PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
MONOGRAFIA JURÍDICA

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD:
DIREITO À PRIVACIDADE NO MUNDO GLOBALIZADO

ORIENTANDO: Rafael Ramos Soares
ORIENTADOR: Porf. Dr. Fausto Mendanha Gonzaga

Goiânia
2020

RAFAEL RAMOS SOARES

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD:
DIREITO À PRIVACIDADE NO MUNDO GLOBALIZADO

Monografia Jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof. Orientador – Dr. Fausto Mendanha Gonzaga

ATENÇÃO: O aluno orientando (autor do presente trabalho) declara que procedeu à sua revisão, para fins de detecção de plágio, assumindo, de forma exclusiva, a responsabilidade por eventual incorporação de textos de terceiros, sem a devida citação ou indicação de autoria.

Goiânia
2020

RAFAEL RAMOS SOARES

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD:
DIREITO À PRIVACIDADE NO MUNDO GLOBALIZADO

Data da Defesa: 24 de novembro de 2020

BANCA EXAMINADORA

_____
Orientador: Prof. Dr. Fausto Mendanha Gonzaga Nota

_____
Examinadora Convidada: Prof. Gabriela Pugliesi F. Calaça Nota

RESUMO

O presente trabalho procurou demonstrar, de forma clara e objetiva, a necessidade de uma legislação para regulamentar o tratamento dos dados pessoais, analisando a Lei Geral de Proteção de Dados (LGPD), no que tange à sua aplicação, conceitos, tratamentos de dados, de forma paralela com as premissas do direito fundamental à privacidade. Foi observado, durante o estudo, que a LGPD traz importantes inovações para o contexto brasileiro, adequando o país às regulamentações exteriores, principalmente a GDPR, trazendo também consigo uma nova abordagem das temáticas de tratamento de dados pessoais, garantindo ainda mais o direito fundamental da privacidade aos cidadãos.

Palavras-Chave: Dados pessoais. Privacidade. Proteção.

SUMÁRIO

INTRODUÇÃO

Nos últimos anos, observou-se um novo modelo de negócio no âmbito da rede mundial de computadores. Pôde-se verificar a migração de pessoas jurídicas e físicas para o mundo virtual, o que foi viabilizado pelos avanços tecnológicos e pela globalização. Diversas empresas e pessoas físicas começaram a disponibilizar os seus serviços online, bem como produtos que possuem conectividade com a internet.

Os usuários, ao utilizarem esses serviços, na maioria das vezes, devem preencher formulários de cadastros, disponibilizando dados de caráter pessoal, que, em muitos casos, são informações sensíveis a respeito do usuário. Ao final do cadastro, é preciso concordar com os Termos e Condições de Uso da empresa. Em tal termo, a empresa evidencia como deve ser feito o uso do serviço, aplicativo ou produto, bem como a forma de utilização das informações que foram cedidas pelo usuário ao se cadastrar.

Um grande problema que se observa é que, em muitos casos, os termos e as condições de uso são elaborados, de forma que o cliente não leia, devido a diversos fatores (complexidade, tamanho, termos difíceis de compreender, dentre outros fatores). Nesse sentido, o usuário fica sujeito ao que concordou, mas sem saber, exatamente, como os dados fornecidos serão utilizados pela empresa, no tocante à forma de coleta, compartilhamento e o potencial uso desses dados pessoais por terceiros.

O segundo grande problema, consequência do primeiro, é que, com o passar dos anos, as empresas vão adquirindo mais clientes e cada vez mais informações a respeito deles, construindo um grande banco de dados, com informações pessoais. Caso não estejam totalmente protegidos, podem ser objeto de ataques. Diversas informações pessoais ficam à mercê da pessoa que o adquiriu. Tais dados possuem um alto valor de mercado.

Observa-se a necessidade de garantir meios para que as informações coletadas sejam armazenadas de forma correta, bem como a pessoa tenha controle dos seus dados pessoais fornecidos para as empresas, podendo modificar, corrigir ou excluir as informações.

A Lei 13.709/2018 - Lei Geral de Proteção de Dados - regulamenta o tratamento dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais. Isso ocorre por qualquer meio, seja por pessoa natural ou jurídica, com princípios, direitos e obrigações, assegurando os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da pessoa natural.

CAPÍTULO I - BREVE HISTÓRICO SOBRE O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS

Para iniciarmos o nosso trabalho, vê-se como necessária a retomada ao passado, para entendermos melhor como o Direito a Privacidade surgiu e como os avanços tecnológicos impactaram na regulação à proteção de dados pessoais, tornando o direito à privacidade um direito fundamental, sujeito à proteção jurisdicional do Estado.

1.1 Direito à Privacidade

O direito à privacidade é um direito fundamental previsto no artigo 5º, inciso X, XI e XII de nossa Constituição Federal de 1988:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (BRASIL, 1988)

No entanto, tal condição de direito fundamental nem sempre foi assim. Houve uma construção histórica para termos hoje um instituo que visa proteger a vida privada dos indivíduos contra condutas que afrontam o cidadão, sejam elas praticadas tanto por particulares ou pelo próprio Estado.

Retornemos, então, à Constituição de 1824, também reconhecida como Constituição do Império, que continha, na sua carta magna, o direito de

inviolabilidade da casa e o segredo da carta. Em outras palavras, dava-se início a um certo direito de privacidade ainda embrionário, que estava em construção.

