PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS:

NECESSIDADE DO APRIMORAMENTO DA TIPIFICAÇÃO PENAL DOS CRIMES CIBERNÉTICOS

ORIENTANDO: GABRIEL CÔVOLO SANTANA
ORIENTADORA PROFª MS. LARISSA DE OLIVEIRA CASTRO BORGES

GOIÂNIA
2021

GABRIEL CÔVOLO SANTANA

CRIMES CIBERNÉTICOS

NECESSIDADE DO APRIMORAMENTO DA TIPIFICAÇÃO PENAL DOS CRIMES CIBERNÉTICOS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Profa. Orientadora Ms. Larissa de Oliveira Costa Borges.

GOIÂNIA

2021

GABRIEL CÔVOLO SANTANA

CRIMES CIBERNÉTICOS

NECESSIDADE DO APRIMORAMENTO DA TIPIFICAÇÃO PENAL DOS CRIMES CIBERNÉTICOS

Data da Defesa: 1º de dezembro de 2021.

BANCA EXAMINADORA

_____

Orientadora: Profª Ms. Larissa de Oliveira Costa Borges Nota

_____

Examinador Convidado: Prof. Ms. Júlio Anderson Alves Bueno Nota

Dedico este trabalho primeiramente a minha família e aos professores que contribuíram de forma significativa para a construção deste conhecimento.

Agradeço a Deus, que sempre me ajudou a superar os obstáculos e a chegar até aqui. A minha família, fonte de todo amor e incentivo. A meus professores, fonte de todo o conhecimento. Aos meus amigos que tornaram a caminhada até mais leve.

SUMÁRIO

CRIMES CIBERNÉTICOS

NECESSIDADE DO APRIMORAMENTO DA TIPIFICAÇÃO PENAL DOS CRIMES CIBERNÉTICOS

Gabriel Côvolo Santana[1]

RESUMO

As novas tecnologias da informação propagadas nas últimas décadas de globalização levaram a sociedade pós-moderna a uma nova era, a era digital. Essa, trouxe consigo avanços, mas também, retrocessos como novos delitos. Dessa forma, houve a necessidade do âmbito jurídico em se adequar a essa nova realidade, definindo e classificando esses novos crimes, bem como, aprimorando legislações que se tornaram obsoletas a fim de aperfeiçoar assim a tipificação penal de crimes cibernéticos.

Palavras-chaves: Delitos informáticos. Crimes Cibernéticos. Tipificação Penal. Avanços. Lacunas. Lei.

INTRODUÇÃO

A internet se tornou um veículo indispensável para a sociedade, além disso, com o advento da globalização nos transformamos em uma sociedade da informação amparada por uma economia digital.

Em tempos de era digital, os crimes praticados com o uso da rede mundial de computadores ganham um novo prefixo e passam a ser chamados de cybercrimes. Eles consistem em crimes já existentes que apenas ganharam uma nova configuração no meio digital, a qual lhes fornecem maior velocidade para se

[1] Acadêmico do 9º período do curso de Direito da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUCGO).

perpetuarem, bem como e novos crimes que só podem acontecer através do cyberespaço. Logo, cabe ao âmbito jurídico também evoluir e se adaptar a eles, criando e colocando em prática legislações efetivas.

O presente trabalho é divido em três capítulos os quais possuem o objetivo de fazer uma análise histórica da sociedade da informação, bem como dos crimes cibernéticos; definir e classificar tais crimes, analisar a evolução das legislações penais que os tipificam e avaliar as lacunas que ainda existem, respectivamente.

No primeiro capítulo, o projeto tratará da dimensão histórica acerca dos computadores, da internet e da evolução dos crimes. O segundo capítulo irá definir e classificar os crimes virtuais, bem como expor superficialmente sobre alguns dos principais cybercrimes. Já o terceiro capítulo fará uma análise profunda da evolução das legislações, bem como tratará das lacunas e omissões existentes nelas, expondo a necessidade de se tipificar tais crimes.

