Revista Ibero- Americana de Humanidades, Ciências e Educação- REASE

doi.org/10.51891/rease.v10i5.14142

DESAFIOS DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS: UMA ANÁLISE DAS DEFICIÊNCIAS ATUAIS

CHALLENGES OF BRAZILIAN LEGISLATION IN RELATION TO CYBER CRIMES: AN ANALYSIS OF CURRENT DEFICIENCIES

Matheus Barroso Borges[1]
Thyara Gonçalves Novais[2]

RESUMO: Em razão da grande incidência de crimes cibernéticos e de tantos problemas causados por conta do vazamento de dados, informações e arquivos pessoais, lançados e veiculados sem nenhum controle ou cuidado na internet, surgiu nesse cenário a Lei Geral de Proteção de Dados (LGPD). A nova normativa trouxe grandes modificações para as relações entre os provedores de aplicação de internet, abarcando os mais diversos aspectos e perspectivas no que se refere às ferramentas de proteção dos dados pessoais com o intuito de evitar os crimes cibernéticos. Diante disso, questiona-se: A LGPD e as demais legislações existentes no sentido de coibir a prática de crimes cibernéticos, são capazes de garantir o direito à privacidade e atuar no combate às condutas criminosas que circundam a internet?) Esse estudo possui grande relevância para a sociedade em geral, pois trata-se de uma problemática da qual várias pessoas já foram vítimas ao se verem completamente expostas por conta da vulnerabilidade diante do grande avanço e crescimento tecnológico. O objetivo do presente trabalho é avaliar o contexto evolutivo das normas diante dos crimes cibernéticos sob a égide do grau de eficácia da Lei Geral de Proteção de Dados, abordar a evolução histórica da internet, realizar um aprofundado estudo acerca das legislações existentes nesse âmbito e traçar os pontos relevantes quanto às ferramentas de proteção disponíveis através da legislação, bem como suas fraquezas. A metodologia aqui aplicada trata-se de uma revisão bibliográfica de caráter qualitativo. Portanto, embora a LGPD e outras legislações relacionadas sejam importantes para proteger a privacidade e coibir os crimes cibernéticos, é necessário um esforço contínuo de atualização das leis, investimento em capacitação das autoridades, cooperação internacional e conscientização pública para enfrentar os desafios em constante mudança do mundo digital.

Palavras-chave: Crimes cibernéticos. Proteção de Dados. Vazamentos. Legislações.

[1] Estudante de Direto da Faculdade de Ilhéus/Madre Thaís.
[2] Mestre em Direito Faculdade de Guanambi/BA.

ABSTRACT: Due to the high incidence of cybercrimes and so many problems caused by the leakage of data, information and personal files, released and transmitted without any control or care on the internet, the General Data Protection Law (LGPD) emerged in this scenario. The new regulations brought major changes to relationships between internet application providers, covering the most diverse aspects and perspectives regarding personal data protection tools with the aim of preventing cybercrimes. In view of this, the question arises: Are the LGPD and other existing legislation aimed at curbing the practice of cybercrimes capable of guaranteeing the right to privacy and acting in the fight against criminal conduct that surrounds the internet?) This study is of great relevance for society in general, as it is a problem that many people have already fallen victim to as they find themselves completely exposed due to their vulnerability in the face of great technological advancement and growth. The objective of this work is to evaluate the evolutionary context of norms in the face of cybercrimes under the auspices of the degree of effectiveness of the General Data Protection Law, address the historical evolution of the internet, carry out an in-depth study of the existing legislation in this area and outline the relevant points regarding the protection tools available through legislation, as well as their weaknesses. The methodology applied here is a qualitative literature review. Therefore, although the LGPD and other related legislation are important to protect privacy and curb cybercrimes, a continuous effort to update laws, invest in capacity building of authorities, international cooperation and public awareness is necessary to face the ever-changing challenges of the Digital world.

Keywords: Cyber crimes. Data Protection. Leaks. Legislations.

1 INTRODUÇÃO

Todos os avanços tecnológicos dos últimos anos têm moldado a sociedade de uma forma jamais vista antes. A internet, foi uma novidade que trouxe características singulares para o comportamento humano e é facilmente perceptível o quanto esta se encontra presente no cotidiano das pessoas na atualidade, fazendo-se presente nas mais variadas atividades que vão do trabalho à vida pessoal.

É impossível não tentar fazer um balanço da infinidade de informações e dados pessoais que essa ferramenta carrega, material esse, muitas vezes de conteúdo sensível, o que faz com que se desencadeia uma grande preocupação em torno das formas de mantê-los sob proteção. Atualmente, as informações pessoais circulam pelos mais variados veículos, quais sejam: redes sociais, empresas privadas e públicas, entre outras. Apesar desta grande circulação de dados, pouco se sabe a respeito de como essas informações são tratadas. Qual o real nível de segurança e de controle que estes possuem sobre elas? Não é possível saber

com propriedade, por parte do particular, o nível de segurança que essas empresas e órgãos possuem sobre as informações que têm em mãos.

O direito fundamental à privacidade sempre esteve em grande evidência em decorrência de sua conexão com o mundo digital, porém, nos últimos anos esse fluxo de informações atingiu parâmetros nunca vistos na história do mundo fazendo com que a segurança do que era privado ao indivíduo ficasse ameaçada. Depois de tantos problemas causados por conta do vazamento de dados, informações e arquivos pessoais, lançados e veiculados sem nenhum controle ou cuidado na internet surge na legislação brasileira a Lei Geral de Proteção de Dados nº 13.709.

A nova normativa trouxe grandes modificações para as relações entre os provedores de aplicação de internet, abarcando os mais diversos aspectos e perspectivas no que se refere às ferramentas de proteção dos dados pessoais com o intuito de evitar os crimes cibernéticos. Diante disso, questiona-se: A LGPD e as demais legislações existentes, no sentido de coibir a prática de crimes cibernéticos, são capazes de garantir o direito a privacidade e tutelar todas as situações criminosas que circundam a internet? A LGPD e as demais legislações existentes no sentido de coibir a prática de crimes cibernéticos, são capazes de garantir o direito à privacidade e atuar no combate às condutas criminosas que circundam a internet?

