasticamente a forma de coleta e armazenamento de dados no país. E para efeito da lei, importante salientar que segundo a LGPD tratamento de dados é

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (Art. 5, X, in verbis)

Ou seja, o simples fato de coletar uma informação pessoal, já traz para as organizações a necessidade de adequação a LGPD.

Visando entender portanto a abrangência da LGPD, foi realizada uma análise da conexão desta com outras legislações.

A LGPD À LUZ DOS DIREITOS FUNDAMENTAIS (CR/88)

A Lei Geral de Proteção de dados (LGPD) tem como um de seus escopos principais a proteção dos direitos fundamentais da pessoa natural previstos na Constituição da República de 1988, em seu artigo 1º tal anteparo é descortinado pelo legislador no seguinte extrato "com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Observa-se que os direitos supramencionados compõem a essência da lei 13.709/18. O direito fundamental da liberdade, segundo FERNANDES (2017), "pode ser compreendido como autonomia (capacidade de autodirigir sua vida e suas escolhas a partir da razão)".

A CR/88 em seu artigo 5º, X, elenca diversos direitos relacionados à proteção da vida pessoal da pessoa natural, destacando-se no âmbito da LGPD a intimidade a imagem e a vida privada. "Assim, o direito à privacidade é explicado como um direito que um indivíduo tem de se destacar (se separar) de um grupo, isolando-se da observação dele ou como, ainda, o direito ao controle das informações veiculadas sobre si mesmo." (FERNANDES, 2017, p. 487)

A Declaração Universal de Direitos Humanos (1948), em seu artigo XII traz luz à necessidade da proteção do direito à privacidade individual da pessoa natural ao dizer que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

Mister salientar que os direitos fundamentais embora não sejam renunciáveis em sua totalidade, podem ser limitados dentro da proporcionalidade, "por isso, também, é que se compreende a necessidade de regular o direito à privacidade sob uma perspectiva econômica, focada (...) no

fluxo internacional de dados – um elemento fundamental para a economia globalizada dos séculos XX e XXI" (VAINZOF, 2019, p. 22).

Desse modo, ainda segundo o autor supramencionado a lei 13.709/18:

> "busca a proteção de direitos e garantias fundamentais da pessoa natural, equilibradamente, mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais". (VAINZOF, 2019, p. 23)

As inovações trazidas pela lgpd na adaptação do cenário empresarial e jurídico, aliadas às novas figuras responsáveis pelo tratamento de dados pessoais

A LGPD tem como função precípua a de garantir que os direitos fundamentais, especialmente os por ele elencados, sejam efetivamente protegidos. Para tanto, traz como definição da dados pessoais "informação relacionada a pessoa natural identificada ou identificável". Que chama atenção para o temor identificável, pois ao contrário que se pode imaginar, algo que leve o titular dos dados também será considerado como dado pessoal, como por exemplo placas de automóveis, número de telefone celular, dentre outros; e como dados pessoais sensíveis "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural", em outras palavras tudo aquilo que possa dar origem a um ato discriminatório.

Visando cuidar dos temas, o seu artigo 5º coloca ainda em cena três importantes figuras que estão intrinsecamente ligados a tal garantia, quais sejam, os agentes de tratamento, controlador e operador (Art 5º, IX) e o encarregado.

Entende-se por controlador a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Art 5º, VI) e operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Art. 5º, VII).

Há também a figura do encarregado, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (Art. 5º, VIII). Isto é, o controlador, operador e encarregado formam uma tríade, na qual o primeiro é responsável pelas decisões de tratamento, o segundo realiza o tratamento e o terceiro é o canal de comunicação entre os primeiros e os titulares dos dados pessoais.

É necessário chamar atenção ao papel do encarregado. Anteriormente foi visto o conceito de tratamento de dados. Diante do exposto, fica explícita a necessidade de adequação dos profissionais que lidam com o tratamento de uma adequação de conceitos e processos. Tornou-se importante que os profissionais de segurança da informação, bem como os demais envolvidos no tratamento de dados (em especial o profissional de TI), entendam que os dados não poderão mais serem utilizados como dantes, uma vez que lei dá o direito dos titulares não querer mais seus dados no banco da dados da empresa. A não ser que se encaixe em uma das justificativa elencada na LGPD, deverá ser dado o consentimento pelo titular (regra básica de tratamento), mas que o poderá ser retirado no momento que o titular julgar necessário.

