A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A *COMPLIANCE* PARA ADEQUAÇÃO DAS INSTITUIÇÕES DE ENSINO SUPERIOR PRIVADAS

Milcíades Alves de Almeida

Aluno do 10º período de Direito
ULBRA Guaíba

Pedro Reinaldo Feiten

Professor Orientador
ULBRA Guaíba

RESUMO: o presente artigo aborda as questões jurídicas e administrativas da adequação e conformidade da Lei Geral de Proteção de Dados Pessoais (LGPD) nas Instituições de Ensino Superior (IES) Privadas, considerando o atual cenário social, em que a informação representa o poder na chamada Sociedade da Informação, em um mundo cada vez mais digital e virtual, no qual a preocupação com a privacidade e a proteção de dados pessoais se torna premente. O universo da educação superior no Brasil inclui mais de 2.500 instituições, entre universidades, centros universitários e faculdades, sendo a grande maioria (88,2%) da iniciativa privada, com um quantitativo de mais de 6,3 milhões de alunos matriculados. As IES processam diariamente os dados pessoais destes milhões de alunos, então, necessitam observar as determinações da LGPD para a devida adequação. Faz-se uma comparação entre a legislação brasileira (LGPD), em vigor desde 2020, e a europeia (Regulamento Geral de Proteção de Dados - RGPD), em vigor desde 2018, e que serviu de base para a LGPD. Por fim, é proposto um programa de *compliance* para adequação das IES privadas à LGPD, contendo algumas etapas e considerações jurídicas, com base na bibliografia especializada, na experiência profissional, nos padrões internacionais e na legislação específica.

Palavras-Chave: Lei Geral de Proteção de Dados; *Compliance*; Instituições de Ensino Superior

1 INTRODUÇÃO

Vive-se hoje a Sociedade da Informação, também conhecida como a Era do Conhecimento, Sociedade Pós-Industrial ou a Indústria 4.0. Um novo modelo de civilização nascendo, envolvendo uma nova maneira de viver e conviver em sociedade. Nesse mundo contemporâneo, a informação é poder. E as principais fontes do conhecimento provêm dos dados brutos e informações sobre as pessoas.

O conhecimento passou a ser a forma dominante de produção da riqueza. Para em uma guerra, por exemplo, a tecnologia digital, representada como um pequeno chip de silício como matéria-prima dos processadores dos computadores, pode substituir milhares de soldados e até toneladas de dinamite (HARARI, 2018). O domínio da tecnologia tornou-se ingrediente principal dos armamentos inteligentes, capazes de atingir alvos específicos com altíssima precisão.

Diante deste novo cenário, a preocupação com a privacidade dos cidadãos e o tratamento de dados pessoais são cruciais (MONCAU, 2018). Assim, surgem novas leis e regulamentos globais que, segundo Oliveira et al (2019), causam impacto direto tanto na atividade econômico-empresarial quanto na atuação do próprio Estado.

Segundo o Censo da Educação Superior Brasileira de 2018 (INEP, 2020), o Brasil possuía 2.537 instituições de ensino superior, sendo 2.238 privadas – o que representa 88,2%. No setor privado havia 27.346 cursos de graduação com 6.373.274 alunos matriculados. Conforme o Sistema Nacional de Avaliação do Ensino Superior (SINAES), todas as instituições de ensino superior devem preencher os dados anuais do censo de todos seus alunos.

Conforme Tepedino *et al* (2019), o termo *compliance* refere-se a uma conformidade ou adequação de uma empresa a uma legislação vigente. Um programa de destes tem o objetivo de uma adequação planejada e monitorada. Com a entrada em vigor da LGPD, este tratamento de dados pessoais de alunos, professores e funcionários deverá ser adequado, por meio de um programa de *compliance* aos requisitos da nova lei.

2 A SOCIEDADE DA INFORMAÇÃO E A PROTEÇÃO DE DADOS PESSOAIS

Abordando a questão da evolução da nossa sociedade nos últimos três séculos, a partir dos adventos das revoluções industriais, que mudaram as relações

jurídicas, relações profissionais e os meios de produção (CORREA, 2018), (HARARI, 2018), (PINHEIRO, 2016) e (REIS, 2020). O reflexo da evolução da sociedade atinge em cheio a educação superior, como o modo de formação de mão de obra especializada para atuar nesta nova realidade do século XXI.

Com a era das comunidades interconectadas, as questões de privacidade e proteção de dados alcançam uma importância ainda maior, considerando o aspecto das ameaças virtuais a que todos os indivíduos ficam expostos com a utilização de tecnologias online, 24 horas por dia, que rastreiam e vigiam os seus passos, sejam virtuais ou não.

2.1 A SOCIEDADE DO SÉCULO XXI E A EDUCAÇÃO SUPERIOR

A primeira Revolução Industrial, no final do século XVIII, mudou a forma de produção da forma artesanal para a mecânica, com a introdução dos motores a vapor. A Segunda Revolução Industrial, no final do século XIX e início do século XX, foi caracterizada pela utilização da energia elétrica e pelo fordismo – linha de produção de Henry Ford. A Terceira Revolução Industrial, por volta dos anos 1970, foi caracterizada pelo uso da computação e suas tecnologias (computadores, software, redes, internet), que alterou com o advento da automação as tarefas mecânicas e repetitivas.