1 ABORDAGEM HISTÓRICA

Inicialmente, cumpre ressaltar que, segundo matéria publicada no site TECMUNDO, embora os computadores mecânicos e os demais eletrônicos tenham surgido durante a Segunda Guerra Mundial, foi no período da Idade Antiga que se originou a primeira máquina de computar, denominado ábaco, uma espécie de calculadora que realizava pequenos cálculos matemáticos. Sobre o ábaco:

> Seu primeiro registro é datado de 5500 a.C. pelos povos que constituíam a Mesopotâmia. Contudo, o ábaco também foi usado por muitas outras culturas, e cada povo tem uma versão de específica dessa máquina, preservando a essência original. Seu nome na Roma Antiga era Calculus, termo do qual a palavra *cálculo* foi derivada (TECMUNDO, 2009, p. 2).

O resumo histórico constante no presente trabalho foi retirado do sítio eletrônico Tecmundo (2009) que descreve o surgimento dos computadores à época do Renascimento, a partir da criação de uma régua de logaritmos predefinidos capaz de realizar multiplicações mais complexas, sendo considerada a mãe das calculadoras modernas. Entretanto, a primeira calculadora mecânica foi desenvolvida pouco tempo depois, a chamada Máquina de Pascal.

Em 1801 foi criada a primeira máquina programável, chamada de Tear Programável. Ato contínuo surgiu a Máquina de Diferenças e, posteriormente, o Engenho Analítico que, só não foram implementadas, em razão das restrições técnicas e financeiras na época (TECMUNDO, 2009).

Assim como, também expõe o Tecmundo (2009), já no século XIX uma máquina analítica com memória e programas foi desenvolvida, garantindo ao seu criador o título de 'Pai da Informática'. Todavia, foi somente na metade do século XX que ocorreu o desenvolvimento dos computadores mecânicos e acessórios eletrônicos.

Com a Segunda Guerra Mundial, o desenvolvimento dos computadores passou a ser cada vez mais incentivados com o objetivo de desencriptar mensagens de inimigos e criar armas mais inteligentes. Inicia-se, pois, a era da Computação Moderna que vigora até os dias atuais. Apesar do computador não ser a única ferramenta utilizada para a prática de crimes cibernéticos, é através dele que grande parte dos crimes são cometidos.

1.1 GLOBALIZAÇÃO E A ORIGEM DA INTERNET

Consoante, o espaço eletrônico Brasil Escola, após a Terceira Revolução Industrial, o processo de globalização cresceu acentuadamente. Esse fenômeno pode ser definido como o processo de expansão econômica, política, social e cultural pelo mundo através da evolução dos transportes e da comunicação, de modo que a distância e as fronteiras geográficas se tornaram cada vez menores.

Nesse sentido, o professor Boaventura de Souza Santos (1997, p. 108) menciona que é necessário abordar uma definição de globalização "mais sensível às dimensões sociais, políticas e culturais", dizendo que:

> A globalização é o processo pelo qual determinada condição ou entidade local consegue estender sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival.

Vale destacar que todo o processo de globalização juntamente com a evolução dos instrumentos de informação, impactou diretamente o Direito. Esse,

então, precisou de forma urgente enfrentar questões jurídicas pertinentes a essa nova era digital.

O termo ciberespaço se originou em 1984 com o autor da ficção científica Neuromancer, de Willian Gibson. Para ele, “ciberespaço é um espaço não físico no qual uma alucinação consensual pode ser experimentada diariamente pelos usuários” (SÓ PEDAGOGIA, 2008, p.1).

Levy (1999, p. 17) ainda complementa:

> [...] É o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.

Nesse sentido, surge a internet como fração de tecnologia e comunicação que faz parte do ciberespaço, além de todas as outras formas de interação entre humanos e a tecnologia. Assim:

> A Internet pode ser vista como parte dessas tecnologias digitais, ou como a infraestrutura de comunicação que sustenta o ciberespaço, sobre as quais se montam diversos ambiente, como a Web, os fóruns, os chats e o correio eletrônico para ficar apenas com os exemplos mais comuns e disseminados. Em suma, o ciberespaço é o ambiente e a Internet uma das infraestruturas (SÓ PEDAGOGIA, 2008, p. 2).

