PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

DIREITO DIGITAL: A NOVA ERA DOS DADOS E DA PRIVACIDADE

ORIENTANDO - MARCELO CARNEIRO GUIMARÃES

ORIENTADOR - PROF. DR. NIVALDO DOS SANTOS

GOIÂNIA
2020

MARCELO CARNEIRO GUIMARÃES

DIREITO DIGITAL: A NOVA ERA DOS DADOS E DA PRIVACIDADE

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 (PUC GOIÁS).
Prof. Orientador – Dr. Nivaldo dos Santos

GOIÂNIA
2020

SUMÁRIO

RESUMO

A humanidade passa por um momento de sua história em que chegamos a um nível muito elevado em relação às tecnologias. A tendência é de que as transformações tecnológicas sejam cada vez mais rápidas e eficazes em grande parte das áreas, como saúde, lazer e educação. A internet, por exemplo, é uma das principais criações de todos os tempos de nossa história, tendo como principal função ser um “encurtador” de distância. Graças a ela, informações são passadas de um lado ao outro do mundo em questões de milésimos de segundos, sendo que, um grande acontecimento, por exemplo na China, rapidamente será informado para todos os outros países e continentes. Este meio digital é de suma importância hoje em dia, ainda mais em momentos de Pandemia, como se vive em 2020, ele é fundamental para que se mantenham as comunicações e também para que a humanidade continue sua história com seus trabalhos e estudos tudo pelo meio virtual, em parte. Com o advento da Internet e com o passar dos anos, escândalos relacionados ao uso de dados dos usuários e a questão da privacidade vêm se escancarando cada vez mais e tornando cada vez mais sério, já que, essa proteção a privacidade se tornou um direito fundamental nos tempos atuais. E é neste momento que se encontra a importância da criação de leis para regular esses espaços e proteger os usuários para que não haja violação de direitos e práticas de abusos e crimes. No Brasil importantes leis foram criadas para reger este espaço, primeiramente o Marco Civil da Internet em 2014 (Lei 12.695) e, para complementar e suprir brechas da citada anteriormente, começou a vigorar em setembro de 2020 a Lei Geral de Proteção de Dados Pessoais (lei 13.709/18), similar à lei adotada na Europa, a chamada GDPR (*Gereral Data Protection Regulation*). Portanto, é de suma importância fazer um estudo das leis que vigoram nos meios digitais, mas com enfoque na relação entre o uso de dados e a privacidade dos usuários.

Palavras chave: internet, dados, privacidade, redes sociais.

ABSTRACT

Humanity is going through a moment in its history when we reached a very high level in relation to technologies. The trend is that technological changes are increasingly faster and more effective in most areas, such as health, leisure and education. The internet, for example, is one of the main creations of all times in our history, having as main function to be a "shortener" of distance. Thanks to it, information is passed from one side of the world to the other in a matter of milliseconds, and a major event, for example in China, will quickly be reported to all other countries and continents. This digital medium is of paramount importance today, even more so in times of Pandemic, as we live in 2020, it is essential for maintaining communications and also for humanity to continue its history with its works and studies all in between. virtual, in part. With the advent of the Internet and over the years, scandals related to the use of users' data and the issue of privacy have been increasingly open and

increasingly serious, as this protection of privacy has become a fundamental right in current times. And it is at this moment that the importance of creating laws to regulate these spaces and protect users is found so that there is no violation of the rights and practices of abuses and crimes. In Brazil, important laws were created to govern this space, first the Marco Civil da Internet in 2014 (Law 12.695) and, to complement and fill gaps in the aforementioned, the General Data Protection Law (law 13,709 / 18), similar to the law adopted in Europe, the so-called GDPR (Gereral Data Protection Regulation). Therefore, it is of utmost importance to study the laws in force in digital media, but with a focus on the relationship between the use of data and the privacy of users.

Keywords: internet, data, privacy, social networks

INTRODUÇÃO

O Direito Digital é um ramo novo e amplamente diversificado, já que, todos os outros ramos se incorporam e agregam a ele, dessarte, a essência do trabalho descrito será sobre Dados e a Privacidade nos meios digitais, com foco na Lei Geral de Proteção de Dados Pessoais.

A lei surgiu após consultas públicas feitas para ver sua necessidade e sua aplicação, acerca, principalmente, de dados e privacidade. Bioni conta, acertadamente, o resultado dessas consultas públicas e ao que levou, ele alega que:

> Após tais consultas públicas, o texto enviado ao Congresso Nacional, que depois veio a ser aprovado e sancionado, acabou por posicionar o consentimento como sendo uma das hipóteses legais e não na cabeça do dispositivo. Isso significa que, em termos de técnica legislativa, o consentimento não só deixou de ser a única base legal para o tratamento de dados, como também foi alocado topograficamente sem ser hierarquicamente superior às demais bases legais por estarem todos elas horizontalmente elencadas em incisos do art. 7º da LGPD. (BIONI, 2019, p. 188)

Sobre a lei, Maciel, explicita bem a função da Lei Geral de Proteção de Dados no Brasil:

> A LGPD 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 de privacidade e o livre desenvolvimento da personalidade da pessoa natural, INCLUSIVE POR MEIO DIGITAL. (MACIEL, 2019, p.16)

Frente a isso, expõe Pinheiro, que por mais que as pessoas fiquem cientes quanto à utilização dos dados e da privacidade, elas provavelmente teriam que abrir mão de alguns conteúdos, como ela diz:

> Afinal, será que estamos dispostos a abrir mão de usar os serviços gratuitos, as redes sociais, em troca dos nossos dados? Acredito que não. Mas com certeza todos nós gostaríamos de sentir que temos controle sobre eles, que o Direito nos protege contra abusos, por mais que nós mesmos que tenhamos, de livre e espontânea vontade, fornecido nossa informação a um terceiro, seja do tipo cadastral, seja do que publicamos na web. Ganhará o mercado quem liderar a proteção da privacidade sustentável, com transparência. Qualquer outro formato, para um extremo do “libera geral” ou do extremo do “protege a pessoa dela mesma” está fadado ao fracasso. (PINHEIRO, 2013, p. 45.)

Portanto, é fundamental o estudo do Direito Digital e suas leis específicas, com o enfoque na privacidade.

CAPÍTULO I – A INTERNET E O DIREITO DIGITAL NO MUNDO

1.1 HISTÓRICO DA INTERNET

A *internet* foi criada no ano de 1969 pelos Estados Unidos da América (EUA) em uma época que se passava a Guerra Fria onde, as duas super potências envolvidas, Estados Unidos e União Soviética, estavam divididos nos blocos socialista e capitalista e disputavam poderes e hegemonias e tinha como função interligar laboratórios científicos com os militares caso houvessem bombardeios que levassem ao isolamento por quebra nos equipamentos. Este primeiro modelo de internet tinha o nome de Arpanet. Inicialmente, somente o estadunidense havia acesso ao Arpanet.

> O projeto da Arpanet foi implementado por Bolt, Beranek and Newman (BBN), uma firma de engenharia acústica de Boston que passou a realizar trabalhos em ciência da computação aplicada; fundada por professores do MIT era integrada em geral por cientistas e engenheiros dessa instituição e de Harvard. (CASTELLS, 2003, p. 14)

Anos mais tarde, em 1982, a área acadêmica dos EUA passou também a ter acesso. No mesmo ano também houve expansão da utilização para outros países, como Suécia e Dinamarca, mas eram poucos. Somente em 1987 houve uma expansão maior devido ao seu uso comercial. Em 1989 começaram a surgiram algumas empresas que se interessaram pelo seu uso e criaram provedores de internet.

Os anos 80 serviram para expansão da jovem internet e fortalecimento da infraestrutura da conexão. Na primeira metade da década surgiu o *Personal Computer* ou Computador Pessoal, entre eles o IBM PC e Macintosh (Linha de computadores fabricados pela grande *Apple*).

Ao final da década de 80 foi criada a *World Wide Web*, a famosa “www”, pelo britânico físico e cientista da comunicação Tim Berners-Lee.