A Quarta Revolução Industrial, ora em curso, também chamada de Indústria 4.0, veio consolidar a era da Sociedade da Informação, na qual um conjunto de tecnologias, como inteligência artificial, robótica e *big data*, permitirá a fusão do mundo físico, digital e até biológico. Este novo panorama da Sociedade da Informação estabelece novos desafios para a vida em sociedade, seja nas relações profissionais – novas profissões, nas relações jurídicas – o Direito Digital (PINHEIRO, 2016), quanto em um novo modelo de educação – a Educação 4.0 (REIS, 2020).

No Brasil, a Lei nº 12.965/2014 – conhecida como Marco Civil da Internet – demonstra a necessidade de novas legislações para o século XXI e a evolução do Direito para se adequar à Sociedade da Informação. Isso determina a própria segurança do ordenamento e da estabilidade do sistema jurídico.

Novas tecnologias, novas relações jurídicas e novas relações contratuais de trabalho requerem um novo perfil para a formação dos profissionais do Direito. Ou seja, o novo ramo do Direito Digital deve ser entendido e estudado de modo a criar

instrumentos capazes de atender aos anseios da nova realidade social, entre os quais, o direito à privacidade, do direito de imagem, da propriedade intelectual, da segurança da informação, dos processos contra *hackers* e outras ameaças digitais (PINHEIRO, 2016).

Um novo modelo de educação superior se faz necessário para acompanhar os desafios da Sociedade da Informação. Novas habilidades e competências, com o uso de tecnologias de informação e comunicação (TICs), em um cenário em que o modelo presencial tradicional está perdendo espaço, em contrapartida do aumento da modalidade de educação a distância (EAD), como pode ser visto nos dados do Censo do Ensino Superior (INEP, 2020).

No final de 2019, o Ministério da Educação publicou a portaria nº 2.117, na qual a oferta de carga horária na modalidade EAD em cursos de graduação presenciais que era de até 20% passou para até 40% da carga horária total dos cursos. O artigo 4º desta portaria dispõe que este percentual EAD deve utilizar metodologias de aprendizagem com o uso de TICs para a realização dos objetivos pedagógicos. Passa-se a um modelo híbrido de educação, em que os alunos podem utilizar de atividades online e este formato vira uma tendência para a educação superior como um todo (REIS, 2020).

Com o advento da pandemia da Covid-19, a partir de março de 2020, que colocou o Brasil e o mundo em estado de calamidade, com o distanciamento social, as aulas presenciais foram suspensas e as Instituições de Ensino Superior (IES) tiveram que utilizar tecnologias da modalidade EAD, como ambientes de aprendizagem virtuais, aumentando para quase 100% dos estudantes de ensino superior a necessidade do uso de recursos tecnológicos conectados à internet.

2.2 A PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

Nesta época de Sociedade da Informação, em que tudo e todos estão interconectados, a questão da privacidade, enquanto direito fundamental do ser humano, também está sendo posta à prova. Redes sociais, como Facebook, Instagram e WhatsApp, programas de computadores para busca de conteúdo na internet, como Google Chrome, Microsoft Edge e Mozzilla Firefox, aplicativos das mais variadas espécies, como Spotify (para músicas), Netflix (filmes e séries) e Waze (geolocalização), utilizam algoritmos para rastrear o que as pessoas estão buscando,

o que estão fazendo ou postando e por onde estão caminhando, com o intuito de oferecer um melhor serviço ao usuário.

Embora haja muitas vantagens na interconexão para o teletrabalho, para o comércio eletrônico, por exemplo, a questão da privacidade do indivíduo geralmente fica prejudicada. O direito à privacidade, conforme o artigo 5º, inciso X, da Constituição Federal, a intimidade, a vida privada, a honra e a imagem das pessoas, é inviolável e é assegurado o direito a indenização se ocorrer alguma violação.

A rastreabilidade das ações humanas na internet, com a utilização de *smartphones* por grande parte da população (79,3%) e mais de 220 milhões de equipamentos (IBGE,2020), trata-se de um grande sistema de vigilância *online*.

Para CORREA (2018), o direito à privacidade está diretamente entrelaçado ao livre desenvolvimento da personalidade dos cidadãos e, até mesmo, à noção de liberdade. O direito à privacidade também protege o cidadão frente ao Estado, ou seja, impõe limites à atuação do ente coletivo e estatal (PINHEIRO, 2016).

Neste sentido, a privacidade e proteção de dados pessoais se transforma em uma espécie de respeito à liberdade e à individualidade – um escudo contra o abuso das grandes empresas de tecnologia que hospedam as redes sociais, que controla e rastreiam o tráfego de dados pela Internet, o comércio eletrônico, os sistemas operacionais dos computadores e smartphones, os aplicativos de música, que gravam suas preferências, os aplicativos de mobilidade que armazenam todo o trajeto por onde transitam as pessoas, enfim, todo um sistema que utiliza os dados pessoais sem o devido consentimento.