Nesse ponto entra uma reflexão em relação a esse profissional que ficará responsável por "responder" (ser responsável) pelos dados pessoais. Este será, sem dúvida, um dos papéis mais importantes (e desafiador) em todo esse processo novo. Esse profissional (o encarregado) irá liderar o processo de adequação à lei. Ele deverá conhecer a fundo as necessidades do negócios, os processos, as pessoas que tratarão os dados, a lei, para permiti-lo criar uma política de segurança que esteja em compliance com a lei, mas não seja um impeditivo para as regras do negócio.

Segundo Pessoa (2016), esse alinhamento estratégico dependerá muito de uma mudança de visão dos gestores das organizações. É preciso no primeiro momento pensar no negócio, nas informações necessárias e demandas pelos tomadores de decisão, conhecer as pessoas envolvidas (bem como seu nível de conhecimento técnico e de gestão). Só então deverão estudar as ferramentas eletrônicas que suportarão o negócio. Segundo o autor, é comum encontrar profissionais que invistam primeiro na tecnologia e depois tentam adequar o negócio à ela. Em se tratando de tratamento de dados pessoais, à luz da LGPD, seria um suicídio empresarial. Isso porque a LGPD traz em sua gênese a necessidade de transparência. Com isso o titular terá o direito de, a qualquer momento, conhecer os seus dados tratados para poder modificá-los (acrescentando ou mudando dados inconsistentes) e até mesmo exigir que sejam apagados. Surge aqui o perigo de tecnologias modernas como Blockchain e Bigdata, que poderão criar um grande desafio aos gestores de TI no momento de eliminar e/ou tratar a informação visando, por exemplo, criação de perfis para atuação no marketing.

Será então necessário um esforço multidisciplinar de uma equipe de gestão, liderada por esse profissional, sob pena de uma das áreas (gestão, segurança da informação, TI ou jurídica) ficar descoberta, o que levaria o processo de compliance a lei ao fracasso.

A segurança, as boas práticas e sigilo de dados, o elo entre compliance e tecnologia da informação na aplicação da LGPD

O capítulo VII da LGPD trata da segurança e boas práticas, mais especificamente em seu artigo 46, aborda a obrigação legal dos agentes de tratamento, para que a segurança supramencionada seja garantida

> "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". (Artigo 46, Lei 13.709/18).
> "Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término". (Artigo 47, Lei 13.709/18).

Embora a lei faça reiteradamente menção ao termo "segurança da informação" não realiza sua definição, como ocorre em outros artigos à exemplo os agentes de tratamento. Mister esclarecer diante de tal omissão da lei que

> "segurança da informação é a disciplina voltada à proteção da informação, considerada um ativo do negócio – ou seja, aquilo que tem valor para a entidade – dos diferentes tipos de ameaças internas e externas (eventos que podem ter impactos negativos, como empregados mal intencionados, ataques cibernéticos, espionagem, concorrência desleal, fraudes digitais etc.) para mitigar os riscos, aumentar o retorno sobre os investimentos e garantir a continuidade do negócio". (JIMENE, 2019, p. 339).

Para que a segurança da informação ganhe aplicabilidade tem-se se a ideia de que os esforços dos agentes de tratamento são primordiais, entretanto é necessário um esforço em conjunto para a garantia da efetividade da segurança, entendida pela lei como a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Artigo 6º, VIII).