> Ele definiu e implementou o software que permitia obter e acrescentar informação de e para qualquer computador conectado através da Internet: HTTP, MTML e URI (mais tarde chamado de URL). Em colaboração com Robert Cailliau, Berners-Lee construiu um programa navegador/editor em dezembro de 1990, e chamou esse sistema de hipertexto de World Wide Web, a rede mundial. O software do navegador da web foi lançado na Net pelo CERN em agosto de 1991. (CASTELLS, 2003, p. 18)

O “WWW” trouxe mais funcionalidades ao meio e queria que seu uso fosse de forma indiscriminada, ou seja, que fosse alcançável a todos. No mesmo ano, Tim se desligou do CERN e criou a World Wide Web Foundation onde ajudava a desenvolver e espalhar os padrões da internet aberta, o que facilitou a difusão da *internet*. Tim continua sendo chefe da fundação. No mesmo ano do surgimento do “*WWW”*, a Arpanet foi desligada.

Um ano antes surgiu o Mosaic, o primeiro navegador realmente funcional que foi evoluindo ao longo dos anos. Muitos buscadores que existem até hoje foram criados nessa época, como “*Yahoo!*” em 1994 e o “*Google*” em 1998, além de famosos sites da época ICQ e Napster, por exemplo, criando novas formas de comunicação online.

A partir daí, a expansão foi cada vez mais intensa e, hoje, no ano 2020, a internet se tornou peça fundamental em grande parte dos lares, comércios, empresas e governos, trazendo com isso novos crimes, novas responsabilidades e novas leis.

1.2 DIREITO DIGITAL NO MUNDO E A PRIVACIDADE

O instituto “privacidade” tem evoluído nas legislações internacionais e nacionais e é um objeto que precisam ser discutidos, já que, a população anseia por direitos que os protejam, então, o legislador busca atender esses anseios da população e, de fato, será visto a importância da privacidade e como foi evoluindo ao longo dos anos e décadas. Maciel explicita bem a relevância de se tratar sobre o histórico do Direito Digital e a privacidade.

> Para compreendermos a Lei Geral de Proteção de Dados Pessoais no Brasil, fundamental fazermos uma volta ao passado e encararmos como a privacidade tornou-se um direito fundamental, sujeito à proteção pelo estado jurisdicional e como permaneceu ou, até mesmo, tornou-se ainda mais importante com o avanço das tecnologias. (MACIEL, 2019, p.7)

Além do explicitado, o estudo que será abordado permite compreender as situações que levaram à ocorrer mudanças instituindo artigos importantes, leis, tratados e constituições ao redor do planeta e, posteriormente, retratando esse histórico no Brasil.

Nos Estados Unidos, Samuel Warren e Louis Brandeis, advogados, em 1890 elaboraram um dos mais importantes artigos referentes ao direito de privacidade, o chamado "*The Right to Privacy*" ou, na época, conhecido como direito de estar só. É neste momento que se introduz o conceito de privacidade como um direito inviolável, independente do rompimento de barreiras físicas. Na época havia um crescente meio de jornalismo em que se divulgava bisbilhotagem e notícias falsas utilizando-se de artifícios e inventos da época, como por exemplo a máquina fotográfica.

> O interesse em divulgar fatos da vida privada de forma sensacionalista e fofocas cada vez mais sendo estampadas nos jornais (Yellow Jornalism) - que ganhavam ainda mais circulação (1000% entre 1850 e 1890) –, somados ao avanço tecnológico com o uso de câmeras fotográficas portáteis, motivou os advogados a levantar a necessidade de se pensar em um direito à privacidade mais amplo e não apenas sobre meios físicos, como o sigilo da carta ou a violação de domicílio. (MACIEL, 2019, p. 7-8)

Na época, vigorava o sistema da "*common law*" na qual o direito é criado ou aperfeiçoado pelos juízes: uma decisão a ser tomada num caso depende das decisões adotadas para casos anteriores e afeta o direito a ser aplicado a casos futuros. Nesse sistema, quando não existe um precedente, os juízes possuem a autoridade para criar o direito, estabelecendo um precedente.

Os advogados diziam que apesar de a Constituição estadunidense não fazer qualquer menção à palavra "*privacy"*, seus princípios já faziam parte da "*common law"* , particularmente no que diz respeito à proteção do domicílio, tendo o desenvolvimento tecnológico apenas tornado necessário reconhecer expressamente e separadamente essa proteção sob o nome de *privacy*.

Já em 1948, há a adoção da Declaração Universal dos Direitos Humanos que estabeleceu como um direito inviolável a privacidade, mas com um viés não material. A Declaração fez essa menção em seu artigo 12, explicitado a seguir: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua

honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques."

Na Alemanha, em 1970, surgiu a primeira lei de proteção de dados pessoais e que deu impulso para o surgimento de diversas outras legislações com intuito de conceituar e dar a devida importância ao tema. Sobre os dados, Schertel (2011) diz que "dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela forte"

Já em 1980 foi aprovado o "*Data Protection Convention (Treaty 108)",* pelo Conselho da Europa e foi a primeira ferramenta legal a retratar a proteção do indivíduo contra abusos na coleta e no processamento de dados pessoais, ou seja, reconhece a privacidade dos dados pessoais no meio informático.

Na mesma década, novamente na Alemanha no ano de 1983, explica Maciel,

> A Corte Constitucional reconheceu o direito à autodeterminação informacional, declarando inconstitucional a Lei do Censo no tocante à obrigatoriedade de os cidadãos fornecerem os dados, sob pena de multa, permitindo ainda que os mesmos fossem compartilhados entre órgãos públicos federais. (MACIEL, 2019, p. 8-9)

Maciel aprofunda-se com a citação de Schertel (2011), que diz

> A sentença da Corte Constitucional, na sua formulação de um direito à autodeterminação da informação, criou o marco para a teoria da proteção de dados pessoais e para as subsequentes normas nacionais e europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados. Dessa forma, o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação.

Portanto, esta normativa criou um marco para essa teoria da proteção de dados pessoais e da privacidade, levando ao reconhecimento de inconstitucionalidade da Lei do Censo Alemão no qual obrigava a população a fornecer seus dados para que constassem em órgãos públicos federais e que fossem compartilhados entre eles. A partir disso, o titular dos dados passou a

ter direito de determinar onde e como seus dados poderiam ser utilizados, reconhecendo esse direito como fundamental.

Precisamente em 1995, foi aprovada a "*European Data Protection Directive*" (Diretiva nº 46 da União Europeia) que trouxe uma série de sugestões ou regulamentos para os países membros, já que, começaram a examinar e entender as transformações tecnológicas e introduziu novos e importantes conceitos de palavras como: processamento, dados sensíveis e consentimento. Durante muito tempo, essa Diretiva foi a que vigorou na Europa até o surgimento e aprovação do GDPR (*General Data Protection Regulation*), Lei de Proteção de Dados Europeu.

Em 2002, na União Europeia, uma diretiva mais específica sobre o regulamento da privacidade nas comunicações eletrônicas, na Europa, a "*ePrivacy"*. Maciel salienta que:

> Na União Europeia, foi aprovado o ePrivacy Directive, instrumento jurídico equivalente à Diretiva 46, ou seja, sem força obrigatória entre os países membros, porém adotada como norte legal para a implementação de proteção aos dados pessoais coletados e tratados em meio eletrônico. Atualmente a Europa discute a aprovação do Regulamento sobre ePrivacy, tornando tais disposições obrigatórias, tal como o GDPR. (MACIEL, 2019, p. 10)

Em 2013, Edward Snowden que é um analista de sistema que trabalhou em grandes organizações governamentais dos Estados Unidos, como a CIA (*Central Intelligence Agency* ou Agência Central de Inteligência) e a NSA (*National Security Agency*, aportuguesando, Agência Nacional de Segurança) ficou conhecido após fazer grandes revelações acerca de tais entidades e resultaram em grandes transformações em todo o mundo.

Antes das revelações, em 2013, viajou para Hong Kong, onde, algum tempo depois, entregou os documentos para um jornalista, o Glenn Greenwald e, para a cineasta/jornalista Laura Poitras. Esses documentos revelaram o programa de monitoramento global de ligações telefônicas e transmissões de internet dos cidadãos americanos e de alguns outros países, que se chamava PRISM. Foi acusado de espionagem, roubo e transferência de propriedade do governo por um tribunal de Virgínia, partindo para Moscou pouco tempo depois.

Tal evento foi de extrema magnitude para todos os países do planeta e passaram a pensar, adotar medidas e agilizar leis para conter situações como essas.