Nessa época, preocupava-se mais com a propriedade, ou seja, com os meios físicos e materiais. Segundo Rafael Fernandez (2020), há apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio, não havendo uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo, mas sim uma proteção apenas contra a invasão, ou seja, o ato de romper uma barreira física.

Com o passar dos anos, com os avanços tecnológicos e a inserção de novas tecnologias, como câmeras fotográficas portáteis, por exemplo, e a crescente invasão da vida privada pelas mídias, viu-se a necessidade de se consagrar um direito à privacidade com uma abrangência maior, ou seja, não respaldando apenas os meios físicos, conforme na época da Constituição do Império, mas sim uma extensão, em que esses direitos fossem um direito geral do indivíduo. Assim, se poderia escolher em qual extensão desejariam comunicar os seus pensamentos, os seus sentimentos e a suas emoções para os outros. Desse modo, em 1890 foi publicado, na Harvard Law Review, um artigo denominado “The Right to Privacy”, em tradução livre “O Direito à Privacidade”, que abrangia a necessidade de um direito à privacidade mais abrangente, evidenciando que a privacidade “ é o direito de ser deixado em Paz” (WARREN,1890).

Dessa forma, viu-se a necessidade de uma maior tutela dos direitos aos dados pessoais, frente ao princípio da privacidade. Foi então, em 1948, na Declaração Universal dos Direitos Humanos, que ficou consagrado o Direito à Privacidade como um direito fundamental do ser humano, dando origem, assim, às diversas legislações, a respeito do tema. A declaração, no seu artigo 12, ainda válida para os dias de hoje, ressalta que: “Ninguém será sujeito a interferências na sua vida privada, família, lar ou na sua correspondência, nem a ataque à sua honra e reputação. Toda Pessoa tem direito à proteção da lei contra tais interferências ou ataques” (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948).

Desde então, o Direito à Privacidade foi sofrendo diversas mudanças no que diz respeito a sua conceituação. O que antes tinha abrangência apenas sobre o aspecto de inviolabilidade do domicílio e ao sigilo da correspondência, teve profundas alterações e inclusões na sua definição, abrangendo, de forma mais ampla, outros pontos. A privacidade nos ajuda estabelecer fronteiras para limitar quem tem acesso aos nossos corpos, lugares e coisas, assim como nossas comunicações e nossas informações.

Nesse contexto, entramos no próximo ponto, a respeito da necessidade de proteção aos dados pessoais, mais especificamente a proteção às informações que são coletadas sobre os indivíduos, pelos mais diversos meios.

1.2 Proteção dos Dados Pessoais

No geral, as leis de proteção de dados pessoais possuem como características em comum a liberdade e a transparência, tendo mais enfoque nessa segunda premissa.

A primeira lei mundial de proteção de dados pessoais foi criada em 1970 na Alemanha. Schertel (2011) notou a necessidade de uma maior proteção dos dados pessoais, visto que eles constituem “uma projeção da personalidade do indivíduo e que, portanto, merecem de forma rígida uma proteção por parte do Estado jurisdicional”.

Foi em 1980 que a Organization for Economic Cooperation and Development (OECD), com um comitê de ministros da OECD, publicou algumas diretrizes que estabeleceram princípios básicos em relação à proteção de dados e sobre o fluxo de informações entre países que possuem as suas leis, em acordo com os princípios elencados nas diretrizes. Porém, essas diretrizes ainda não possuíam força para implementar um padrão, ocorrendo, muitas vezes, uma interpretação ampla, gerando diversos dispositivos legais em vários países. Cada nação possuía uma interpretação a respeito da proteção de dados.

Em 1981 foi aprovado o *Data Protection Convention*, o primeiro instrumento legal internacional, que buscava proteger o indivíduo contra a coleta e o processamento de dados pessoais de forma abusiva, proibindo o

processamento de dados confidenciais sobre a raça, politica, saúde, religião, vida sexual, antecedentes criminais de uma pessoa, dentre outras informações. Também se consagrava o direito do indivíduo de saber quais informações são armazenadas sobre ele e, se fosse o caso, corrigi-las (COE, 1981).

Já no Brasil, os primeiros instrumentos legais que alcançavam a proteção de dados pessoais e mudavam a concepção sobre a importância desses dados, foram instituídos a partir do ano de 1990. Um exemplo que podemos citar de lei que mudou essa concepção é o Código de Defesa do Consumidor (Lei 8.078/90). Dentre outras questões, previa-se o direito do consumidor de acessar às informações existentes em cadastros, registros, fichas de dados pessoais e de consumo arquivados sobre eles e que fosse alertado no caso de abertura de cadastro, contendo essas informações e permitindo, ainda, a correção ou a alteração desses dados. Temos também, em 1996, a Lei de Interceptação Telefônica e Telemática (Lei 9.296/96), que restringiu o uso de tais medidas, apenas em casos específicos e sempre com a devida autorização judicial, bem como a Lei do *Habeas Data* (Lei 9.507/97), que regulou o rito de acesso e a correção de informações pessoais e se tornou um direito constitucional.

