OAB ESA RIO GRANDE DO SUL

REVISTA ELETRÔNICA DA ESA/RS

Volume 8 – Número 2 (2020) - Porto Alegre – Rio Grande do Sul – Brasil

SEGURANÇA DA INFORMAÇÃO: TRANSPARÊNCIA E PROTEÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA: LGPD, ACESSO À INFORMAÇÃO E OS INCENTIVOS À INOVAÇÃO E À PESQUISA CIENTÍFICA E TECNOLÓGICA NO ÂMBITO DO ESTADO DE MINAS GERAIS

Carolina Montolli[1]

Resumo: A Internet e as redes sociais estão cada vez mais presentes na vida cotidiana dos brasileiros e de pessoas por todo o mundo. O Estado deve garantir, em seu ordenamento jurídico que os indivíduos tenham o amparo da lei também na vida virtual. A mudança para uma cultura de acesso envolve investimentos em recursos tecnológicos, operacionais e humanos, por meio de ações planejadas e interligadas. Logo, os processos de trabalho, além dos sistemas informatizados e dos bancos de dados, devem ser revistos, de modo que a transparência seja considerada na realização das atividades cotidianas, e não somente na disponibilização das informações.
Palavras-chave: Lei Geral de Proteção de Dados. LGPD. Decreto 47.442, Lei 13.853.

Abstract: The Internet and social networks are increasingly present in the daily lives of Brazilians and people around the world. The State must guarantee, in its legal system, that individual shave the protection of the law also in virtual life. The shift to an access culture involves investments in technological, operational and human resources, through planned and interconnected actions. Therefore, work processes, in addition to computerized systems and databases, must be reviewed, so that transparency is considered when carrying out daily activities, and notonly when making information available.

Keywords: General Data Protection Law. LGPD. Decree 47.442. Law 13.853.

1. INTRODUÇÃO

O consumo de serviços através do meio digital tem crescido de maneira significativa em todo o mundo. A transmissão de dados e informações pela internet ocorre de maneira rápida, relativamente simples e descomplicada. Diante disso, os provedores de serviços digitais têm a intenção de atrair, cada vez mais, um número grande de usuários aumentando assim, a divulgação e consequente consumo de seus produtos e/ou serviços.

As empresas que controlam as redes sociais sempre mantiveram uma postura distante do assunto da proteção de dados, como se não tivessem qualquer responsabilidade pelos dados

[1] Servidora Pública Estadual da Fundação João Pinheiro MG. Pós doutora em Direito. Advogada de Imigração. Conselheira Seccional da OAB/MG. Conselheira do CAP/AGE/MG. OAB/MG - 120.497

que são inseridos para a abertura de contas pessoais. Entretanto, a nova lei repercutirá diretamente nessas empresas, pois a partir do momento em que a empresa exige dados pessoais do usuário para a abertura de contas ou qualquer outro tipo de transação, essas empresas são responsáveis pelo tratamento dos dados, devendo assegurar a segurança e o sigilo dos mesmos.

Por outro lado, grande parte dos serviços encontrados nessas redes exigem a identificação do usuário através do cadastramento de dados pessoais. Esses dados são informações solicitadas pelos provedores com o objetivo de oferecer trabalhos personalizados, aumentar a visibilidade, prover o marketing e a propaganda, ou até mesmo ser utilizado para o envio de brindes.

Por essa razão, o usuário tende a fazer cadastros em plataformas digitais de maneira desenfreada, permitindo que os provedores tenham acesso a praticamente todos os tipos de informações pessoais e, os proprietários dessas informações percam o controle de onde fez ou não cadastros. Além disso, pode ocorrer a captura de determinadas informações do usuário, sem o devido consentimento, o que culmina na utilização de forma irrestrita, influenciando na sua privacidade.

O principal dilema relacionado a essa atitude as plataformas e provedores digitais é a alta probabilidade da exposição indesejada, da possível discriminação e da falta de controle sobre suas próprias informações.

Com essa quantidade exagerada de repasse de informações dos usuários, passou-se a existir uma preocupação alta, uma vez que apenas com o conhecimento claro acerca dos usos e finalidades o consentimento se tornará válido.

A previsão jurídica do instituto já foi debatida em todo o mundo, em especial na Europa, que desde a sua Carta de Direitos Fundamentais da União Europeia já previa a proteção dos dados pessoais como um direito fundamental. Contudo, no Brasil, apenas em 2018 com a Lei Geral de Proteção de Dados Pessoais o tema recebeu a sua devida atenção. Por meio desde diploma, o consentimento apresenta-se como uma dentre outras medidas autorizadoras da coleta, tratamento e compartilhamento das informações dos usuários, passando a ser adjetivado a fim de evitar a invalidade de tal instituto.

Diante desses fatos, esse artigo tem como objetivo principal demonstrar em quais situações o uso de dados pessoais pode ser caracterizado como invasão ao direito de privacidade.

O método para a realização desse estudo foi o levantamento bibliográfico, no qual buscou-se através de pesquisa na literatura científica informações a respeito da do decreto 47.442 de 04 de julho de 2018 e da lei 13.853, de 8 de julho de 2019.