Em 2014, a Corte Europeia trouxe o direito ao esquecimento para os buscadores, que é o direito da pessoa de não permitir de que determinado fato de sua vida, sendo ou não verídico, seja exposto ao público em geral perante a internet.

Em 2016, o *General Data Protection Regulation* foi aprovado e entrou em vigor no ano de 2018 em 25 de maio. O GDPR não foi apenas uma sugestão, ele foi regulamentado para todos os países membros e sendo obrigatório.

CAPÍTULO II – DIREITO DIGITAL E A PRIVACIDADE NO BRASIL

2.1 HISTÓRICO

Em 1824, com a Constituição do Império, a questão da privacidade foi abordada de forma mais implícita ao se referir ao Segredo de Carta e Inviolabilidade da Casa, ou seja, são termos muito materiais e havia a necessidade de rompimento de matéria física. Havia a proteção sobre o rompimento de barreira e não o conteúdo presente.

> No entanto, naquele momento, a privacidade estava submetida a um conceito mais lastreado na propriedade, ou seja, a carta magna protegia o meio físico e não o conteúdo em si. Por isso, vê-se apenas referência ao sigilo da correspondência e à inviolabilidade do domicílio. Perceba-se que não há uma proteção da privacidade por si só, pelo seu conteúdo ou por um aspecto mais subjetivo. O que se protegia ali era a invasão, o ato de romper barreiras físicas. (MACIEL, 2019, p. 7)

No Brasil, a saga da Privacidade e Proteção aos Dados Pessoais se iniciou no ano de 1988 com a promulgação da Constituição Federal que prevê a proteção à vida privada no rol de direitos fundamentais, conforme a seguir:

> 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;
> [...]

E também, na Constituição Federal, está previsto o *Habeas Data* que é um remédio constitucional previsto no artigo 5º, inciso LXXII em que foi designado para assegurar que um cidadão tenha direito de ter acesso a dados e informações suas que estão sendo utilizados pelo governo ou por empresas privadas com caráter público, portanto, é o direito de sabermos o que o Estado sabe sobre nós. O artigo 5º, inciso LXXII expressa:

> LXXII - conceder-se-á *habeas data:*
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
>
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Já em 1990, com o Código de Defesa do Consumidor, começou a ter uma preocupação maior em relação ao Banco de Dados do Consumidor, ou seja, dados dos consumidores e o próprio consumidor passou a ter direito de obter informações de seus cadastros e dados pessoais. MACIEL (2019) alega que, embora o Código citado não tenha previsto o consentimento para coletar tais dados, exigiu que o consumidor fosse informado sobre a abertura do cadastro.

No ano de 1996, começou a vigorar a Lei de Interceptação Telefônica e Telemática que trazia o direito a intimidade da pessoa investigada e só poderia haver o rompimento dessa intimidade mediante ordem judicial.

No ano seguinte, em 1997, a Lei do Habeas Data vem prever o direito previsto na constituição na qual o cidadão tem o direito de retificar as suas informações.

Já no ano de 2002, com o novo Código Civil, reconheceu e incluiu-se a inviolabilidade da vida privada como direito da personalidade. A partir daí, o conceito de privacidade começara a ter aspectos mais relacionados ao íntimo das pessoas, ou seja, os aspectos subjetivos e não mais materialmente falando

especificamente. MACIEL (2019) fala que a relevância dessa inclusão, ainda que tardia, revela a privacidade como um direito subjetivo e não focado no direito à propriedade.

Anos mais tarde, já em 2011, começa a vigorar a Lei do Cadastro Positivo (Lei nº 12.414/11) que criou um banco de dados, com histórico de crédito, sobre o adimplemento de pessoas naturais ou jurídicas, mas precisava da aprovação prévia do consumidor. Com a aprovação da Lei Geral de Proteção de Dados, esta lei precisou de mudanças para se adequar e foi feita através da Lei Complementar nº 166 de 08 de Abril de 2019. Maciel fala sobre essa adequação, assim como a seguir:

> Assim, a partir da sua entrada em vigor, as pessoas físicas e jurídicas (cadastrados) serão inscritas automaticamente, sem necessidade de consentimento prévio, assegurando, todavia, o direito de exclusão e respeitado o princípio da finalidade. Interessante que para fornecer o histórico de crédito (conjunto de dados financeiros e de pagamentos, relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica) do cadastrado para um consulente é preciso de autorização específica do cadastrado. (MACIEL, 2019, p. 11)

No mesmo ano, vigora também a Lei de Acesso à Informação (Lei nº 12.527/11), que, segundo Maciel (2019),

> [...] trouxe a definição de informação pessoal como sendo aquela relacionada à pessoa natural identificada ou identificável, determinando aos órgãos públicos e entidade do poder público a proteção da informação sigilosa e pessoal, observando a sua “disponibilidade, autenticidade, integridade e eventual restrição de acesso. (MACIEL, 2019, p. 11)

Em 2012, a atriz Carolina Dieckmann teve o seu computador invadido por *hackers* e espalharam diversas fotos íntimas. Na época, o caso ganhou manchetes em todos os noticiários nacionais com grande notoriedade. No final deste mesmo ano, foi sancionada a Lei 12.737/12, a Lei Carolina Dieckmann que tipificou penalmente a invasão a dispositivos informáticos com o objetivo de obter vantagens ilícitas ou excluir ou adulterar informações sem autorização do titular dos dados e, ainda, havia um aumento de pena no caso de a invasão resultar a obtenção de conteúdo de natureza privada.

No ano seguinte, foi editado o Decreto do Comércio eletrônico que visava atualizar uma parte do Código do Consumidor determinando ao lojista/fornecedor utilizar de meios para a proteção de dados do consumidor e do seu meio de pagamento.

2.2 OS TIPOS DE DADOS E O MARCO CIVIL DA INTERNET

A humanidade sempre buscou facilitar a sua vida, desde os primórdios e a busca pelo fogo, pela caça mais eficaz ou com plantações. A partir de nosso surgimento fomos passando por transformações que, para alguns, podem até serem pequenas, mas que para a linha cronológica e tecnológica, só chegamos onde estamos hoje devido a tudo que aconteceu no passado, todas as experiências certas ou erradas ocasionou no ponto que chegamos agora, mais precisamente no ano de 2020 depois de Cristo.

A partir dos anos 2000 a humanidade deu um passo gigantesco comparado com qualquer outra época de nossa história. A invenção dos computadores e a internet começaram a trazer grandes transformações em todos os campos e áreas de nossa vida. Tudo que vemos ou fazemos tem tecnologia envolvida.

Agora, já em 2020, chegamos a um ponto da linha cronológica em que as tecnologias ficarão cada vez mais avançadas e de maneira mais rápida, já que, as tecnologias de agora são muito mais eficazes e encurtadoras de distâncias. O que antes cientistas do mundo inteiro precisam se deslocar de um país para outro para discussões, tudo pode ser feito virtualmente e com um “clique”. E tudo isso trouxe enormes melhorias para nossas vidas em todas as áreas possíveis, como educação, saúde, alimentação, lazer e a própria ciência.

Mesmo com tanta tecnologia envolvida e todo seu benefício, qualquer coisa criada pode vir a trazer um malefício, de certa forma, e a internet é um local considerado de extrema liberdade, para todas as raças, cores, pensamentos, gêneros e escolhas sexuais e, essa liberdade excessiva traz alguns problemas.

A partir de 2010, principalmente, houveram diversos escândalos relacionados a vazamentos de dados, vazamentos de fotos e vídeos e coisas afins. Os principais foram o caso do Edward Snowden e também da rede social

“Facebook” em que, este, houve vazamentos de milhões de dados de seus usuários.

Em jornais, revistas e na própria internet muitas vezes se ouvem falar sobre dados, mas raramente é explicado certamente. O Marco Civil da internet não traz expressamente o que seria o dado pessoal. A Lei Geral de Proteção de Dados traz que o dado pessoal é “qualquer informação relacionada à pessoa natural identificada ou identificável”. Segundo Maciel o dado pessoal:

> Dado pessoal é toda informação que pode identificar um indivíduo ainda que não diretamente. Portanto, incluem-se na referida definição, por exemplo, os números de Internet Protocol – IP, número de identificação de funcionário dentro de uma empresa, e até mesmo características físicas. Isso em razão da presença do léxico “identificável”, que amplia a definição de dados pessoais. (MACIEL, 2019, p.30)

Portanto, os dados pessoais é toda informação que de alguma forma possa nos identificar e, como citado anteriormente, podendo ser:

- Endereço;
- Nome e sobrenome;
- CPF;
- E-mail;
- Número de telefone;
- Número do PIS/PASEP;
- IMEI do celular;
- Dados utilizados para formação de perfil comportamental.

