PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

LGPD: UM ESTUDO SOBRE AS PRINCIPAIS RESPONSABILIDADES E PENALIDADES PREVISTAS NA LEI

GABRIEL BADIM VILELA

GOIÂNIA
2021

GABRIEL BADIM VILELA

LGPD: UM ESTUDO SOBRE AS PRINCIPAIS RESPONSABILIDADES E PENALIDADES PREVISTAS NA LEI

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.
Orientador(a): Prof.(a) Dr.(a) Fábio Barbosa Rodrigues
Banca examinadora: Prof. Dr. Eugênio Júlio M Carvalho
Prof. Dr. Jose Luiz de Freitas Junior

GOIÂNIA
2021

GABRIEL BADIM VILELA

LGPD: UM ESTUDO SOBRE AS PRINCIPAIS RESPONSABILIDADES E PENALIDADES PREVISTAS NA LEI

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia de Computação, em _____/_____/_____.

_____
Orientador(a): Fábio Barbosa Rodrigues

_____
Prof. Me. Ludmilla Reis Pinheiro dos Santo
Coordenador(a) de Trabalho de Conclusão de Curso

GOIÂNIA
2021

AGRADECIMENTOS

Ao Professor Fábio B. Rodrigues, orientador acadêmico, pelo apoio no desenvolvimento deste trabalho e pela confiança depositada.

Aos vários professores e amigos feitos, pela inestimável colaboração nesta jornada acadêmica.

À Coordenação da Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás por auxiliar-me durante toda esta jornada.

Aos meus vários colegas pelo apoio, auxílio e colaboração durante toda a jornada.

A todos aqueles que direta ou indiretamente colaboraram para a materialização deste trabalho.

“STAY HUNGRY, STAY FOOLISH”

(Steven Paul Jobs)

RESUMO

Este trabalho, conjecturando que a existência de uma lei de proteção de dados é imprescindível em um país, tem como foco principal a exposição da Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018), abordando sobre sua história, desde sua origem, necessidade da sua criação, passando pela comparação da mesma com a *General Data Protection Regulation* (GDPR), na qual foi inspirada. Para atender também ao objetivo do presente trabalho, foram abordadas principais responsabilidades e penalizações previstas na LGPD, apresentando as responsabilidades administrativas e civis presentes na lei, juntamente com as penalidades por ela previstas. Procedeu-se à exploração das vulnerabilidades, fragilidades e tendências de modo a complementar a compreensão da LGPD, além de dispor os impactos da lei na engenharia da computação, para construir uma melhor interpretação e entendimento do assunto. Constatou-se, que a LGPD cumpre, então, o seu papel na criação de normativas que visam proteger e fiscalizar de forma efetiva os dados por ela salvaguardados.

Palavras-Chave: *LGPD, Penalidades, Responsabilidades.*

ABSTRACT

This study, conjecturing that the existence of a data protection law is essential in a country, has as its main focus the exposure of the Lei Geral de Proteção de Dados (LGPD) (Law nº 13.709 / 2018), addressing its history, since its origin, need for its creation, going through its comparison with the General Data Protection Regulation (GDPR), in which it was inspired. In order to also meet the objective of the present work, the main responsibilities and penalties foreseen in the LGPD were addressed, presenting the administrative and civil responsibilities present in the law, together with the penalties foreseen by it. The vulnerabilities, weaknesses and trends were explored in order to complement the understanding of LGPD, in addition to providing the impacts of the law on computer engineering, in order to build a better interpretation and understanding of the subject. It was found, then, that the LGPD fulfills its role in the creation of regulations that aim to protect and effectively inspect the data it safeguards.

Keywords*: LGPD, Penalties, Responsibilities.*

LISTA DE IMAGENS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

Art.	Artigo
Inc.	Inciso
§	Parágrafo

LISTA DE SIGLAS

ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de dados Pessoais
CDC	Código de Defesa do Consumidor
CNH	Cadastro Nacional de Habilitação
CPF	Cadastro de pessoa Física
CRFB	Constituição da República Federativa do Brasil
CVE	*Common Vulnerabilities and Exposures*
DETRAN	Departamento Estadual de Trânsito
EC	*European Constitution*
GDPR	*General Data Protection Regulation*
GPS	*Global Positioning System*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral da Proteção de Dados
MCI	Marco Civil da internet
PUC GO	Pontifícia Universidade Católica de Goiás
RG	Registro Geral
T.I.	Tecnologia da Informação
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

A informação pode ser definida como meio necessário para a extração e expansão do conhecimento, porém para outros, ela é tida como um ativo, com isso, necessita de proteção adequada. (MACHLUP; MANSFIELD, 1983).

De acordo com Böger e Bodemüller, é possível obter um nível de segurança desejado se for bem aplicado às políticas de segurança. Formando um grupo de regras sobre o sistema, como prover os serviços, limitar os acessos de acordo com o usuário, como administrar os dados, proteção e modo de distribuição interna (BÖGER; BODEMÜLLER, 2007).

Para Mitnick, mesmo que uma empresa gaste fortunas na compra de sistemas de segurança, mas a sua rede é antiga e vulnerável, de nada adiantou o investimento, já que exploraram o elo fraco (MITNICK, 2001).

O setor da informática vem crescendo exponencialmente a cada dia que se passa. Profissionais que atuam no ramo estão se atualizando e evoluindo suas práticas e conhecimentos dos recursos e novidades nesta área. É necessário compreender o mercado e as variabilidades, entendê-lo e assim tornar as ameaças obsoletas. Do mesmo modo em que os gestores se preocupam com as informações, os invasores veem nesta dependência um meio para querer explorar tais dados. Tendo que se preocupar cada vez mais com possíveis ataques e o risco de um acesso indevido das informações, pondo a confiabilidade das informações em constante *check.* Tornando necessário uma constante manutenção da segurança onde se armazena os dados, prevenindo-se de ações criminosas.

A gestão dos dados vem evoluindo ano após ano, com ela, as ferramentas de segurança e análise vem se tornando cada vez melhor, consecutivamente, o tratamento dos dados como item valioso e que requer cuidados de invasões externas.

No início de 2019, a empresa *Avast* publicou em seu *blog* uma análise feita por Martin Hron, onde listou os 10 maiores vazamentos de dados do ano anterior. Dentre elas, estava o *FaceBook* em 7º lugar, onde a Empresa *Cambridge Analytica* coletou ilegalmente as informações de 87 milhões de usuários da plataforma. Outro caso foi o da empresa *Starwood* que ocupou a posição de 2º lugar, onde após sofrer um ataque, foi possível efetuar um acesso não autorizado no servidor, expondo todos os dados de 500 milhões de pessoas.

Já em 2019, dois ataques que valem ser mencionados são os DETRAN aqui no Brasil, onde 70 milhões dos dados dos registros de CNH vazaram. Esse ataque expôs todos os dados de 97% das CNHs vinculadas ao sistema (TAGIAROLI, 2021). O segundo foi com a empresa Canva, onde 137 milhões de usuários tiveram seus dados visualizados, porém não roubados por hackers (SWINHOE, 2020).

No Brasil a falta de priorização no surgimento de regimentos e normas, resultava na possibilidade dos usuários que tinham acesso a dados pessoais agirem da forma que desejavam, sem que houvesse consideração com qualquer direito do titular de dados pessoais. Em 2018 foi criada a Lei Geral de Proteção de Dados (lei nº 13.709/18) que entrou em vigor a partir de 16 de Agosto de 2020 e determina que empresas e poder público se adequem às novas normas de segurança de compartilhamento e proteção de dados no País. Unindo-se a outros países que já tinham legislação sobre segurança de dados (BRASIL, 2018).

Este trabalho propõe como objetivo geral, apresentar através de uma revisão bibliográfica, as principais responsabilidades e penalizações previstas na Lei Geral de Proteção de Dados (LGPD). Trazendo uma análise sobre seus principais dispositivos e mudanças no tratamento das informações.

Este trabalho será apresentado em 5 (cinco) de seus 6 (seis) capítulos, a fim de cumprir o objetivo citado neste mesmo tópico. Escrito de modo objetivo e claro, no intuito de melhorar o entendimento e maior clareza a aqueles interessados no tema.