Esse estudo possui grande relevância para a sociedade em geral, pois trata-se de uma problemática da qual várias pessoas já foram vítimas ao se verem completamente expostas por conta da vulnerabilidade diante do grande avanço e crescimento tecnológico. Ademais, cita-se ainda o fato de que a Rede Mundial de Computadores assume uma posição de extremo destaque no cenário global, sendo a casa das diversas empresas mais valiosas do planeta, um elemento fundamental à rotina da maioria dos habitantes do país, impulsionadora de revoluções democráticas e maior responsável pela globalização e difusão de informações. Sendo assim, é extremamente importante discorrer sobre o direito fundamental à privacidade na internet, pois é essencial que se conheça a tutela jurisdicional para que esta seja prestada da melhor forma possível.

O objetivo do presente trabalho é avaliar o contexto evolutivo das normas diante dos crimes cibernéticos sob a égide do grau de eficácia da Lei Geral de Proteção de Dados, abordar a evolução histórica da internet, realizar um aprofundado estudo acerca das legislações existentes nesse âmbito e traçar os pontos relevantes quanto às ferramentas de proteção disponíveis através da legislação, bem como suas fraquezas.

A metodologia aqui aplicada trata-se de uma revisão bibliográfica de caráter qualitativo segundo (Lakatos e Marconi, 1991; Gil, 2002; Minayo, 2002). Foram utilizadas publicações científicas indexadas em bases de dados como o Google Acadêmico e demais plataformas digitais de conteúdos jurídicos, bem como, foi feito uso de toda a doutrina e legislações vigentes pertinentes ao tema. Por meio da seleção, classificação e documentação de todo o material pertinente disponível na internet tornou-se possível responder aos quesitos estabelecidos para esse estudo.

2 REVISÃO DE LITERATURA

2.1 Evolução histórica

No contexto da Guerra Fria, que vigorou no mundo entre 1945 e 1991, envolvendo as duas superpotências político-econômicas da época, quais sejam Estados Unidos da América e União Soviética, a busca por inovações tecnológicas com potencial de uso militar era incessante, e desta forma foi criada a ARPA (*Advanced Research Projects Agency*), uma agência federal norte-americana focada no desenvolvimento de projetos militares. Em 1962, Joseph Carl Robnett Licklider foi contratado pela ARPA, sendo o primeiro a utilizar o termo "Rede Intergaláctica de Computadores" significando uma vasta comunidade interligada em tempo real e o responsável por inúmeros avanços na pesquisa que resultaria na internet como conhecemos hoje (Naughton, 2000, p. 76).

No final dos anos 1980, um homem chamado Tim Berners-Lee criou uma nova rede, transformando o foco praticamente exclusivo de envio de e-mails verificado à época para em uma nova forma de estruturar, armazenar e acessar informação. Ele chamou esta rede de World Wide Web (Rede Mundial de Computadores) (Naughton, 2000, p. 213). Desta forma, a Rede Mundial de Computadores como conhecemos conectou todos os usuários em uma grande plataforma neutra, com espaços vazios praticamente ilimitados, prontos para serem preenchidos de informações que poderiam ser armazenadas, acessadas, modificadas ou alteradas, fornecidas por qualquer um que tivesse um ponto de acesso conectado à internet.

Bossoi (2019, p. 3/4), assevera:

> Em 1999, o filósofo Michel Serres esteve em São Paulo para uma série de conferências no quadro do 1º Congresso Internacional de Desenvolvimento Humano. Em meio ao amplíssimo espectro de temas, versou principalmente sobre as transformações em curso no mundo contemporâneo, que vêm sendo impulsionadas, sobretudo, pelas novas tecnologias de comunicação desde 1965-70,

> numa sociedade em que a comunicação assumiu uma importância jamais alcançada, uma vez que os meios técnicos de comunicação se desenvolveram de uma forma exponencial.

A implantação, de fato, da internet no cenário brasileiro só ocorreu depois que foi criado no ano de 1989 pelo Ministério da Ciência e Tecnologia (MCT), o Projeto da Rede Nacional de Pesquisa – RNP. Isso se deu graças ao apoio de várias instituições governamentais de diversos Estados, dentre as quais se encontrava a Fundação de Amparo à Pesquisa do Estado de São Paulo. Todavia, somente depois de 1995 é que a rede brasileira foi além dos muros de academias e centos de pesquisa, estendendo-se assim, a usuários individuais e empresas (Silva e Silva, 2018).

Com o advento da internet, foram verificadas mudanças em todos os âmbitos da sociedade, não só brasileira, mas mundial. Provedores de pesquisa começaram a existir, facilitando a busca por sites de conteúdo educacional e modificando o processo de aprendizado daqueles que buscavam informação; não era mais preciso ir até uma biblioteca e ficar horas tentando localizar um trecho específico de um livro, bastavam apenas alguns 10 minutos de pesquisa com as palavras-chave relacionadas ao tema. Houve também mudanças nos sistemas bancários, com a possibilidade de pagamentos online e contas inteiramente digitais; o mercado de jogos eletrônicos, que já vinha em ascensão, não tardou em obter um faturamento maior do que a consolidada Hollywood; as redes sociais surgiram, trazendo um engajamento entre os usuários de forma a propagar diversos tipos de conteúdo e promovendo a socialização digital em um processo de globalização interno e externo.

> O modelo de produção capitalista favorece, e até mesmo incentiva a acumulação de bens e a informatização crescente das várias atividades desenvolvidas individualmente ou coletivamente na sociedade, colocando novos instrumentos, plataformas e produtos nas mãos dos internautas, fazendo surgir, a cada dia, com a coleta, guarda e processamento dos dados de forma indiscriminada, novas modalidades de lesões aos mais variados bens e interesses, dentre eles os dados pessoais concentrados nos diversos bancos de dados. Em razão desta nova realidade encontramos um movimento mundial relativo à segurança jurídica e aos marcos regulatórios para a proteção desses dados, acabando por expor o atual panorama do Brasil, com uma proteção dispersa, incipiente, não específica, cenário este diverso do internacional (Bossoi, 2019, p. 1).

O crescimento da internet aconteceu de forma exponencial e em um período muito curto de tempo. Seu aspecto neutro, caótico e desvinculado de qualquer regulação estatal assustou, de certa forma, o direito, não apenas brasileiro, mas mundial. Neste mesmo teor, da globalização decorrente do surgimento da internet e das mudanças sociais trazidas por

ela, o direito vem, incessantemente, se adaptando e encontrando as melhores formas de lidar com as novas demandas e fatos jurídicos advindos dessa revolução tecnológica.