Cabe destacar aqui também que CNPJ, nome de empresa, endereço comercial, e-mail de contato entre a empresa e o consumidor e os dados anônimos não são dados pessoais.

Outro importante conceito é o dado sensível que é aquele extremamente pessoal e que possa causar algum tipo de descriminação contra o titular, são eles:

- Origem Racial ou étnica;

- Convicção religiosa;
- Opinião política;
- Dado referente à saúde ou vida sexual;
- Dado biométrico ou genético;
- Filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O Bioni ressalta muito bem o que são esses dados sensíveis e a sua importância.

> Os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação. Quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade. Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado "trivial" pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos, tal como ocorreu com a loja de departamentos que identificou quais consumidoras estariam grávidas, precisando, inclusive, o período gestacional. É possível, portanto, identificar individualidades mais sensíveis das pessoas, tais como orientação sexual, raça e estado de saúde, a partir de informações triviais. (BIONI, 2019, p. 119)

Há também outro tipo de dado que é o dado anônimo em que, Bioni e Maciel, com a ajuda da própria LGPD, retrata bem o seu significado.

> Também não é considerado dado pessoal o dado anônimo, considerado como aquele em que o indivíduo "não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Um dado pessoal pode deixar de ser alvo de proteção, caso seja anonimizado, com a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". Ainda, deixa de ser anônimo um dado, se o "processo de anonimização ao qual foi submetido for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido". MACIEL, 2019, p. 30)

> A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto. Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização. Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados, variando entre: a) supressão; b) generalização; c) randomização e; d) pseudoanonimização. (BIONI, 2019, p. 105)

Resumindo então, o dado anônimo é aquele dado que não é facilmente identificável, pode acontecer de identificar, mas tem que ser uma empresa ou um *hacker* especializado nisso e, normalmente, é ilegal.

Diante de todo o exposto, é de se notar então a grande notoriedade da revolução tecnológica que está acontecendo principalmente nas últimas décadas, trazendo diversas transformações em todos os âmbitos de nossas vidas e, devido a isso, novas leis tiveram que ser criadas regulando todo esse espaço da rede mundial de computadores.

Em uma enquete feita recentemente entre 130 pessoas, se extraiu que 100% delas utilizam a internet frequentemente e, o interessante é que a pesquisa foi feita para pessoas entre 16 a 70 anos, ou seja, a internet está aí presente dos mais novos aos mais velhos de forma expressiva.

A Lei 12.695 de 23 de abril de 2014, mais conhecida como Marco Civil da Internet trouxe um aprofundamento ainda maior sobre a questão do uso da internet, o uso de dados e a privacidade aqui no Brasil como nunca visto antes.

Quando foi aprovada e passou a vigorar, alguns usuários da internet achavam que começaria ali uma ditadura na internet, houve até mesmo diversas postagens de usuários em todas as redes sociais demonstrando enorme descontentamento e desconfiança, mas uma breve pesquisada nas ferramentas de busca mostraria a real intenção da lei e, digamos que, é uma causa bem nobre e pensando no bem estar dos usuários e sua segurança.

Naquela época achavam que o Governo começaria a impor diversas regras totalitárias de uso, acesso e até mesmo regular o tempo que as pessoas ficavam nas redes. Patrícia Peck Pinheiro preceitua que:

> O Marco Civil será importante para a Sociedade da Informação porque será um sistema complementar às leis já existentes e preencherá lacunas legislativas. A privacidade é um dos princípios a serem discutidos: da mesma forma que existe a proteção constitucional, ela também é garantida na Internet, e é essa proteção de dados pela guarda de logs nos provedores que o anteprojeto discute, e uma das questões mais importantes para a sua aprovação. (PINHEIRO, 2013, p. 44)

Já segundo Gonçalves (2017, p. 6) O Marco Civil é uma legislação cujo objetivo precípuo é o de regular as relações sociais entre os usuários de internet.

> O Marco Civil é uma legislação cujo objetivo precípuo é o de regular as relações sociais entre os usuários de internet. A internet é um fenômeno tecnológico recente que alterou a forma das relações e a percepção social de situações que, no mundo físico, seriam simples e banais. Um simples comentário, depreciativo ou não, emitido na rua, propagava-se e perdia-se naquele momento. O mesmo comentário, na internet, fixa-se indefinidamente nos programas e servidores dela, que nunca se esquecerão e registrarão aquele simples evento para sempre. (GONÇALVES, 2017, p. 6)

Uma outra parcela dos usuários a favor de uma legislação para a internet estava fervorosa em relação aos casos divulgados por Edward Snowden que trouxe mudanças significativas em legislações sobre dados e privacidade no planeta inteiro. Devido a isso, esses usuários aclamavam por uma nova legislação que os protegessem contra essa divulgação de dados e ferimento da sua privacidade contra sua vontade.

Sobre a liberdade de expressão exposta no artigo 5º, inciso IX da Constituição Federal de 1988, é de fundamental importância para reger toda a sociedade brasileira e, inclusive, é um dos princípios extremamente relevantes principalmente após a ditadura militar iniciada em 1964 em que este direito foi praticamente extinto. No Marco Civil da Internet ele já está presente no artigo 2º como um dos principais fundamentos reguladores da lei, de modo que, deveria causar uma maior confiança e respeitabilidade por parte da população, mas, no primeiro momento, não foi o que ocorreu, já que houve muita desinformação, mesmo a internet sendo um local de enorme abrangência de informações. Inclusive, grandes influenciadores da época contestavam duramente a lei.

Como estabelecido logo no artigo 1º, a lei determina o modo de atuação do Estado, União e Municípios e também estabelece deveres, direitos e princípios para o uso da internet no nosso país. Ela traz fundamentos muito relevantes em seu artigo 2º, além da liberdade de expressão, assim como a seguir:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.

O Marco Civil trouxe à tona fundamentos marcantes e inclusivos como a pluralidade e a diversidade, citados no inciso III. Já em seu inciso V é mais direcionado às empresas, estabelecendo a livre concorrência, a defesa do consumidor e a livre iniciativa como um fundamento da lei.

A Lei 12.695 então foi criada para proteger os usuários da internet em relação aos seus dados e privacidade que são visados por empresas situadas da internet e será explicado a seguir.

Tudo que fazemos na internet fica registrado, onde passamos, os *sites* que visitamos, as fotos e vídeos que tiramos e colocamos nas redes sociais, pesquisas, as nossas buscas (por exemplo por viagens ou produtos) e a nossas compras e tudo isso, em sua grande maioria, não é feita de forma onerosa para nós usuários, ou seja, não pagamos por isso. Contudo, diante do capitalismo, podemos concluir que as empresas não fazem praticamente nada de graça e, na internet, não é diferente.

Todos nós já vimos as propagandas que aparecem enquanto estamos navegando pela internet e, se parar para observas, normalmente as propagandas são de produtos relacionados à pesquisas feitas anteriormente nas plataformas e é aí que está uma forma de as empresas ganharem dinheiro com seus dados. O algoritmo do sistema dos buscadores (Google, Yahoo! e etc.) analisa todos os seus dados, inclusive nas redes sociais, como por exemplo os seus interesses por moda, esporte ou se busca um eletrodoméstico e lhe seleciona propagandas que possuem relação com suas pesquisas de forma que, as empresas pagam à esses buscadores e redes sociais para expor

essa propaganda para todos nós, e é assim que funciona o mercado dos dados.

A advogada e escritora, Patrícia Peck Pinheiro, especializada em Direito Digital resume bem o que foi dito anteriormente:

> “Não existe almoço grátis.” Como já dizia a máxima popular, o modelo de negócios da internet está totalmente baseado no uso de informações como moeda de troca, de pagamento. Conteúdo é essencial na sociedade do conhecimento, e as pessoas comuns, os usuários digitais, se tornaram produtores e consumidores simultâneos de dados de forma frenética, em tempo real, globalizada. (PINHEIRO, 2013, p. 44)

É neste momento que se faz necessária a presença de lei para regular o espaço digital no mundo da internet. O Marco Civil surgiu então com uma opção mais rápido e viável para a época para resolver o conflito que estava a aumentar cada vez mais.