2. DADOS PESSOAIS NO MEIO DIGITAL

A construção da identidade humana pode ser considerada uma das maiores incógnitas na qual a humanidade se deparou, seu processo evolutivo e desenvolvimento são temas de debates e especulação não só pela comunidade médica que investiga o tema de um ponto de vista científico, como também é tema de discussão para as mais diversas áreas que passam pela filosofia e sociologia com o intuito de decifrar a essência da consciência humana (Bezerra, 2019).

Parte da identidade do indivíduo vem do meio em que se encontra e, se pararmos para fazer uma análise temporal, este ambiente historicamente sempre carregou um caráter de limitação, pois, por boa parte da história humana o indivíduo não tinha muitas oportunidades de sair da sua terra natal por razões práticas: contato com outras comunidades era algo que demandava um gasto de tempo e recursos que muitas vezes não era justificado e, em alguns casos, hostil.

A privacidade e a segurança da informação (SI) na internet têm correspondido a uma área que desperta interesse de estudo, devido à grande quantidade de informações pessoais e corporativas que são obtidas, armazenadas, transmitidas e publicadas na rede mundial de computadores.

Quanto ao uso da internet, a expansão das comunicações por rede de computação. Nessa nova ordem global, cada indivíduo se torna protagonista, produzindo e recebendo informação por diversos mecanismos desenvolvidos na internet. Logo, a esfera pública midiática tem menos influência no controle das informações transmitidas e processadas (Lemos, 2010).

Atualmente podemos afirmar que o ser humano vive em dois planos de existência simultaneamente: o físico e o virtual. O primeiro é o clássico, limitado pela presença corpórea do indivíduo e temporal, onde ele carrega consigo sua identidade da qual ele é indissociável, o segundo é meio digital que, em contraste com o físico, não se limita pela presença física de seu indivíduo, bem como possui um caráter atemporal, sua identidade pode ser acessada a qualquer momento em qualquer lugar do globo, teoricamente, qualquer pessoa (Lemos, 2010).

Com a atual configuração tecnológica, a demanda pelo fluxo de informações aumentou exponencialmente não por design, mas por necessidade derivada da própria arquitetura dos sistemas e da configuração de armazenamentos na qual os bancos de dados se constituem. Desde muito tempo empresas e governos coletam dados e informações sobre as pessoas em forma de cadastros, sensos, lista de e-mail, históricos médicos, históricos de transações bancária e qualquer outro tipo de cadastro que fosse necessário para a identificação de um usuário de um serviço.

Diante do contexto no qual os direitos à privacidade e proteção de dados foram elevados ao nível dos direitos humanos no cenário internacional, os governos têm dispensado especial atenção para lidar com esses desafios. Nesse cenário, destaca-se o Regulamento Geral sobre a Proteção de Dados (GDPR), publicado em 2018, pela União Europeia (EU), que visa a proporcionar aos usuários maior controle sobre seus dados pessoais e a aumentar as restrições sobre as organizações que tratam e lidam com esses dados.

O dado pessoal está associado e relacionado a uma pessoa. Por meio de um conjunto de dados, que permite a identificação da pessoa. É fundamental deixar evidente a diferença do conceito entre dados e informação. Um dado é uma palavra, sem qualquer significado relevante. Uma vez que se torna compreendido, com um significado e contexto, se transforma em informação. Os dados pessoais são informações, fatos, ações, vontades e preferências que se referem um indivíduo identificado ou identificável. Por estarem relacionados a uma pessoa, são atributos que caracterizam a personalidade do indivíduo (Mendes, 2014).

Pode-se perceber que os dados pessoais podem ser categorizados como instrumento que permite com que seu titular desenvolva a sua personalidade de forma livre, representando, assim, um prolongamento do próprio indivíduo e uma perspectiva de suas relações (Bioni, 2018).

No meio digital, o compartilhamento de dados pessoais na internet ocorre de forma frequente. Em algumas situações, esse tratamento é descrito, por exemplo, no termo de uso e privacidade do serviço. Contudo, há hipóteses em que o tratamento dos dados ocorre sem qualquer cientificação, permissão ou consentimento do titular do dado. Uma tecnologia frequentemente utilizada por serviços na internet, para obter informações sobre o usuário sem qualquer consentimento, são os cookies (Goodrich, 2013).

Estes são utilizados para manter a sessão do usuário em um determinado site, ou seja, para evitar se autenticar frequentemente. Outro exemplo de uso é para promover anúncios publicitários, em que a publicidade ocorre de uma forma mais objetiva, reconhecendo suas preferências e possíveis necessidades e desejos, com anúncios de produtos recentemente pesquisados na internet (Goodrich, 2013).

Neste sentido, os "dados são simplesmente fatos brutos", os quais necessitam passar por certo mecanismo de processamento e serem organizados para que possam transmitir alguma informação (Bioni, 2015). Pode-se dizer, ainda, que o conceito contempla aqueles dados que além de indicarem atos de uma pessoa, também identificam seus pensamentos e seu modo de agir. Tendo em vista sua exposição, há a possibilidade de eles passarem pelo processo, via digital, de coleta, armazenamento, processamento ou, inclusive, transferência a terceiros (Santos, 2014).

Tamanha é a importância do vínculo entre o dado e o seu titular para a sua caracterização que "os dados pessoais chegam a fazer as vezes da própria pessoa em uma série de circunstâncias nas quais a sua presença física seria outrora indispensável" (Doneda, 2011).

Com a atual capacidade computacional, o cruzamento e o processamento de dados se tornaram algo difícil (senão impossível) de ser controlado, o que dificulta a possibilidade de o usuário tomar qualquer decisão com relação a forma como seus dados são compartilhados.