Será abordado no capítulo 2, a construção de todo embasamento teórico para o desenvolvimento do trabalho.

Será abordado no capítulo 3, a exposição de mecanismos repressivos na Lei, discorrendo tanto sobre as responsabilidades quanto as penalidades previstas.

Será abordado no capítulo 4, uma discussão sobre a LGPD em um âmbito macro.

Será abordado no capítulo 5, a conclusão chegada ao final do estudo sobre o tema.

Será abordado no capítulo 6, todas as referências bibliográficas utilizadas neste trabalho como material de estudo e coleta de informação para embasamento e solidez a este trabalho.

2 REVISÃO BIBLIOGRÁFICA

2.1 Breve História da LGPD

Com o intuito de minimizar o risco de abusos no tratamento, coleta, tratamento e uso de transferência de dados na União Europeia, em 2016, foi divulgado o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*), estabelecendo um regime regulatório novo para os membros da União Europeia, substituiu a antiga diretiva 95/46 EC, de 199514 (Directive No. 95/46/EC. 1995) (UNIÃO EUROPEIA, 2016).

GDPR serviu como catalisador para que o Brasil criasse uma legislação própria para proteção de dados pessoais, caso o país não realizasse o mesmo, seria privado de trocar dados com a União Europeia (UE). A não adaptação à lei europeia e uma agenda regulatória para se adequar às regras globais prejudicaria diversos setores brasileiros, principalmente as empresas, enfraquecendo a competitividade e inovação da economia (BIONI, 2018).

Há uma década vem sendo debatido sobre a proteção de dados no âmbito nacional, porém judicialmente não havia um marco regulatório federal disciplinar completo e unificado, era realizado de forma esparsa, necessitando de padronização e segurança jurídica (BIONI, 2018).

A principal resposta jurídica aos problemas que vinham relacionados à hiper conectividade, até então, era a constituição federal. O artigo 5, inciso X, da Constituição da República Federativa do Brasil (CRFB) já apontava a inviolabilidade da vida privada, honra e imagens do indivíduo, com direito a indenização pelo dano material ou moral decorrente de sua violação. Outras leis como Lei do Acesso à Informação (LAI), código do consumidor (CDC), Marco civil da internet (MCI), Lei de Cadastro Positivo e a Lei de Delitos Informáticos também eram utilizadas em algumas situações quando dados pessoais eram violados (DONEDA, 2011).

O CDC aponta os direitos básicos do consumidor, como a prática comerciais utilizadas para captura de dados, algumas situações se enquadram como abusivas no contexto (BLUM, 2018). O MCI apresentou preocupação com a tutela de privacidade dos dados pessoais e segurança, ao limitar o uso ou acesso de informações privadas na internet, o mesmo prevê inviolabilidade da intimidade vida privada, respeito às regras de consumo, confidência no fluxo de comunicações pela

internet; guarda e disponibilização dos registros de acesso a aplicações de internet, atender à preservação da intimidade, honra e imagem dos envolvidos (DONEDA, 2011).

Na sociedade da informação, o desenvolvimento das técnicas de marketing e tecnologia, estavam ao mesmo tempo apresentando benefícios e desafios à tutela de direitos fundamentais. Assim, pode ser observado com clareza que as vigentes legislações presentes no país eram insuficientes para proteção da vida privada, imagem e hora das pessoas, intimidade e aos novos problemas que estavam surgindo (BRANCO, 2017).

O MCI no decreto n° 8.771/2016, apresentou o conceito de dado pessoal, porém não mostrou a definição de dados sensíveis. Neste cenário os dados não tem limites, o Brasil teve a necessidade de criar uma pauta urgente sobre Lei Geral de Proteção de Dados pessoais, com a finalidade de alinhar com os países que já possuíam leis prontas e em vigor (A Lei Federal nº 10.406, 2002).

O caminho até o atual modelo, teve início em 2010, com o tema tendo sua primeira consulta pública feita pelo Ministério da Cultura. No início de 2011, empresas e pessoas da área contribuíram com o primeiro debate, propondo uma regulamentação na proteção de dados pessoais no país (MINISTÉRIO DA CULTURA, 2018).

O vazamento feito por Edward Snowden em 2013, revelou com detalhes o sigiloso programa norte-americano de espionagem e vigilância global sobre tráfego de informações e comunicações de diversos países, causando em locais como Brasil e Europa um alerta e preocupação com seus dados pessoais. Assim, acelerando o processo de aprovação do Marco Civil da Internet (MCI), visto como um pontapé inicial no processo de proteção dos dados pessoais. Entretanto, havia ainda a necessidade de preencher algumas lacunas específicas no qual não foram tratadas no MCI (EWEN MACASKILL, 2013).

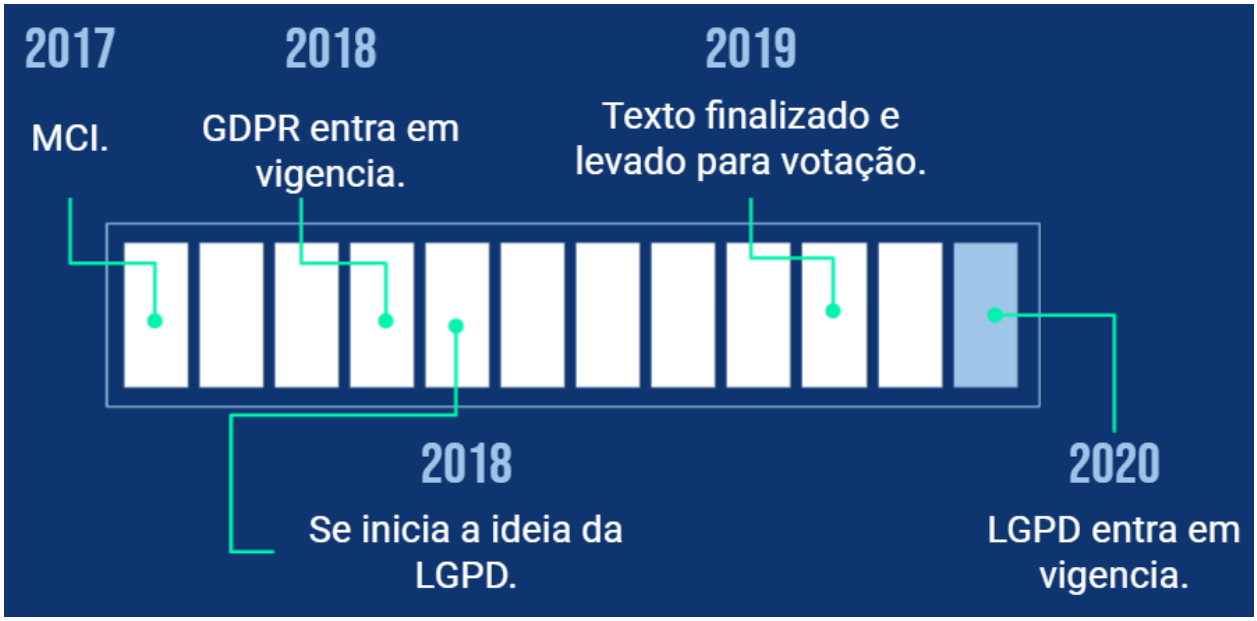
Com uma segunda consulta do tema em 2016, foi criada uma comissão especial, para opinar na proposta legislativa. Diversas entidades públicas nacionais e internacionais naquela ocasião, contribuíram no amadurecimento das ideias.

Com a vigência da GDPR em maio de 2018, onde substituiu a antiga diretiva, o Brasil viu a necessidade de uma legislação similar. Já que, a mesma dispõe de uma normativa onde só pode haver fluxo de dados internacionais, se o outro país possuir normativas adequadas à proteção de dados similar à europeia.

Dada a aprovação por meio de voto no plenário do Senado Federal em julho de 2018, as alterações no MCI para melhor proteger os dados pessoais no Brasil e normatizar como as informações podem ser tratadas e coletadas. Colocando assim o Brasil no rol dos países que possuem legislação similar e específica do tema (BNDES, 2016).