Como explicita Gonçalves, dito anteriormente, um dos objetivos do Marco Civil é regular as relações entre os usuários da internet, já que, as pessoas acham que qualquer comentário que façam não poderia ser alvo de lei, mas isso não é verdade e, principalmente, após a lei 12.965/14. Mas, pelo que demonstra, parece ter sido feito às pressas, o que traz algumas falhas como a não conceituação e aplicabilidade de alguns destes conceitos.

.

> O Marco Civil deveria ser um guia de orientação para todas essas questões e outras mais, que são construídas diuturnamente com o uso das tecnologias de informação e comunicação. Este não pode ser o lugar da resposta fácil, mas um lugar legislativo para a busca do entendimento dessa transição do mundo atual para o virtual. Contudo – e essa é a maior crítica que devemos fazer ao Marco Civil da internet – como marco regulatório, esse objetivo desejado não é alcançado. Nem sequer chegou perto. O Marco Civil é uma legislação que repete muitos preceitos constitucionais sem contextualizá-los a uma ideia do que seria essa construção do ser humano no século XXI. Não a construção de um ser humano universal e igual em qualquer lugar. Partindo do conceito de que a tecnologia, por ser transformadora, equaliza a todos, o que é incorreto. Ela potencializa as diversidades, eliminando barreiras exclusivas e impedimentos para a conquista de direitos. (GONÇALVES, 2017, p. 6)

O Marco Civil traz e fala sobre direitos dos usuários na internet; os fundamentos da lei; sobre a privacidade e a liberdade de expressão;

neutralidade da rede; Proteção dos registros, dados pessoais e comunicações privadas; Procedimentos de coleta, armazenamento, guarda e tratamento de registros de conexão e de acessos a provedores; as sanções cíveis, criminais ou administrativas a ilícitos na guarda e coleta de dados; Procedimentos de guarda de registros de conexão; Vedação à guarda de registros de acesso a aplicações de internet; Procedimento de guarda dos registros de acesso a aplicações de internet; Causas de vedação da guarda de registros de acessos a aplicações de internet; Guarda de registros de acesso a aplicações de internet é optativa; Responsabilidade por danos de conteúdo gerado por terceiros; Responsabilidade subsidiária do provedor de aplicações de internet por danos causados por terceiros; Notificação aos usuários sobre a exclusão de conteúdos e procedimentos de contestação; Retirada de conteúdos pornográficos de usuários mediante notificação extrajudicial; atuação do poder público na internet e definições de planos e metas pelos poderes públicos direcionados ao desenvolvimento da internet no país.

CAPÍTULO III – A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

3.1 APRESENTAÇÃO E OBJETIVOS DA LEI

Em meio a tantos casos de vazamentos de dados e escândalos envolvendo aplicativos e redes sociais, muito se comentava sobre as mudanças que deveriam ser feitas para reger o Direito na Internet, ou seja, o Direito Digital com o objetivo principal proteger os dados dos usuários, com isso, iniciou-se em 2014 com o Marco Civil da Internet (MCI) a importante discussão e a regência sobre esse tema.

Já em 2018 e, vigorando a partir de setembro de 2020, A LGPD (Lei Geral de Proteção de Dados Pessoais) surgiu com o intuito de complementar o Marco Civil da Internet em relação ao tratamento de dados pessoais, de forma mais detalhada do que o Marco Civil da Internet fez, regulando novos direito e deveres das pessoas envolvidas nas relações virtuais.

A LGPD começa a atender as necessidades atuais de segurança e indica as figuras envolvidas, além de suas responsabilidades e penalidades. A abrangência dela é bem maior, assim como o seu impacto.

A lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais, foi aprovada em 14 de Agosto de 2018 no governo do então presidente Michel Temer. Desde lá, muito se discutiu sobre a data em que iria vir a vigorar e se deveriam prorrogar. Inicialmente, a previsão era de que começasse a vigorar já em agosto de 2020, mas, o atual presidente, Jair Bolsonaro, editou uma Medida Provisória com o intuito de postergar para maio de 2021.

A tramitou por vários meses até ser aprovada pela Câmara dos Deputados, mas ao chegar no Senado, a situação mudou. Decidiram antecipar a vigência da Lei para somente 15 dias e, com isso, o atual presidente sancionou a lei no dia 17 de Setembro de 2020, passando a vigorar no dia seguinte, dia 18 de Setembro de 2020, mas, por enquanto, foi decidido que, as medidas que seriam aplicadas pelo descumprimento da Lei começarão em agosto de 2021, até lá haverá apenas medidas educativas.

Em enquete feita recentemente com 130 pessoas, 83,1% delas não conheciam ou não conhecem a Lei Geral de Proteção de Dados e nunca ouviram falar. Outros dados indicam que cerca de 16,3% dessas pessoas frequentemente deposita seus dados em *sites*, sejam eles de compras ou nas redes sociais. 50% das pessoas ocasionalmente colocam os seus dados nos meios virtuais e isso demonstra um percentual considerável da confiança dos usuários.

De certa forma, hoje em dia, seja em redes sociais, ou em aplicativos de lojas, jogos, aplicativos de edição e outros diversos sempre temos que colocar algum tipo de dado nosso, seja pessoal, sensíveis ou de conexão. E, em sua grande maioria, esses aplicativos, *sites* e redes sociais nos pedem para ler e aceitar se quiser continuar a utilizar os serviços com os famosos “Termos de Privacidade e Uso de Dados” que, muitas vezes, passam despercebidos. Esses termos, por serem grandes, desperta certo desleixo do usuário e não é para menos, já que, são páginas e páginas de termos e, muitas vezes com muito “jurisdiquês” (termos relacionados a justiça/Direito).

Desse modo, as pessoas acabam aceitando os termos para começarem rapidamente a utilizar os serviços dos aplicativos e assim acabam

se expondo mais na rede da internet, já que não sabem o que os aplicativos estão coletando sobre você e sobre os seus “rastros” pela internet.

Um documentário muito interessante sobre esse tema é “O dilema das redes”, produzido e disponível na plataforma de *streaming* “Netflix”, que retrata e muito bem misturando entrevistas com cenas gravadas por atores para reproduzir como é feito. As entrevistas foram feitas com pessoas importantes do ramo de redes sociais e da internet, como ex-presidentes, programadores e administradores do *Google*, *Youtube*, *Facebook*, *Pinterest* e *Twitter*.

Os entrevistados contam de que forma os aplicativos utilizam seus dados e como nos influencia a utilizá-los cada vez mais, de forma que, se deixarmos de utilizar por um tempo eles até possuem táticas para chamar nossa atenção novamente.

Dizem que, apesar de ofertarem os seus serviços para nós, na maioria das vezes de forma gratuita, não quer dizer que eles vão ficar no prejuízo, eles possuem uma boa forma de ganhar dinheiro que é vender, de certa forma, seus usuários. Outras empresas pagam para eles divulgarem os seus produtos para os usuários, não qualquer produto, mas produtos que estão relacionados com o próprio internauta de modo que, eles traçam a personalidade de cada usuário seguindo o que pesquisam, o que consomem na internet e até mesmo as “curtidas” que dão em redes sociais e, desse modo, conseguem descobrir mais ainda sobre nós e passam a oferecer os produtos relacionados a nós.

Tem um ditado, de autor desconhecido, que diz: “se o serviço é de graça, você é o produto” e isso se encaixa perfeitamente aos casos explicitados.

A Lei Geral de Proteção de Dados dispõe então sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, além de que, seu objetivo é de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural, inclusive nos meios digitais, mas vale para todos os ambientes, como dito em seu artigo 1º.

A lei também traz em seu artigo 2º os seus fundamentos, que são importantíssimos para qualquer estudo relacionado a ela, e são eles:

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;

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

3.2. CONSENTIMENTO E REQUISITOS LEGAIS PARA O TRATAMENTO DE DADOS

O Marco Civil da Internet trouxe o termo consentimento à tona, mas não explicou do que se tratava explicitamente. Felizmente a lei conseguiu trazer um pouco a sua importância e como ela deveria ser aplicada, mas ainda de maneira muito amena.