Em continuidade, a referida autora entende que:

> "medidas técnicas são aquelas adotadas no âmbito da Tecnologia da Informação, como o uso de recursos informáticos dotados de funcionalidades voltadas a garantia da segurança da Informação. São exemplos dessas tecnologias: ferramentas de autenticação de acesso ao sistema, mecanismos de segurança em software e hardware, recursos de controle de tráfego de dados em rede, instrumentos detectores de invasões de sistemas, recursos de criptografia." (JIMENE, 2019, p. 329)

Mister salientar que no tocante a citação do autor em supra, entende-se que não se limita apenas ao âmbito tecnológico, visto que a Lei Geral de Proteção de Dados também visa a proteção de dados que estejam no mundo físico, à exemplo, o papel, quando traz em seu artigo 1º que a lei "aplica-se a toda informação, inclusive papel".

A norma ISO/IEC ABNT 27.002 (2013, pg. X) diz que "A informação pode existir em diversas forma. Ela pode ser impressa, ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas." E vai além ao dizer que segurança da informação, por tudo isso é "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". É portanto algo que deve ser analisado com muito detalhe.

Portanto, como dito anteriormente, o papel do encarregado é de grande responsabilidade. Apesar da LGPD não esclarecer o conceito, ela diz claramente que deverá haver investimentos no setor, focada nas melhores práticas de segurança da informação. E como visto no conceito da ISO 27.002, segurança da informação está totalmente ligada ao negócio.

Destarte, visando o sucesso da implantação, é fundamental reforçar a necessidade uma equipe multidisciplinar que abrange quatro grande grupos de conhecimento a saber: gestão, segurança da informação, tecnologia da informação e comunicação e jurídica. Tudo isso, dificilmente, será encontrada só na função do encarregado (em somente uma pessoa). Esse profissional deverá, indubitavelmente, ser o líder de um grupo de profissionais que terá essa missão nas organizações. É primordial conhecer os processos envolvidos nos tratamento das informações, conhecer as normas e melhores práticas de segurança informação, conceitos do ciclo da informação dentro da organização, realizar análise de riscos, conhecer as ferramentas tecnológicas que suportarão dos os processos e serviços da empresa e também toda a legislação envolvida para estar em compliance legal. Somente assim poderá ser feito um planejamento que envolva toda a informação da empresa, seja ela eletrônica ou física (papel), uma vez que como já foi dito, a lei também se aplica a informações físicas e todo o legada da organização. Nunca é demais lembrar que, o encarregado, deverá ter apoio irrestrito da alta gestão da organização, pois deverá ter autonomia necessária para as tomadas de decisão.

No que concerne às medidas administrativas, elas estão apontadas para a prática gerencial e jurídica dos agentes de tratamento, tais medidas são aquelas entendidas como, políticas da empresa voltadas para a proteção de dados, políticas de privacidade, código de ética e conduta, etc.

Em suma, para que as empresas estejam adequadas a cumprir fielmente a obrigação emanada pela lei, não é suficiente que os agentes de tratamento, bem como o encarregado estejam cientes de suas funções, é necessário a integração dos setores (e profissionais) para que se alcance o objetivo da lei, tendo em vista que o seu não cumprimento poderá e irá acarretar a aplicação de sanções administrativas e de responsabilidade civil. Conforme entendimento de Cots e Oliveira

(2019) “não se trata de faculdade: é uma obrigação legal que, se não cumprida poderá ensejar a aplicação de sanções administrativas e responsabilidade civil”.

A política de segurança da informação deverá ser construída com conceitos das áreas elencadas, sob pena de, caso falte um deles, tornar-se inútil no momento da aplicação na empresa, ou de defesa de um possível contencioso.

A responsabilidade civil na lei geral de proteção de dados

Obedecendo princípios legais e constitucionais, a LGPD vem para transformar todo o contexto que envolve o tratamento de dados pessoais de cidadãos brasileiros. No silêncio normativo, tem sido fácil, para aqueles que coletam, se respaldarem em contratos de adesão que versam sobre termos de privacidade de forma genérica e ininteligível, deixando o consumidor, titular dos dados, sem outra saída que não seja o consentimento. O vigor da LGPD suprime essa possibilidade, garantindo maior transparência e objetividade no consentimento e nas outras nove hipóteses que legitimam o tratamento de dados pessoais, arroladas exaustivamente em seu artigo 7º.