A internet pode ser considerada uma das maiores revoluções do último século. Originada no contexto da Guerra Fria diante da necessidade de compartilhamento de informações e arquivos entre locais distantes entre si durante o período de guerra, é considerada, hoje, como indispensável à sociedade.

> A internet surgiu nos Estados Unidos em 1962, por criação de Paul Baran, como consequência de pesquisas na área de tecnologia militar, que objetivava estabelecer uma rede de telecomunicação o menos vulnerável possível a um ataque nuclear soviético, na época da guerra fria entre americanos e russos, e a primeira rede, denominada Arpanet, foi conectada em 1969 entre quatro potentes computadores da época (FERREIRA, 2010, p. 80).

Todavia, muitos estudiosos acreditam que sua origem teve como objetivo principal a pesquisa científica. Nesse sentido, entende Maria Eugênia Finkelstein (2008, p. 407) sobre a finalidade da Internet:

> Sua predecessora chamava-se ARPANET, tendo sido desenvolvida em 1969. Sem dúvida há boatos de que a ARPANET foi desenvolvida para fins militares, mas a tese dominantes é a de que a Internet surgiu com o objetivo

> de pesquisa de um projeto da agência norte-americana ARPA. A conexão teve início ao interligarem-se os computadores de quatro universidades, passando, a partir disso, a ser conhecida como ARPANET. Em 1970, esse projeto foi intensamente estudado por pesquisadores, o que resultou na concepção de um conjunto de protocolos que é a base da Internet. Depois, o ARPA integrou redes de computadores de vários centros de pesquisa. Em 1986, a NSFNET, da entidade americana NSF, interligou-se a ARPANET, o que deu finalmente origem às bases da atual Internet.

No Brasil, ela se originou, sobretudo com o fim acadêmico. Somente em 1995 passou a ser utilizada comercialmente por empresas e pessoas privadas. Sobre o assunto, Carlos Tadeu Queiroz de Morais (2012, p. 42) explica:

> Somente em 1995 foi possível, por iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia, a abertura ao setor privado da Internet para exploração comercial da população brasileira. A rede brasileira deixou de ser somente acadêmica, como já acontecera em 1994 nos EUA, e empresas e indivíduos também passaram a usar os serviços da Internet.

Isto porque, a Agência Nacional de Telecomunicações - ANATEL, objetivando regular o uso de meios da Rede Pública de Telecomunicações e os Serviços de Conexão à Internet, elaborou a Norma 044/1995, que assim a definia como:

> Internet: nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores;

Dessa forma, como exposto no sítio eletrônico enciclopédia livre, a internet pode ser entendida como uma rede mundial de computadores interligados entre si, de forma que, todos que nela estão conectados, usufruam de todos os serviços que ela possa oferecer, seja de pesquisa, informações ou comunicação em escala global

Carla Rodrigues de Araújo de Castro (2003, p. 3) conceitua Internet como sendo:

> Internet é uma grande rede de comunicação mundial, onde estão interligados milhões de computadores, sejam eles universitários, militares, comerciais, científicos ou pessoais, todos interconectados. É uma rede de redes, que pode ser conectada por linhas telefônicas, satélites, ligações por microondas ou por fibra ótica.

É certo que a internet revolucionou a vida pós-moderna trazendo sensíveis vantagens. Porém também se tornou o meio mais rápido e fácil de cometer diversos crimes virtuais, uma vez que, acreditando estarem protegidos pelo anonimato, os criminosos praticam atos ilícitos como acessar e copiar dados bancários, danificar dados, cometer crimes contra a honra e contra a intimidade, entre outros. Consoante relatório publicado pela Norton Cyber Security, o Brasil desde 2017, entrou em segundo lugar no ranking de países com maior número de casos de crimes cibernéticos.