Já a Lei Geral de Proteção de Dados trouxe explicitamente em seu artigo 5º, inciso XII qual o conceito de consentimento, sendo ele: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Por mais que o consentimento seja um fator fundamental e determinante para que se faça o tratamento dos dados dos usuários, com a Lei Geral de Proteção de Dados Pessoais, foram incluídos outros requisitos legais, mas antes, cumpre ressaltar e informar o conceito de tratamento de dados que também foi trazido pela mesma lei e pelo menos artigo 5º, mas no inciso X, sendo designado como:

> tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

Além do próprio consentimento existem ainda outros nove requisitos para que seja realizado o tratamento de dados e todos eles estão previstos na Lei Geral de Proteção de Dados em seu artigo 7º, sendo que, já no inciso I, o requisito é o fornecimento de consentimento pelo titular.

Uma decisão bastante interessante foi dada pela "*Commision Nationalte Informatique e Libertés*" (CNIL), que é a autoridade francesa de proteção de dados, na qual, à luz do GDPR, condenou e multou o *Google* em cinqüenta milhões de euros com base na ilegalidade de consentimento, já que, a plataforma se utilizava unicamente de um único consentimento para todos os outros serviços e sem especificar, sendo que o *Google* é dono de múltiplas plataformas como *Google Home*, *PlayStore* e *Youtube*, fazendo o consentimento se tornar não específico e não inequívoco. Além disso, a plataforma deixou algumas opções de concordância pré-validadas, de forma que também invalida o consentimento.

Maciel ressalta a importância de tais decisões para o cenário mundial, dizendo que:

> A análise de tais decisões paradigmas são fundamentais para que seja dada mais objetividade em conceitos legais que a princípio podem parecer extremamente subjetivos, ajudando na construção da doutrina sobre o tema e ajudando os agentes de tratamento e profissionais da área a adotarem a base legal do consentimento, quando necessário, de forma legítima. (MACIEL, 2019, p.36)

Cumpre ressaltar aqui que o usuário possui o direito de revogação do seu consentimento de maneira gratuita, além de que, se mudar a finalidade pela qual os dados serão tratados deverá informar ao usuário e buscar um novo consentimento.

A segunda hipótese está prevista no inciso II, no qual estabelece o tratamento de dados para o cumprimento de obrigação legal ou regulatória pelo controlador. Significa dizer que há dados, como por exemplo o famoso IP, *Internet Protocol*, que é considerado um dado pessoal, em que não possui a necessidade do consentimento, já que a lei exige que se faça. Sobre o IP, está definido pelo Marco Civil da Internet, em seu artigo 5º, inciso VIII que deverá ser tratado. Outro exemplo são dados do empregado, como o e-social, FGTS e INSS.

O CPF também se enquadra aqui no que tange a emissão de nota fiscal identificada ou para participar de programas do Governo, como a “Nota Legal”,

A terceira hipótese presente no inciso III é em relação a administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas, no qual a administração pública, segundo Maciel (2019, p. 37) poderá tratar dados pessoais dos cidadãos para fins de implementar políticas públicas, como por exemplo o Bolsa Família e o Minha casa, minha vida. Mesmo não havendo necessidade do consentimento, há a necessidade de se prestar informações claras e com o objetivo de atender finalidades públicas e de interesse público.

O quarto item, definido no inciso IV, diz por “estudos por órgão de pesquisa, garantida, sempre que possível a anonimização dos dados pessoais”. O artigo 5º, inciso XVIII da própria LGPD conceitua o que seria o órgão de pesquisa para não restar dúvida:

> órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Maciel explicita que não pode a empresa possuir fins lucrativos, como dito:

> Vedado, portanto, a uma empresa privada com fins lucrativos executar pesquisa com base em dados pessoais, exceto se para isso obtiver um consentimento, vez que a base legal será outra. Sempre que possível, o órgão deve buscar a anonimização ou pseudonimização dos dados e manter os dados em ambiente seguro e controlado, sobre seu próprio controle, sendo vedada a transferência a terceiros. (MACIEL, 2019, p. 38)

Já o inciso V, diz “quando é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados”. Não há que se ter um consentimento em casos em que se é necessários os dados para a execução de contratos, por exemplo advogados com suas procurações. Contudo, não se pode utilizar os

dados para finalidades que não sejam as estipuladas pelo interesse legítimo. Maciel, novamente, explicita e exemplifica bem o dito:

> Não seria adequado exigir de um contratante que obtivesse do titular dos dados um consentimento apartado para que pudesse utilizar seus dados pessoais na elaboração de um contrato pedido pelo próprio titular. É o caso, por exemplo, da aquisição de um imóvel. O cliente procura a construtora e preenche um cadastro para análise e possível futura contratação, desnecessário o consentimento expresso, haja vista tratar-se de um procedimento preliminar. O mesmo em relação à própria execução de um contrato. Não poderá, todavia, o controlador utilizar os mesmos dados para outras finalidades sem informar ao titular a base legal correta, como o interesse legítimo para ações de promoção comercial da contratada. (MACIEL, 2019, p. 39)

Já a sexta hipótese, inciso VI, diz “para o exercício regular de direitos em processo judicial, administrativo ou arbitral”. Nesta hipótese, não há que se ter consentimento para se utilizar os dados pessoais de uma parte para ingressar em um processo judicial, administrativo ou arbitral. Maciel (2019, p. 39) cita um exemplo bem útil ao dizer que seria inimaginável pensar que deveríamos pedir autorização a uma parte para ingressar um processo, já que, os dados são dela.

O inciso VII se refere a proteção da vida ou da incolumidade física do titular ou de terceiro. Aqui teria certo conflito se o inciso não existisse, já que teriam conflitos envolvendo a privacidade e a vida, mas o fato é que a vida prevalece sobre a privacidade do usuário. Por exemplo no caso de um acidente grave em que a vítima está abatida e precisando de atendimento, seria inimaginável pedir um consentimento neste caso.

E, neste viés de proteção a vida do ser humano, surge o inciso VIII, no qual diz “para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”, ou seja, se refere a dados coletados em procedimentos médicos, como consultas e exames.

Já a hipótese IX, diz “quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais”. Este é o caso em que se ficou mais subjetivo de todas as bases legais, mesmo com alguns critérios definidos pelo artigo 10, mas não se pode esquecer que sempre deverá estar dentro das definições de

legalidades e de transparência, além de poder ainda ter futuras definições ou orientação da Autoridade Nacional de Proteção de Dados Pessoais, que será o órgão máximo em assuntos de proteção de dados pessoais, seguindo sempre o artigo 10, que diz:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

A última hipótese, o inciso X, se refere a proteção do crédito. Tanto a Lei do Cadastro Positivo, como a LGPD, estabelecem hipóteses de não necessidade de consentimento prévio, sendo elas: (a) abrir cadastro em banco de dados com informações de adimplemento de pessoas naturais e jurídicas; (b) fazer anotações no cadastro; (c) compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de dados; (d) fornecer “a nota ou pontuação de crédito elaborada com base nas informações de adimplemento armazenadas”.

Portanto, mesmo o consentimento sendo um termo fundamental para este ramo, nem sempre é necessário que se faça presente, mas deve-se respeitar sempre a transparência, a legalidade e a finalidade dos dados.

Para o tratamento de dados pessoais sensível também há a necessidade de se haver o consentimento de forma específica e destacada, mas, como os dados pessoais normais, há formas em que não se precisa haver o consentimento, sendo elas: para o cumprimento de obrigação legal, ou regulatória pelo controlador; tratamento compartilha de dados necessários à execução pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida sempre

que possível a anonimização dos dados pessoais sensíveis; exercício regular de direitos, inclusive em contratos e processo administrativo, arbitral ou judicial; proteção da vida ou da incolumidade física do titular ou de terceiro; tutela da saúde em procedimentos realizado por profissionais da área da saúde; garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Há hipóteses em que não poderá haver o tratamento de dados pessoais sensíveis, exceto se houver consentimento, sendo elas: (a) Pela administração pública com base em contratos, convênios ou instrumentos congêneres. O tratamento compartilhado de dados sensíveis necessário a execução de políticas públicas deve sempre ser lastreado em leis ou regulamentos; (b) Dados sensíveis não devem ser considerados como necessários para execução de contratos ou procedimentos preliminares. Caso contrário, certamente seriam utilizados com viés discriminatório; (c) Com base em interesse legítimo; (d) Para proteção do crédito.