Consequentemente, o indivíduo é submetido a um processo de despersonalização, pois, ele perde totalmente o controle exclusivo de seus dados para que seja criada uma aproximação virtual do seu real ser. Mesmo em um primeiro momento, a despersonalização pode parecer apenas um efeito inofensivo justamente por se tratar de um conceito abstrato como também suas reais consequências ainda são obscuras pela falta de documentação e pro se tratar de um problema recente, entretanto, é possível ver que há um certo perigo à espreita, algo que vá vilipendiar os mais básicos dos direitos e, por isso, o Direito não pode se furtar de versar sobre (Solove, 2004).

É através da Internet, bem como por meio dos avanços quantitativos e qualitativos nas manipulações das informações utilizadas como fontes de riqueza, que a sociedade pré-informacional se transforma na sociedade informacional. Por meio desta, agora o consumidor deixa de ser apenas o polo passivo no ciclo do consumo, passando a ter uma participação ativa

através de seus dados – "tamanha é a valiosidade das informações dos consumidores que o seu controle e organização são termos essenciais do marketing" (Bioni, 2018).

Para sua proteção como tal, devem estar assegurados como um direito subjetivo do indivíduo, de modo a resguardar sua defesa e limita a atuação do poder estatal ou privado diante de tal. Ademais, deve também possuir uma visão como um dever estatal de proteção, numa visão objetiva, por meio da qual "representa a necessidade de concretização e delimitação desse direito por meio da ação estatal, a partir do qual surgem deveres de proteção do Estado para garantia desse direito nas relações privadas" (Mendes, 2014).

3. A LEI DE ACESSO À INFORMAÇÃO E SEUS PRINCIPAIS ASPECTOS

Com a propagação do princípio da dignidade humana pelas constituições em todo o mundo, principalmente com o término da Guerra Mundial de 1939 e com a Declaração Universal de Direitos Humanos do ano de 1948, os interesses essenciais da existência humana passaram a ser prioridade nas discussões dos juristas.

O termo privacidade pode ser entendido tanto como o desempenho da liberdade do indivíduo, quanto como algo que encontra-se interno a este sujeito, de modo que faz parte da sua natureza enquanto ser humano. "Ter privacidade é fundamental ao indivíduo, não apenas em oposição ao público, mas numa relação interna, visto que não será possível a assunção de seus desejos sem a construção de seu espaço íntimo" (Cancelier, 2017).

Apesar de encontrar dificuldade em delimitar um conceito da privacidade, Doneda (2011) apresenta a origem da palavra que, em que pese constantemente empregado na língua inglesa, o vocábulo em si possui raiz latina, derivado do verbo privari, que possui como adjetivo a forma privatus. "De fato, o desenvolvimento do termo privacy na língua inglesa não teve paralelo em idiomas latinos, ao menos como um substantivo simples".

A informação é o oxigênio da democracia. Nessa toada, esclarece que a democracia acontece nos países nos quais os cidadãos possuem capacidade de tomar decisões que os atingem. Depreende-se, pois, que a informação é princípio fundamental das democracias, em todas suas acepções. Assim, as sociedades democráticas devem dispor de mecanismos diversificados e eficazes de envolvimento das ações estatais, não só por eleições periódicas, mas, principalmente, nos campos de fiscalização e avaliações dos projetos e políticas públicas (Mendel, 2009).

No século XX, foram aprovadas quatro gerações de normas de proteção aos dados pessoais em todo o mundo. A primeira surgiu na década de 70 e foi contra a concepção de centralização de bancos de dados nos países. A segunda geração está relacionada ao consentimento do cidadão e o real exercício de sua liberdade de escolha. A terceira (iniciada na década de 80) é marcada pela formulação de um direito à autodeterminação informativa, fornecendo uma participação maior do cidadão sobre seus dados pessoais desde a coleta, o armazenamento e a transmissão. A quarta geração surgiu para tentar melhorar as gerações anteriores. Nesta última geração, algumas normas fortaleceram a posição do indivíduo por meio de normativas (Doneda, 2011).

Ainda com relação a quarta geração, as que mais se destacam globalmente são: Lei Federal de Proteção de Dados alemã, legislação da Noruega, da Finlândia, da Dinamarca, da França, da Grã-Bretanha, da Suíça e a Diretiva Europeia sobre proteção de dados pessoais de 1995. Essa geração tem como principal característica oferecer aos usuários das redes de internet maior autocontrole sobre seus dados pessoais, com a preocupação de não permitir que o titular dos dados considerados sensíveis possa decidir se fornece ou não, ou seja, cria-se uma imposição para a proteção dos dados sensíveis. O aumento de normas setoriais sobre a proteção de dados pessoais visa à complementação das normas gerais, fornecendo detalhes específicos e culturais para a proteção dos dados dos cidadãos dos respectivos países (Bezerra, 2019).

Em 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) emitiu o *privacyguidelines*e, em 1985 a *declarationontransborderdata flows.* Esses documentos tiveram influência global no desenvolvimento da proteção dos dados pessoais, estabelecendo padrões normativos e princípios objetivando que todos os países membro tenham um ambiente regulatório uniforme, além de disseminar as orientações normativas no mundo. Depois de 30 anos, as *guidelines* foram atualizadas e uma nova versão disponibilizada em 2013 (Bioni, 2019).