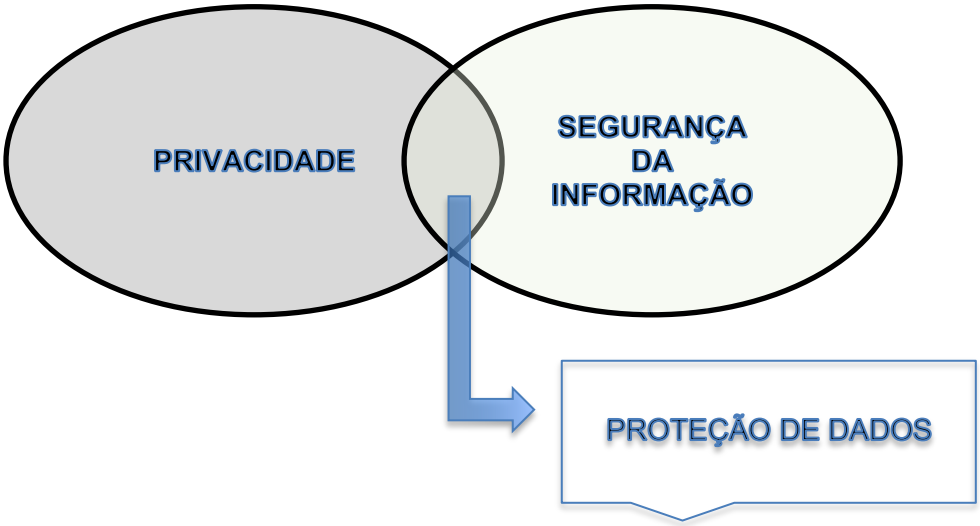
Um dos marcos históricos para a problemática da privacidade, e da consequente necessidade da proteção de dados pessoais, foi o vazamento de dados do Facebook no caso da empresa inglesa Cambridge Analytica, envolvendo cerca de 87 milhões de usuários, em que a manipulação de dados por essa empresa teve impacto na eleição presidencial dos Estados Unidos e no processo de votação para o chamado “Brexit” – a saída do Reino Unido da União Europeia (BOTELHO, 2020).

A privacidade engloba todo o ciclo de vida dos dados pessoais, desde a coleta, o tratamento e a exclusão destes dados (HINTZBERGEN et al, 2018). A segurança da informação é o requisito básico que toda organização deve proteger para manter a confidencialidade, a integridade e a disponibilidades de seus dados (FONTES, 2020).

A proteção de dados seria a intersecção entre a privacidade e a segurança da informação, visando proteger os dados pessoais contra acessos não autorizados.

Nesse contexto, os termos privacidade, proteção de dados e segurança da informação são utilizados quase como sinônimos, embora possam ser diferenciados para que se possa compreender melhor, conforme a Figura 1 a seguir.

Figura 1: Compreensão da relação entre os conceitos de privacidade, segurança da informação e proteção de dados pessoais.



Fonte: Elaborado pelo autor.

3 A LEGISLAÇÃO BRASILEIRA (LGPD) E A EUROPEIA (RGPD)

Nos últimos anos, com a Quarta Revolução Industrial em pleno desenvolvimento, dezenas de países elaboraram suas legislações com o foco na proteção de direitos e garantias fundamentais para os cidadãos, com o objetivo de diminuir os riscos à privacidade dos dados pessoais. A entrada em vigor do RGPD, somada ao interesse do Brasil em entrar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige como requisito a vigência de uma regulamentação sobre o tema, foi forte incentivo para que a lei brasileira saísse do papel (MULHOLLAND, 2020).

A LGPD (Lei nº 13.709/2018) foi aprovada em 10 de julho de 2018 pelo Senado Federal, sendo sancionada pelo presidente Michel Temer em 14 de agosto de 2018. Sobre a vigência da LGPD, as Leis nº 13.853/2019 e 14.010/2020 alteraram o prazo previsto inicial, permanecendo três datas diferentes. Quanto aos artigos referentes à Autoridade Nacional de Proteção de Dados (ANPD) e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, vigência iniciou-se a partir de 28 de dezembro de 2018. Quanto aos artigos referentes às sanções administrativas, a vigência será a partir de 1º de agosto de 2021. E quanto aos demais artigos, a vigência começou em 14 de agosto de 2020 (vinte e quatro meses após a publicação).

O artigo 8º da Carta dos Direitos Fundamentais da União Europeia, do ano 2000, dispõe que todos têm direito à proteção dos dados pessoais, que devem ser tratados de forma justa, para fins específicos, com base no consentimento do titular ou em outra base legítima, além de terem o direito de acessar os seus dados coletados e o direito de retificá-los (MALDONADO; BLUM, 2020).

Em 2016, o parlamento da União Europeia aprovou o Regulamento Geral de Proteção de Dados (RGPD), sob o número EU 2016/679, com vigência a partir de 25 maio de 2018. Anteriormente, o Parlamento Europeu já havia aprovado a Diretiva[1] 95/46/CE, que consistia em uma orientação para estabelecer uma melhor proteção da vida privada das pessoas e a livre circulação de dados pessoais na União Europeia (ITGP, 2020) e (MALDONADO; BLUM, 2020).

3.1 O RGPD COMO BASE PARA A LGPD

A estrutura do RGPD é composta de 99 artigos dispostos em 11 capítulos e 173 considerandos[2] - localizados antes da disposição dos artigos. A abrangência envolve a proteção de dados pessoais dos titulares localizados na Área Econômica Europeia, formada por 30 países, independentemente de onde o tratamento estiver acontecendo.