> O primeiro aspecto a ser considerado diz respeito às circunstâncias em que esta aceitação ocorre. Formuladas a partir de um modelo de adesão, onde ao usuário só cabe aceitar os termos que lhe são apresentados, podendo acessar o serviço, ou rejeitá-los, no que lhe será negado o acesso. Muito embora este modelo de manifestação de vontade não seja novo, eis que apenas replica no meio eletrônico os contratos de massa surgidos na sociedade industrial, há de se considerar que já existiam ali inúmeras ressalvas quanto à validade e alcance da manifestação volitiva nestas circunstâncias. (PAULINO, 2015, p.10)

> Existe também a questão do consumidor estar sujeito a um contrato de adesão na maioria absoluta das plataformas, que tem como característica primordial a prevalência do fornecedor, que redige o contrato, sobre o consumidor, que apenas aceita os termos. Esses contratos de adesão digitais em regra são expostos em uma janela separada nos navegadores, de maneira pouco destacada, e mesmo que o consumidor queira ler, o contrato é incompreensível para ele[...]. (SCHMIDT, 2018, p.38)

A LGPD, em seu artigo 8º, incumbe ao controlador o ônus da prova de que o consentimento foi obtido dentro dos ditames legais. Este consentimento, que “deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular”, será destinado a finalidades específicas, sob pena de nulidade. A lei determina ainda o direito à revogação a qualquer momento por manifestação expressa do titular, e que, para tanto, o procedimento será gratuito e facilitado. Cabe aqui salientar que, conforme o inciso IV do artigo 15, o tratamento de dados também poderá ser interrompido por determinação da autoridade nacional, se violadas as regras da referida lei.

Comparando o disposto na lei nº 12.965/14, conhecida como o Marco Civil da Internet, em seu artigo 11, caput, e o disposto no artigo 3º da lei nº 13.709/18 de que trata o presente estudo, é possível notar a maior preocupação do legislador em proteger o titular dos dados, no tocante à abrangência da LGPD. Enquanto aquela limita-se a operações com atos realizados no território nacional, esta aplica-se independentemente do país onde realizam-se os atos, desde que o titular dos dados esteja em território nacional.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (Lei n.12.965 de abril de 2014)
>
> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - 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
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (Lei n.13.709 de agosto de 2018)

Faz-se necessário porém, visando um bom entendimento do tema, estudar o consentimento do titular.

O consentimento do titular

Obedecendo princípios legais e constitucionais, a LGPD vem para transformar todo o contexto que envolve o tratamento de dados pessoais de cidadãos brasileiros. No silêncio normativo, tem sido fácil, para aqueles que coletam, se respaldarem em contratos de adesão que versam sobre termos de privacidade de forma genérica e ininteligível, deixando o consumidor titular dos dados sem outra saída que não seja o consentimento. O vigor da lei LGPD suprime essa possibilidade, garantindo maior transparência e objetividade no consentimento e nas outras nove hipóteses que legitimam o tratamento de dados pessoais, exaustivamente arroladas em seu artigo 7º.

> O primeiro aspecto a ser considerado diz respeito às circunstâncias em que esta aceitação ocorre. Formuladas a partir de um modelo de adesão, onde ao usuário só cabe aceitar os termos que lhe são apresentados, podendo acessar o serviço, ou rejeitá-los, no que lhe será negado o acesso. Muito embora este modelo de manifestação de vontade não seja novo, eis que apenas replica no meio eletrônico os contratos de massa surgidos na sociedade industrial, há de se considerar que já existiam ali inúmeras ressalvas quanto à validade e alcance da manifestação volitiva nestas circunstâncias. (PAULINO, 2015, p.10)
>
> Existe também a questão do consumidor estar sujeito a um contrato de adesão na maioria absoluta das plataformas, que tem como característica primordial a prevalência

> do fornecedor, que redige o contrato, sobre o consumidor, que apenas aceita os termos. Esses contratos de adesão digitais em regra são expostos em uma janela separada nos navegadores, de maneira pouco destacada, e mesmo que o consumidor queira ler, o contrato é incompreensível para ele[...]. (SCHMIDT, 2018, p.38)