Sancionada em 14 de Agosto de 2018, a Lei Federal de Nº 13.709, nomeada de LGPD, entrou em vigor no final de 2020. A lei trata de diversos pontos que não possuíam previsão legal ou de modo esparso em leis setoriais. A unificação desses assuntos em 65 artigos, estabeleceu como empresas devem tratar os dados e preservar a privacidade dos indivíduos (BRASIL, 2018).

Imagem 1: Fluxograma LGPD



Fonte: Elaborado pelo autor (2021), com base evolução cronológica.

2.2 Principais Aspectos da LGPD

A Proteção de Dados está diretamente vinculada à cultura da internet e a inclusão digital, em função disso, se instrumentaliza na Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018). Desta forma, é uma ferramenta com intuito de estimular uma cultura de proteção de dados, tanto de pessoas jurídicas quanto físicas, e é regida pela autodeterminação informativa e a respeito da privacidade (art. 2º, I e II). Nessas condições podem ser compreendidas as políticas inovadoras de

ética e educação informacional na rede como método público de defesa aos crimes cibernéticos (BRASIL, 2018).

Pontos a serem destacados na LGPD:

- Dados pessoais: Segundo a LGPD, toda informação que permite identificar diretamente ou indireto, um indivíduo vivo é um dado pessoal, como: RG, CPF, nome, gênero, data e local de nascimento, endereço residencial, telefone, localização (GPS), fotografia, prontuário de saúde, renda, cartão bancário, renda, hábitos de consumo, preferências de lazer, endereço entre outros.

- Consentimento do indivíduo: o consentimento é um ponto de extrema importância dentro da LGPD. Sendo assim, é a base de dados do usuário a ser tratada. Todavia, existem exceções. Caso seja indispensável para acatar critérios legais, é viável tratar dados sem consentimento.

- Garantia ao indivíduo: LGPD traz diverso direito ao indivíduo, como revogar um consentimento e transferir dados para outro fornecedor de serviços, possibilita a solicitação da exclusão de dados, correção dos dados, portabilidade dos dados, informações sobre a possibilidade de não consentir o tratamento e as consequências negativas, informações sobre compartilhamento de dados pessoais.

- Agentes responsáveis e fiscalização centralizada: A Autoridade Nacional de Proteção de dados Pessoais (ANPD) é encarregada da penalização e fiscalização em caso de incumprimento da lei. As organizações devem ter agentes específicos para controlar, operar e serem encarregados dos tratamentos de dados, dependendo do seu volume e porte. É exigido que os gestores de base de dados pessoais das empresas façam a administração de riscos e falhas, com foco em adotar medidas preventivas de segurança, redigir normas de governança, replicar boas práticas e certidões existentes no mercado, fazer auditorias, elaborar planos de contingência e resolver incidência com agilidade. Abrangendo tudo com transparência e responsabilidade de notificar a ANPD e os cidadãos afetados quando ocorre vazamento de dados.

- Penalidades: A negligência e a falta de segurança na proteção dos dados pessoais dos usuários acarretará em altas multas. Organizações e subcontratadas para tratar dados são responsáveis por responderem juntos por eventuais danos causados. A ANDP fixa nível de penalidade de acordo com a gravidade da falha com o envio de notificações e orientações prévias antes de aplicar as sanções. As multas chegam até a 2% do faturamento anual da organização no Brasil e no limite de R $50 milhões por infração.

2.3 Princípios Gerais da LGPD

A aplicabilidade da Lei Geral de Proteção de Dados é voltada para pessoa natural e física, que os dados individuais estão nos bancos dos órgãos públicos e empresas. A lei tem como finalidade proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Desta forma, podemos afirmar que a LGPD não se aplica (BRASIL, 2018):

- A dados de pessoa jurídica, já guarnecidos na esfera da propriedade intelectual.

- A tratamento de dados pessoais realizados por indivíduo natural para fim econômico, jornalístico, particular, artístico ou acadêmico.
- Para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.
- A dados de pessoas falecidas e dados em trânsito, ou seja, aqueles que não têm como destino Agentes de Tratamento no Brasil.

A LGPD será aplicada aos dados tratados sobre o âmbito geográfico de proteção no território brasileiro, mesmo que envolva um estrangeiro.

É viável notar que a GDPR e a LGPD têm mais convergência entre si do que pontos de diferença. Os dados pessoais devem ser relevantes, limitados e adequados em relação aos fins característicos que são processados. Isso dá garantia, assim, impedindo o uso ilimitado dos dados pessoais coletados, de formas variadas que os donos dos dados poderiam esperar (LORENZON, 2021).

No 6 artigo da lei geral de proteção, cita os princípios da mesma para direcionar o tratamento de dados pessoais (BRASIL, 2018):

1) Princípio da finalidade: é o mais importante para a proteção de dados pessoais, tornando isento o consentimento ao tratamento de dados pessoais, caso não seja visto pelo operador ou controlador. De acordo com a lei, este princípio é a realização do tratamento para propósitos legítimos específicos explícitos sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. É vedado aos agentes de tratamento que utilizem dados pessoais dos usuários exceda a finalidade informada ao interessado antes da coleta dos dados. Obriga o responsável de tratamento de dados disponha de forma clara a finalidade do tratamento de dado, com a penalidade de se julgar ilegítimo o tratamento feito com base em finalidades vastas (Rossnagel, 2003, p.140).

2) Princípio da adequação: Define que o tratamento de dados deverá ser compatível com a finalidade informada ao titular. Sendo assim, controladores e operadores não podem usar dados incompatíveis com a finalidade que se destina (DONEDA, 2006).

3) Princípio da necessidade: Limita ao mínimo necessário a realização do tratamento para suas finalidades. Englobando dados pertinentes, proporcionais e não excessivos no que desrespeita a finalidade do tratamento de dados.

4) Princípio do livre acesso: Permite o titular obter uma cópia gratuita dos seus dados coletados, também como seus dados estão sendo processados pelo controlador, tendo de cumprir com prazo máximo de 1 (um) mês. Garantindo-se ao mesmo o direito de retificar e acrescentar seus dados pessoais, ou até excluí-los quando irrelevantes (DONEDA, 2006).

5) Princípio da qualidade de dados: Exige que os bancos de dados constantes sejam tratados de forma legal e leal, não excessivos e adequados de acordo com a finalidade declarada, além de serem claros, precisos e atuais. Neste princípio se inclui o cancelamento dos dados, o direito de acesso e retificação.

O acesso traz o direito ao indivíduo de obter as informações sobre ele registrado quando assim requisitar (CUEVA, 1990). Já o cancelamento e a retificação têm o intuito de assegurar a qualidade dos dados, de forma que deve ser cancelado ou excluído em caso de equívocos.

6) Princípio da transparência: O princípio da transparência, as organizações devem prover informações extensivas ao indivíduo em relação ao processamento dos dados pessoais, sendo de forma concisa, acessível, transparente, claro e de fácil acesso ao titular dos dados. Deve ser conhecimento público o banco de dados. O intuito do princípio da transparência de driblar possíveis abusos que possam ser realizados por agentes de tratamento.

7) Princípio da segurança e prevenção: No princípio da segurança e prevenção, tem como foco, determinar que todos os dados venham a ser processados de modo que se garanta a segurança adequada, protegendo de processamentos não autorizados ou ilegais. Estabelecendo proteção contra danos, perdas e acidentes, por meios de técnicas organizacionais adequadas. Os agentes de tratamentos aderiram medidas preventivas para esquivar de eventuais danos em virtude do tratamento de dados pessoais. Revalidando à prevenção contra eventuais danos provenientes do tratamento dos dados pessoais.

8) Princípio da não discriminação: Refere que o tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos. Não pode se ter restrição de titulares de dados pessoais na hora de seu tratamento de dados por características (origem racial, étnica, opinião política, religião/convicção, geolocalização, filiação sindical, estado genético, saúde ou orientação sexual). Só poderá ocorrer tal exclusão em situações específicas previstas em lei.

9) Princípio da responsabilização e prestação de contas: visa garantir a reparação correta e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade. O agente tratador

dos dados pessoais deverá apresentar as medidas cabíveis e suficientes para comprovar o cumprimento da LGPD.

2.4 Definição dos Conceitos de Dados na LGPD

De acordo com a LGPD, os dados podem ser divididos nas seguintes categorias.