[1] Vale ressaltar a diferença entre diretiva e regulamento, conforme art. 288 do Tratado sobre o Funcionamento da União Europeia, de 13 de dezembro de 2007. O regulamento é imediatamente aplicável na ordem jurídica interna dos países da União Europeia após a sua entrada em vigor, como foi o caso do RGPD. A diretiva não é diretamente aplicável, devendo ser objeto de transposição para o direito nacional para que possa ser aplicável em cada país (ITGP, 2020).

[2] Considerandos são utilizados pelo Tribunal de Justiça da União Europeia para esclarecer um contexto da aplicação da legislação.

3.1.1 Definições principais do RGPD

O artigo 4º do RGPD traz as principais definições utilizadas na legislação, entre as quais, a definição de dados pessoais, ou seja, a informação relativa a uma pessoa singular identificada ou identificável (o titular dos dados).

A definição de tratamento de dados como um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados. Isto significa que não somente operações em sistemas de computadores representam tratamento. Operações sobre dados em papel, datilografados ou manuscritos também são consideradas.

A Pseudonimização refere-se ao tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares – uma espécie de codificação.

O responsável pelo tratamento é a pessoa física ou jurídica que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais - as empresas, organizações ou outras pessoas que efetuam as operações sobre os dados. O subcontratante é a pessoa física ou jurídica que trate os dados pessoais por conta do responsável pelo tratamento.

Por fim, a definição de consentimento como a manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

3.1.2 Princípios aplicáveis ao tratamento de dados

O artigo 5º do RGPD descreve os princípios aplicáveis ao tratamento de dados pessoais, como o princípio da Licitude, lealdade e transparência, no qual, os dados pessoais devem ser objeto de tratamento lícito (de acordo com o Regulamento), leal (senso de justiça) e transparente (clareza de propósito).

O princípio da limitação das finalidades expressa que só devem ser coletados para finalidades específicas, explícitas e legítimas.

O princípio da minimização de dados, que devem ser limitados ao que é necessário para as finalidades para as quais são tratados.

O princípio da exatidão, no qual os dados devem ser corretos e atualizados sempre que necessário.

O princípio da limitação da conservação, em que os dados devem ser armazenados por tempo limitado, necessário para as finalidades do tratamento.

O princípio da integridade e confidencialidade, que tem relação com as garantias de segurança da informação, para que seja evitada a violação dos dados pessoais.

E, por fim, o princípio da responsabilidade, no qual a pessoa física ou jurídica que faz o tratamento de dados pessoais deve ser responsável pelo cumprimento dos princípios anteriores.

3.1.3 O direito dos titulares no tratamento de dados

Os titulares têm os seguintes direitos, conforme o RGPD: direito de informação; direito de acesso; direito de retificação; direito ao apagamento de dados (“direito a ser esquecido”); direito à limitação de tratamento; direito à portabilidade de dados; direito de oposição; e o direito de objeção quanto a decisões individuais automatizadas. Estes são os direitos que as organizações devem respeitar para o tratamento de dados pessoais.

O tratamento de dados pessoais somente é permitido se o responsável pelo tratamento cumprir os princípios expostos anteriormente e atender a uma das seis hipóteses taxativas previstas no artigo 6º: a) O consentimento para o tratamento dos dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa física; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

3.1.4 Autoridades públicas independentes

O RGPD também dispõe que os Estados Membros da União Europeia devem designar uma ou mais autoridades públicas independentes para a fiscalização e aplicação do Regulamento, sob a supervisão geral do Comitê de Proteção de Dados Europeu. Estas autoridades devem fazer cumprir o Regulamento em cada país membro, incluindo as sanções.

O artigo 83 estabelece as condições gerais para aplicação de sanções pecuniárias. Entre os fatores que influem na dosimetria das penas, que são decididas de acordo com as particularidades de cada caso (MALDONADO; BLUM, 2020). As multas administrativas[3] devem, dependendo das circunstâncias de cada caso individual, ser impostas em complemento a outras sanções, como advertências, repreensões, obrigações de cumprimento de direitos, estabelecimento de medidas específicas ou, até mesmo, a limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição (ITGP, 2020).

O RGPD prevê duas faixas de multa, de acordo com a gravidade das infrações: no caso de infrações mais leves, as multas podem chegar a 10 milhões de Euros ou 2% do faturamento bruto mundial da empresa ou conglomerado no exercício fiscal anterior a instauração do processo – o que for maior; e para as infrações mais graves, o patamar é elevado para 20 milhões de Euros e 4% do faturamento bruto.

No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública, criada pela LGPD (artigo 55-A), está se estruturando para regulamentar várias questões ainda pendentes, como por exemplo:

i) Artigo 12, § 3º - sobre comunicação ou uso compartilhado de dados pessoais sensíveis;
ii) Artigo 13, § 3º - sobre padrões e técnicas para processos de anonimização;
iii) Artigo 18, V – sobre portabilidade de dados;
iv) Artigo. 27, parágrafo único – sobre o compartilhamento entre da pessoa jurídica de direito público a pessoa de direito privado;
v) Artigo 30 – sobre normas complementares para as atividades de comunicação e de uso compartilhado;

[3] O valor total em multas pecuniárias até 21/05/2021 já somava mais de 283 milhões de Euros, em um total de 648 multas aplicadas – fonte: https://www.enforcementtracker.com/?insights.

vi) Artigo 40 - sobre padrões de interoperabilidade e tempo de guarda de registros;
vii) Artigo 46, § 1º - sobre padrões técnicos mínimos para medidas de segurança;
viii) Artigo 53, caput - sobre sanções administrativas a infrações; e
ix) Art. 63 - sobre a adequação progressiva de bancos de dados.