No Brasil, a Constituição Federal de 1988 já apresentava em seu inciso X do art. 5º como direito fundamental inviolável, a intimidade, a vida privada e a imagem das pessoas, e não apenas isso, mas também a inviolabilidade do sigilo de correspondência, podendo haver indenização pelo dano material ou moral decorrente de sua violação.

Por sua vez, a Carta Magna traz ao direito do acesso à informação pública o caráter de garantia fundamental, buscando-se o rompimento com a cultura de sigilo presente à época da Ditadura Militar, sob o pretexto de preservação da segurança nacional. Portanto, a máxima

divulgação das ações governamentais deve ser atividade constante na administração pública, excluindo, apenas, informações que devam ser sigilosas, em casos específicos previstos em lei. O direito ao acesso à informação evocado pela Constituição demonstra que a informação pública pertence à sociedade, e o Estado é, somente, o detentor da informação, devendo disponibilizar a quem tenha o interesse de obter os dados (Cancelier, 2017)

O Marco Civil da Internet surgiu em 2009, a partir da iniciativa de diversas discussões, sobre a necessidade da criação de uma lei que regulasse os direitos e deveres de usuário e provedores, no uso da internet no país. Em seguida surgiu o Projeto de Lei nº 2.126/2011 (Brasil, 2011), com projeção robusta após a divulgação do famoso escândalo de violação de privacidade pelo Edward Snowden, em 2013. Foi aprovado pelo Congresso Nacional, depois pelo Senado e por fim, sancionado pela então presidente Dilma Rousseff em 2014 (Souza, 2016).

A Lei de Acesso à Informação (LAI) regula, o parágrafo 2º do artigo 216 da Constituição (1988), que descreve que "cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem". Assim, a Lei de Acesso à Informação deve ser obedecida por toda a Administração Pública. Dessa feita, sujeitam-se ao regime da LAI: os órgãos da administração direta de todos os Poderes (Executivo, Legislativo, Judiciário e Ministério Público), as entidades controladas direta ou indiretamente pelo poder público e todas as esferas de governo (federal, estadual, distrital e municipal).

A Lei 12.527/11 tem como principal diretriz a observância da publicidade como preceito geral e sigilo como exceção, ou seja, a administração pública deve divulgar as informações de interesse coletivo ou geral, restringindo, somente, aquelas cuja segurança da sociedade ou do Estado assim a justifiquem. Nesse contexto, a LAI define os graus de sigilo da informação, estabelecendo prazos máximos para restrição de acesso, vigorando a partir da data da produção da informação, considerando, ainda, a gravidade do risco à segurança nacional e utilizando o critério menos restritivo possível.

A Lei nº 12.965/2014, no artigo 3º, lista alguns princípios que disciplina o uso da internet no Brasil. Essa lista, que não é taxativa, destaca-se três principais: "garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; proteção da privacidade; e proteção dos dados pessoais, na forma da lei."

A garantia de liberdade de expressão, comunicação e manifestação de pensamento é a reafirmação de que os direitos fundamentais se mantêm, independentemente do ambiente (virtual ou real), devendo seguir as prerrogativas constituintes184. A privacidade no Marco Civil da Internet está diretamente associada à proteção dos dados pessoais, armazenados e transitados pela internet e daqueles que controlam os dados. A definição de dado pessoal surgiu somente no Decreto nº 8.771/2016, ou seja, durante dois anos de vigência desta lei, o conceito ficou sem uma delimitação mais precisa (Oliveira, 2017).

A Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que determina como os dados dos cidadãos podem ser coletados e tratados, e que prevê punições para transgressões. No dia 14 de agosto de 2018, foi sancionado no Congresso Nacional o PLC 53/2018, o qual dispõe sobre a proteção de dados pessoas e altera a Lei 12.965/16 (Marco Civil da Internet), consolidando-se assim como a Lei Geral de Proteção de Dados brasileira.

A iniciativa desse regulamento partiu de toda a sociedade científica e foi liderada pela então Secretaria de Desenvolvimento Tecnológico e Inovação (SETEC) do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e a Secretaria de Inovação e Novos Negócios (SIN) do então Ministério da Indústria, Comércio Exterior e Serviços (MDIC), consumindo mais de dois anos de trabalho, com a participação de diversos atores e representantes de órgãos e instituições e contando com uma consulta popular.

A Lei Geral de Proteção de Dados Pessoais foi sancionada pela Lei nº 13.709, em 14 de agosto de 2018 e estava prevista para entrar em vigor 24 meses após a sua a data de publicação, em 14 de agosto de 2020, porém, devido a pandemia causada pelo novo corona vírus (COVID19), o prazo para entrar em vigor foi prorrogado para 3 de maio de 2021, conforme disposto pela medida provisória 959, de 29 de abril de 2020, tendo sua validade em todo território nacional e se sobrepondo a qualquer lei estadual ou municipal.

Tal como a General Data Protection Regulation (GPDR) que é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu, a LGPD motivará mudança de paradigma na gestão dos dados, evidenciando a necessidade de adequações internas e da construção de uma cultura de proteção de dados no Brasil.