Importante observar a dispensa do consentimento para tratamento de "dados tornados manifestamente públicos pelo titular", prevista pelo parágrafo quarto do referido artigo, o que não exclui os demais direitos e princípios por esta lei reconhecidos. Porém, em contrapartida a isso, os ministros do STJ em decisão unânime[2], decretou que "bancos de dados que compartilham informações de consumidores devem informá-los previamente acerca da utilização desses dados, sob pena de terem que pagar indenização por danos morais". A decisão vai além ao dizer que, mesmo que o titular tenha divulgado seus dados em redes públicas, não quer dizer que foi dado o consentimento do uso. Como base legal foi usado o artigo 5º da constituição federal ao "qual assegura ao cadastrado o direito de ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais". Nota-se portanto que a LGPD só reforça o que outras leis já trazem em seu conteúdo mas, que até então, passava despercebido, talvez por não haver um foco na discussão.

Prestigiando a transparência da atividade, a lei garante conhecimento facilitado do titular sobre informações relativas ao tratamento, e, dentre elas, elege quatro a serem obrigatoriamente a ele comunicadas no caso de alterações. Elencadas nos incisos I, II, III e V do artigo 9º, são elas: a finalidade específica, forma e duração, identificação do controlador e o uso compartilhado de dados pelo controlador. Com isso, o titular dos dados terá maior consciência sobre o que está sendo feito com seus dados, garantido o direito à revogação do consentimento uma vez insatisfeito com as alterações do contrato ou regulamento.

A LGPD, em seu artigo 8º, incumbe ao controlador o ônus da prova de que o consentimento foi obtido dentro dos ditames legais. Este consentimento, que "deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular", será destinado a finalidades específicas, sob pena de nulidade. A lei determina ainda o direito à revogação a qualquer momento por manifestação expressa do titular, e que, para tanto, o procedimento será gratuito e facilitado. Cabe aqui salientar que, conforme o inciso IV do artigo 15, o tratamento de dados também poderá ser interrompido por determinação da autoridade nacional, se violadas as normas legais.

A responsabilidade civil e as sanções administrativas na LGPD

[2] Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Compartilhamento-de-informacoes-de-banco-de-dados-exige-notificacao-previa-ao-consumidor.aspx

Comparando o disposto na lei nº 12.965/14, conhecida como o Marco Civil da Internet, em seu artigo 11, caput, e o disposto no artigo 3º da lei nº 13.709/18 de que trata o presente estudo, é possível notar a maior preocupação do legislador em proteger o titular dos dados, no tocante à abrangência da LGPD. Enquanto aquela limita-se a operações com atos realizados no território nacional, esta aplica-se independentemente do país onde realizam-se os atos, desde que o titular dos dados esteja em território nacional.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (Lei n.12.965 de abril de 2014)
>
> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - 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
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. (Lei n.13.709 de agosto de 2018)

Contudo, a preocupação do legislador vai muito além da maior abrangência. O verdadeiro destaque dentre as inovações inseridas pela LGPD, verifica-se nas penalidades que passam pela responsabilidade civil por danos causados, chegando às sanções administrativas. Essas medidas coercitivas são mecanismos que visam assegurar a eficácia da norma. A multa prevista, que poderá alcançar o valor de 50 milhões de reais por infração, representa grande provocação aos agentes e gestores para que busquem estar em *compliance* com esta lei.

No artigo 42 está prevista a obrigação do controlador ou operador de reparar os danos por ele causados em razão do exercício da atividade de tratamentos de dados pessoais violando a legislação de proteção de dados. Tal responsabilidade engloba, expressamente, o dano moral, patrimonial, individual e coletivo. A responsabilidade do operador é solidária quando descumprir suas obrigações legais ou não seguir instruções lícitas do controlador, nesse caso, equipara-se ao controlador. Os controladores diretamente envolvidos no tratamento também respondem solidariamente. É garantida àquele que repara o dano, ação regressiva na medida de sua responsabilidade pelo evento danoso.

> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. (art.42, lei n.13.709 de agosto de 2018)

Exime-se da responsabilidade o agente que provar não ter realizado o tratamento a ele atribuído, não haver vício de legalidade no procedimento ou a culpa exclusiva do titular ou de

terceiro pelos danos. Mais uma vez faz-se necessário um planejamento da implantação, baseado em gestão eficaz da informação, pois será necessário criar um laudo de auditoria que consiga comprovar, de fato, a inexistência do tratamento, ou caso exista, como é feito todo o tratamento dos dados pela organização, de forma transparente.

Vale frisar que a sanção em esfera cível não exclui a possibilidade das sanções administrativas aplicáveis pela autoridade nacional após procedimento administrativo, observado o direito à ampla defesa.

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> (art.52, caput, lei n.13.709 de agosto de 2018)

Salienta-se ainda às sanções tratadas no inciso V e VI, que tratam de bloqueio e eliminação dos dados pessoais (banco de dados). Apesar das multas chamarem, no primeiro momento, maior atenção, essas duas são mais pesadas, uma vez que a proibição e/ou eliminação dos uso dos dados poderá acarretar o fim da empresa, uma vez que sem os dados para trabalharem, dependendo do negócio da mesma (e isso se aplica a grande maioria), será um impeditivo fatal.

É de fundamental importância entender que, para a fixação dessas sanções, serão observados critérios de proporcionalidade ao grau do dano, à natureza da infração e dos direitos violados; assim como a vantagem auferida ou pretendida e a condição econômica do infrator, sua boa-fé, reincidência e cooperação. Considerar-se-á ainda a adoção de mecanismos internos capazes de mitigar os riscos e das medidas corretivas, restando proporcionais a intensidade da sanção e a gravidade da falta.

Poderá ser considerado o faturamento total da empresa ou grupo de empresas para o cálculo do valor da multa elencada pelo inciso II acima transcrito, quando não demonstrado de forma completa, inequívoca e idônea, o valor do faturamento no ramo de atividade em que ocorreu a infração (art. 52, parágrafo 4º). O artigo 54 exige fundamentação pela autoridade nacional sobre o valor fixado como multa diária.

Criada pela lei n.13.853 de julho de 2019 que modifica o texto da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão federal responsável por “zelar pela proteção

dos dados pessoais, nos termos da legislação" (art.55-J, caput, inciso I), com suas competências detalhadas em um rol de 24 incisos.

> Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação (art.55-K, Lei n.13.853 de julho de 2019).
>
> Art. 55-C. A ANPD é composta de:
> I - Conselho Diretor, órgão máximo de direção;
> II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
> III - Corregedoria;
> IV - Ouvidoria;
> V - órgão de assessoramento jurídico próprio; e
> VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. (Lei n.13.853 de julho de 2019)

Os direitos do titular

No que tange a transparência da gestão, a LGPD sustenta em seu capítulo III, uma gama de direitos inovadores, dentre os quais é oportuno que se destaquem: o direito à portabilidade dos dados, ao esquecimento e à explicação.

O controlador está obrigado a disponibilizar os dados tratados mediante requisição expressa do titular. Tal acesso deverá ser fornecido em formato simplificado, possibilitando que o titular faça a leitura do documento em seu computador pessoal, por exemplo. E mais importante, poderá encaminhar os dados tratados a fornecedor concorrente, resguardados os segredos comercial e industrial dispostos no regulamento do órgão controlador. Trata-se do direito à portabilidade dos dados (artigo 18, inciso V), que não engloba aqueles já anonimizados.

O direito ao esquecimento consiste na "eliminação dos dados pessoais tratados com o consentimento do titular" mediante requisição do mesmo (art.18, caput, VI). A eliminação dos dados se torna regra a ser seguida ao término do tratamento, seja pelo alcance da finalidade, fim do período de tratamento, comunicação do titular ou determinação da autoridade nacional. Esse direito, porém, é excepcionado pelas hipóteses do artigo 16 da mesma lei. "[...]o cerne da tutela do direito ao esquecimento decorre do direito ao livre desenvolvimento da personalidade. Este conta como argumento-essência favorável a dignidade da pessoa humana". (TORRES, 2019, p.30)

Por fim, o direito à explicação está relacionado às decisões tomadas por mecanismos automatizados, utilizados para traçar "perfil pessoal, profissional, de consumo e de crédito" do titular. Nesse sentido, os bancos de dados são preciosos para o ramo do marketing direcionado

e de concessão de crédito. A novidade é que, com o vigor da LGPD, o titular dos dados passa a ter o direito de solicitar a revisão dessas decisões automatizadas que afetem seus interesses (art.20, caput), uma vez que o dispositivo legal veda o uso de dados referentes a exercício regular de direitos pelo titular em seu prejuízo.