Essa tecnologia, que chega até mesmo a ser considerada como potente e onipresente para Bossoi (2019), propõe incontáveis questões e problemáticas, não deixando de exigir respostas do jurista, dentre as quais se encontra a defesa e proteção desses dados lançados na rede e a justificativa para todo esse paradigma jurídica que envolve a proteção da pessoa sob uma perspectiva de valor fundamental.

2.2 Lei Carolina Dieckmann (Art. 154-A e 154-B do Código Penal)

A Lei n. 12.737, de 30 de novembro de 2012, também conhecida como Lei Carolina Dieckmann, complementa o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), e foi a primeira legislação brasileira a tratar sobre crimes informáticos. O nome dado à lei tem sua origem devido a invasões cibernéticas (*hacking*) em um dispositivo de propriedade da atriz e apresentadora homônima, ocorrido em maio de 2012.

À época de sua publicação a lei ganhou grande notoriedade porque, antes mesmo de ser publicada e sancionada, a mesma passou a ser reconhecida como a "Lei Carolina Dieckmann". Tudo isso se deu devido a repercussão do caso em que a atriz teve seu computador invadido e seus arquivos pessoais furtados onde até mesmo fotos íntimas foram veiculadas na internet e rapidamente se espalharam nas redes. O mundo contemporâneo exige que o direito acompanhe suas evoluções, principalmente quando envolve a informática que abre inúmeros caminhos para a prática de atos ilícitos, onde muitas vezes o criminoso não tem rosto

De acordo com Quintino (2013), os simples mecanismos de proteção dos sistemas de computadores já não dão conta de evitar a invasão de máquinas digitais em decorrência disso foi necessário ao direito ganhar um espaço também no campo cibernético para que pudesse criar barreiras protetivas que visassem a segurança e fosse capaz de garantir a privacidade que os indivíduos possuem o direito constitucional de gozar livremente. Nessa perspectiva, a Lei 12.737 de 2012 entrou em vigor alterando o Código Penal Brasileiro fazendo com que este ganhasse um acréscimo de duas novas disposições (artigos 154-A e 154-B) a fim de inibir a prática de crimes cibernéticos e, também punir aqueles que transgredirem a medida

O Código Penal traz no caput que seu artigo 154-A, a seguinte previsão:

> 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 [...] (Brasil, 2012).

Dessa forma, extrai-se do diploma legal a finalidade de condenar a prática de invasão da privacidade digital alheia, conduta essa em que o agente dribla mecanismos de segurança de máquinas digitais adulterando, propagando ou fazendo uso indevido de informações que não lhe pertencem, instalando vulnerabilidades com o intuito de obter vantagem ilícita.

A partir disso, observa Quintino (2013) que há a necessidade de que exista algum mecanismo de segurança no próprio sistema do aparelho a ser burlado, uma vez que a ocorrência do crime descrito na legislação acima está condicionado a isso para que seja considerada a violação indevida. Mediante esse fato, percebe-se que a invasão de quaisquer dispositivos informáticos que ocorrerem sem que haja a violação de algum mecanismo de segurança, seria, inevitavelmente, configurado enquanto fato atípico.

Nesse sentido, Ferreira (2019, p. 97) traz uma crítica à legislação afirmando que: "Não parece razoável!". Isso, devido ao fato do art. 154-A traz em seu parágrafo 2º que somente haverá crime "mediante violação indevida de mecanismo de segurança", e sem isso não existe a configuração do delito.

Por conta disso, fazia-se extremamente necessário que os aparelhos fossem protegidos com antivírus, senhas, firewall, bem como outras formas de defesas digitais. No entanto, nada disso chegou nem perto de ser o suficiente para que ocorrências similares e até mesmo piores continuassem a ocorrer na rede cibernética, dando a impressão, por muitas vezes, que a internet era uma "terra sem lei", fazendo extremamente necessário que outras medidas fossem tomadas e que novas leis advirem para suprir essa legislação que foi tão importante no que se relaciona ao mundo digital, mas que não foi o suficiente.

Importa frisar, que essa lei que trata do crime de invasão de dispositivo informativo (nomeada de Lei Carolina Dieckmann, em referência à atriz brasileira que teve fotos íntimas vazadas na internet) recebeu 4 (quatro) alterações para o art. 154-A do CP por meio da Lei nº 14.155, de maio de 2021. Primeiramente, houve uma ampliação da incidência de tipo penal, através de uma modificação no caput, foi majorada a pena do crime previsto no caput e houve também a majoração dos limites da causa de aumento de pena previsto no § 2º e foi aumentada a pena da qualificadora prevista no § 3º.

2.3 Marco Civil da Internet

A partir de uma publicação feita em 24 de março de 2014, o site World Wide Web Foundation tornou público um pronunciamento de Sir Tim Berners-Lee, considerado como o inventor da internet na forma que conhecemos atualmente, demonstrando demasiado entusiasmo com a Lei n. 12.965, de 23 de abril de 2014 conhecida como o "Marco Civil da Internet" (Ponticelli, 2018).

Na mesma manifestação de ideias de Sir Tim Berners-Lee, no que se refere a legislação traz uma reflexão de que a internet deveria ser uma rede aberta, neutra e descentralizada, de forma que os usuários representam uma espécie de motor para a colaboração e inovação. Neste seguimento, o Marco Civil da Internet se preocupou em abordar diversos direitos, deveres e garantias no que tange à rede mundial de computadores, com foco exploratório nas novas perspectivas acerca do direito fundamental à privacidade online (Ponticelli, 2018)

Nesse sentido, é o que informa Teixeira (2016, p. 84) apud Ponticelli (2018, p. 31:

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computador. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet.

O Marco Civil da Internet trouxe em seu artigo 3º, incisos I e II, a proteção à privacidade e aos dados pessoais enquanto princípios essenciais para disciplinarem o uso da internet no Brasil. Sendo assim, o ambiente digital, bem como as atividades e atores nele envolvidos deveriam ser preparados tendo como orientação ou diretriz a proteção de dados, ainda que houvesse previsão de uma lei específica para sua disciplina.

É importante ressaltar que no tocante às decisões judiciais, tomadas de decisão e também modelos de negócio esses princípios são basilares e norteadores no sentido possibilitar uma melhor interpretação, aplicação da norma e adequação legal, motivo pelo qual, devem servir como parâmetro também para as escolhas políticas, econômicas, jurídicas e sociais no que se refere ao uso da internet no Brasil, contribuindo para a adequação à Lei Geral de Proteção de Dados (Klee e Pereira Neto, 2019).