A LGPD visa estimular não apenas o desenvolvimento econômico, mas a proteção dos direitos fundamentais. A LGPD vem para adequar as práticas de empresas brasileiras a estes

novos padrões e ao cenário atual, inserindo o Brasil no rol dos mais de 120 países que contam com uma lei de proteção de dados. A proteção de dados de acordo com comunidade internacional facilitará a obtenção da chancela da Comissão Europeia classificando o Brasil como país com nível adequado de proteção de dados.

Para sua proteção como tal, devem estar assegurados como um direito subjetivo do indivíduo, de modo a resguardar sua defesa e limita a atuação do poder estatal ou privado diante de tal. Ademais, deve também possuir uma visão como um dever estatal de proteção, numa visão objetiva, por meio da qual "representa a necessidade de concretização e delimitação desse direito por meio da ação estatal, a partir do qual surgem deveres de proteção do Estado para garantia desse direito nas relações privadas" (Doneda, 2011).

A LGPD também definiu alguns tipos de dados pessoais como dados sensíveis. São informações que podem ser utilizadas de forma discriminatória e carecem de proteção especial. O art. 5o, II, da lei define dados sensíveis como aqueles sobre origem racial ou étnica de um indivíduo; convicções religiosas; opiniões políticas; filiação a sindicatos ou organizações de caráter religioso, filosófico ou político; dados sobre saúde ou vida sexual; e dados genéticos ou biométricos.

A LGPD é aplicada para tipos específicos de dados cujo tratamento deverá acontecer seguindo uma série de critérios e exceções, conforme demonstrado a seguir:

a) ao tratamento de dados de pessoas físicas no Brasil, independentemente do meio e/ou da forma de tratamento dos dados, incluindo dados on-line ou off-line, bem como independentemente de localização da base de dados, sede da empresa e nacionalidade dos titulares;

b) às pessoas físicas ou jurídicas, de direito público e privado, incluindo dados relacionados a relações trabalhistas, de consumo, de Internet, B2B, B2C5, que (i) realizam a operação de tratamento no Brasil; (ii) oferecem bens ou serviços ao mercado consumidor brasileiro; e/ou (iii) coletam e tratam dados de pessoas localizadas no território brasileiro;

c) às empresas que realizam operações de tratamento de dados fora do Brasil quando (i) os dados pessoais forem coletados no Brasil; (ii) os dados sejam relacionados a indivíduos localizados no território brasileiro; e/ou (iii) tiver por objetivo a oferta de produtos e/ou serviços ao público brasileiro; e

d) em conjunto com normas setoriais que também regulamentam dados pessoais.

O consentimento para o tratamento de dados é parte importante para que haja o respeito ao direito à liberdade de escolha, e deve ser livre, informada, inequívoca, específica, determinada e expressa. O consentimento é a principal ferramenta para que haja o tratamento de dados, e deve ser respeitada a forma prevista em lei, seja por escrito ou qualquer meio que demonstre a vontade do titular. Tal consentimento pode ser ainda revogado a qualquer momento pelo titular (Ribeiro, 2016).

De acordo com o art. 5, inciso XVII, da LGPD, "o relatório de impacto à proteção de dados é uma 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 desses riscos".

Os relatórios de impacto são resultado de uma avaliação de impacto que tem como objetivo avaliar, mapear, planejar, implementar e monitorar todo o processo de conformidade com as leis gerais e setoriais de proteção de dados. Tudo isso como forma de demonstrar conformidade com as obrigações da lei e, mais ainda, como uma das formas de demonstrar responsabilidade e prestação de contas perante a ANPD.

No decorrer de 2018, ainda foram editados dois dispositivos para complementar a recém lei de proteção de dados. Em 26 de dezembro houve aprovação do Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação (PNSI). Em 27 de dezembro de 2018 foi editada a medida provisória nº 869/2018, que autorizou a criação da Autoridade Nacional de Proteção de Dados (ANPD), aumentou o prazo de entrada em vigor para 24 meses após publicação e, ademais, alterou a obrigatoriedade de revisão humana das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais.

A segurança de dados não envolve somente a troca de informações ou investimentos em ciber segurança, mas do conhecimento de quem utiliza e de quem disponibiliza as informações. Nesse contexto, as empresas deverão se adequar aos mandamentos da LGPD, desde a indicação de um encarregado, como a elaboração e implantação de procedimentos internos, aproveitando-se já do conceito de governança corporativa já implementados para outras áreas da administração.

A LGPD prevê sanções para quem não tiver boas práticas. Elas englobam advertência, multa ou até mesmo a proibição total, ou parcial de atividades relacionadas ao tratamento de dados. As multas podem variar de 2% do faturamento do ano anterior até a R$ 50 milhões,

passando por penalidades diárias. A Lei também prever a obrigação de divulgação de incidentes, a eliminação de dados pessoais e a inversão de ônus da prova a favor do titular do dado.

Em 24 de julho de 2019, foi editado o Decreto nº 9.936/2019, que regulamenta a Lei nº 12.414/2011 (Lei do Cadastro Positivo) no que diz a respeito da formação e consulta aos bancos de dados, bem como o seu tratamento, incluindo dados pessoais, para formação de histórico de crédito. As medidas provisórias e decretos tem relação (de alguma forma) com a LGPD, por envolver cadastros de dados pessoais, manipulação ou tratamentos. Recentemente, foi permitida a criação de um Cadastro Base do Cidadão, de acordo com o Decreto nº 10.046/2019 que trata a forma que será conduzida em conjunto com a LGPD.