A legislação obriga o controlador, a requerimento do titular, fornecer as informações claras e adequadas sobre os critérios e procedimentos utilizados nessas decisões. Esse direito não suprime os segredos comercial e industrial, hipóteses nas quais é lícito à autoridade nacional, realizar auditoria para verificação de aspectos discriminatórios no procedimento (art. 20, parágrafo 2º).

> Um dos setores da economia e do mercado que mais se vale do uso e tratamento de dados pessoais, principalmente para viabilizar decisões automatizadas para ofertar seus serviços, é o de consumo. Este setor é caracterizado pela necessidade de se entender o consumidor e, inclusive, influenciar seus hábitos. No entanto, neste cenário, o consumidor se encontra em posição vulnerável em sua relação com as empresas e, por isso, deve ser protegido. Entre as medidas de proteção, deve-se incluir o fornecimento de informações adequadas para que possa exercer seus direitos e evitar práticas abusivas e discriminatórias. (MONTEIRO, 2018, p.6)

Considerações Finais

O Brasil passa hoje por um contexto de fragilidade política, onde nota-se graves ofensas aos direitos fundamentais e princípios constitucionais em todos os Três Poderes. A despeito deste cenário instável, a promulgação da LGPD representa um passo democrático que alinha o Brasil aos países mais desenvolvidos no que se refere à nova cultura de proteção de dados, adotada inicialmente pela União Europeia e alguns países do Mercosul. A nova legislação mostra-se bastante estratégica para o favorecimento das relações comerciais entre o Brasil e o restante do mundo.

A partir do estudo apresentado, é possível observar o propósito do legislador de preservar a privacidade dos brasileiros dando a cada um a autoridade e controle sobre os próprios dados pessoais e sensíveis. A nova legislação conta com mecanismos institucionais preventivos e repressivos que já demonstram efetividade nos países pioneiros, principalmente evitando, mas também punindo e reparando qualquer dano moral ou patrimonial causado ao titular pelo uso indevido de dados pessoais. O disposto na Lei Geral de Proteção de Dados vai ao encontro dos princípios do direito do consumidor, protegendo a parte mais frágil da relação.

A preservação dos direitos fundamentais bem como dos direitos da personalidade, compõe a essência da LGPD, afastando práticas abusivas contra o consumidor, que demonstram um

efeito colateral de um mundo informatizado. A efetividade da norma é no mínimo promissora, mas o que pode ainda gerar preocupação é a segurança jurídica que vem sendo mitigada pelo desrespeito ao processo legislativo brasileiro. Prova disso é o sancionamento de medidas provisórias versando sobre matérias que não cumprem os requisitos de relevância e urgência necessários para tanto. A LGPD já foi alvo desse disparate ao ter seu texto editado algumas vezes pelo congresso e Presidente da República, bem como adiado a sua efetiva validade.

Porém, todo arcabouço legal traz consigo uma obrigação para as empresas, criar uma equipe eficaz que saberá alinhar o seu negócio ao compliance da lei. Ficou evidente na análise a dificultada que será enfrentada para o profissional que assumirá a função criada pela lei: O encarregado dos dados pessoais. Como visto, a esta função caberá alinhar os conhecimentos das áreas de gestão (mapas de processos, gestão de pessoas), segurança da informação (mapas de risco, compliance às normas, melhores práticas), tecnologia da informação e comunicação (ferramentas e infraestrutura para suportar todo os processos e serviço) e jurídica (compliance à LGPD e as demais leis do país). Este profissional portanto deverá ter uma visão estratégica do negócio e do fluxo informacional, para que possa alinhar, sem prejuízo técnico e financeiro, às necessidades da empresa, com as exigências da legislação e recursos tecnológicos. Será portanto o um desafio e uma grande oportunidade de virada estratégica das empresas, uma vez que já deveria ter feito toda esta análise, independente da lei, mas nunca o fizeram por consequência da rotina existente. É uma mudança cultural, difícil como qualquer outra, mas de importância fundamental para o contexto mundial.