Observando que cada país possuía a sua forma de estabelecer as suas medidas de proteção aos dados pessoais e não havendo uma harmonização quanto à aplicabilidade delas, a Diretiva 95/46 veio para nortear e harmonizar todas as leis já existentes anteriormente, no âmbito da União Europeia. De forma geral, estabeleciam-se conjuntos de regras que reforçavam as antigas diretrizes existentes nas leis nacionais, mas, também, criavam direitos quanto ao processamento de dados nos ambientes eletrônicos, nas formas automatizadas ou até mesmo no âmbito manual das coisas. Exigia-se, além disso, que todos os países da União Europeia editassem as suas leis a respeito da proteção e do processamento de dados pessoais (DIRETIVA 46/95), sendo esse um dos diplomas legais mais difundidos ao redor do mundo até a aprovação do GDPR – *General Data Protection Regulation,* que trataremos mais adiante.

No nosso país, em 2002, o Código Civil Brasileiro inovou e trouxe um capítulo sobre os Direitos da Personalidade, no qual fornecia instrumentos para coibir a violação da vida privada das pessoas, revelando a privacidade como um

direito subjetivo de cada ser humano e não focando mais na premissa de privacidade apenas no âmbito da propriedade.

Ainda no Brasil, em 2011 foi aprovada a Lei de Acesso à Informação (Lei nº 12.527/11), que, dentre outras questões, definia a informação pessoal como

> aquela relacionada à pessoa natural identificada ou identificável, determinando aos órgãos e entidades do poder público a proteção da informação sigilosa e pessoal, observando a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Ademais, eram ressaltados alguns princípios, como liberdades e garantias individuais, que seriam consagradas, também, na nossa Lei Geral de Proteção de Dados (LGPD), como o princípio da transparência, vida privada, honra, respeito à intimidade e imagem das pessoas.

Outra lei que vale destaque é a Lei 12.737/12 - Lei Carolina Dieckman, que criminalizou a invasão de dispositivos de informática, evidenciando em um dos seus dispositivos da lei:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Em 2013, o nosso mundo se viu diante de um acontecimento, que causou um grande impacto nas legislações referentes à proteção e ao tratamento de dados pessoais, bem como à consciência da necessidade de se ter uma maior proteção em relação às informações pessoais. Edward Snowden veio à tona, revelando alguns detalhes quanto à utilização de um software, chamado *PRISM* e outros, que eram utilizados para monitorar e vigiar, de forma global, informações que eram transmitidas na rede mundial de computadores. Esses programas coletavam informações em massa, vigiando não apenas terroristas, mas qualquer cidadão que transmitia informações na web, sendo utilizado,

também, para espionar países e grandes empresas estrangeiras. Podemos citar como uma das inúmeras vítimas, na época, a presidente do Brasil, Dilma Rousseff, demonstrando ao mundo todo o quanto é vulnerável a privacidade no âmbito da rede mundial de computadores.

Um dos grandes impactos no Brasil quanto a esse vazamento, foi a urgência em colocar em tramitação o PL 2126/11, que dizia respeito ao Marco Civil da Internet, que apesar de não trazer consigo qualquer tipo de proteção prática quanto à espionagem internacional, tinha alguns conceitos e princípios a respeito da privacidade e da proteção de dados pessoais. O Marco Civil da Internet foi votado e aprovado, entrando em vigor em 2014 e passou a constar no seu texto legal, pela primeira vez, a palavra privacidade, dando enfoque à necessidade da proteção dos dados pessoais, consagrando-o, mais uma vez, como um princípio fundamental das pessoas.

Outro ponto que vale ressaltar é a regulamentação da privacidade no âmbito da rede mundial de computadores, que o Marco Civil da Internet trouxe consigo, como, por exemplo, o artigo 3º, que abordou o princípio da proteção da privacidade e dos dados pessoais: “Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei.,” bem como o artigo 7º no inciso VII, VIII e X:

> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação;
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (BRASIL, 2014)

Vale ressaltar que todos esses princípios e vários desses regramentos seriam implementados na Lei Geral de Proteção de Dados posteriormente,

ficando clara a importância desses regramentos jurídicos para a então confecção da LGPD.

Em 2016, na União Europeia, surgiu um debate que deu origem ao GDPR – Regulamento Geral de Proteção de Dados Pessoais Europeu, que foi aprovado em 2016 e entrou em vigor em 2018. Tinha-se como objetivo a elaboração de normas e diretrizes, que visavam a proteção das pessoas físicas, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses respectivos dados e exigia que os demais países e empresas que quisessem manter relações comerciais com a União Europeia, deveriam criar uma legislação do mesmo âmbito que a GDPR. Isso gerou um grande impacto em todo o mundo e, consequentemente, a criação de normas em vários países, visto que a não implementação de tais medidas poderia gerar algumas barreiras econômicas e, consequentemente, dificuldades de realizar negócios com a União Europeia.

Podemos citar como objetivos da GDPR:

> a) contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas;
> b) assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno;
> c) garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo;
> d) impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais;
> e) possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros.

De forma geral, segundo Patricia Peck Pinheiro (2018), a GDPR veio para inovar as legislações já existentes, padronizando, ou melhor, normalizando, quase como uma norma padrão mundial, o que seriam os atributos qualitativos da proteção dos dados pessoais. Caso não estivessem presentes tais atributos gerariam uma penalidade, tendo, principalmente, efeitos econômicos, sociais e políticos, buscando equilibrar as relações em um cenário de negócios digitais sem fronteiras.