Além disso, o Código de Defesa o Consumidor inovou, ao tratar sobre a privacidade e a proteção de dados pessoais de forma moderna. Na relação de consumo ocorre, na maioria das vezes, a inclusão de dados pessoais do cliente no banco de dados do fornecedor. Esta lei regulou (mesmo que de forma simples) como os dados devem ser tratados, quais regras sobre o compartilhamento e privacidade a dos dados pessoais dos clientes. Na seção VI do Código de Defesa do Consumidor (composto pelos artigos 43 e 44) estão as normativas para informar os direitos do consumidor, em relação aos cadastros realizados nos serviços no meio digital e os bancos de dados que serão usados para armazená-los (Brasil, 1990).

Ademais, o mérito da proteção dos dados pessoais pode ser analisado devido ao fato de que, além das informações retiradas de tais, são eles que representam os indivíduos na sociedade da informação, uma vez que é a partir deles que os organismos sociais criam perfis virtuais e, desse modo, tomam decisões que afetam suas vidas e suas personalidades (Doneda, 2011).

3.1 Governança de dados

A Governança Corporativa trabalha com a empresa como um todo, estudando seus aspectos mais diversos, prevenindo riscos e estabelecendo procedimentos para incidentes. Nesse sentido, aplica-se às questões societárias, regulatórias, de anticorrupção e compliance. Com o decorrer do tempo, aperfeiçoamento da tecnologia e a dependência das empresas à sua utilização, a necessidade de aplicação dos conceitos de governança para as questões aqui mencionadas, fez-se presente para questões de informática, fazendo nascer mais essa área de governança, a Governança Corporativa aplicada à Tecnologia da Informação (também

conhecida por Governança em Tecnologia da Informação ou simplesmente Governança em TI), que se apresente como as regras, métodos e práticas, voltadas para o setor de tecnologia de determinada empresa.

A Governança Corporativa bem executada cria boas práticas, que então se convertem em princípios básicos e recomendações objetivas para as pessoas que dirigem as empresas e para que essas pessoas disseminem a cultura que se forma, alinhando interesses empresariais imediatos com a finalidade de preservar e otimizar a perenidade da organização, sua durabilidade e valorização de todas as pessoas envolvidas (Fernandes, 2020).

Muito embora e Governança Corporativa tenha se iniciado com enfoque nas questões societárias e de relação com investidores, seus quatro pilares foram estendidos a outras áreas, como tecnologia da Informação, contratos, servindo também como base e impulso para as questões voltadas a Gestão de Riscos, Compliance e Canais Éticos (Fernandes, 2019).

A fim de fiscalizar e controlar as boas práticas de governança, recomenda-se que as empresas mantenham órgãos de controles internos e externos. Controles são, por sua vez, compostos pelas políticas e procedimentos adotados pelas empresas de forma a minimizar os riscos e incrementar os processos internos. Fernandes (2019) cita que os controles devem ter "foco na prevenção, revisão e atualização contínuas, visando proteger os ativos e a reputação da empresa, disponibilizar informações adequadas, gerando confiabilidade, promover a eficácia operacional e a aderência às leis e regulamentos aplicáveis". Existem diversos tipos de controles: a) preventivos, visando a redução da possibilidade de ocorrência de um evento , e consequentes resultados indesejados; b) detectivos, com relação à eventos já ocorridos; c) corretivos, tanto dos efeitos de um evento indesejável como das causas de um risco detectado; d) diretivos ou orientativos, de maneira a de provocar e/ou encorajar a ocorrência de fatos desejáveis; e) compensatórios das fraquezas de controle em áreas-chave.

Para que a implantação de planos de gestão de riscos para adoção de tecnologias seja bem-sucedida, necessário se faz o envolvimento direto dos conselhos de administração e dos executivos. Todavia, podem ocorrer situações nas quais as pessoas que compõem tais conselhos não detenham o conhecimento, a expertise, surgindo a necessidade da figura da Governança em TI.

A governança de dados é uma gestão eficiente de toda informação gerada, e tem como objetivo a organização, a estruturação e o uso estratégico dos dados que são coletadas,

armazenados e tratados dentro da organização, tendo em vista que esses dados são capazes de auxiliar no planejamento e tomada de decisão.

De acordo com inciso X do artigo 5º da LGPD: "X - tratamento: 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".

Diante da realidade proporcionada pela evolução das ferramentas tecnológicas, a privacidade tornou-se um elo da personalidade perdido e as informações ditas como pessoais passaram a ser transportadas para toda a sociedade. Com a conexão diária e instantânea à Internet, os dados que antes eram particulares e privados de cada indivíduo são transportados para a rede e deixam seus titulares à mercê desse sistema virtual mundial. Nesse sentido, Marineli (2017) destaca que "entre as violações perpetradas por pessoas e redes sociais mal intencionadas, os danos à privacidade ganham destaque e já figuram entre as principais preocupações dos internautas".

Desse modo, percebe-se que, a fim de deixar de ser enquadrado como um simples meio de fornecimento de dados, o indivíduo passa a figurar como um elemento central ao longa da evolução da proteção dos dados pessoais, a ponto desta proteção ser equiparada "ao direito do cidadão autogerenciar as suas informações pessoais" (Malheiro, 2017).