> O Marco Civil da internet segue a ideia de que o consentimento estaria na base das relações que envolvam a coleta, tratamento, armazenamento e processamento de dados pessoais. O modelo do consentimento, apesar de bem intencionado e fundamentado no exercício da autonomia do titular dos dados, não fica livre de questionamentos. Muitos deles envolvem a eficácia do pedido de consentimento a cada titular de dados tratados, em um contexto em que as interações virtuais geram não apenas uma maior quantidade de dados, mas também aumentam a velocidade (em alguns casos, praticamente instantânea) e potencialidade de usos, trocas e compartilhamentos (Brandão, 2019, p. 40).

Todas as transformações que resultaram do livre uso da internet ainda são capazes de gerar certa perplexidade nas pessoas, principalmente porque muitas delas ainda não sabem exatamente como se comportar no que Filho (2016) chama de "terceira esfera de ação humana". Com o avanço da Rede Mundial de Computadores os mais variados crimes também começaram a ocorrer nesse campo denominado ciberespaço, passando-se uma ideia que a internet deveria ser uma "terra sem lei", onde tudo poderia ser permitido diante da impossibilidade de descobrir a verdadeira identidade dos criminosos. Percebeu-se então a grande deficiência do Direito Penal tradicional no tocante ao combate de crimes virtuais, sendo as legislações existentes afetadas por essa nova realidade tecnológica, especialmente porque o Direito Penal é completamente ligado a questão da soberania nacional, mas a internet, por sua vez, não conhece Estados por se tratar de uma verdadeira aldeia global (Tomasevicius Filho, 2016).

O Marco Civil da Internet veio para trazer esperança, pois foi a primeira legislação a tratar mais especificamente dos crimes virtuais. Seu texto deu uma atenção especial ao direito à privacidade e sob o ponto de vista do legislador tratou da responsabilidade civil dos provedores de internet em razão da ofensa aos direitos da personalidade das pessoas que envolvem sua honra, imagem, vida privada e intimidade. O art.18 contemplou a irresponsabilidade civil do provedor de acesso diante dos danos causados por seus usuários. Em contrapartida, o art.19 trouxe regulamentação para a responsabilidade civil dos provedores de conteúdo como os armazenadores de arquivos fotográficos e musicais, e também páginas da internet, blogs, entre outros. Dessa forma foi estabelecida a responsabilidade subsidiária entre os usuários praticantes de atos ilícitos civis e provedores de conteúdo (Tomasevicius Filho, 2016).

O Marco Civil da Internet disciplinou a forma de atuar do Poder Público no que se refere ao desenvolvimento da internet no cenário brasileiro. Assim sendo, nos artigos 24 e 25 ficaram previstos os mecanismos de governança multiparticipativa, que envolvem o

governo, a sociedade civil, as empresas e comunidade acadêmica, bem como ficou estabelecido a racionalização da gestão, expansão e uso da internet no Brasil, especialmente, na implementação de serviços de governo eletrônico e também serviços públicos, bem como a adoção preferencial de tecnologias, padrões e formatos abertos e livres, informações públicas na internet, a publicidade de dados e, principalmente, o estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados neste país. Os artigos 26 e 27, por sua vez, vieram para tratar do uso da internet enquanto instrumento no exercício da cidadania, do desenvolvimento tecnológico e promoção da cultura, possibilitando a inclusão digital, a redução de desigualdades sociais e, também o fomento de produção e circulação de conteúdo nacional (Tomasevicius Filho, 2016).

A verdade é que o MCI trouxe importantes mudanças para o campo legislativo no que se refere à Rede Mundial de Computadores, e apesar de sua efetividade ampla ser questionada devido às lacunas, todos os avanços que advieram nesse sentido decorreram dela.

> Fato é que muitos dos problemas relacionados à Internet podem hoje ser resolvidos pelo Marco Civil da Internet, ou pela legislação esparsa existente, contudo ainda remanesce uma certa insegurança por parte dos usuários, ante a grande facilidade de violação da privacidade. A defasagem entre a realidade que vivemos e a legislação pode ser perigosa, pois esta não foi concebida para abranger a todas as nuances e especificidades do ambiente da Internet, que é ambiente bastante diferente do real (Almeida e Cunha, 2018, pág. 9).

Entretanto, Tomasevicius Filho (2016) ressalta que muito embora o Marco Civil da Internet tenha sido imensamente comemorado e celebrado por ser a primeira legislação mundial a disciplinar os direitos e deveres dos usuários da rede, não foram perceptíveis mudanças substanciais já que está pouco acrescentou à legislação vigente. Percebe-se que foi criada uma expectativa errônea acerca dessa lei de que outras normas como as contidas na Constituição Federal, Código Civil, Código Penal, entre outros, não teriam aplicação nas relações jurídicas estabelecidas na internet, o que passa muito longe da verdadeira realidade dos fatos.

> Apesar de não entrar em especificidades no que se refere à proteção da privacidade e dos dados pessoais, o Marco Civil da Internet define princípios, diretrizes e direitos pertinentes a esses temas. Dessa forma, ainda com a vigência da Lei Geral de Proteção de Dados (LGPD) prevista para agosto de 2020, a Lei nº 12.965/2014 continua a fazer parte do arcabouço normativo brasileiro que se aplica às interfaces digitais. Aliás, é importante destacar que não apenas à internet ou às tecnologias que se baseiam no Big Data será aplicável a Lei Geral de Proteção de Dados, mas também aos dados coletados e utilizados em outros contextos, inclusive analógicos. Os dados relacionados à internet, por sua vez, também incluem as disposições

> normativas do Marco Civil da Internet, bem como de seu decreto regulamentador e ainda de outros instrumentos normativos vigentes no Brasil (Klee e Pereira Neto, 2017, p. 37).

Dessa forma, entende-se que se faz necessário uma verdadeira ação conjunta no combate aos crimes cibernéticos, uma vez que uma legislação complementa a outra a fim de suprir o máximo de lacunas possíveis para que se alcance a maior finalidade nesse sentido, que é evitar que o mau uso da internet continue a fazer vítimas.