Outro acontecimento que vale ressaltar, que teve um grande impacto na criação de leis de proteção de dados, inclusive impulsionou o Brasil a criar a

LGPD, foi o *Cambridge Analytica* - caso do *Facebook,* no qual foram divulgadas informações a respeito de operações irregulares com dados coletados de usuários da rede social *Facebook*. Segundo as investigações e os relatos, esses dados estariam sendo usados na política, inclusive surgindo a possibilidade de tais informações terem influenciados as eleições dos EUA e Brasil. Esse episódio impulsionou não só o Brasil, mas outros países a respeito da necessidade de uma legislação a respeito da proteção e do tratamento de dados pessoais. (FERNANDEZ, 2020, p. 15)

De forma geral, segundo Bruno Ricardo Bioni (2019), podemos dividir a história da criação das leis de proteção de dados pessoais em quatro gerações. A primeira geração seria o momento em que aparece a preocupação com o processamento massivo dos dados pessoais na esfera do governo, na conjuntura da formação do Estado Moderno, possuindo o seu foco na esfera governamental. Nesse momento, foram estabelecidas normas rígidas, que regulavam o uso das tecnologias, no tocante ao processamento e à coleta de dados pessoais das pessoas componentes do governo. A segunda geração tinha como centro uma mudança regulatória, não se preocupando apenas com os dados pessoais das pessoas governamentais, mas, também, dos indivíduos da esfera privada, transferindo, assim, para os próprios titulares dos dados a responsabilidade de mantê-los protegidos. Em outras palavras, decidia-se quais informações poderiam ser coletadas, usadas e compartilhadas, tudo com o seu devido consentimento, dando uma maior autonomia para o indivíduo, em gerir as suas informações pessoais.

A terceira geração se trata de regulamentos, que dão ao indivíduo a prerrogativa na participação de todo o processo, desde a coleta até o compartilhamento das informações, ou seja, deu-se uma autonomia maior para a pessoa titular daquelas informações. Na quarta geração entrou novamente o Estado, regulamentando certos tipos de dados pessoais que seriam considerados sensíveis, tirando da autonomia do indivíduo a prerrogativa de auto escolha, passando para o Estado a prerrogativa de gerir tais informações, com base nos regulamentos das leis de proteção de dados.

CAPÍTULO II - LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Antes de adentrarmos na Lei Geral de Proteção de Dados, devemos fazer uma breve conceituação a respeito do que é LGPD e algumas terminologias usadas na Lei.

2.1 O que é a LGPD?

Conforme conceitua Rafael Fernandez na sua obra “Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais”, a LGPD é uma Lei que:

> dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, inclusive por meio digital (FERNANDEZ, 2020, p. 17).

Em outras palavras, podemos dizer que a LGPD trata da proteção aos dados coletados ou processados de alguma forma, protegendo a privacidade dos cidadãos, sejam eles brasileiros ou estrangeiros, que se encontrem no Brasil, buscando sempre um equilíbrio entre os novos modelos de negócios que vêm surgindo cada vez mais com o avanço das tecnologias e a globalização. Com relação ao uso e à proteção da privacidade desses dados coletados, atualmente, conforme já mencionado nos capítulos anteriores, esse é um direito cada vez mais em pauta pelos cidadãos.

A LGPD na sua Lei nº 13.853/2019, no seu Artigo 2º tem como fundamentos para a devida utilização dos dados pessoais:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Conforme podemos observar, os fundamentos da LGDP estão relacionados com o texto presente na nossa Constituição Federal de 1988, sendo eles: artigo 3º, I e II; artigo 5º, X e XII; artigo 7º, XXVII; artigo 219 e artigo 4º, II. Evidencia-se, portanto, mais uma vez, que a LGPD tem como base a proteção e a garantia à privacidade, liberdade, segurança, justiça das pessoas, bem como a evolução econômica e social, garantindo, assim, uma segurança jurídica do país.

Outro ponto importante diz respeito à conceituação de algumas expressões utilizadas na Lei, quais sejam: pessoa natural, pessoa jurídica, dados pessoais, titular dos dados, tratamento dos dados, dados pessoais sensíveis, consentimento, banco de dados, controlador e operador.

De forma breve e objetiva vamos conceituar esses termos:

a) A pessoa natural é o ser humano capaz de direitos e obrigações na esfera civil;

b) A pessoa jurídica é uma entidade à qual se atribui uma personalidade jurídica, tendo como principal característica a de atuar na vida jurídica, com personalidade distinta dos indivíduos que fazem parte dela;

c) Os dados pessoais concernem a qualquer informação relacionada a uma pessoa natural;

d) O titular dos dados é a quem pertence os dados pessoais que são objeto de tratamento;

e) O tratamento dos dados é toda e qualquer operação realizada com dados pessoais, como, por exemplo ressalta a LGPD: coleta, recepção, produção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

f) Os dados pessoais sensíveis são os dados que podem se relacionar a uma pessoa natural, com algum tipo de associação, movimento, sindicato, partido político ou até mesmo questões de ordem étnica, religiosas, politicas, filosóficas, vida sexual, dentre outros fatores, estando incluídos também dados médicos, biométricos e genéticos;

g) O consentimento é a manifestação livre, informada e inequívoca pela qual o titular aceita o tratamento dos seus dados pessoais para uma finalidade determinada;

h) O banco de dados é o conjunto de informações pessoais estabelecido em um ou em vários locais;

i) O controlador é a pessoa natural ou jurídica, podendo ser direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais;

j) O operador, que também pode ser chamado de processor, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

O operador e o controlador são os denominados agentes e tratamento, respectivamente.