Os resultados mais consistentes da mudança cultural de transparência pública serão observados somente no longo prazo, quando, finalmente, todos os servidores públicos tiverem a idealização da transparência das informações como seu dever. Com isso em mente, mais do que cursos e treinamentos acerca da importância do acesso às informações e suas implicações, as estratégias de mudança devem estar envoltas no aspecto da transparência ser assimilada e aplicada como um instrumento em todas as atividades administrativas. Enfim, há de se preocupar com a institucionalização do princípio da transparência nas ações do dia a dia (Bertazzi, 2011).

4. SEGURANÇA DA INFORMAÇÃO NO ESTADO DE MINAS GERAIS: INCENTIVO A PESQUISA E INOVAÇÃO

A promulgação da Lei de Acesso à Informação é um passo fundamental para a efetiva transparência das informações públicas. No entanto, a cultura e incentivos organizacionais são mais eficazes no atingimento de resultados do que um normativo vigorando acerca do assunto. A negativa de acesso às informações não passa pela análise de apenas um servidor, mas pelo contexto institucional e suas crenças. Afinal, a cultura organizacional exerce mais influência nas decisões administrativas do que as normas, e deve receber a atenção necessária para sua mudança (Oliveira, 2017).

Diversos são os motivos apontados como limitadores da promoção das atividades de CT&I no País, como o isolamento da academia, o excesso de burocracia e a falta de mecanismos de descentralização e de desverticalização das ações. As mudanças promovidas pelo novo marco legal, Lei n.º 13.243/2016, estimulam a superação desses obstáculos, mas, sem a regulamentação, era difícil colocar em prática essas alterações (Nazareno, 2016).

A gestão pública necessita olhar atentamente ao fomento das atividades de disponibilização de informações, cuja efetividade somente será atingida com novas atitudes e melhoria dos processos de trabalho, distanciando-se, gradativamente, da rotina atual. Portanto, as ações de aperfeiçoamento do funcionamento de todos os órgãos públicos brasileiros devem visar ao resultado final de mecanismos eficazes para atendimento das necessidades da população e atenção ao princípio da impessoalidade na prestação de informações (Oliveira, 2017).

Para regulamentar medidas de incentivo à inovação e à pesquisa científica e tecnológica, à capacitação tecnológica, ao alcance da autonomia tecnológica de Minas Gerais, foi publicado, em 05 de julho de 2018, o Decreto 47.442/2018 que estabelece, no âmbito do Estado, regulamentação semelhante à Federal. O propósito do Decreto é apoiar a inovação e efetivar política estadual de desenvolvimento científico e tecnológico, tanto no ambiente produtivo, como no meio acadêmico e nos centros de pesquisas mineiros.

O Decreto informa como agências de fomento, além da Fundação de Amparo à Pesquisa do Estado de Minas Gerais (Fapemig), já consolidada há mais de 30 anos, Companhia de Desenvolvimento Econômico de Minas Gerais e o Banco de Desenvolvimento de Minas Gerais

(BDMG), este como agência financeira de fomento. Outro destaque é a instituição do Sistema de Ciência, Tecnologia e Inovação de Minas Gerais (Secti-MG), que contará com a participação tanto de setores públicos, como privados, englobando universidades, Instituições de Pesquisa Científica, Tecnológica e de Inovação (ICTs), empresas, agências de fomento, fortalecendo assim o ecossistema de inovação mineiro. O principal objetivo é que todos os envolvidos nesse ambiente apoiem a criação, a implantação e a consolidação de ambientes promotores de inovação, permitindo o desenvolvimento tecnológico, o aumento da competitividade e a interação entre as empresas e as ICTs.

O Decreto institui o Sistema de Ciência, Tecnologia e Inovação de Minas Gerais (Secti-MG), com o objetivo de incentivar o desenvolvimento econômico e sustentável do Estado por meio da inovação tecnológica e do estímulo a projetos e programas especiais, articulados entre o setor público e privado. Entre os principais agentes deste sistema estão o Governo do Estado, que é o responsável por aplicar e fomentar essas políticas públicas de ciência e tecnologia; as Universidades e institutos de pesquisa, que realizam pesquisas, geram e disseminam os conhecimentos científicos e tecnológicos; e as Empresas, que transformam esse conhecimento em produtos, processos e serviços. O Secti-MG é integrado por: ICTMG; agências de fomento; parques científicos e tecnológicos, incubadoras de empresas de base tecnológica, polos tecnológicos, ambientes promotores de inovação e demais arranjos institucionais, que atraem empreendedores e recursos financeiros; empresas brasileiras, instituições econômicas e financeiras, sociais e culturais que impulsionam o desenvolvimento tecnológico do Estado; Sedectes.

As ICTMG públicas estaduais poderão celebrar contrato de transferência de tecnologia e de licenciamento para outorga de direito de uso ou de exploração de criação por ela desenvolvida isoladamente ou por meio de parceria. Os critérios e as condições para a contratação serão estabelecidos de acordo com a política de inovação das ICTMG públicas, podendo inclusive ser estabelecidos preços e condições diferentes para a transferência e o licenciamento para empresas diferentes, desde que devidamente motivado. A transferência de tecnologia e o licenciamento para exploração de criação reconhecida, em ato do Poder Executivo, como de relevante interesse público, somente poderão ser efetuados a título não exclusivo.