1.2 A PRÁTICA DE CRIMES COMO CONSEQUÊNCIA DO USO INADEQUADO DA INTERNET

Com base no artigo 19, item 3, do Pacto Internacional de Direitos Civis e Políticos, de 1966, bem como, do relatório emitido pela Organização das Nações Unidas - ONU, o acesso à internet deve ser universal, devendo cada país garantir que todos a ela tenham acesso.

No entanto, não se pode olvidar que, por trás de um computador, sobretudo com acesso à internet, é possível assumir diversas faces e identidades, bem como desenvolver diversos papéis ou, ainda, ser qualquer pessoa. Porém, as consequências advindas dessa liberdade virtual podem ser inclusive, criminais.

Sob essa ótica Carla Rodrigues Castro (2003, p. 9) ensina que:

> Os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através dele. A maioria dos crimes são praticados através da internet, e o meio usualmente utilizado é o computador.

Assim, o uso da internet em larga escala trouxe consigo novos riscos que não se podem ser tolerados ou ignorados, sobretudo, no campo do Direito. Entretanto, sabe-se que a punição pelos crimes tecnológicos ainda é deficiente, nas palavras do Professor Marco Antônio de Barros (2007, p. 275):

> A tutela punitiva tecnológica é um tema ainda pouco explorado para os padrões da chamada Sociedade da informação, na qual se sobressai a intensa utilização de ultra modernos meios de comunicação filiados à tecnologia, notadamente a internet (cadeia de redes em escala mundial

> utilizada para circulação de informações de todos os tipos) os quais revolucionaram os hábitos diários de grande parte da população planetária.

A utilização do ambiente da internet facilitou a prática de crimes já existentes, bem como possibilitou a criação de novas práticas criminosas que atingem os mais diversos direitos, causando prejuízos de todas as ordens a diversas pessoas em escala global.

Na opinião do Professor Reginaldo César Pinheiro (2001, p. 183):

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a Internet um espaço livre, acabam por exceder em suas condutas criando novas modalidades de delito: os crimes virtuais.

Dessa forma, um dos crimes que ocorrem com maior frequência por meio de acesso à Internet e às redes sociais, são os tipificados no Capítulo V do Código Penal, os chamados crimes contra a honra. Nesse sentido:

> Os crimes contra a honra, nas modalidades de calúnia, injúria e difamação, ocorrem com bastante frequência nas redes sociais e se alastram com extrema facilidade, pela ágil disseminação das ofensas postadas na rede, potencializando as consequências nefastas para as vítimas, ante as características da circulação dos conteúdos veiculados pela internet. Outros ilícitos graves, como a invasão de privacidade, ameaças, assédio sexual, assédio moral (Bullying), têm permeado constantemente os diversos sítios, correios eletrônicos e redes sociais. A falsificação de perfil é o ilícito mais comum em vários tipos de mídias, como blogs e sites de relacionamento. (KUNRATH, 2017, p. 29).

Além disso, existe ainda, o rol de crimes relacionados à pedofilia, exploração sexual, propagação de vírus, fraudes financeiras e diversas outras tipificações que serão estudadas no decorrer do presente trabalho.

Destarte, tem-se a constatação notória de que os crimes praticados pelo mau uso dos meios eletrônicos constitui iminente perigo aos direitos fundamentais e à dignidade da pessoa humana na proporção que, da mesma forma que o crime comum está inserido na realidade das pessoas, o cibercrime é uma realidade inerente ao ciberespaço e, tal como aquele, precisa ser combatido veemente através de efetiva aplicação penal no Brasil e no mundo.

2 CRIMES CIBERNÉTICOS

Entende-se por crimes cibernéticos toda e qualquer conduta ilegal não ética, ou não autorizada que envolva processamento de dados e/ou transmissão de dados, conforme a definição proposta pela Organização para a Cooperação Econômica e de desenvolvimento (OECD). No mesmo sentido, Rosa (2015, *apud* RAMOS 2002, p.18), define:

> A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processo automático e/ou eletrônico de dados ou sua transmissão [...] Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado etc.