2.4 Lei Geral de Proteção de Dados

A proteção de dados pessoais foi inicialmente admitida no ordenamento jurídico brasileiro como um princípio relativo ao uso da Internet, consagrado pelo Marco Civil da Internet (Lei nº 12.965). O Marco Civil da Internet, em vigor desde 23 de junho de 2014, ficou reconhecido como uma legislação pioneira em todo o mundo, pois foi a primeira a regular direitos e deveres dos usuários diante da Rede Mundial de Computadores e estabeleceu, em seu artigo 3º, inciso III, a criação de lei específica para a proteção dos dados pessoais, o que só veio a ocorrer em 10 de julho de 2018, quando a LGPD foi finalmente aprovada (Vieira, 2019).

A LGPD discorre sobre o tratamento de dados pessoais, abrangendo também os meios digitais, seja por pessoa natural ou jurídica de direito público ou privado, visando a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. As normas dispostas na LGPD são de interesse nacional, devendo ser constantemente observadas pela União, pelos Estados, pelo Distrito Federal e Municípios (Klee e Pereira Neto, 2019).

> A LGPD regulamenta o uso, a proteção e a transferência de dados pessoais em território nacional, em âmbito público ou privado. O seu objetivo é garantir um efetivo controle por parte dos titulares sobre suas informações pessoais. A LGPD, entre outras disposições, exige consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados (Vieira, 2019, p.10).

A necessidade de utilização cada vez mais ampla de dados pessoais para as mais diversas atividades que envolvem a identificação, autorização, classificação, entre tantas outras, que chegam por muitas vezes fazem o papel da própria pessoa, não sendo preciso estar presente fisicamente pois se configuram como os elementos essenciais para que os indivíduos transitam nos corredores do que hoje é comumente chamada e denominada de Sociedade da Informação (Bossoi, 2019).

A LGPD, de acordo com o art. 5º, inciso I define como dados pessoais toda e qualquer informação que esteja relacionada a pessoa natural que a torne identificada ou identificável (Brasil, 2018). O mesmo dispositivo de lei define ainda o que é dado pessoal sensível, banco de dados, dado pessoal anonimizado e anonimização de dados (Vieira, 2019).

Os dados pessoais se definem por todas aquelas informações que tornam possível a identificação da pessoa a quem estas se referem. Sua proteção tem como objeto o direito à intimidade e o direito à identidade pessoal. O primeiro pauta-se na autodeterminação informativa, o segundo, por sua vez, busca o impedimento da alteração da identidade pessoal através de informações errôneas, inexatas e até mesmo incompletas. Conforme destacam Klee e Pereira Neto (2019) e Ferreira (2019) a LGPD se traduz na evolução da autodeterminação informativa em benefício do direito à proteção dos dados pessoais, e, se bem aplicada, virá a proteger a privacidade dos usuários e de seus dados pessoais de maneira que seja mais adequada e segura.

> Mendes e Doneda asseveram que a LGPD objetiva a proteção dos dados do cidadão, independentemente de quem realiza o seu tratamento, aplicando-se tanto ao setor privado como ao setor público (empresas e Governo), sem distinção de tratamento de dados, inclusive pela Internet. Blum e Schuch são categóricos: a importância da proteção dos dados pessoais está no fato de que a informação passou a ser um bem extremamente valorizado na sociedade e no mercado ("a informação é o ativo mais valioso da atual sociedade, servindo de instrumento de conhecimento, poder e controle"), porque a partir dela é possível traçar perfis de comportamento, tais como econômico, familiar, político, profissional e de consumo e fundamentar a tomada de decisões econômicas, políticas e sociais (Klee e Pereira Neto, 2019, pág. 15).

Nesse sentido, nota-se que o objetivo principal da LGPD é a proteção dos dados pessoais dos indivíduos, visando a preservação de sua personalidade. Em última *ratio*, a LGPD busca proteger os direitos de personalidade dos indivíduos e das garantias constitucionais decorrentes (Klee e Pereira Neto, 2019).

Apesar de inúmeros avanços terem sido verificados no que concerne ao direito fundamental à privacidade no âmbito da Rede Mundial de Computadores ao longo dos últimos tempos, principalmente aqueles que advieram recentemente por intermédio da Lei Geral de Proteção de Dados e especialmente com relação à proteção de possíveis abusos comerciais cometidos por empresas que realizam o tratamento de dados, como quando existe a necessidade de fornecimento de um consentimento específico acerca de uma cláusula destacada para as hipóteses de tratamento, a legislação trouxe alguns institutos que podem ser prejudiciais ao titular dos dados diante desse tratamento realizado quando objetivadas a

segurança pública e/ou defesa nacional, uma vez que tais conceitos se traduzem em uma vasta amplitude hermenêutica dando margem para certos tipos de arbitrariedade que podem acabar prejudicando a segurança jurídica e a privacidade dos indivíduos (Ponticelli, 2018).

Mesmo que a LGPD traga inúmeras inovações legislativas no que se refere à proteção dos dados pessoais, o Marco Civil da Internet ainda deverá ser compreendido como complementar a ela. Isso ocorre porque ambas as leis se centram na perspectiva do titular dos dados pessoais ou, no caso da Lei 12.965, que cuida dos usuários da internet. Identifica-se que, diante dos dois textos legais, encontram-se elementos que abraçam um outro fundamento em comum: a autodeterminação informativa. E a cada dia que passa esse conceito vai ganhando mais notoriedade em meio às discussões europeias acerca da proteção de dados, levando em consideração que a lógica da economia com base em dados gira o tempo todo em torno de informações que são construídas e desenvolvidas sobre e a partir de pessoas (Bossoi, 2019).

2.5 A vulnerabilidade da proteção de dados e a velocidade da propagação de informações na rede

O veloz mundo contemporâneo fornece poucos valores essenciais à vida em equilíbrio, enquanto novas "necessidades" são artificialmente criadas a cada dia, imbuídas da falsa promessa de bem-estar. A cultura dominante em centros urbanos incentiva a pressa, a praticidade e o consumo imediato, que, supostamente, aplicariam a angústia e a ausência de sentido para a existência. Atualmente, grande parte dos relacionamentos ocorre pela oferta dos meios ágeis de comunicação, que favorecem a interface superficial com muitas pessoas (redes de relacionamento via Internet), incitando relações descartáveis. A tecnologia da comunicação está presente em expressiva porção da vida cotidiana e substitui a própria necessidade do "outro" para o indivíduo interagir, comunicar, ensinar e aprender (Peres *et al.*, 2012).

A Internet tem a capacidade de fazer com que uma informação se espalhe mundialmente e de forma extremamente rápida, sem que se tenha muita clareza acerca da origem destas informações, dando azo a um enorme risco de potencialização de qualquer questão que possa se mostrar ofensiva à intimidade (Almeida e Cunha, 2018).