2.2 GPDR e a LGPD

A *General Data Protection Regulation* (GPDR) foi a grande base de inspiração para a nossa LGPD. Ela possui como objetivo, assim como a nossa norma, a garantia de um maior controle sobre a coleta e tratamento de dados pessoais dos usuários, definindo diretrizes a serem seguidas, bem como aplicando sanções para quem não as colocar em prática, conforme bem explicito na lei.

Outro ponto que vale salientar diz respeito à aplicabilidade das normas, enquanto a LGPD se destina a proteger os cidadãos brasileiros, a GDPR se destina aos cidadãos originários de países da União Europeia. A unificação de um regulamento geral, que possui 28 Estados-Membros participantes e que se vinculam ao mesmo ordenamento, faz com que a aplicabilidade no continente Europeu ocorra de forma mais eficiente, padronizando os processos e as diretrizes a serem seguidor por todos os integrantes.

Infelizmente, isso não foi o que ocorreu com o Brasil. Houve, no entanto, várias bases sólidas vindas da GPDR, utilizando-a como uma “mãe”, um padrão

para a criação da nossa Lei de Proteção de Dados, porém, em muitas situações, dependendo do tipo de operação das empresas, deve-se utilizar uma análise comparativa, ou seja, uma comparação entre as leis para então ver qual regra seria aplicável em determinado caso concreto que envolva dados de um determinado titular.

Como exemplo, Patricia Peck Pinheiro cita:

> [...] uma instituição brasileira que capture dados no Brasil, em território nacional, mas que tenha um aplicativo que permita que o cliente seja de qualquer cidadania, nacionalidade, residência, e, portanto, o usuário do serviço, titular dos dados, pode ser um europeu, que mantém sua vida em um país da União Europeia, mas está temporariamente a trabalho no Brasil, utiliza cartão de crédito internacional, acaba por atrair, em termos de aplicação de leis e jurisdição para a sua operação, tanto a regulamentação nacional (LGPD) como também a regulamentação europeia (GDPR). Se essa instituição brasileira utilizar recursos na nuvem e fizer a guarda internacional dos dados pessoais em outro país, poderá atrair ainda outras regulamentações (como o Cloud Act, dos EUA). (PINHEIRO, 2018, p. 30 - 31)

De forma geral, a LGPD se destina a proteger cidadãos brasileiros, enquanto a GPDR se destina aos cidadãos de países da União Europeia. Porém, dependendo de cada caso concreto, pode-se aplicar mais de uma regulamentação, conforme exemplo supramencionado.

No campo dos dados pessoais, a GPDR é mais rígida no tocante à obrigatoriedade da implementação de políticas de governança, proteção de dados e segurança da informação, tendo uma regulamentação a respeito do tema. Já a LGPD não há até o momento previsões expressas na lei, podendo ser regulamentado posteriormente.

Em relação aos dados da criança e do adolescente, na nossa Lei Geral de Proteção de Dados, os menores de 18 anos necessitam de consentimento de pelo menos um dos seus pais ou responsáveis para autorizarem a coleta e o tratamento dessas informações. Já no regulamento europeu, os menores com 16 anos ou mais podem dar seu próprio consentimento.

Quanto à responsabilidade de fiscalização e aplicação de multas, a LGPD ressalta que a ANPD (Autoridade Nacional de Proteção de Dados), é a responsável pela fiscalização, mas poderá delegar a aplicação de sanções administrativas e multas aos demais organismos, como, por exemplo, o MPF. A GPDR possui um órgão central, que se chama Comitê Europeu para a Proteção de Dados e é o responsável para a fiscalização e a aplicação das sanções e das multas.

Quanto ao tratamento dos dados sensíveis, a GPDR os proíbe expressamente, com duas exceções, a saber: dados sensíveis tornados públicos pelo titular; dados relativos a atuais ou ex-membros de fundações, associações ou organizações sem fins lucrativos, tratados para fins legítimos e com medidas de segurança apropriadas. Já na LGPD possui a previsão de tratamentos de dados considerados sensíveis.

Quando falamos a respeito da notificação da violação de dados, ou seja, no caso das informações em que os indivíduos forem violados e vazados na LGPD, não há prazo expresso para que seja feita a notificação para a autoridade competente de supervisão. A regulamentação apenas deve ser em um prazo razoável, deixando-o muito subjetivo. Já no regulamento europeu há uma determinação de que, no prazo de 72 horas, quaisquer incidentes que acontecerem deverão ser notificados às autoridades competentes.