2.1. CLASSIFIÇÃO DOS CRIMES CIBERNÉTICOS:

Apesar de serem consideradas um tanto obsoletas, devido à dinâmica das tecnologias e da internet, bem como aos crimes que surgem e evoluem a todo momento; os crimes cibernéticos possuem duas classificações. A primeira os divide em puros, mistos e comuns. Já a segunda os divide em próprios e impróprios.

2.1.1 Crimes cibernéticos puros, mistos e comuns

Segundo abordagem publicada no site Jusbrasil, entende-se por crimes cibernéticos puros aqueles que possuem como único objetivo o sistema de computador, seja através de invasão física ou técnica. Dessa forma, o criminoso, como por exemplo os hackers, possuem o objetivo de afetar o aparelho computador, bem como os dados e informações nele contidos. É o caso de duas ameaças que foram destaques nos anos 1990, os vírus Michelangelo e Melissa.

Os crimes cibernéticos mistos tratam-se de crimes cujo o uso da internet é condição primordial, ou, assim como muitos autores afirmam, condição *sine qua non*

para a efetivação da ação delituosa. Ele fica bem evidente em crimes de furto de senhas para acesso a informações confidencias e realizações de transações ilegais.

Para finalizar tal classificação, também de acordo com o Jusbrasil, os crimes comuns consistem naqueles em que o uso da internet é utilizada apenas como meio para a efetivação de um delito já tipificado por lei. Isso fica claro, tendo em vista que a internet é apenas um meio virtual para a realização de um crime, e não meio essencial para que ele ocorra. A pornografia infantil é um exemplo

2.1.2 Crimes próprios e impróprios

Na visão de Damásio de Jesus (2016) os crimes de informáticas podem ser classificados em próprios e impróprios. Os crimes próprios são aqueles em que o sistema informático da vítima é o objeto e o meio do crime. As condutas praticadas por hackers se enquadram bem nessa divisão, isto é, crimes de invasão, alteração, inserção de dados que objetivam afetar diretamente o software do dispositivo. Para alguns doutrinadores, como Marco Túlio Viana:

> São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados) (VIANA, 2003 *apud* CARNEIRO, 2012, p.78)

Já os crimes impróprios, de acordo com o Jusbrasil, também são cometidos através de um computador, entretanto, esse é apenas um meio de execução, isto é um *animus operandi*. Além disso, consistem em crimes que atingem um bem jurídico comum, como o patrimônio. Entram nessa classificação crimes como: calúnia, injúria, difamação, ameaça, furto, estelionato, pedofilia entre outros.

2.2 PRINCIPAIS CRIMES CIBERNÉTICOS

2.2.1 Pornografia infantil

Tendo em vista a abordagem publicada pela revista eletrônica Âmbito Jurídico (2020), entende-se como pornografia infantil a guarda ou veiculação de imagens contendo nudez ou caráter erótico de crianças e adolescentes para fins comerciais ou de exposição pública. Tal crime não necessita da internet para acontecer, porém é fato que, atualmente, a internet é o principal meio em que ela ocorre, uma vez que acontece, na maioria das vezes, através de uma rede que armazena, autoriza e veicula para outros usuários tal conteúdo.

De acordo com uma pesquisa realizada pela Safernet (2021) os crimes cibernéticos tiveram aumento de 5.000% desde o início da pandemia do Covid-19, sendo que a pornografia infantil é um dos principais crimes. O levantamento registou, entre março e julho de 2020, 428931 denúncias de pornografia infantil, isto é, o dobro do registrado no mesmo período de 2019.

Os artigos 240 e 241 da Lei 11.829/2008 (Estatuto da Criança e Adolescente) estabelecem que a pornografia infantil é uma forma de violência gravíssima, sujeita a punição rigorosa

> Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008) Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008). Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008) Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008).