Em 18 de outubro de 2018, o jornal Folha de São Paulo acusou várias empresas de estarem realizando a compra de pacotes de disparos em massa de mensagens contra o PT no

WhatsApp e ressaltou que o fato tinha o poder de afetar diretamente o resultado das eleições presidenciais no segundo turno. Em 30 de outubro de 2017 foi a vez do jornal The Guardian publicar uma reportagem também nesse sentido, e afirmou que conteúdos financiados pela Rússia podem ter atingido cerca de 126 milhões de americanos no Facebook tanto durante quanto depois das eleições presidenciais de 2016 (Ponticelli, 2018).

O The Guardian também indicou que de acordo com o testemunho do Facebook que foi submetido ao comitê de justiça do Senado norte americano, cerca de 120 (cento e vinte) contas de perfis falsos criaram aproximadamente 80.000 (oitenta mil) postagens que acabaram sendo recepcionadas por 29 milhões de americanos diretamente, tudo isso, financiado pela Rússia. Nota-se que em ambos os casos existem dúvidas no que diz respeito a materialidade e a autoria dos fatos, todavia, torna-se cristalino que essa disseminação de informações na internet, especialmente quando esses conteúdos viralizam sendo espalhados sem nenhum controle e de forma exponencial, causa um grande impacto mundial fazendo com que até mesmo a validade e lisura das eleições sejam questionadas (Ponticelli, 2018).

A *Cambridge Analytics* tornou-se famosa depois de sua atuação na campanha eleitoral de Donald Trump, atual presidente dos Estados Unidos, bem como por suas ações no *Brexit*. A empresa recebeu acusações de estar coletando dados, usando e vendendo indevidamente os dados de milhões de estadunidenses, além de viralizar fake News com o intuito de moldar o pensamento dos usuários da internet à sua maneira, formando opiniões com base em mentiras. Em analogia, no Brasil, também ocorreu um suposto esquema de venda de dados pessoais de brasileiros pelo Serviço Federal de Processamento de Dados (Serpro) e de acordo com o G1 os dados dessas pessoas, como endereço, sexo, nome da mãe e data de nascimento de inscritos no Cadastro de Pessoa Física (CPF) e Jurídica (CNPJ) estavam sendo vendidos por até R$ 273 mil (Vieira, 2019).

Ponticelli (2018) pontua que em pesquisa realizada pelo Cetic no ano de 2017 foi possível apurar 74% das pessoas já acessaram a internet no Brasil, o que equivale a cerca de 140 milhões de indivíduos com acesso às redes. Nesse cenário, para que uma informação ganhe um efeito de viralização basta apenas que um indivíduo encaminhe uma informação para cerca de 520 pessoas distintas, que por sua vez, enviarão para mais pessoas, que também mandaram para outras e, de repente, já não é possível ter um controle sobre isso e ao final, muito mais do que os 140 milhões de pessoas iniciais já terão tido acesso às informações.

> Desta forma, como a transmissão de informação não ocorre de um único portal centralizado que tenta atingir o máximo de pessoas possíveis com as suas publicações, e sim através de um processo espontâneo e difuso de propagação de conteúdo realizado pelos próprios usuários, com base no relacionamento interpessoal proporcionado pelas redes sociais e aplicativos de troca de mensagens, o alcance e a velocidade de transmissão de informação dependem apenas da vontade dos indivíduos de compartilharem aquele conteúdo (Ponticelli, 2018, p.19)

Tudo isso apenas piora quando envolve a disseminação de dados pessoais, considerados por Bossoi (2019) como o Petróleo da internet. Nunca antes na história da humanidade houve qualquer registro de tantas informações alocadas em um único e poderoso sistema como o de hoje e nem com tanto potencial para serem usadas. Ainda naquele ano o autor fez uma estimativa de que o tráfego mundial de dados de dispositivos móveis cresceria em cerca de dezoito vezes até o ano de 2016, o que corresponderia a um volume de 130 *exabytes*, que seria equivalente a 33 bilhões de DVDs, 4,3 quatrilhões de arquivos de MP3 e a 813 quatrilhões de mensagens de texto.

Arrisca-se a dizer, que ele não estava enganado. Atualmente a propagação de informações, notícias e até mesmo *Fake News* é assustadora, pois alcança níveis alarmantes em questão de minutos.

> A administração e o armazenamento destes grandes volumes de informações é algo problemático, com o que se está apenas começando a lidar, e os reflexos de uma má política de administração da informação dentro de corporações são visíveis para além das questões envolvendo dados pessoais, e abrangem o vazamento de segredos industriais e comerciais, planos de negócios, estruturas organizacionais e tantos outros dados que tenham caráter reservado (Bossoi, 2019, p.11).

A cada dia que passa tem se tornado mais frequentes os casos de vazamento de dados pessoais, e isso, ultimamente, tem provocado grande desconfiança no cidadão no que se refere à corporação que os deixou vazar, seja esta privada ou estatal. Em contrapartida, o uso de dados pessoais tornou-se uma importante ferramenta para o desenvolvimento das mais diversas atividades nos mais variados segmentos da sociedade.

No ano de 2023, de acordo com G1, cerca de 530 milhões de usuários (sendo 8 milhões, brasileiros) tiveram seus dados vazados pelo *Facebook*, a plataforma chegou a ser condenada a indenizar todas as pessoas que foram afetadas pela situação. Outras 4 milhões de pessoas também foram vítimas do vazamento de dados diante do programa Auxílio Brasil e a Caixa Econômica Federal também foi condenada a pagar uma indenização de 15 (quinze) mil reais para os beneficiários atingidos.

As maneiras que essas informações ganham utilidade são extremamente preocupantes pois muitas delas se encontram à venda no conhecido "mercado secundário de

dados", em razão de verdadeiros dossiês contendo números de documentos pessoais, situação cadastral no INSS, endereço, telefones, renda familiar, padrões de consumo, dados do cônjuge, status na Receita Federal, título de eleitor, informações de cheques, e, inclusive, dados bancários e números de cartões de crédito, entre outros (Bossoi, 2019).

Porém, conforme assevera Leonardi (2005, p. 7) apud Vieira (2019, p. 12) "a disseminação de informações de modo instantâneo entre milhões de pessoas não traz apenas benefícios. Como qualquer nova tecnologia, a Internet também criou oportunidades inéditas para a prática de atos ilícitos". É justamente na prática desses atos ilícitos que ocorre a violação do direito à privacidade, a partir do uso indevido de dados pessoais por corporações nacionais e internacionais e até mesmo por órgãos governamentais.