Celebrados esses contratos, os dirigentes, criadores ou quaisquer outros servidores, empregados ou prestadores de serviços deverão repassar os conhecimentos e informações necessários à sua efetivação. Os contratos também poderão ser celebrados com empresas que tenham, em seu quadro societário, a própria ICTMG ou pesquisador público de ICTMG, inclusive quando este for o próprio criador, de acordo com a legislação e o disposto em sua política institucional de inovação.

5. CONSIDERAÇÕES FINAIS

O Brasil agiu, no decorrer dos últimos anos, para que não fique defasado frente às grandes potências nesse sentido. O país possui duas legislações que foram contextualizadas para tratar do regulamento do uso da internet, e do regulamento do tratamento de dados pessoais. O Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para os usuários da internet buscarem garantir a segurança, a integridade dos dados pessoais, o consentimento no uso da rede e suas aplicações. Já a Lei Geral de Proteção de Dados Pessoais é mais específica sobre a regulamentação dos dados pessoais, contendo mais princípios e definições tanto para o setor privado quanto para o público.

Com o avanço da mobilidade digital e a entrada da Lei Geral de Proteção de Dados, a indústria de segurança de dados tem fortalecido seu relacionamento com o sistema de inovação para assegurar maior proteção aos usuários. Isso implica na criação de programas de mentoria ou contato mais estreito com os agentes do sistema.

Finalmente, a mudança para uma cultura de acesso envolve investimentos em recursos tecnológicos, operacionais e humanos, por meio de ações planejadas e interligadas. Logo, os processos de trabalho, além dos sistemas informatizados e dos bancos de dados, devem ser revistos, de modo que a transparência seja considerada na realização das atividades cotidianas, e não somente na disponibilização das informações. Enfim, a preocupação maior deve ser quanto à conscientização dos servidores públicos, conquanto estes se configurarem como os principais influenciadores da mudança cultural.

REFERÊNCIAS

BERTAZZI, Danilo Marasca. *O projeto de lei de acesso à informação e seu impacto sobre os servidores públicos.* Estudos em Liberdade de Informação: dilemas da implementação, [S.l.], 2011, p. 25-38.

BEZERRA, Maria Ruth Borges. Autoridade nacional de proteção de dados pessoais: a importância do modelo institucional independente para a efetividade da lei. *Caderno Virtual*. Brasília, v. 2, n. 44, 2019.

BIONI, B. R. *Xeque-Mate*: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. GPoPAI/USP, 2015.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2018.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. E-book. Acesso restrito via Minha Biblioteca.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990.* Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm.

BRASIL. *Projeto de lei nº 2.126, de 2011***.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Câmara dos Deputados, 2011. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255.

CANCELIER, Mikhail Vieira de Lorenzi; CRISTO, Camila Kohn de; MAFRA, Gabriela. *Evasão de informações privadas:* proteção à privacidade nos casos de pornografia de vingança. 2017.

DONEDA, Danilo. *A proteção de dados pessoais como direito fundamental*. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011.

FERNANDES, R.A. *Governança de tecnologia da informação com o advento da Lei Geral de Proteção de Dados.* 2020. 44f. Monografia. Universidade de São Paulo. 2020.

FERNANDES. R. A. *Governança Corporativa no Cenário Brasileiro*. Disponível em: https://swisscam.com.br/publicacao/doing-business-in-brazil/5-governancacorporativa-no-cenario-brasileiro/. 2019. Acesso em: 23 nov 2020.

GOODRICH, Michael T.; TAMASSIA, Roberto. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013. E-book. Acesso restrito via Minha Biblioteca.

LEMOS, André; LÉVY, Pierre. *O futuro da internet:* em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

MALHEIRO. Luíza Fernandes. *O consentimento na proteção de dados pessoais na Internet*: uma análise comparada do Regulamento Geral de Proteção de Dados europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (Bacharelado em Direito) — Universidade de Brasília, Brasília, 2017.

MARINELI, Marcelo Romão. *Privacidade e redes sociais virtuais*. Rio de Janeiro: Lumen Juris, 2017.

MENDEL, Toby. *Liberdade de informação*: um estudo de direito comparado. 2. ed. Brasília: UNESCO, 2009.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. E-book. Acesso restrito via Minha Biblioteca.

NAZARENO, C. *As mudanças promovidas pela Lei n°13.243, de 11 de janeiro de 2016* (novo Marco Legal de Ciência, Tecnologia e Inovação) e seus impactos no setor. Consultoria Legislativa da Câmara dos Deputados. Estudo Técnico. 2016.

OLIVEIRA, Mike Henrique Jacinto de. *Marco regulatório da internet brasileira*: a proteção ao direito à privacidade com elemento fundamental nas relações de comércio eletrônico. Iuris in mente: revista de direito fundamentais e políticas públicas. Itumbiara, ano II, n. 2, p. 40-61, 2017.

RIBEIRO, L. *Proteção de dados pessoais:* Estudo comparado do regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016. Brasília, p. 5 – 24, 2016.

SANTOS, Manoel J. Pereira dos. *Responsabilidade Civil na Internet e demais Meios de Comunicação.* 2. ed. São Paulo: Saraiva, 2014.

SOLOVE, D. J. (2004). *The digital person*: technologyandprivacy in theinformation age. New York: New York University Press.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco civil da internet*: construção e aplicação. Juiz de Fora: Editar Editora Associada Ltda, 2016. E-book. Disponível em: https://itsrio.org/wpcontent/uploads/2017/02/marco_civil_construcao_aplicacao.pdf.