Isso posto, entende-se que o advento da Lei Geral de Proteção de Dados constitui um marco de progresso para o Estado Democrático de Direito e da estratégia empresarial; e, se devidamente aplicada e fiscalizada, trará incalculáveis benefícios para a sociedade brasileira como um todo, para as organizações, além de favorecer a imagem do Brasil em perspectiva mundial, como um país confiável para a constituição de relações internacionais.

Referências

ABNT ISO/IEC 27.001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. 2013

ABNT ISO/IEC 27.002 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação, 2013

BENTO, Beatrice Helena Silveira. **A nova lei de proteção de dados no Brasil e o general data protection regulation da União Europeia**. Disponível em <

https://www.migalhas.com.br/dePeso/16,MI289555,11049-A+nova+lei+de+protecao+de+dados+no+Brasil+e+o+general+data+protection > Acesso em 05 Jul 2019.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada.** São Paulo: Ed. Thomson Reuters Brasil, 2018. P. 238

Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 03 de Jul 2019

Declaração Universal de Direitos Humanos. Disponível em: < https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf> Acesso em: 03 de Jul 2019

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional / Bernardo Gonçalves Fernandes.** 9 ed. Ver., ampl. E atual. – Salvador: JusPOIVM, 2017.

GOMES, Helton Simões. **Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo; entenda.** <Disponível em: https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml> Acesso em: 04 Jul 2019

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa,** Universidade Federal do Rio Grande do Sul, 2009 disponível em: http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf, acessado em 25/02/2020

JIMENE, Camilla do Vale. In: **LGPD: Lei Geral de Proteção de Dados Comentada** / Viviane Nóbrega Maldonado, Renato Opici Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.

Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 02 de Jul 2019.

Lei 8.078 - Cödigo de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acessado em 10 de fevereiro de 2020

Lei 12.965 - Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessada em 2 de janeiro de 2020

MOREIRA, André de Oliveira Schenini. **A lei de proteção de dados pessoais da União Europeia (GDPR) e sua aplicação extraterritorial às entidades e empresas brasileiras.** Disponível em: < https://www.migalhas.com.br/dePeso/16,MI267772,81042-

A+lei+de+protecao+de+dados+pessoais+da+Uniao+Europeia+GDPR+e+sua> Acesso em: 04 Jul 2019

PESSOA, Cláudio Roberto Magalhães, **Gestão da informação e do conhecimento no alinhamento estratégico em empresas de engenharia**. Tese de doutorado defendida na Universidade Federal de Minas Gerais, 2016. disponível em: https://repositorio.ufmg.br/handle/1843/BUOS-AMXG58?locale=pt_BR

REINALDO FILHO, Demócrito. **A diretiva europeia sobre proteção de dados pessoais - uma análise de seus Aspectos Gerais.** <Disponível em:http://www.lex.com.br/doutrina_24316822_A_DIRETIVA_EUROPEIA_SOBRE_PROTECAO_DE_DADOS_PESSOAIS__UMA_ANALISE_DE_SEUS_ASPECTOS_GERAIS.aspx> Acesso em: 05 Jul 2019

SANTIAGO, Vanessa Cristina e TAMBA, Debora Harumi. **Proteção de dados no Brasil: novo marco regulatório**. Disponível em: < https://www.migalhas.com.br/dePeso/16,MI290866,91041-Protecao+de+dados+no+Brasil+novo+marco+regulatorio> Acesso em: 05 Jul 2019.

VAINZOF, Rony. In: **LGPD: Lei Geral de Proteção de Dados Comentada** / Viviane Nóbrega Maldonado, Renato Opici Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.