2.4.1 Titular dos Dados

É uma pessoa singular no qual os dados se referem, identificável e reconhecível. Tornando possível a identificação do titular de modo direto ou indireto (MACIEL, 2019).

A LGPD traz no artigo 18, nove dispositivos em prol do direito do titular já mencionado no artigo 5 (BRASIL, 2018).

> “Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I - confirmação da existência de tratamento;
>
> II - acesso aos dados;
>
> III - correção de dados incompletos, inexatos ou desatualizados;
>
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
>
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
>
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.”

2.4.2 Dados Sensíveis

São aqueles que, caso roubados, podem causar danos ao titular, já que estes dados estão vinculados com a personalidade, caráter e dia a dia. No artigo 5, inciso segundo, trata sobre dados sensíveis (BRASIL, 2018).

> “Art. 5º Para os fins desta Lei, considera-se:
> II - dado pessoal sensível: 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;”

2.4.3 Dados Pessoais

São aqueles que, caso roubados, podem identificar a pessoa de modo direto ou indireto. No artigo 5, inciso primeiro, trata sobre dados sensíveis (BRASIL, 2018).

> “Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;”

2.4.4 Dados Anónimos

Tem o intuito de ocultar informações sensíveis antes de serem disponibilizadas para uso. Tornando inviável saber de qual perfil a informação é oriunda. No artigo 5, inciso terceiro, trata sobre dados anônimos (BRASIL, 2018).

> “Art. 5º Para os fins desta Lei, considera-se:
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;”

2.4.5 Encarregado

Sua função consiste em intermediar ações entre o titular, o controlador e a ANPD. Detendo total liberdade para tratamento dos dados, fiscalizar tanto o operador quanto o controlador e efetuar denúncias em caso de irregularidades. No artigo 5, inciso oitavo, que trata sobre encarregados (BRASIL, 2018).

> "Art. 5º Para os fins desta Lei, considera-se:
> VIII - 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 (ANPD);

O encarregado deve ser nomeado pelo controlador obrigatoriamente, conforme o artigo 41 (BRASIL, 2018).

> "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais."

Entretanto, vale salientar que no artigo 23, também apresenta a obrigatoriedade de indicação do encarregado pelo tratamento de dados pessoais por pessoa jurídica de direito público (BRASIL, 2018).

> "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência"

2.4.6 Agentes de Tratamento

No artigo 5, inciso nono, trata sobre agentes de tratamento (BRASIL, 2018).

> "Art. 5º Para os fins desta Lei, considera-se:
> IX - agentes de tratamento: o controlador e o operador;"

2.4.6.1 Controlador

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, ou seja, as próprias empresas que recebem os dados dos titulares, sejam eles consumidores e/ou

empregados, dentre outros. Os dados são recebidos pelo controlador e preparado a estrutura para recepção, tratamento, destinação e eliminação dos dados, passando todas as diretrizes para a materialização do tratamento pelo operador.

É de responsabilidade do controlador:

- Expor que houve consentimento do titular dos dados e instruir o mesmo a respeito da modificação do consentimento para tratamento de dados, com destaque de forma específica do teor das modificações, quando se trata de mudança de finalidade, prazo, controlador e do compartilhamento dos dados (Art. 8, § 2º e 6º) (BRASIL, 2018).
- Adotar medidas para assegurar transparência do tratamento de dados e dar acesso ao relatório de impacto à proteção de dados pessoais à ANPD, quando requerido (Art. 10, § 2º e 3º) (BRASIL, 2018).
- Providenciar ao titular de dados pessoais, mediante requisição a comprovação da existência de tratamento de dados, assim como, acesso, correção e ainda a anonimização, bloqueio ou eliminação desses dados, observando as disposições da Lei (Art. 18) (BRASIL, 2018).
- Criar relatório de impacto à proteção de dados pessoais (Art. 38) (BRASIL, 2018).
- Redigir instruções para o tratamento de dados realizados por operador, observando as próprias regras e as normas sobre a matéria (Art. 39) (BRASIL, 2018).
- Nomear o encarregado, salvo nas hipóteses de dispensa, a critério da ANPD (Art. 41) (BRASIL, 2018).
- Informar a autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Art. 48) (BRASIL, 2018).

2.4.6.2 Operador

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Trata-se do responsável efetivo pelo tratamento dos dados na prática, podendo ser um funcionário da empresa receptora dos dados/controlador, uma empresa terceirizada ou até

mesmo um profissional autônomo. Normalmente, este operador será alguém com experiência na área de tecnologia da informação e tratamento de dados. Assim sendo, compete ao operador fazer o tratamento segundo as instruções oferecidas pelo controlador, que irá conferir a observância das próprias instruções e das normas sobre a matéria. Controlador e Operador atuam conjuntamente, como verdadeiros agentes de tratamento (Art. 39) (BRASIL, 2018).

2.5 Autoridade Nacional de Proteção de Dados Pessoa (ANPD)

A Medida Provisória n° 869, de 2018 (LGPD) fundou a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), Administração pública federal que faz parte da autonomia técnica da estrutura da presidência da república. O órgão é constituído por Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Conselho Diretor, Ouvidoria, Corregedoria, Unidade administrativas e especializada e órgão de assessoramento jurídico próprio (BRASIL, 2018).

A ANPD tem como função primordial zelar pela proteção de dados pessoais, para isso suas principais funções são:

1. Editar normas e procedimentos sobre a proteção de dados pessoais" (inc. II);
2. Deliberar sobre a interpretação da LGPD, suas competências e os casos omissos (inc. III);
3. Requisitar informações aos controladores e operadores de dados pessoais (inc. IV);
4. Implementar mecanismos para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a Lei (inc. V);
5. Fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo (inc. VI);
6. Comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (inc. VII).

O poder de fiscalização da ANPD é significativo, o emprego de critérios de ação por esse órgão auxiliar para o cumprimento das normas. De modo que o ajustamento dos dados pessoais será realizado por uma agência nacional, a execução

da sanção deve estar de acordo com os nortes e princípios do direito administrativo (MAROSO, 2020).

O modelo de regulação de risco e sua efetividade podem ser ameaçados no País, devido a judicialização de medidas administrativas e reguladoras, por interesse econômico específico há a imposição de barreiras e procedimentos estratégicos. A efetividade dos métodos institucionais de proteção de dados está diretamente ligada a capacidade dos usuários encarregados no ambiente interno e da ANPD, de fazer com que a atividade empresarial esteja conforme as normas da LGPD, por meio de adoção de ações de formulação de boas práticas e governança, medidas de segurança e implementação de mecanismo preventivo de proteção de dados (MAROSO, 2020).

2.6 Impacto Econômico

Pode-se afirmar que com a implantação da LGPD, irá fomentar o desenvolvimento econômico e tecnológico por meio de suas regras que asseguram os interesses de todos os setores econômicos e sociais que é cada dia mais movida por dados. De modo que a iniciativa privada poderá expor como um diferencial competitivo, a proteção correta dos dados pessoais, assim tendo uma vantagem econômica e sendo mais um diferencial a ser analisado pelo consumidor na hora de escolher um serviço.

No livro “Entre dados e robôs”, Eduardo Magrani cita que com o alto crescimento do compartilhamento de dados e técnicas na computação, a pressão econômica e evolução tecnológica se espalham rapidamente e os algoritmos são ótimos recursos para a inovação e o mercado. A rápida difusão dos algoritmos e sua influência trazem consequências para o mercado e a sociedade, incluindo ética e governança na questão. Algoritmos são capazes de estarem presentes em nossas vidas em diversos ramos conforme vem se tornando mais modernos, úteis e independentes. Há uma possibilidade que no lugar dos seres humanos eles tomem decisões importantes.

A nova legislação brasileira tem dentro de seus objetivos normativas diretas para as empresas, estabelecendo premissas simples sobre armazenamento, coleta, tratamento e compartilhamento de dados pessoais a terceiros, em cenários de comercialização das informações. Além disso, a LGPD tem como objetivo incentivar

o desenvolvimento, impulsionando o desenvolvimento tecnológico e econômico e também garantir ao consumidor direito à livre concorrência e a livre iniciativa (BIONI, 2018).