Apesar das diferenças existentes entre a LGPD e a GPDR, há muitas semelhanças entre elas também e, conforme já falado, esta serviu como base para a criação daquela. Vale frisar, também, que por ser a LGPD uma Lei, possui disposições mais abertas e subjetivas, ou seja, permite-se uma interpretação em alguns aspectos, como, por exemplo, no tempo de notificação. Já a GPDR é um regulamento, mais objetivo e direto nos seus dispositivos, com regras bem determinadas para diversas situações que possam acontecer.

2.3 Aplicação da LGPD

Inicialmente, é importante salientar, conforme já mencionado anteriormente, que a LGPD é aplicável a todos que realizem o tratamento de

dados pessoais, sejam elas pessoas de direito público ou privado, pessoa física ou jurídica, desde que estejam realizando qualquer tipo de operação que se enquadre em tratamento de dados pessoais. Isso ocorre independentemente do meio, do país da sua sede ou da nação em que estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens, serviços ou o tratamento de dados de indivíduos localizados no território nacional; os dados pessoais objeto do tratamento tenham sido coletados no território nacional conforme expresso no artigo 3º, I, II e III da Lei 13.709/2018 (LGDP).

Outro ponto que vale destaque é no tocante à extraterritorialidade da lei. Desde que os dados tenham sido coletados em território nacional, até mesmo por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil, a LGPD será aplicada com efeitos internacionais. Em outras palavras, caso uma empresa colete dados pessoais no território nacional, porém a sua sede seja em outro país, essa organização, ainda assim, terá que se enquadrar nos termos da LGPD.

Quanto à inaplicabilidade da LGDP, temos no artigo 4º a seguinte redação:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Observa-se que a lei trouxe consigo uma certa limitação de aplicabilidade em relação aos tipos de dados que são regulados pela LGPD. Segundo Patricia Peck (2018, p. 43-44): “o tratamento de dados pessoais deve seguir um propósito

certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado.” Têm-se, nesse sentido, uma certa limitação, buscando consigo uma maior segurança em temas relevantes da sociedade.

Infere-se, do texto da Lei, que essas limitações buscam consigo, contribuir para um melhor equilíbrio entre a proteção da privacidade e da segurança pública, ou seja, há sempre a busca do equilíbrio, do que é benéfico para o indivíduo quanto aos seus dados pessoais, nunca ultrapassando, porém, a barreira de se tornar um perigo para o Estado e toda a sociedade.

Outro ponto que vale destaque é o fato de que a LGDP se aplica apenas nos casos que tem a busca da oferta ou do fornecimento de bens ou serviços, ou seja, uma questão econômica por trás. Nos casos em que não há esse propósito e quando tratar-se de pessoa natural, não há que se falar em aplicação da LGDP. O que a Lei busca de forma direta com essa especificação é a proteção dos dados pessoais, que se tornou, nesses últimos tempos, a principal moeda de troca pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

2.4 Tratamento de Dados Pessoais

Antes de entrarmos nas atividades que compõem o que se chama de tratamento de dados pessoais, é importante falar sobre os princípios aplicáveis e que validam o tratamento dos dados.

Temos como princípios norteadores do tratamento de dados pessoais: adequação, finalidade, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas, prevenção, não discriminação e qualidade de dados.

Pelo princípio da finalidade, os dados que forem coletados dos indivíduos devem ter um fim específico e o tratamento de tais informações devem ater-se à tal finalidade, devendo, ainda, estar claro para qual fim foram coletados tais dados pessoais.

Segundo o princípio da adequação, todo processo de tratamento dos dados deve ter uma relação direta com as finalidades anteriormente informadas pelo princípio da finalidade, devendo se adequar ao que for solicitado. Um exemplo disso é quando o usuário solicita que os seus dados sejam deletados do banco de dados, mas a empresa que os possui não deletam, apenas ocultam do usuário. Isso constitui uma violação ao princípio da adequação, podendo a empresa sofrer punições.

O princípio da necessidade ressalta que os dados coletados dos usuários devem ter um motivo, ou seja, devem ter realmente a necessidade da coleta para o fim que seja destinado.

O princípio do livre acesso evidencia que os dados pessoais que forem coletados devem estar a todo momento disponíveis de forma gratuita e facilitada, para consulta por parte dos seus titulares. Todas as informações a respeito do usuário, até mesmo por quanto tempo os dados serão tratados, a forma, dentre outras informações devem estar disponíveis para acesso.

Pelo princípio da qualidade dos dados, aos portadores e titulares dos dados pessoais deve haver uma garantia de que as suas informações serão tratadas de forma correta, clara, relevante e atualizada, de acordo com a necessidade e para o cumprimento específico da finalidade que os dados foram coletados.

O princípio da transparência afirma que os dados e tratamentos oferecidos devem ser informados de maneira clara, precisa e transparente, ou seja, deve ser descrito de forma abrangente todo o processo de tratamento que os dados passarão.

Todos os dados devem ser tratados de forma que as técnicas utilizadas garantam a maior proteção contra acessos não autorizados, bem como de situações acidentais ou ilícitas, que possam causar destruição, perda, alterações, vazamentos ou difusões de forma não autorizada. O possuidor desses dados pessoais deve garantir, pelas formas adequadas, que os dados dos usuários estarão seguros, podendo ser responsabilizado caso ocorra alguma violação. Desse princípio que é denominado princípio da segurança, temos como decorrência o princípio da prevenção, que destaca que devem ser

adotadas medidas preventivas, para evitar que ocorram quaisquer tipos de danos aos dados pessoais dos titulares.