Nesse sentindo, é evidente que a veiculação de pornografia infantil é um dos principais crimes em ascensão no país, em especial na pandemia, momento no qual crianças e adolescentes ficaram mais tempo em casa. Logo, é nítido que as leis já existentes se tornaram frágeis e necessitam de reformulação e rigor.

2.2.3 Crimes contra a honra

Há três tipos de crimes contra a honra previstos no Código Penal brasileiro: calúnia, difamação e injúria. De acordo com o art. 138, caluniar alguém é imputar-lhe falsamente um fato tipificado como crime. De acordo com o art. 139 difamar alguém é imputar-lhe fato ofensivo a sua reputação. Por fim, de acordo com o art. 140, injuriar alguém é ofender a dignidade e o decoro de outro.

Tais crimes sempre ocorreram através do meio físico e, com o advento da globalização e o surgimento da internet passaram a ocupar espaço também no cyberespaço, uma vez que através de dispositivos eletrônicos a irradiação das condutas criminosas. A internet tornou-se prato cheio para tais crimes, uma vez que o criminoso entende que está protegido pelo anonimato das telas, fato que nem sempre é verdade, uma vez que com as novas tecnologias consegue-se rastrear facilmente o IP de um computador e detectar a identidade do criminoso através do histórico de vinculações do provedor de internet, como afirma matéria publicada no site do G1 por Altieres Rohr, especialista na defesa contra ataques cibernéticos.

Um dos principais crimes contra honra cometidos virtualmente é o racismo. Segundo o art. XX do CP, para este crime a pena é de reclusão de 2 (dois) a 3 (três anos). Entretanto, quando praticado através da internet a reclusão pode ser 2 (dois) a 5 (cinco) anos e multa.

2.2.3 Espionagem e sabotagem

Consoante Takushi e Aquott (s/d), a espionagem configura-se pela alteração de programas ou trocas de peças, modificando a programação originária facilitando dessa forma o acesso aos dados, registros de uma máquina. Dessa forma, sempre que alguém acessa sem autorização um sistema informático que não é de sua posse constitui-se crime. A lei Carolina Dieckmann, como veremos posteriormente, trouxe mudanças significativas e alterou o art. 154 do Código Penal, amparando tais delitos.

Entende-se como sabotagem a destruição ou danificação de material ou componente de um computador. Ela tem por finalidade causar danos ao sistema. Legislações como o Marco Civil e a Lei Geral de Proteção de Dados também tratam sobre esse tema, o que se verá adiante.

3 LEGISLAÇÃO PENAL CONTRA CRIMES CIBERNÉTICOS

Segundo Carneiro (2013), os primeiros crimes virtuais no Brasil, ocorreram na década de 1960 a partir de onde criminosos invadiam e roubavam dados contidos em computadores, praticando atos delituosos, como o de espionagem e sabotagem, até mesmo contra sites do próprio governo brasileiro. Com o passar dos anos tais crimes foram se aperfeiçoando e se estendem até os dias atuais, logo, a criação de legislações que amparassem tais crimes tornou-se urgente.

3.1 LEI 12.737, DE NOVEMBRO DE 2012 (LEI CAROLINA DIECKIMANN)

Como foi visto, o avanço tecnológico da era pós-moderna contribuiu para o aumento de crimes virtuais, bem como colocou em voga o surgimento de um novo bem jurídico, isto é, a segurança da informação. Dessa forma, tornou-se urgente a criação de uma lei que amparasse tais conflitos. Sendo assim, a Lei nº 12.737 de 30 de novembro de 2012, mais conhecida como Lei Carolina Dieckmann, foi o marco inicial da legislação virtual. A Lei foi assim nomeada devido ao vazamento de 36 fotos íntimas e sensuais da atriz global que teve seu computador invadido por dois hackers. Esses, divulgaram as fotos em diversas redes sociais após a falha tentativa de extorsão da atriz. Dessa forma, como não havia uma legislação que amparasse efetivamente tal crime, os hackers responderam por extorsão, furto e difamação, mas não pela invasão em si, assim como afirma matéria publicada pelo site do G1 em maio de 2012.