Cumpre estabelecer que, se houver finalidade econômica, mesmo com consentimento, não poderá compartilhar dados ou comunicação sobre dados relativos à saúde, exceto em casos de portabilidade e prestação de serviços de saúde. Há um projeto de lei de conversão para adicionar um parágrafo que se refere a vedação do uso de dados pessoais sensíveis para prática de seleção de riscos que é aquela em que se descobre doenças pré-existentes, ocasionando o aumento dos planos de saúde, por exemplo.

Cabe enfatizar que, em qualquer hipótese sempre deverá observar o princípio da transparência e da finalidade.

3.3. TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES E O TÉRMINO DO TRATAMENTO

As crianças e os adolescentes não poderiam ficar de fora desta abrangente lei, já que, representa uma parcela significativa em relação a uso de jogos eletrônicos e vídeos em plataformas como *Youtube*. Ganharam um artigo na LGPD, que diz:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Com a vigência da LGPD as plataformas terão que pedir o consentimento do pai ou do responsável legal da criança para que haja o tratamento do dado e, como dito “deverá ser realizado em seu melhor interesse”, ou seja, sem aproveitar da inocência das crianças e adolescentes para conseguir um outro fim específico desejado. A lei foi bem específica em relação a essa faixa etária, como pode ser analisado. Diz ainda que não deve condicionar a utilização dos programas desejados ao fornecimento das informações pessoais além das realmente necessárias, ou seja, só se pode exigir dos responsáveis dados estritamente necessários para a utilização dos jogos e plataformas, de modo que, o controlador deve encontrar um meio de se verificar o consentimento fornecido pelo responsável e considerando a tecnologia disponível no momento.

As informações sobre os tratamentos de dados perante as crianças devem ser elaboras de maneira simples, clara e acessível, já que está lidando com crianças e adolescentes, de forma que deve proporcionar a criança de que

deve pedir o consentimento para seus pais, sendo que, para ter esse consentimento, o controlador deve realizar todos os esforços necessários e possíveis para obtê-lo.

Maciel atenta que:

> Uma vez que o provedor de aplicações oferte serviços a uma criança ou adolescente ele deverá cuidar para obter o consentimento parental. Obviamente, caso o serviço não tenha esse foco, entendo que não há como exigir uma verificação prévia em ambiente online. (MACIEL, 2019, p.45)

Para houver o término do tratamento de dados pessoais, é importante se observar o artigo 15 da Lei Geral de Proteção de Dados Pessoais, que elenca quatro hipóteses, sendo elas:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada, ou seja, o tratamento alcançou a sua finalidade específica e não se faz mais necessária então deverá ser finalizado;

II - fim do período de tratamento, ocorre ao finalizar o prazo designado para o tratamento

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público, ou seja, o usuário/titular dos dados revoga o seu consentimento;

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei, portanto, a própria Agência Nacional de Proteção de Dados Pessoais poderá finalizar um tratamento se houver algum tipo de violação à lei.

Maciel (2019, p.45) cita ainda que, essas hipóteses do artigo 15 não são taxativas, já que, poderá haver também o término ou interrupção do tratamento por revogação da lei ou regulamento que dava a respectiva base legou ou por mera opção do controlador dos dados.

3.4. A PRIVACIDADE

A privacidade começa a ganhar uma importância maioria com a Declaração Universal dos Direitos Humanos da ONU (Organizações das Nações Unidas) quando trouxe em seu artigo 12, que:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

Pode extrair do artigo que, a questão da privacidade estava ainda muito ligada a aspectos materiais, como a invasão a domicílio e furto ou abertura de correspondência de outrem, já que, na época, era de extrema relevância que se discutisse de tal modo, materialmente.

Atualmente, a situação mudou. Apesar de o conceito de privacidade ter mudado um pouco, no fundo, permanece a mesma, mas seguindo os parâmetros atuais, ou seja, seguindo principalmente, fatores tecnológicos. Os fatores anteriores, como a correspondência já não perturbam tanto, a questão agora é a privacidade na internet.

A Constituição Federal de 1988 seguiu um pouco o raciocínio dos Direitos Humanos, em seu artigo 5º, estabelece em seu inciso X que “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”. Desse modo, saiu um pouco do lado expressamente material e partiu para a subjetividade, qual seja a intimidade, por exemplo.

O Marco Civil da Internet trouxe a expressão privacidade em diversos artigos, como o artigo 3º, inciso II, mas de maneira muito branda, mas trazendo-a como um dos fundamentos da lei. Para efeitos de comparação, a palavra privacidade aparece somente quatro vezes em todo o texto da lei 12.955/14. Já na Lei Geral de Proteção de Dados, que é mais extensa, aparece vinte e oito vezes e, logo em seu primeiro artigo, traz que a privacidade é um direito fundamental.

Pode-se conceituar a privacidade então como aquilo que é privado, que diz respeito a alguém em particular, a sua vida privada por exemplo a sua intimidade. A privacidade e os dados possuem um intensa conexão entre si, já que, nesse meio digital, ambas caminham juntas.

Toda a pessoa que utiliza algum programa de computador ou alguma rede social precisou passar pelos famosos e ignorados “Termos de Uso de Dados e Privacidade”. Nestes termos, estão presentes todos os seus direitos e deveres perante o que vai utilizar, mas não só isso. Estão presentes também questões como a utilização de nossos dados de alguma forma e envio de e-mails com propagandas.

Em uma enquete feita na plataforma “*Google Forms*” foi perguntado a 130 (cento e trinta) pessoas se já chegaram a ler ou costuma ler os termos de privacidade e uso de dados de redes sociais, aplicativos, e-mail e sites de compras e, a maioria esmagadora com 80,5% não chegou a ler esses importantes termos.

Um site de pesquisas chamado “*Measuring Usability”* estima que 95% das pessoas não lêem os termos de privacidade e uso de dados e isso traz grandes prejuízos para os usuários, já que, com o consentimento, que é dado ao aceitar os termos, as plataformas, programas e redes sociais podem fazer coisas que não se pode imaginar.

Para colocar isso a prova, uma empresa de games chamada “*GameStation*”, no Dia da Mentira, adicionou nos seus termos uma cláusula em que, o usuário que aceitasse, estaria aceitando entregar a sua alma ao diabo. Estima-se que 7,5 mil pessoas caíram na brincadeira. Após aceitar, a empresa enviava um e-mail a cada usuário explicando o ocorrido e dizendo a importância de se ler os termos.

Para Maciel,

> As tradicionais políticas de privacidade, costumeiramente publicadas com sem maiores reflexões, precisam se atentar à previsão do artigo 9º. São as políticas de privacidade que costumeiramente dão sustentação ao direito do titular de acesso facilitado às informações sobre o tratamento de seus dados, devendo serem disponibilizadas de forma clara, adequada e ostensivas [...]. (MACIEL, 2019, p.47)

Já, segundo Bioni,

> [...] O surgimento das políticas de privacidade é uma resposta a essa demanda regulatória. Por meio de tal técnica contratual, colher-se-ia o prescrito e necessário consentimento para legitimar toda e qualquer operação de tratamento dos dados pessoais.
> Ocorre que tal mecanismo tem se mostrado falho por inúmeras razões, seja porque ele reforça a aventada assimetria do mercado informacional, seja porque se trata de uma ferramenta que não

> capacita, efetivamente, o cidadão para exercer controle sobre as suas informações pessoais.
> Sob a primeira perspectiva, nota-se que as políticas de privacidade são, por excelência, um contrato de adesão. A massificação das relações contratuais ordinárias de consumo é também característica marcante no mercado informacional.[...]
> Essa dinâmica dos contratos de adesão assinala, sobretudo, a assimetria de forças das relações de consumo, na medida em que o seu elo mais forte fixa unilateralmente o programa contratual. Isso significa, em termos de proteção de dados pessoais, que será o fornecedor quem determinará os rumos do fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada.
> Dada essa dinâmica contratual, os usuários não têm poder de barganha para colocar em curso as suas preferências de privacidade. Isso, somado à proeminência de uma série de plataformas que condicionam a própria participação social do cidadão, acaba por tornar falaciosa a prometida esfera de controle dos dados pessoais. É nesse contexto que a lógica do "tudo" ou "nada" das políticas de privacidade acaba por mistificar a autodeterminação informacional. As políticas de privacidade, ora escoradas nessa dinâmica dos contratos de adesão, têm sido uma ferramenta inapropriada para garantir ao consumidor o controle dos seus dados pessoais.