Vale ressaltar as vantagens de uma Lei Geral, dentre elas, a padronização das regras, tornando único o meio a ser seguido e de modo harmônico, independentes do setor da economia. Havendo uma considerável redução de custos, já que, será possível diminuir custos operacionais causados por incompatibilidades entre sistemas de feitos por agentes diversos, além de incentivar uma maior qualidade dos dados circulando. Tornando o Brasil apto para maiores interações internacionais, de modo que passará a processar dados de países que exigem nível de proteção dos dados. Promovendo mais liberdade ao indivíduo, podendo transferir seus dados de um serviço para outro, aumentando assim a competitividade entre empresas (MONTEIRO, 2019).

2.7 Inclusão digital

A Inclusão digital pode ser definida como o fomento da cidadania que reconhece a segurança digital e reconhece a dimensão do espaço virtual como peça essencial na introdução na sociedade da informação (MARTINI, 2005).

A educação informacional concede autonomia ao indivíduo no contexto digital também está ligado à colocação insuficiente nas relações de consumo, identificando o desequilíbrio técnico que o cidadão dispõe frente às vastas bases de dados dos estabelecimentos (MIRAGEM, 2019).

Ao mesmo tempo que a cidadania digital reconhece as assimetrias tecnológicas da estrutura social, ela também pressupõe o empoderamento técnico do indivíduo. No ponto de vista de empresas, observa-se o princípio de políticas de segurança e normativas atento ao princípio da preservação dos dados digitais e da privacidade, sendo assim, políticas corporativas que determinam normas e diretrizes administrativas de segurança da informação. O fortalecimento de uma cultura de proteção de dados para as organizações é o legado possível para a LGPD, tendo em vista pontos primordiais como confiança e reputação no ambiente da empresa (BIONI, 2019).

Por meio de políticas organizacionais corretas e efetivas à segurança dos

dados através de modos participativos e que eduquem os usuários nas práticas de proteção e privacidade em suas atividades. A LGPD representa esta evolução no âmbito organizacional, seja em meios públicos ou privados, ao se basear no fundamento de responsabilidade e ética. As certificações privadas de adequação à proteção de dados têm se tornado uma prática comum nas empresas desde então.

O objetivo da fixação de controles internos é ser um reforço a estatal ao cumprimento da lei, no caso da proteção de dados (FRAZAO; OLIVA; ABILIA, 2019), é necessário a adequação ao risco de atividade, a regulação *by design*, a criação de um programa de treinamento dos empregados em relação a segurança de dados e um efetivo monitoramento do próprio programa de conformidade. Assim criando proteção de dados da empresa que objetiva alinhar os preceitos legais acerca da segurança e da privacidade e atividade empresarial, transformando a empresa e os usuários menos vulneráveis a golpes digitais (RECIO, 2017).

Este conjunto de medidas protetivas concilia a necessidade de auditabilidade social à auto checagem das empresas, a programação deverá priorizar os princípios jurídicos que conduzem os direitos humanos e deve ser submetida a inspeção crítica do meio. A privatização da regulação deve se fazer presente aliada com a privatização das responsabilidades, através dos algoritmos que são de suma importância para as empresas (MARTIN, 2019).

Ponderar a necessidade de criação de espaços na programação, atentando aos valores sociais e democráticos, assim, conduzindo para dentro dos algoritmos da melhor forma os objetivos das leis (WEBER, 2018).

3 PRINCIPAIS RESPONSABILIDADES E PENALIZAÇÕES PREVISTAS NA LEI

Há dois mecanismos repressivos de proteção de dados pessoais dentro da LGPD. Um deles é a responsabilidade administrativa por meio de sanções aplicadas pela ANPD, como multas, advertências, bloqueio e eliminação de dados pessoais e a publicização da infração. O outro mecanismo é a responsabilidade civil juntamente com o ressarcimento de danos, através da jurisdição do poder Judiciário (BRASIL, 2018).

3.1 Responsabilidade Administrativa

A LGPD prevê no artigo 52 (BRASIL, 2018). “Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

> 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;”

Após o procedimento administrativo as sanções serão aplicadas, assegurando a oportunidade de defesa que sigam os parâmetros de:

- Gravidade e natureza da infração e dos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, reincidência, grau do dano, cooperação do infrator;

- A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; Adoção de política de boas práticas de governança;
- A pronta adesão de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Ao aplicar a multa, a ANPD é obrigada pela LGPD a examinar o faturamento total do grupo de empresas ou da empresa, desde que não disponha do valor de faturamento no ramo de atividade empresária, que ocorreu a infração (art. 52, § 4°). O órgão responsável pela aplicação das multas é obrigado a emitir regulamento próprio sobre método de cálculo do valor base das sanções de multas já previstas na lei geral de proteção de dados após a consulta pública. No evento de cálculo do valor da multa diária, a ANPD deverá analisar parâmetros como a extensão dos danos ou prejuízos causados ou a gravidade da falta (art. 53/54) (BRASIL, 2018).

A maior efetividade da norma se deve a penalidades por multa levando em consideração valores elevados. Pode haver infração e incidente de vazamento de dados mesmo que o operador siga todas as melhores práticas e aplique todos os controles.

A palpabilidade da responsabilidade administrativa por meio de sanções para proteção de dados pessoais deve se basear na não isenção da responsabilização civil e na indenização de danos pelo Poder Judiciário.

3.2 Responsabilidade Civil e Ressarcimento de Danos

A possibilidade de ajuizamento de ação perante o poder judiciário é prevista pela LGPD para defender o interesse e do direito do titular de dados, segundo o artigo 22 “A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva” (BRASIL, 2018).

A previsão de responsabilidade civil de pessoas jurídicas e físicas no Código Civil por eventuais atos ilícitos podem gerar danos, que consequentemente geram o dever de reparação civil (JUNIOR; RICARDO, 2019).

A LGPD propõe no primeiro inciso do primeiro parágrafo do artigo 42 que" O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". No intuito de prover uma indenização consistente ao titular dos dados (BRASIL, 2018).

A LGPD define que o magistrado poderá proporcionar um contraposto do ônus da prova a favor do titular dos dados quando houver similaridade das alegações, falta de recursos para se autossustentar para finalidades de provas ou produção ou se for excessivamente onerosa a sua produção (art. 42, § 2º). A lei claramente autoriza a avaliação de ações de reparação de danos coletivos (art. 42, § 3º) (BRASIL, 2018).

A responsabilidade civil de empresas, está em concordância com o código de defesa do consumidor. A relação de consumo pode ser destacada no caso em que o dono dos dados é o consumidor direto ou indireto e a empresa o fornecedor do serviço e/ou produto.

Em amplo espectro, não há segurança alguma que será apta a cobrir todos os riscos das atividades. Mas com o fundamento do código do consumidor, o judiciário irá considerar a suposição do risco de atividade para finalizar pela responsabilidade do fornecedor.

No artigo 43, contêm similaridades com os artigos 12 (doze) e 14 (quatorze) do CDC, mencionando a responsabilidade civil em relação ao serviço e produto. Nele é mencionado que os agentes são excluídos de responsabilidades, salvo os casos onde sua conduta não é ilícita, ou quando o titular ou terceiros é o responsável do dano decorrente (BRASIL, 2018).

Já o artigo 44 na LGPD define quando o ato será considerado ilícito e passível de reparação civil. No caso de um vazamento, se for constatado que a empresa não se adequou às normas ou a segurança eram inadequadas e insuficientes, sendo assim, passível de ser responsabilizada na esfera civil. De modo que o Judiciário será mobilizado para pôr em prática a reparação civil ditada na LGPD e para casos de judicialização de normas tomadas pela ANPD (BRASIL, 2018).

Acontece que, não há nenhum tipo de segurança que consiga despir todos os riscos da atividade. Quando falamos sobre responsabilidade objetiva, o foco é mudado para a assunção de risco, que é possível controlá-lo. Claramente, o risco não deve

chegar a zero, porém a falta de um mecanismo de controle pode possibilitar a responsabilidade civil por esse deslize dos envolvidos.

A inovação que temos que nos adaptar é a técnica de desenvolvimento do projeto (*privacy by design*) para integrar a segurança. No artigo 46 §2º da LGPD expõe que os projetos de ofertas de serviço que logo depois irão tratar dados necessitam incorporar as práticas mais favoráveis de segurança desde o começo (BRASIL, 2018).