2.6 A proteção dos dados pessoais à Luz da LGPD

Atualmente a Internet oferece uma miríade de serviços a serem utilizados e acessados, correspondendo a tipos de conteúdo ou informações como notícias, vídeos, imagens, blogs, entre outros, que podem ser disponibilizadas por provedores de Internet, em websites tanto de autoria própria quanto de terceiros. Um aspecto que sofreu demasiadamente com as transformações trazidas pela internet foram as relações interpessoais.

Outrora as pessoas possuíam o hábito de escrever suas próprias cartas, postando-as nos correios e levando dias no aguardo de uma resposta e a internet veio como um verdadeiro furacão ocupando todos os espaços desses serviços considerados tradicionais e atualmente, até arcaicos. De forma rápida e gratuita os e-mails são escritos instantaneamente, cada vez mais resumidos e com possibilidade de envio para vários destinatários ao mesmo tempo (Tomasevicius Filho, 2016).

O uso da internet na contemporaneidade também permite que sejam realizadas videoconferências, gerando uma economia de custos e recursos, principalmente nesse momento da história do país, quando em meio a maior pandemia da história do país todos estão precisando resolver tudo de casa por conta do isolamento social. Nunca a internet foi tão necessária quanto nesse momento, e a ferramenta que geralmente é inimiga dos contatos físicos, pois a cada dia mais as pessoas tem menos tempo para encontros, serviu justamente para aproximar quando todo e qualquer encontro deixou de acontecer.

Devido a toda a popularidade da internet o público das redes sociais cresceu absurdamente, tornando-se uma espécie de vitrine onde todos querem ver e ser vistos. As antigas salas de bate papo abriram caminho para aplicativos de relacionamento como o tão conhecido "*Tinder*". Por outro lado, toda essa tecnologia deu espaço para uma nova modalidade de emprego, o teletrabalho, onde diversas atividades intelectuais podem ser feitas de casa mesmo através do computador.

Uma outra possibilidade, muito utilizada na contemporaneidade é a troca de informações entre empregadores e empregados que podem ser feitas através da rede. Percebe-se que até mesmo as atividades comerciais foram modificadas pelo novo cenário da internet e comércios que existiam apenas em lojas físicas passaram a vender também nas mídias digitais onde alguns sites especializados permitem a pesquisa imediata dos menores preços, reduzindo os custos da transação dependendo essencialmente do cadastro contendo informações relevantes. Inclusive os serviços bancários foram ampliados para atender através dos internet bankings, economizando o tempo dos usuários. Nesse sentido, diversos serviços públicos estão sendo prestados pela internet, o que contribui para a redução da burocracia, e também para a formação da democracia (Tomasevicius Filho, 2016).

Muito embora a ação de coletar dados pessoais e de navegação de internautas se demonstre com um fato irrelevante, o tratamento desses dados agrega-lhe valor econômico, valores esses que geralmente são destinados para a manutenção de um website, que como qualquer outro empreendimento não deixa de produzir despesas, todavia, não deixa de ser um negócio lucrativo a ponto de até mesmo se tornará atrativo do ponto de vista empresarial. e também lucrativo suficiente para que seja atrativo do ponto de vista empresarial. No entanto, para isso, é extremamente importante compreender o que são os dados pessoais, que numa visão ampla se caracteriza como informações, mas sob um ponto de vista estrito são definidas como as informações relativas a pessoa que permita identificá-la e/ou a tornem identificável (Nakata, 2019).

Nakata (2019) destaca que os dados pessoais podem ser classificados em três categorias:

Dados não sensíveis, que correspondem a todas as informações que simplesmente identificam uma pessoa, individualizando-a.

Dados sensíveis, são aqueles intimamente ligados à vida tanto pessoal como familiar.

Dados de tratamento proibido, são os que estão relacionados ao âmbito do segredo.

Diante disso, é importante saber que a disciplina da proteção de dados pessoais tem como base princípios consagrados que se encontram elencados no ordenamento jurídico brasileiro que são: o respeito à privacidade; a liberdade de expressão, informação, comunicação e de opinião; a autodeterminação informativa; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Klee e Pereira Neto, 2019, p. 16).

> A LGPD deverá ser interpretada e aplicada à luz dos princípios garantidos pela Constituição da República de 1988, tais como a dignidade da pessoa humana, a privacidade, o sigilo de dados e a proteção do consumidor, de maneira a dialogar com as demais fontes normativas do ordenamento jurídico brasileiro (Klee e Pereira Neto, 2019, p. 13).

A LGPD ampara-se na ideia central de que as pessoas devem ter completo conhecimento e controle acerca da coleta e do processamento de suas informações, principalmente no que tange àquelas que as identificam, tratando-se de dados pessoais que possibilitam a limitação de todo esse processamento, em conformidade com a boa-fé que deve pautar todas as relações jurídicas (Klee e Pereira Neto, 2019).

> O principal fundamento da Lei é a proteção dos direitos fundamentais dos cidadãos, sejam eles consumidores ou não. A relevância da proteção de dados nas relações de consumo está no fato de que a informação tem valor econômico e pode significar uma vantagem competitiva para as empresas que utilizam os dados pessoais de seus consumidores para fazer publicidade e ofertar produtos e serviços a um público consumidor em potencial, inclusive nos meios digitais (Klee e Pereira Neto, 2019, p. 16).

A legislação em discussão deverá ser aplicada e interpretada e respeitando dos princípios garantidos e especificados na Carta Magna de 1988, tendo como preceito fundamental a dignidade da pessoa humana, o direito à privacidade, a preservação sigilo de dados e a proteção do consumidor, de forma que dialogue harmoniosamente com as demais fontes normativas do ordenamento jurídico brasileiro, sendo estas o Código Civil, o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet no Brasil, a Lei do Cadastro Positivo e a Lei do Acesso à Informação, uma vez que todas nasceram a fim de assegurar os direitos no que dizem respeito à proteção de dados e à privacidade, dentro de seu campo de aplicação.

Entretanto, nenhuma das legislações supracitadas tem sido suficientemente capazes de coibir que os crimes cibernéticos continuem a ocorrer, o que leva a crer que ainda há um

longo caminho a ser percorrido para que todos os desafios sejam superados e a legislação seja eficiente o bastante para coibir a violação de direitos nesse campo.