Percebe-se que Bioni fez uma importante crítica aos termos de uso e privacidade, no qual alega que, é como se fosse um contrato de adesão, o qual cabe ao titular/usuário somente aceitar se desejar utilizar o serviço fornecido e não há a possibilidade de se negociar. Ou aceita e utiliza o serviço, ou recusa e não utiliza.

Com a Lei Geral de Proteção de Dados, as políticas de privacidade devem observar as seguintes características:

I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Entende-se então que deve informar como utilizarão os dados e a finalidade, deve-se identificar a empresar passando informações e contatos, dizer os direitos do titular e as responsabilidades dos agentes que realizarão o tratamento. Agora, com a LGPD, as empresas terão que se organizar ou sofrerão grandes multas, assim como o *Google* na Europa.

Portanto, é fundamental que a privacidade seja respeitada, mas isso não depende somente da criação de leis, depende também e muito dos

usuários observarem de que modo estão utilizando os seus dados e o que pode ser feito.

CONCLUSÃO

Anteriormente às leis que possuímos hoje, os usuários/titulares dos dados viviam a mercê das redes sociais, lojas e grandes empresas já que não havia uma regulação específica para este meio no Brasil. Finalmente após diversos e gigantescos escândalos de vazamentos de dados e utilização indevida deles os governantes de todos os países começaram a “mexer os pauzinhos”. No Brasil, 2014, surgiu o Marco Civil na Internet, que na época inovou, mas não foi abrangente e tão explícito, tendo ainda muitas falhas. Na Europa surgiu a GDPR que, pouco depois de passar a vigorar, multou uma das empresas mais poderosas do mundo, o Google, em cinquenta milhões de euros por desrespeitar e utilizar do consentimento de maneira indevida. Com a GDPR e os governantes e empresas europeus forçando os outros países a se adequarem também a política de proteção de dados pessoais e é aí que o Brasil começou a desenvolver a sua Lei Geral de Proteção de Dados Pessoais, inspirando no GDPR europeu e, de certa forma, copiando o que foi feito por lá, já que, merece todos os elogios por ser bem feito. A partir daí e, agora, com a vigência da LGPD a partir de setembro de 2020, os usuários se viram mais protegidos, seguros e confiantes.

Cumpre ressaltar que, mesmo com a nova lei sendo bem abrangente, específica e explícita em seus artigos, a proteção dos dados não dependem somente do próprio Governo e mesmo das empresas, mas depende e muito dos próprios titulares/usuários da rede mundial de computadores que devem sempre observar os seus direitos, os programas e redes sociais que utilizarão e utilizam, observam também tudo o que colocam em na internet, de forma que, não se deve expor tanto a sua vida pessoal, já que muito se descobre sobre as famosas postagens nas redes sociais.

Portanto, a questão dos dados não deve ser somente um problema do Estado, a lei agora está aí, em vigência, mas a população deve também fazer a sua parte e sempre ficar em alerta em tudo que está na rede e, nunca esquecer que sempre deverá haver transparência sobre o que fazer com os

dados dos usuários e respeitando sempre a finalidade ao qual foi dado. Um dado não é somente um dado qualquer, o dado pessoal hoje pode ser considerado o objeto mais valioso do mundo, já que, através dele pode-se conseguir quase de tudo e conhecer muito sobre uma pessoa. O dado pessoal é uma parte do ser humano, é a identificação, portanto, é privativo a nós. Não respeitá-lo seria como uma enorme ofensa e ainda mais por ser considerado, um Direito Humano Fundamental, a privacidade.

REFERÊNCIAS

ANDRADE, Marcio Roberto, **LGPD Brasil: como se adequar à Lei Geral de Proteção de Dados Pessoais**, Disponível em: < https://blog.contaazul.com/lgpd-lei-geral-protecao-dados-pessoais Acesso em: 02 mar. 2020

BIONI, Bruno Ricardo, **Por que proteção de dados pessoais importa?**, Disponível em: https://www.youtube.com/watch?v=TzI5VfvQA, Acesso em: 07 mar. 2020

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

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em: 30 set. 2020.

BRASIL, **LEI Nº 12.965**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30 set. 2020.

BRASIL. Serviço Federal de Processamento de Dados, **SERPRO e LGPD: segurança e inovação**, Disponível em: https://www.serpro.gov.br/lgpd Acesso em: 07 mar. 2020

CASTELLS, Manuel, **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**, tradução Maria Luiza X. de A. Borges – Rio de Janeiro: Zahar, 2003.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GONÇALES, Fernanda, **Lei geral de proteção aos dados e suas implicações**, Disponível em: http://www.defesanet.com.br/cyberwar/noticia/35804/Lei-geral-de-protecao-aos-dados-e-suas-implicacoes/ Acesso em: 03 mar. 2020

GONÇALVES, Victor Hugo Pereira, **Marco civil da internet comentado** – 1. ed. – São Paulo : Atlas, 2017.

MACHADO, Ralph, **Proposta adia para 2022 a vigência da Lei Geral de Proteção de Dados Pessoais**, Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/626827-proposta-adia-para-2022-a-vigencia-da-lei-geral-de-protecao-de-dados-pessoais/ Acesso em: 02 mar. 2020

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)** - 1ª Edição. Goiânia: RM Digital Education, 2019.

MARGARIDA, Silvania Mendonça Almeida, **Direito Digital**, Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/52823/direito-digital Acesso em: 07 mar. 2020

PINHEIRO, Patrícia Peck, **Direito digital** — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013.

PRODANOV, Cleber Cristiano e FREITAS, Ernani Cesar de, **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico** – 2. ed. – Novo Hamburgo: Feevale, 2013

SCHERTEL, Laura Mendes. O Direito Fundamental à proteção de dados pessoais. Revista de Direito do Consumidor, vol. 79/2011, Editora RT.

SOUZA, Carlos Affonso, **Privacidade e Proteção de Dados no Brasil**, Disponível em: https://www.youtube.com/watch?v=Zau-x-j_Uu8 Acesso em: 07 mar. 2020

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 Marcelo Carneiro Guimarães
do Curso de Direito, matrícula 2016.2.0001.02070,
telefone: 62 99910-2382 e-mail marcelocarneiroguimaraes@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 Direito Digital: A nova era dos Dados e da Privacidade, 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, 05 de Dezembro de 2020.

Assinatura do(s) autor(es): Marcelo Carneiro Guimarães

Nome completo do autor: Marcelo Carneiro Guimarães

Assinatura do professor-orientador: 2 1 A

Nome completo do professor-orientador: Nivaldo dos Santos

PONTIFICIA UNIVERSIDADE CATÓLICA DE GOIAS
Pró-Reitoria de Graduação
Escola de Direito e Relações Internacionais
Núcleo de Prática Jurídica
Coordenação Adjunta de Trabalho de Curso
Trabalho de Curso II – JUR 1052

ATA PARA EXAME DE DEFESA

No dia 21 do mês de novembro do ano de 2020, às 11:15 horas, na sala *Teams Microsoft* da PUC Goiás, ambiente virtual da Escola de Direito e Relações Internacionais da PUC GOIÁS, reuniram-se, o/a aluno/a orientando/a MARCELO CARNEIRO GUIMARÃES, o/a Professor/a Orientador/a Prof. Nivaldo dos Santos e o/a Convidado/a Prof./a MILLENE BALDY DE S BRAGA GIFFORD, para a realização da Banca do EXAME DE DEFESA TRABALHO DE CURSO, com base no Regulamento Trabalhos de Conclusão do Curso de Direito da PUC Goiás, com o título: DIREITO DIGITAL: A NOVA ERA DOS DADOS E DA PRIVACIDADE

AVALIAÇÃO:	A nota da DEFESA do Trabalho de Curso II é composta por:	NOTAS
0 a 10	Trabalho escrito	10
0 a 10	Exposição oral 10	10
0 a 10	Questionamentos da Banca Examinadora 10	10
0 a 10	NOTA FINAL (N2):Média aritmética 10	10

Ocorrências: _____

Assinaturas:
Professor/a Orientador/a: _____

Convidado para Banca de Defesa: Millene Braga

Aluno/a Orientando/a: Marcelo Carneiro Guimarães