3.2 COMPARAÇÃO ENTRE LGPD E RGPD

Baseada no RGPD, a LGPD está dividida em 65 artigos dispostos em dez capítulos. A própria estrutura geral dos capítulos da LGPD segue semelhante à organização do RGPD, sendo a legislação brasileira mais resumida em vários aspectos (MULHOLAND, 2020).

A LGPD apresenta diversos pontos de convergência com o RGPD, de maneira que o consentimento para o tratamento de dados pessoais se faz extremamente necessário e protegido por ambas as leis (PINHEIRO, 2018). A informação aos titulares dos dados sobre eventuais incidentes, prova do consentimento, portabilidade de dados, indicação e responsabilidade dos agentes encarregados pela operacionalidade dos dados e as regras de segurança para armazenamento, transmissão e manuseio são pontos essenciais e regulados pela LGPD que constam também no Regulamento europeu (TEPEDINO *et al,* 2019).

As definições são semelhantes, porém algumas nomenclaturas diferem entre as legislações, tais como: controlador e operador na LGPD e responsável pelo tratamento e subcontratante no RGPD, na versão em língua portuguesa (de Portugal). Na versão em língua inglesa, usam-se os termos *controller* e *processor*. O Quadro 1 a seguir demonstra um comparativo genérico entre as legislações brasileira e europeia.

Quadro 1: Comparativo genérico entre a LGPD e o RGPD.

Item de Comparação	LGPD	RGPD
Estrutura	10 capítulos e 65 artigos	11 capítulos, 99 artigos e 173 considerandos

Item de Comparação	LGPD	RGPD
Multa	Até 20 milhões de Euros ou 4% do faturamento bruto	Até 50 milhões de Reais ou 2% do faturamento bruto
Princípios	Finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização	Licitude, lealdade e transparência; limitação das finalidades; minimização de dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade
Bases legais para o tratamento de dados pessoais	Consentimento explícito; necessidade contratual; execução de políticas públicas; interesse vital; obrigação legal; interesse legítimo; a proteção da saúde em um procedimento realizado por profissionais de saúde; realização de estudos por um órgão de pesquisa; exercício de direitos em processos judiciais; proteção ao crédito	Consentimento explícito; necessidade contratual; execução de políticas públicas; interesse vital; obrigação legal; interesse legítimo.
Prazo para notificação sobre violação de dados	Não especifica, apenas cita prazo “razoável”	72 horas
Prazo para atendimento às solicitações de acesso dos titulares	15 dias	30 dias
Nomeação do responsável pela proteção de dados	Exige apenas dos controladores	Exige que tanto os controladores quanto os operadores
Avaliação de impacto sobre a proteção de dados pessoais	Declara que a ANPD pode decidir quando um controlador deve conduzir tal avaliação e não dispõe de detalhes sobre os critérios para essa avaliação	Detalha quando requer tais avaliações, assim como os aspectos que as avaliações devem cobrir

Fonte: Elaborado pelo autor.

Tanto o RGPD quanto a LGPD exigem que controladores e operadores implementem medidas de segurança apropriadas para proteger os dados pessoais. O primeiro é mais normativo a este respeito, enquanto a LGPD atribui à ANPD a emissão de orientações sobre medidas de segurança específicas a serem adotadas.

O Regulamento europeu, de forma geral, tem mais detalhes sobre a implantação, visto que se trata de uma legislação que serve para 30 países, onde cada um pode fazer alguns ajustes e adequações. A legislação brasileira ainda deixa muitos pontos a serem definidos pela ANPD, que apenas muito recentemente começou a funcionar efetivamente e as primeiras orientações e definições ainda estão sendo elaboradas e publicadas.

4 *COMPLIANCE* PARA IMPLEMENTAÇÃO DA LGPD EM INSTITUIÇÕES DE ENSINO SUPERIOR NO BRASIL

O termo *compliance* vem sendo utilizado no Brasil, principalmente ligado às áreas de governança corporativa e para a área legal, como sinônimo de conformidade ou integridade. As organizações estão utilizando programas de *compliance* como um conjunto de ações que devem ser implantadas no meio corporativo para que seja reforçada e comprovada a adequação e a conformidade da empresa à legislação vigente, de modo que se tenha uma prevenção para a ocorrência de infrações ou, se já tiver ocorrido algum ilícito, que seja possível o retorno imediato ao contexto de normalidade e legalidade (TEPEDINO; FRAZÃO; OLIVA, 2019).

Em se tratando da LGPD, para que as Instituições de Ensino Superior façam a adequação e, consequentemente, a conformidade com essa legislação, faz-se necessário a proposição de um programa de *compliance*. Cada organização deve elaborar seu próprio programa, de acordo com o caso concreto e a realidade com que trata as questões de privacidade e proteção de dados pessoais.