Ao aderir a definição do *privacy by design*, a empresa deixa claro que aderiu a cautelas de segurança satisfatória desde quando o produto estava em desenvolvimento. Sendo assim, cautela é uma obrigação geral, que não corresponde com a responsabilidade objetiva, que qualquer avaliação de culpa é dispensada (CARVALHO, 2019)

O que não pode ser feito é a conduta *privacy by desire,* onde se espera por uma falsa esperança de que ninguém note suas falhas de segurança e que com isso, os dados estarão protegidos.

3.3 Penalidades

Diferente da GDPR, o artigo 52 fala sobre as penalidades e sanções na LGPD, adaptando-se à realidade e contexto socioeconômico do Brasil. Alguns aspectos e requisitos podem alterar o critério de avaliação, haja vista o da proporcionalidade (BRASIL, 2018).

> “Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> 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;
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

As penalidades acima indicadas somente serão aplicadas após instauração de procedimento administrativo, por meio do qual será possibilitado o exercício de ampla defesa, de forma gradativa, isolada ou cumulativa, considerando as particularidades do caso, por força do § 1º, do artigo 52, da Lei n° 13.709/2018.

O referido dispositivo dispõe que para a aplicação das penalidades indicadas, será observado o seguinte:

> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II - a boa-fé do infrator;
>
> III - a vantagem auferida ou pretendida pelo infrator;
>
> IV - a condição econômica do infrator;
>
> V - a reincidência;
>
> VI - o grau do dano;
>
> VII - a cooperação do infrator;

> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
>
> IX - a adoção de política de boas práticas e governança;
>
> X - a pronta adoção de medidas corretivas; e
>
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Portanto, todas as condições acima indicadas deverão ser levadas em consideração quando da aplicação da penalidade do agente infrator.

Para o cálculo do valor da multa do inciso II de acordo § 4°, é de acordo com faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea (BRASIL,2018).

O que está definido nesta lei não substitui a aplicação de sanções administrativas civis e penais definidas no código de defesa do consumidor (lei n°8.078) (art. 52, § 2º).

O valor que é arrecadado das multas será direcionado ao fundo de Defesa de Direitos Difusos (Art. §5°).

A Lei já está em vigor desde agosto de 2020, mas as sanções começam a ser aplicadas a partir de agosto de 2021.

4 DISCUSSÃO

Imagem 2: Mapa LGPD e GDPR

Fonte: Elaborado pelo autor (2021), com base nas localidades.

4.1 Particularidades Entre a LGPD e a GDPR

Devido à compatibilidade com a legislação de países que adotaram a lei Geral de proteção de dados, o regime jurídico interno foi baseado na *General Data Protection Regulation* (GDPR) que tem como foco a proteção e privacidade dos dados dos indivíduos da União Europeia e espaço Econômico Europeu. Essencial é a conexão feita da LGPD com a GPDR, uma vez que conforme a lei europeia, poderia deter o compartilhamento e transferência de dados ao Brasil, afetando diretamente no desenvolvimento econômico do Brasil (LORENZON,2020).

A LGPD apresenta diversos aspectos de convergência com a GDPR, apresentando similaridade em alguns pontos e outros onde uma lei sobressai sobre a outra. O quadro a seguir apresenta comparações entre a lei brasileira e europeia:

Tabela 1: Quadro Comparativo

LGPD	**GDPR**
TRATAMENTO DE DADOS	
Poderá ser usado nas seguintes hipóteses: II sem fornecimento de consentimento o titular, nas hipóteses em que for indispensável para: b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. **(ART. 11, II," B" e "G")**	Proíbe o tratamento de dados sensíveis, porém estabelece algumas exceções. Sendo duas delas providas da lei brasileira: d) Dados tornados públicos pelo seu titular; e) Dados relacionados a membros ou ex membros de uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais **(art. 9, § 2º, "D" e "E")**
TRATAMENTO DE DADOS DE MENORES	
Aplica o mesmo regime às crianças e adolescentes, assim, cumprindo os termos do estatuto da criança e do adolescente, aonde requer o consentimento de algum responsável pelo menor. **(Art. 14, § 1º)**	Aceita o consentimento de dados por adolescente a partir de 16 anos, caso o adolescente ou criança seja menor de 16 necessita do consentimento de algum responsável legal. **(Art. 8, § 1º)**
POLÍTICA DE PROTEÇÃO DE DADOS	
Apresenta a implementação de programas de controle em privacidade e governança, como faculdades dos controladores de dados. **(Art. 50)**	Os controladores têm a obrigação de adotar medidas técnicas e organizacionais adequadas para assegurar o tratamento de dados de acordo com a lei. **(Art. 24, § 2°)**
REPRESENTANTES	
Diferente da GDPR a LGPD prevê que empresas estrangeiras serão notificadas e intimadas por sua responsável no Brasil. **(Art. 61)**	Um representante deve ser constituído pelo controlador ou processador em seus estados membros. **(Art. 27)**

RESPONSABILIDADES DOS AGENTES	
Soma-se mais uma hipótese em relação a GDPR onde o agente é isento de responsabilidade, quando comprovado que o vazamento foi realizado pelo titular ou terceiros. **(Art. 42 e seguintes)**	Ela enumera duas possibilidades onde o vazamento pode ter sido causado aos titulares pelo controlador ou operador. Salvo os casos realizados em conformidade com a lei. **(Art. 82)**
MARKETING DIRETO	
Não há artigos específicos expondo normas sobre esse assunto, está presente superficialmente apenas nas regras gerais de consentimento, transparência e direito.	O titular pode e tem direito de se opor à forma que seus dados estão sendo tratados e comercializados. **(Art. 21)**
RELAÇÃO ENTRE CONTROLADOR E OPERADOR	
Apesar de estabelecer que o operador deverá realizar o tratamento e o acordo como controlador deseja, ela não obriga a formalização deste contrato. **(Art. 39)**	Além de indicar quais matérias que devem constar no contrato, ela obriga que todo tratamento de dados realizado por um operador deve vir de um contrato ou documento similar que una ele ao controlador. **(Art. 28, § 3º)**
TRANSFERÊNCIA INTERNACIONAL DE DADOS	
Permite a transferência de dados para órgãos internacionais que proporcionem uma proteção adequada, porém a lei é extremamente genérica e não define de forma transparente o que seria os elementos adequados. **(Art. 3 e seguintes)**	Pode ocorrer sem a necessidade de uma autorização específica, caso reconheçam que o país proporciona uma segurança adequada, do contrário será feito uma autorização específica ao agente, onde oposto ao Brasil, apresenta detalhadamente quais medidas de segurança devem ser tomadas. **(Art. 44 e seguintes)**
ÓRGÃOS RESPONSÁVEIS	
A LGPD previa a criação da autoridade nacional de proteção de dados (ANPD), entretanto, os dispositivos previstos para sua criação e responsabilidades foram vetados por serem inconstitucionais ao processo legislativo, devido a ANPD ser criada como órgão administrativo público, seria de iniciativa privada do presidente da república. **(Art. 55 a 59)**	O comité europeu para proteção de dados foi criado pela GDPR, para ser responsável por aplicar de forma coerente a lei. **(Art. 68 e seguintes)**

Fonte: Elaborado pelo autor (2021), com base na LGPD e GDPR.

4.2 Impactos na Computação

Com o advento da LGPD, as empresas desenvolvedoras de softwares terão que se adequar à lei, atualizando seus produtos já no mercado e separando um setor na gestão de novos sistemas só para a área de segurança digital. Um tema que às vezes passava despercebido ou feito superficialmente, agora recebe uma enorme carga de responsabilidade.

Gerando um aumento na busca de profissionais capacitados no mercado para adequar sistemas já implementados e/ou juntar-se aos gestores de desenvolvimento para adequar o sistema desde o início de seu desenvolvimento. Trazendo uma maior qualidade nos sistemas oferecidos e proporcionando uma segurança digital maior para os usuários.

Consecutiva haverá um aumento no custo do desenvolvimento e manutenção, porém nada comparado aos custos a serem enfrentados caso haja uma violação na segurança dos dados por omissão ou descumprimento das normativas.