Por fim, temos o princípio da não discriminação e o da responsabilização e prestação de contas. O primeiro reforça que os dados não devem ser tratados com finalidades discriminatórias, abusivas ou ilícitas. Já o segundo aponta que o agente de tratamento é responsável pelos dados pessoais bem como deve, a qualquer momento que for solicitado, ser capaz de demonstrar que está adotando as medidas necessárias para o devido cumprimento das normas de proteção dos dados pessoais, inclusive evidenciando a eficácia das medidas que estão sendo adotadas.

Após falarmos um pouco sobre os princípios aplicáveis ao tratamento de dados pessoais, podemos citar algumas ações que são entendidas como atividade de tratamento de dados, sendo assim, passíveis da aplicação da LGPD, sendo elas: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, dentre outros atos.

Outro ponto que vale destacar é referente aos requisitos, ou seja, às bases legais pelas quais é permitido que os dados pessoais sejam tratados, contidas no artigo 7ª e nos seus incisos e parágrafos. Primeiramente, vale ressaltar que sempre que houver um consentimento de forma explícita por parte do titular dos dados, o tratamento deles é permitido, sempre frisando que tal consentimento deve ser direcionado para um fim específico, conforme bem preceitua os princípios aplicáveis ao tratamento de dados pessoais, podendo, ainda, revogar esse consentimento a qualquer momento que desejar.

Está permitido o tratamento sempre que houver a necessidade de cumprimento com alguma exigência legal ou regulatória, desde que ela seja admissível, buscando evitar, nessa interpretação, a possibilidade de a lei entrar em conflito com outras legislações vigentes no país, devendo, ainda, mesmo que permitido, o agente de tratamento notificar o titular sobre esses dados.

No caso de execução de políticas públicas e estudos realizados por órgãos de pesquisas, também está autorizado o tratamento dos dados, porém sempre seguindo os princípios necessários para o devido tratamento e

conformidade com a Lei. No caso dos órgãos de pesquisas, sempre que possível, esses dados deverão ser anonimizados, garantindo a sua privacidade.

Outro ponto que está autorizado o tratamento é no caso de execução de contrato, ou seja, o próprio titular solicitará o tratamento deles para garantir a execução de um contrato ou dos seus procedimentos preliminares, tendo uma relação com o primeiro caso que citamos, o de consentimento. Contudo, a diferença é que, no caso de execução de contrato, o titular não poderá revogar o fornecimento desse tratamento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD, para poder manter as informações fornecidas pelo titular enquanto durar a vigência do contrato.

A LGPD também permite o tratamento nos casos de exercício regular do direito em processos judicial, administrativo ou arbitral, como, por exemplo, um credor que judicialmente pode tratar os dados dos seus devedores, sem solicitar o seu consentimento.

Busca-se garantir a proteção da vida e a incolumidade física, desde que fique devidamente comprovada a necessidade. Com a finalidade bem definida e clara da situação em questão, a LGDP autoriza o tratamento de dados pessoais. Deriva dessa última autorização, a tutela da saúde, havendo uma autorização de tratamento de dados pessoais, sempre que necessário, para procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária.

Outra previsão da lei que expressa o consentimento de tratamento de dados é no caso de interesse legítimo. Nesse ponto, Sergio Pohlmann, na sua obra “LGPD Ninja”, destaca que:

> Entendamos interesse legítimo como algo que é importante para alguém, tendo como base uma justificativa amparada pelo bom senso. Para que o interesse legítimo possa ser aceito como um caso de tratamento de dados válidos, o mesmo deve cumprir com os três pilares a seguir:
> 1. O legítimo interesse não poderá ser exercido no caso de prevalecerem direitos e liberdades fundamentais do titular, que exijam a proteção de seus dados.
> 2. As finalidades devem ser legítimas.
> 3. O caso deve estar baseado em situações concretas (POHLMANN, 2019, p. 84 - 85).

Outro ponto que está expressamente previsto nos casos de autorização é o tratamento dos dados pessoais na proteção do crédito. Em outras palavras,

informações, como por exemplo as contidas no Serasa ou Cadastro Positivo, podem ser consultadas por outras empresas.

CONCLUSÃO

Podemos afirmar que a implementação de uma Lei que visa garantir a regulamentação de todo o tratamento de dados pessoais dos cidadãos brasileiros dentro e fora do Brasil é de suma importância.

Como bem observado, durante este trabalho, o avanço das tecnologias, bem como a introdução de novos modelos de negócio, traz consigo a necessidade de uma maior proteção à privacidade dos cidadãos. Dessa forma, a privacidade - não só no Brasil, como também no mundo - é um valor que jamais fora abandonado. Pelo contrário, o direito à privacidade vem sendo cada vez mais fortalecido, diante de inúmeras denúncias de utilizações de informações pessoais de forma abusiva, invasiva e indevida, sem mesmo que o titular tivesse qualquer controle sobre elas, havendo, inclusive, a sua utilização para fins políticos, econômicos ou sociais.