Para este trabalho, é proposto um modelo genérico, com base no levantamento bibliográfico, na experiência profissional de quase trinta anos do autor na área de informática e gestão e de mais de vinte e dois anos na área de ensino superior, e na legislação concernente ao assunto da privacidade e proteção de dados pessoais.

O foco deste modelo está na questão dos dados pessoais dos alunos, especialmente, por este representar o maior universo de dados tratados nas IES.

Questões relacionadas a funcionários, docentes, fornecedores, serviços terceirizados e dados enviados para o exterior também são importantes e estão previstos na LGPD, mas por questão de limitação da pesquisa, não serão abordados neste trabalho.

4.1 ETAPAS PARA ADEQUAÇÃO À LGPD

4.1.1 Aspectos primordiais no tratamento de dados de alunos

Alguns pontos principais de atenção para as IES no tratamento de dados pessoais dos alunos envolvem, primeiramente, o tratamento de dados de menores de idade - de acordo com o artigo 14, § 1º, da LGPD, o consentimento deverá ser a base legal, devendo ser manifestado por um de seus pais ou pelo responsável legal. Este é um tópico que a gestão da IES deve levar em consideração, pois os menores de 18 e maiores de 16 anos – idade comum para a entrada de novos alunos, são relativamente incapazes, nos termos do artigo 4º do Código Civil.

O tratamento de dados como religião, raça ou cor da pele, biometria e identidade de gênero, que são dados sensíveis, nos termos do artigo 5º, inciso II, e do artigo 11, da LGPD, muitas vezes coletados durante a matrícula em algumas IES. Isto envolve a questão da minimização, ou seja, cuidar da devida adequação e finalidade dos dados pessoais tratados, e das obrigações legais – exigência de compartilhamento com outros entes, como o INEP/MEC.

Além desses aspectos relacionados acima, a segurança, o local e os prazos de armazenamento dos dados pessoais dos alunos são primordiais para a definição de um programa de *compliance* para adequação da IES à LGPD.

4.1.2 Uma proposta de etapas para adequação

Em uma compilação de vários autores, como (DONDA, 2020), (TEPEDINO; FRAZÃO; OLIVA, 2019), (MULHOLLAND, 2020) e (PINHEIRO, 2020), as etapas de adequação à LGPD, de forma geral, abrangem as seguintes atividades, conforme descritas a seguir.

Primeiramente, a criação de um Sistema de Gerenciamento de Privacidade e Proteção de Dados (SGPPD) alinhado com o planejamento da IES. Documentos, planos e relatório elaborados pela gestão institucional, como o planejamento

estratégico, contendo, geralmente, o plano de ações e responsabilidades de projetos para um determinado período. O alinhamento ao PDI (Plano de Desenvolvimento Institucional), que é o documento oficial que as instituições devem protocolar junto ao MEC, contendo o projeto quinquenal de desenvolvimento pedagógico, administrativo e de sustentabilidade.

Dependendo do tamanho da instituição, o modelo de governança corporativa e o programa de *compliance* institucional já existente devem alimentar a elaboração e implantação do SGPPD.

Em seguida, a criação de um Comitê de Privacidade e Proteção de Dados Pessoais, com a participação da alta gestão, nomeando uma equipe de profissionais (internos com possibilidade de participação externa) para definir os rumos de adequação à LGPD.

Dentre estes profissionais, se enquadra a figura do Encarregado de Proteção de Dados (função similar ao DPO – *Data Protection Officer* – do RGPD), nos termos dos artigos 5º, inciso VIII, e 41, da LGPD. As atribuições do DPO envolvem a gestão de comunicação (reclamações, prestar esclarecimentos e adotar providências) com os titulares e com a ANPD, a orientação de funcionários e os contratados da IES a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, além de outras atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O DPO pode ser tanto uma pessoa física, de dentro do quadro de colaboradores da IES, quanto uma terceirizada, ou ainda uma pessoa jurídica. Algumas empresas de consultoria e assessoria jurídica oferecem o serviço de terceirização da função de DPO.

Para avaliação de riscos de vulnerabilidade e violação de dados pessoais, deve ser realizado o mapeamento do ciclo de vida dos dados dos alunos na IES, desde a coleta, geralmente na inscrição para o processo seletivo ou vestibular, até a entrada de dados para efetivação da matrícula.

Já no site de inscrição no vestibular, deve constar a devida definição da finalidade dos dados dos alunos, inclusive com as cláusulas contratuais e consentimentos devidos, nos termos do artigo 8º da LGPD. Se a inscrição for presencial ou manual, o formulário também deve conter a finalidade de coleta e armazenamento dos dados dos alunos.

Além da coleta, o mapeamento do ciclo de dados, inclui a retenção, o processamento, o compartilhamento e a eliminação dos dados dos alunos.

Quanto à retenção, deve-se analisar as formas de armazenamento e catalogação (documentos em papel, documentos eletrônicos, bancos de dados).

No processamento, a definição de quais os tratamentos são realizados com os dados dos alunos.

O compartilhamento, ou seja, com quem os dados são compartilhados, como o MEC, empresas de cobrança, assessorias de marketing, ambientes virtuais de aprendizagem de terceiros, bancos e instituições financeiras. Estes são os operadores, nos termos do artigo 5º, inciso VII, da LGPD, que recebem os dados e realizam o tratamento de dados pessoais dos alunos em nome do controlador (a IES).