Outra grande mudança vem com o novo método para a coleta e tratamento de dados, onde com o desenvolvimento de novas e melhores inteligências artificiais para a análise de perfil, as empresas de marketing conseguem entregar propagandas e anúncios mais bem direcionados aos usuários. Tendo assim um aumento na procura de profissionais qualificados de ambos os ramos, gerando um maior desenvolvimento e aprimoramento nas áreas.

4.3 Fragilidades

A ANPD é vinculada à Presidência da república, com isso, o órgão que deveria ser independente (como as demais agências reguladoras) sofre com a restrição orçamentária e a falta de estrutura (sendo passiva de oscilar de acordo com interesses do governo em vigência). Em vista disso, quando necessário a ANPD pede reforço a polícia federal e ao gabinete de segurança institucional diante da ausência de

regulamentações da lei que delega ao órgão o poder de fiscalizar e punir infrações de modo autônomo.

4.4 Vulnerabilidades

Uma discussão indispensável quando se fala de segurança da informação e na aplicabilidade da lei são as vulnerabilidades, uma definição da tecnologia, descrita como condição que quando explorada pelo atacante, pode resultar na violação da segurança (HOEPERS, 2019).

Quando uma vulnerabilidade é detectada, eventualmente é catalogada e documentada em sites, como por exemplo o *Common Vulnerabilities and Exposures* (CVE) (U.S. DEPARTMENT OF HOMELAND SECURITY et al., 2021) de modo que viabilize para os responsáveis pela segurança digital de empresas e demais órgãos implementem técnicas prevenindo incidentes.

De modo que, se caso houver um dano aos dados devido ao não cumprimento de uma normativa, relacionada a uma vulnerabilidade já detectada, evidência negligência vinda do agente de tratamento dos dados.

Entretanto, o dano pode se derivar de violações por vulnerabilidades não documentadas, conhecidas como *0-Day*. Sendo uma falha conhecida pelo desenvolvedor, porém ignorada e não corrigida pelo mesmo, assim, deixando uma brecha passiva de ser explorada por criminosos (NORTON, 2019). Nesta situação, não é cabível uma responsabilização civil, devido a não ciência de sua existência, não há como obrigar o dever de segurança.

Consequentemente, não é possível delegar ao agente de tratamento a responsabilidade de assegurar e proteger os dados a qualquer possível meio de violação, sendo somente passível de responsabilizá-lo em casos conhecidos ou já detectados. Outro ponto a se destacar, é a impossibilidade de se garantir 100% de segurança e inviolabilidade dos dados ao titular.

4.5 Tendências

Com a implementação da LGPD, a identificação e coleta de dados por cookies está tendo uma queda considerável, já que é necessário o consentimento do usuário. Assim, mudando todo o modo de identificação de usuários, porém, aumentando a qualidade dos dados. Trouxe poder de volta ao usuário, podendo agora decidir o que deseja, com isso, os anunciantes terão maior trabalho para melhor atender os usuários e enfrentar a competitividade com as demais empresas.

Com o advento da LGPD, trará uma evolução no modo de coleta de dados e com isso, o surgimento de uma maior e melhor personalização nas publicidades voltadas para o usuário, onde através de uma pesquisa, a *Accenture Interactice* apurou que mais de 70% dos usuários estão dispostos a compartilhar seus dados, caso haja transparência. Isso trará uma melhor análise de perfil de cada usuário, de modo que as propagandas e produtos entregues se encaixam melhor ao cliente.

O ramo da inteligência artificial deve apresentar uma alta considerável, pois para a publicidade conseguir atingir melhor, terá de analisar diversos novos dados e entregar em escala propagandas personalizadas aos usuários. Sendo muito útil na análise de perfil comportamental, para assim gerar um perfil cada vez mais acurado com o estilo do usuário e entregando ao mesmo, apenas o que vai de encontro com seus interesses. Sendo assim, uma grande aliada e parceira na publicidade digital nos próximos anos.

4.6 Limitações

A ANATEL, apresentou um estudo (“Novos mercados nas telecomunicações”) em 2020, feito por Guido Lorencini Schuina, onde alguns aspectos da lei estariam engessando o setor. No estudo feito, mostrou que modificações no regulamento são necessárias nos pontos sobre fusões e aquisições, compartilhamento de

infraestrutura, neutralidade da rede e outros demais aspectos que interferem no aproveitamento máximo provido pelo 5G.

Um exemplo apresentado no estudo, são as vedações sobre transferências internacionais de dados ou o acesso a base de dados de planos de saúde. Sendo questionado o real alcance da lei e os riscos presentes na legislação.

No documento, foi indagado o método aplicado, já que vedações poderiam ser mecanismos velados de impor barreiras ou custo, podendo afetar o relacionamento com empresas externas. Apresentando como uma melhor solução acordos bilaterais ou multilaterais.

No documento, ainda comparou o artigo 6º da LGPD com o Marco Civil já que assegura de modo isonômico os dados pessoais, de modo que inibe a diferenciação no tratamento e texto aparentemente protetivo contra atos de abuso ou ilícitos. Além disso, é passivo de dupla interpretação, podendo ser norteado pelas intenções e interesses das autoridades.

Imagem 3: 5G

Fonte: Elaborado pelo autor (2021), com base no estudo da ANATEL

5 CONCLUSÃO

No Brasil a falta de investimento na área de segurança digital é notória e o setor de T.I. é normalmente visto como custo e não investimento. Investir em segurança sempre requer um capital significativo visto que essas despesas incluem pagar profissionais, ferramentas e frequentes atualizações dos processos, porém, é indispensável para evitar maiores prejuízos.

Até o ano de 2014, não havia nenhuma normativa ou lei que tivesse como intuito de tipificar o que são crimes contra a privacidade e/ou normatizando os padrões mínimos de segurança para proteção dos dados. A partir desta data, com a ascensão do Marco Civil da internet, deu-se o primeiro passo para o foco nessa área e consecutivamente o aprimoramento da lei com o surgimento da LGPD em 2018, onde trouxe um texto mais completo e detalhado sobre o assunto, surgindo também órgãos fiscalizadores. Com isso, reconhecendo os crimes cibernéticos, assim punindo os responsáveis de formas que protegem a vítima.

Para a LGPD, toda e qualquer informação que permita identificar um indivíduo (vivo) de forma direta ou não, é considerada como dado pessoal e necessita de proteção. Além de ter seus dados protegidos, o cidadão tem algumas garantias sobre o que deseja fazer com as informações. Caso o usuário note algum descumprimento, a ANPD está para ampará-lo, fiscalizar e se caso necessário, punir aqueles que não seguirem a lei.

Inspirada na GPDR (Lei Europeia), a LGPD tem como propósito fazer com que o indivíduo seja proprietário de seus dados. Com isso, tendo total responsabilidade e transparência sobre seus dados, podendo impor que o conteúdo seja excluído a qualquer momento. Pode ser comparada ao Código de Defesa do Consumidor, devido a sua ampla abrangência.

A lei é aplicada tanto para pessoas físicas quanto jurídicas, em setor público ou privado, que realizam atividades com dados pessoais de outros indivíduos. Basicamente todos os tipos de negócios estão sendo afetados pela LGPD. Diante disso, todos precisam se empenhar em sua adequação.

Podendo concluir que a LGPD veio regulamentar e disciplinar o tratamento dos dados pessoais na relação de cliente e fornecedor de produtos e/ou serviços. Tais como:

- Empregados e empregadores ou outras relações nas quais dados pessoais sejam recebidos;
- Prestadores de serviços;
- Enviados e/ou processados.

6 REFERÊNCIAS BIBLIOGRÁFICAS

BERGER, Leoni. Estudo do emprego de técnicas da análise transacional e da programação neurolinguística na melhoria da comunicação pessoal e organizacional. Dissertação (mestrado em Engenharia de Produção). 1999. Universidade Federal de Santa Catarina.

BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais.

BLUM, Rita Peixoto Ferreira. O direito à privacidade e à proteção dos dados do consumidor. São Paulo: Almedina, 2018, p. 61).