CONSIDERAÇÕES FINAIS

Embora a LGPD (Lei Geral de Proteção de Dados) e outras legislações relacionadas tenham um papel fundamental na proteção da privacidade e na mitigação dos crimes cibernéticos, é importante reconhecer que nenhum conjunto de leis pode eliminar completamente todas as ameaças online ou garantir uma proteção absoluta da privacidade.

A LGPD estabelece diretrizes importantes para o tratamento de dados pessoais por organizações, impondo requisitos como o consentimento explícito para o uso de dados, a transparência sobre como os dados são tratados, a implementação de medidas de segurança adequadas e a responsabilização das organizações em caso de violações de dados. No entanto, a eficácia da LGPD depende da aplicação adequada das suas disposições e da capacidade das autoridades competentes em fiscalizar e punir infrações.

Além da LGPD, outras leis e regulamentações, como o Marco Civil da Internet no Brasil e o Código Penal, também abordam questões relacionadas à segurança cibernética e à privacidade online. Essas leis ajudam a coibir práticas criminosas, como invasões de dispositivos, fraudes online, *cyberbullying* e violações de privacidade, fornecendo um arcabouço legal para investigação e punição.

No entanto, é importante reconhecer que a natureza dinâmica e global da internet apresenta desafios significativos para a aplicação da lei e para a proteção da privacidade. Novas ameaças cibernéticas surgem constantemente, e os criminosos muitas vezes operam além das fronteiras nacionais, dificultando a aplicação das leis locais. Além disso, a evolução tecnológica pode criar novas vulnerabilidades e desafios de privacidade que as leis existentes podem não abordar adequadamente.

Portanto, embora a LGPD e outras legislações relacionadas sejam importantes para proteger a privacidade e coibir os crimes cibernéticos, é necessário um esforço contínuo de atualização das leis, investimento em capacitação das autoridades, cooperação internacional e conscientização pública para enfrentar os desafios em constante mudança do mundo digital.

REFERÊNCIAS

ALMEIDA, Nathalie Dutra de; CUNHA, Leandro Reinaldo da. **Avanços tecnológicos, o direito à privacidade e o cyberbullyng.** 3º Congresso Internacional de Direito e Contemporaneidade. 27 a 29 de maio de 2015 - Santa Maria/ RS.

BOSSOI, Roseli Aparecida Casarini. **A proteção dos dados pessoais face às novas tecnologias.** Editora CONPEDI, 2014. Disponível em: http://publicadireito.com.br/publicacao/ufsc/livro.php?gt=122. pag 86-111.

BRANDÃO, Luíza Couto Chaves. **Cadernos Adenauer**xx (2019), nº3. Proteção de dados pessoais: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. isbn 978-85-7504-230-4.

BRASIL. **Lei nº 2.848 de 07 de dezembro de 1940**. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 11 de abril de 2024.

BRASIL, **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 28 de novembro de 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, Brasília, DF, abril 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em 28 de novembro de 2023.

BRASIL, **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Brasília, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em 28 de novembro de 2023.

Facebook é condenado a indenizar brasileiros em R$ 500 por vazamento de dados; saiba como se proteger. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/03/25/facebook-e-condenado-a-indenizar-brasileiros-em-r-500-por-vazamento-de-dados-saiba-como-se-proteger.ghtml. Acesso em 11 de abril de 2024.

FERREIRA, Rafael Freire. **Autodeterminação informativa e a privacidade na sociedade da informação.** Rafael Freire Ferreira – 3. Ed. – Rio de Janeiro :Lumen Juris, 2019.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo.** Estud. av. vol.30 no.86 São Paulo Jan./Apr. 2016. Disponível em: https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269 ou pdf http://dx.doi.org/10.1590/S0103-40142016.00100017.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

KLEE, Antonia Espíndola Longoni e PEREIRA NETO, Alexandre. **Cadernos Adenauer**xx (2019), nº3. Proteção de dados pessoais: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. isbn 978-85-7504-230-4.

MARCONI, M. de A; LAKATOS, E. M. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 5 ed. São Paulo: Atlas, 2002.

MELO, Ademir Torres. **O crime de invasão de dispositivo informático e as alterações promovidas pela Lei nº 14.155/2021**. Disponível em: https://jus.com.br/artigos/100538/o-crime-de-invasao-de-dispositivo-informatico-e-as-alteracoes-promovidas-pela-lei-n-14-155-2021. Acesso em 08 de maio de 2024.

MINAYO, MCS. **O desafio do conhecimento, pesquisa qualitativa em saúde**. (2a ed.). Editora Hucitec, São Paulo, 2002.

NAKATA, Alexandre. A responsabilidade civil de provedores de aplicação de internet à luz da Lei de Proteção de Dados Pessoais e do Código de Defesa do Consumidor. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 24, n. 5989, 24 nov. 2019. Disponível em: https://jus.com.br/artigos/69968. Acesso em 11 de abril de 2024..

PERES et. al. Cultura tecnológica e vulnerabilidade ao trauma psíquico. **O Mundo da Saúde**, São Paulo - 2012;36(2):303-310.

PONTICELLI, Murilo Meneghel. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da lei geral de proteção de dados.** Monografia apresentada ao Curso de Direito da Universidade do Sul de Santa Catarina.

QUINTINO, Eudes. **A nova lei Carolina Dieckmann.** Jusbrasil. Disponível em: https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann. Acesso em 28 de novembro de 2023.

Seus dados do Auxílio Brasil vazaram? Instituto abre consulta para checar; veja o passo a passo. Disponível em: https://g1.globo.com/economia/noticia/2023/10/11/dados-do-auxilio-brasil-vazados-veja-o-passo-a-passo-para-checar.ghtml. Acesso em 11 de abril de 2024.

SILVA, Letícia Brum; SILVA, Rosane Leal da. **A proteção jurídica de dados pessoais na internet: Análise comparada do tratamento jurídico do tema na União Europeia e no Brasil.** Editora CONPEDI, 2014. Disponível em:http://www.publicadireito.com.br/publicacao/unicuritiba/livro.php?gt=122. pag 183-212

TEIXEIRA, Tarcísio. **Marco Civil da Internet Comentado.** São Paulo: Almedina Brasil, 2016.

VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados: uma análise da tutela dos dados pessoais em casos de transferência internacional**. Monografia apresentada à Graduação em Direito da Universidade Federal de Uberlândia.