E a eliminação, ou seja, o descarte dos dados armazenados (em papel ou em meio eletrônico), dentro da legislação educacional.

O resultado do mapeamento do ciclo de vida de dados é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), nos termos do artigo 5º, inciso XVII, da LGPD, que é a documentação da IES que contém a descrição dos processos de tratamento que podem gerar riscos à privacidade e proteção de dados pessoais dos alunos.

Por fim, a elaboração de um plano de ações para situações de emergência, com a adoção de padrões de segurança da informação, como as normas ABNT ISO 27001, 27002, 27701 (HINTZBERGEN *et al*, 2018), nos termos do artigo 50, inciso I, da LGPD.

4.2 A *COMPLIANCE* PARA AS INSTITUIÇÕES DE ENSINO SUPERIOR

Um programa de *compliance* vai muito além da conformidade com as leis. Deve ser encarada como uma forma de autorregulação, por meio de normas de conduta que estabelecem valores éticos e boas práticas de convivência em uma organização.

O artigo 50 da LGPD estabelece que as IES podem elaborar regras de boas práticas e de governança, definindo em seu inciso I o programa de governança de privacidade, enquanto o inciso II define o objetivo de um programa de *compliance*, ao citar a necessidade de demonstração de efetividade, para uma eventual solicitação da ANPD ou outra entidade, para promover o cumprimento das determinações da LGPD.

Embora o foco deste trabalho seja a LGPD, quando se trata de *compliance*, outras legislações também devem ser envolvidas, principalmente as que cuidam da

relação jurídica entre o aluno e a IES, formalizada por um instrumento contratual de prestação de serviços educacionais, geralmente de período semestral ou anual. Ou seja, uma relação de consumo entre cliente (aluno) e prestador de serviço (IES), implicando no âmbito do Código de Defesa do Consumidor (CDC).

O CDC e a LGPD reforçam as necessidades de consentimento do consumidor para uso de seus dados pessoais, com a devida definição de finalidade do uso destes dados. Por isso, a adequação das IES à LGPD deve levar em consideração a reavaliação dos contratos dos alunos, assim como com fornecedores com os quais os dados pessoais são compartilhados.

A implantação de um programa de *compliance*, com base na legislação, na bibliografia especializada, nas normas padronizadas e nas boas práticas do mercado, deve envolver um monitoramento de conformidade que contemple:

i) Comitê de auditoria internas, composta por profissionais da própria IES, estando sempre presentes o jurídico e o setor de privacidade;
ii) Auditoria externa, realizada por empresa ou profissional terceirizado independente;
iii) Gestão de riscos, por meio de análise de vulnerabilidades e possibilidades de ocorrências de não-conformidade;
iv) Indicadores de acompanhamento, definidos pelo comitê de auditoria, para que sejam acompanhados continuamente.

Esta estrutura e funcionamento propostos podem variar muito nos casos concretos, a depender do tamanho da instituição e da sua estrutura de governança corporativa.

O setor de *compliance*, que pode ser um funcionário, uma equipe interna ou até mesmo uma consultoria externa, será o responsável por assegurar a conformidade legal, com a missão de adequar a IES à LGPD e acompanhar o desempenho da organização efetuando os ajustes necessários.

A LGPD traz consigo o dever de segurança, ética e responsabilidade quando se trata de dados pessoais dos alunos. O objetivo é que as regras e princípios de privacidade e proteção de dados pessoais sejam incorporados pela instituição, passando a integrar sua missão e seus valores.

5. CONSIDERAÇÕES FINAIS

A LGPD é uma legislação recente e que está sendo implantada em uma situação histórica atípica - a pandemia do coronavírus, que está acelerando a Sociedade da Informação no uso de tecnologias para o trabalho e para o processo de ensino-aprendizagem, principalmente, com a questão da necessidade de distanciamento social e outras medidas sanitárias, que impulsionaram as tendências do teletrabalho e do ensino híbrido com o uso de tecnologias da informação e comunicação.

O objetivo deste trabalho foi o de realizar uma análise dos desafios jurídicos e administrativos, por meio de um programa de *compliance* para adequação das IES privadas à LGPD, mais especificamente no que concerne ao tratamento de dados pessoais dos alunos.

Foi demonstrada a herança da LGPD de vários aspectos do RGPD, que também influenciou diversos outros países, visto que será um requisito para que as empresas de outros países possam fazer negócios com a Comunidade Europeia. Embora a LGPD já esteja em vigor para a maioria de seus artigos desde agosto de 2020, somente em agosto deste ano entrarão em vigor os artigos 52 a 54 das sanções administrativas. Há ainda uma série de regulamentações complementares pendentes na LGPD, conforme elencados no tópico 3.1.

Foram apresentados, com base na legislação, na experiência profissional e nas melhores práticas do mercado, etapas e processos para adequação e conformidade da LGPD, além da proposta de implantação de um programa de *compliance*, abordando aspectos jurídicos e administrativos para as IES privadas.

Para esta adequação, as IES precisarão conduzir uma mudança de cultura organizacional, de forma a conscientizar todos sobre as determinações da LGPD e sobre o ônus que a não-conformidade pode trazer para a organização. Além de ter as ferramentas de controle, é preciso criar a cultura de proteção de dados pessoais e fazer bom uso da tecnologia disponível para isso.