BNDS, governo, Estudo internet das coisas: Um plano de ação para o BRASIL. 2018

BRANCO, Sergio. Memória e esquecimento na internet. Porto Alegre: Arquipélago Editorial, 2017, p. 145-146.

BRASIL. Lei nº. 12.965, de 24 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 nov. 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em:12 de out. 2020.

BRASIL. Lei n° 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 janeiro.2002.

CARVALHO, Thaís Abreu. Aplicabilidade da lei geral de proteção de dados e da metodologia "privacy by design" nos termos de uso e de política de privacidade. 2019.

Trabalho de Conclusão de Curso (Bacharelado em Direito) - Faculdade de Direito de Vitória, Vitória, 2019.

Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

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

DONEDA, Danilo, p. 213. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

EWEN MACASKILL and GABRIEL DANCE, NSA FILE Produced by FEILDING CAGE and GREG CHEN Published on November 1, 2013.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. Fundamentos de Segurança da Informação. [S. l.]: Escola de Governança da Internet no Brasil. Disponível em: https://bit.ly/2unOasd. Acesso em: 27 set. 2019.

HRON, Martin. Os últimos 10 maiores vazamentos de dados. 14 de Fevereiro 2019. Avast Blog. Disponível em: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados. Acesso em: 16 de Abril de 2021.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (LGPD E GDPR) E SEUS RESPECTIVOS INSTRUMENTOS DE *ENFORCEMENT. Faculdade Getúlio Vargas. Rio de Janeiro.* 15 de março de 2021.

MACHLUP, Fritz; MANSFIELD, Una. The Study of Information: Interdisciplinary Messages. New York: John Wiley, 1983, p.641-671

MAGRINI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade. 2 ed. Arquipélago Editorial. Porto Alegre.2019.

MAROSO, Bárbara. LGPD: O papel da Autoridade Nacional de Proteção de Dados. 20 de novembro de 2020. Colégio Registral, Rio Grande do Sul. Disponível em: https://www.colegioregistralrs.org.br/doutrinas/artigo-lgpd-o-papel-da-autoridade-nacional-de-protecao-de-dados-por-barbara-maroso/. Acesso em: 13 de Abril de 2021.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MONTEIRO, Renato Leite. A nova Regulação de Proteção de Dados Pessoais aprovada na União Europeia e sua influência no Brasil. Disponível em: . Acesso em: 21/05/2019.

NORTON (US). Zero-day vulnerability: What it is, and how it works. [*S. l.*], 28 set. 2019. Disponível em: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html. Acesso em: 26 abr. 2021.

PINHEIRO, P. P. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

SCHUINA, Guido Lorencini. Novos mercados nas telecomunicações. Setembro de 2020. ANATEL. Disponível em: https://www.eventos.momentoeditorial.com.br/wp-content/uploads/2020/10/ESTUDO-COMPETIcao-20_compressed.pdf. Acesso em: 28 de Abril de 2021.

SWINHOE, Dan. Os 15 maiores vazamentos de dados do século 21. 27 de Abril de 2020. Computer World. Disponível em: https://computerworld.com.br/seguranca/os-

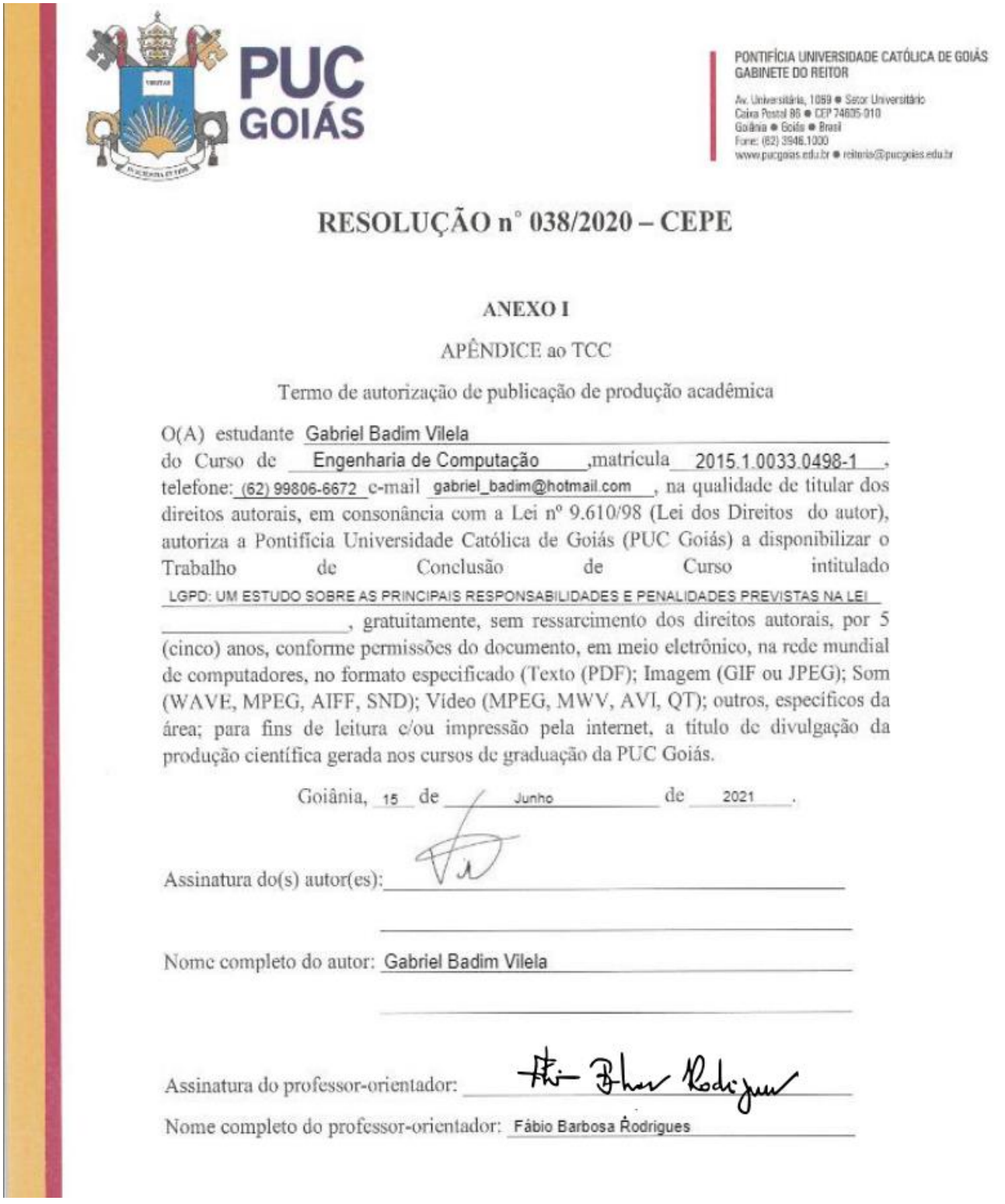
15-maiores-vazamentos-violacoes-de-dados-do-seculo-21/. Acesso em: 16 de Abril de 2021.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, 2016. Disponível em: . Acesso em:15 abr. 201

U.S. DEPARTMENT OF HOMELAND SECURITY *et al*. CVE: The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.. *In*: Common Vulnerabilities and Exposures. [*S. l.*], 2021. Disponível em: https://cve.mitre.org/. Acesso em: 23 mar. 2021.

TAGIAROLI, Guilherme. Falha no site do Detran-RS expôs RG e CNH de 5,1 milhões de motoristas. 29 de Janeiro de 2021. UOL Tilt. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/01/29/falha-de-seguranca-no-detran-rs-expos-dados-de-mais-de-51-mi-de-motoristas.amp.htm. Acesso em: 16 de Abril de 2021.

7 ANEXO



PUC GOIÁS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR
Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Gabriel Badim Vilela
do Curso de Engenharia de Computação, matricula 2015.1.0033.0498-1,
telefone: (62) 99806-6672 e-mail gabriel_badim@hotmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado LGPD: UM ESTUDO SOBRE AS PRINCIPAIS RESPONSABILIDADES E PENALIDADES PREVISTAS NA LEI, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 15 de Junho de 2021.

Assinatura do(s) autor(es): _____

Nome completo do autor: Gabriel Badim Vilela

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: Fábio Barbosa Rodrigues