Dessa necessidade nasceu a Lei Geral de Proteção de Dados: uma lei brasileira, baseada na regulamentação Europeia (GDPR). A LGPD visa um equilíbrio entre o direito à privacidade e o uso massivo das informações pessoais. Sua missão, portanto, não é outra, senão proteger direitos fundamentais, tais como a liberdade, a privacidade, o livre desenvolvimento e a personalidade.

Como fundamentos da LGPD podemos destacar o respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade, livre iniciativa, defesa do consumidor, direitos humanos, dignidade e exercício da cidadania. Na prática, a LGPD se aplica aos governos e às empresas, tendo que garantir maior segurança aos dados pessoais, sempre observando a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilização e a prestação de contas de tudo que se refere aos dados pessoais, conforme bem explicado durante o presente trabalho.

De forma geral, conforme delineado no corpo desta monografia, os pontos mais importantes do panorama geral da LGDP podem ser sintetizados da seguinte forma: a LGPD é uma regra para todos, ou seja, cria um cenário de segurança jurídica válido para todo o país; estabelece de maneira clara, o que

são os dados pessoais e como deverá ser feito o devido tratamento deles; como regra, para que os dados pessoais possam ser tratados, deve haver o consentimento do seu titular, tendo como exceção apenas os casos em que seja indispensável cumprir critérios legais; não importa se a organização ou o centro de dados estão dentro ou fora do Brasil, sendo a sua abrangência extraterritorial, conforme bem pontuado durante o trabalho; no caso de inobservância da legislação, há aplicação de penas rígidas; a lei traz consigo definições de que são dados pessoais indispensáveis ao bom entendimento da legislação; a lei evidencia as responsabilidades de cada agente de tratamento e as suas funções.

Por fim, cada vez mais as pessoas estão exigindo uma maior transparência no uso dos seus dados pessoais e a efetiva proteção à privacidade não pode ser negligenciada, sob pena de se inviabilizar qualquer forma de atuação no mercado global. Portanto, é indispensável que as empresas que coletam dados e realizam o tratamento dele deixem claro aos usuários o objetivo da captura das referidas informações, indicando como será feita a sua utilização, podendo o usuário exercer a prerrogativa de autorizar ou não o seu tratamento, ficando, assim, no controle efetivo das suas informações pessoais.

REFERÊNCIAS

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Ed. Forense Ltda, 2019.

BRASIL. *Lei Carolina Dieckmann***.** Brasília, DF: Congresso Nacional, 2012.

BRASIL. *Lei Geral de Proteção de Dados Pessoais***.** Brasília, DF: Congresso Nacional, 2018.

BRASIL. *Marco Civil da Internet***.** Brasília, DF: Congresso Nacional, 2014.

CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje*: perspectiva histórica e o cenário brasileiro. Disponível em: https://www. https://www.scielo.br/scielo.php?script=sci_arttext&pid=S217770552017000200213&lng=en&nrm=iso. Acesso em: 29 abr.2020.

COTS, Marcio. *Lei Geral de Proteção de Dados Pessoais Comentada*. São Paulo: Editora Revista dos Tribunais. 2018

COUNCIL OF EUROPE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 Acesso em: 20 abr. 2020

EUROPA. *Directiva 95/46/CE do parlamento europeu e do conselho***.** Luxemburgo: 1995

MACIEL, Rafael Fernandes. *Manual prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)*. Goiânia: RM Digital Education, 2019.

NAÇÕES UNIDAS BRASIL. *Artigo 12: Direito à privacidade*. Disponível em: https://nacoesunidas.org/artigo-12-direito-a-privacidade/. Acesso em: 20 maio 2020.

NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos***.** Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 22 maio 2020.

MENDES, Laura Schertel. O Direito Fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor*. https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1228/1155. Acesso em: 19 maio 2020

NETTO, Thais. *Aplicabilidade e Inaplicabilidade da LGDP*. 2020. Disponível em: https://direitoreal.com.br/artigos/aplicabilidade-e-inaplicabilidade-da-lgpd. Acesso em: 15 de jul. de 2020.

PINHEIRO, Patricia Peck*. Proteção de dados pessoais* – Comentários à Lei N. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

POHLMANN, Sérgio Antônio. *LGPD Ninja* – Entendendo e implementando a Lei Geral de Proteção de Dados nas empresas. São Paulo: Editora Fross, 2019.

SERPRO. *Serpro e LGPD*: segurança e inovação. 2020. Disponível em: https://www.serpro.gov.br/lgpd/. Acesso em: 20 jul. 2020.

ANEXOS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL
Av. Universitária, 1069 | Setor Universitário
Caixa Postal 86 | CEP 74605-010
Goiânia | Goiás | Brasil
Fone: (62) 3946.3081 ou 3089 | Fax: (62) 3946.3080
www.pucgoias.edu.br | prodin@pucgoias.edu.br

RESOLUÇÃO n°038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Rafael Ramos Soares
do Curso de Direito, matrícula 2018.1.0001.1535-7,
telefone: 62 98221 8279 e-mail rafa-ramos2@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 Lei Geral de Proteção de Dados - LGPD : Direito à Privacidade no Mundo Globalizado,
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, 24 de novembro de 2020.

Assinatura do(s) autor(es): Rafael Ramos Soares

Nome completo do autor: Rafael Ramos Soares

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: Fausto Mendanha Gonzaga