Como possibilidade de trabalhos futuros, pode-se indicar o aprofundamento em dados pessoais de professores e funcionários e os reflexos nas relações de trabalho, o que envolve o Direito do Trabalho e Direito Civil. Da mesma forma, as outras legislações, posições doutrinárias e a futura jurisprudência quando a LGPD tiver mais tempo de vigor e os casos concretos estarão acontecendo com mais frequência.

REFERÊNCIAS

BRASIL. Guia de boas práticas da Lei Geral de Proteção de Dados (LGPD**)**. **Governo Digital**, Brasília, DF, 20 abr. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 27 ago. 2020.

_____. Decreto nº 13.709, de 26 de agosto de 2020. **Diário Oficial da União**. Poder Executivo, Brasília, DF, 27 ago. 2020. Seção 1, Página 6. Disponível em: https://in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020/274389226. Acesso em: 29 ago. 2020.

_____. Lei nº 10.474, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 ago. 2020.

_____. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet no Brasil**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 ago. 2020.

_____. Supremo Tribunal Federal. Medida cautelar na ação direta de inconstitucionalidade 6.390 Distrito Federal. 27 abr. 2020. **Diário da Justiça Eletrônico**, n. 102 p. 62-65. Disponível em: https://www.stf.jus.br/arquivo/djEletronico/DJE_20200427_102.pdf. Acesso em: 20 ago. 2020.

BOTELHO, Marcos César. A proteção de dados pessoais enquanto direito fundamental: considerações sobre a Lei Geral de Proteção de Dados Pessoais. **Argumenta Journal Law**. Jacarezinho, n. 32 p. 191-208, janeiro-junho 2020. Disponível em: http://seer.uenp.edu.br/index.php/argumenta/article/view/1840. Acesso em: 25 ago. 2020.

CORREA, Rodrigo Henrique Luiz. **Big data e criptografia: o lugar do direito fundamental à privacidade diante das novas tecnologias da informação e comunicação**. Dissertação (Mestrado em Direito), Faculdade de Direito, Universidade Estadual do Rio de Janeiro. Rio de Janeiro, 2018. Disponível em: http://152.92.4.120:8080/handle/1/9851. Acesso em 23 ago. 2020.

DONDA, Daniel. **Guia prático de implementação da LGPD**: tudo que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

FONTES, Edison Luiz Gonçalves. **Segurança da informação: gestão e governança**. São Paulo: Edição do Autor, 2020.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

HARARI, Yuval Noah. **21 Lições para o século 21**. São Paulo: Companhia das Letras, 2018.

IBGE (Instituto Brasileiro de Geografia e Estatística. **Uso de internet, televisão e celular no Brasil**. Rio de Janeiro: IBGE, 2020. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html/. Acesso em: 24 abr. 2021.

INEP. **Resumo Técnico do Censo da Educação Superior**. Brasília: INEP, 2020. Disponível em: http://portal.inep.gov.br/web/guest/resumos-tecnicos1/. Acesso em: 10 out. 2020.

ITGP (IT Governance Privacy Team). **EU general data protection regulation (GDPR):** an implementation and compliance guide**.** 4. ed. Cambridshire: IT Governance Plubishing, 2020.

HINTZBERGEN, Jule. HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação:** com base na ISO 27001 e ISO 27002. Rio de Janeiro: Brasport, 2018.

LENZA, Pedro. **Direito constitucional esquematizado**. 20 ed. São Paulo: Saraiva, 2016.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR:** regulamento geral de proteção de dados da União Europeia. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MONCAU, Luiz Fernando Marrey. **Direito ao esquecimento: entre a liberdade de expressão, a privacidade e a proteção de dados pessoais**. Tese (Doutorado em Direito), Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2018.

MULHOLLAND, Caitlin (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

OLIVEIRA, Ana Paula; ZANETTI, Dânton; LIMA, Flávio Santos; SAMPAIO, Themis Ortega. A Lei Geral de Proteção de Dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**. Curitiba, v. 4 n. 1 p. 172-

200, maio 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-9.pdf. Acesso em: 25 ago. 2020.

PINHEIRO, Patrícia Peck. **Direito Digital.** 6. ed. São Paulo: Saraiva, 2016.

_____. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD)**.** São Paulo: Saraiva, 2018.

REIS, Fábio (organizador). **Revolução 4.0:** a educação superior na era dos robôs**.** São Paulo: Editora da Cultura, 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei geral de proteção de dados e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

PARECER DE ADMISSIBILIDADE

O acadêmico MILCÍADES ALVES DE ALMEIDA apresenta o Trabalho de Conclusão de Curso sobre o tema: "A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E A COMPLIANCE PARA IMPLEMENTAÇÃO NAS INSTITUIÇÕES DE ENSINO SUPERIOR PRIVADAS". Analisamos e discutimos juntamente o trabalho elaborado, o mesmo encontra-se em conformidade com as normas e diretrizes do regulamento que o disciplina. Assim, o acadêmico preencheu com satisfação todos os requisitos de admissibilidade do presente trabalho, tendo condições de entrega-lo à Coordenação do Curso de Direito da ULBRA/Guaíba.

Guaíba, 21 de junho de 2021.

Professor Ms. PEDRO REINALDO FEITEN

Orientador