Vale destacar que a Lei nº 12.737 alterou o Código Penal acrescentando os artigos154-A e 154-B. Além disso, também trouxe pequenas modificações nos artigos 266 e 298 do CP.

O artigo 154-A diz respeito à invasão de dispositivos informáticos e determina pena de 3 (três) meses a 1 (um) ano, e multa para ações delituosas como:

> 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.

Na opinião de Misael Neto (2013), a pena máxima de 1 (um) ano, arrasta o crime para o rito sumaríssimo dos Juizados Especiais, implicando na suspensão condicional do processo, na conciliação, na composição civil dos danos e na transação penal.

Nesse mesmo viés, assim como afirma Opice Blum (2013), a natureza branda das penas impostas ao réu primário pode estimular o delito ao invés de coibi-lo, visto que penas leves, inferiores a quatro anos, podem ser facilmente convertidas à prestação de serviços à comunidade, como o pagamento de cestas básicas. Segundo ele:

> Tem muito computador por aí com informação que vale muito mais do que uma cesta básica […], aos criminosos, cometer o delito, ser pego e ter de pagar pelo crime de invasão pode compensar. Isso se o sujeito for pego, identificado e julgado a tempo. Como as penas para o crime são pequenas, elas prescrevem rapidamente, inviabilizando a punição. (BLUM, 2013, p. 64).

Consoante João Loes (2013) a promulgação dessa lei foi apenas o primeiro passo, já que as lacunas na redação do texto e a infraestrutura deficitária da polícia investigativa podem atrapalhar. Tudo fica ainda pior tendo em vista principalmente o curto tempo para a prescrição dos crimes devido às pequenas penas, o que inviabiliza a punição efetiva dos criminosos.

João Loes (2013) destaca que um dos principais obstáculos para o progresso da Lei Carolina Dieckmann consiste na falta de capacitação técnica dos agentes estatais, isto é, da polícia investigativa, para apurar crimes informáticos. Tal falta de capacitação, provoca demora na investigação, fato que culminado à irrisória pena do crime implica na impunidade do réu, já que ocorre prescrição do crime:

> Hoje, por exemplo, quem busca a polícia para registrar um boletim desse tipo de ocorrência, pode esperar até três meses para ter seu equipamento periciado. (LOES, 2013, p. 64)

Logo, além de penas mais rígidas, é imprescindível que exista uma equipe competente e ágil, pois como afirma Leandro Bissoli (2013) os rastros do crime digital são frágeis e sem uma perícia competente e rápida, pouco se salva.

É importante salientar, também, que o artigo 154-A contém outros dois grandes pontos críticos, sendo a primeira a respeito do termo 'dispositivo informático', pois tal termo é obsoleto, já que atualmente, o acesso à internet é possível não só através de um computador, mas também através de uma infinidade de dispositivos, como celular, tablet, notebook, televisão, por exemplo.

O segundo trecho alvo de críticas e digno de alterações é: "mediante violação indevida de mecanismo de segurança". Para constituir crime é necessário que o dispositivo seja dotado de um 'mecanismo de segurança', isto é, antivírus firewall, senhas, tela de bloqueio etc. Dessa forma, entende-se que a invasão de dispositivos desprotegidos é considerada fato atípico.

Assim como afirma Auriney Brito (2013, p. 69): "só haverá o crime do art.154-A se o autor da conduta usar sua habilidade para superar a proteção do sistema informático, por mais simples que ela seja".

Dessa forma, entende-se que, se o indivíduo, através de suas habilidades físicas ou através de malwares e, sem o uso da violência, conseguir com que a vítima lhe forneça o seu conteúdo privado/íntimo, esse não pode ser considerado criminoso e, tampouco, ser punido. Consoante Wanderlei José Reis (2013, p. 34):

> O ato de "entrar à força, apoderar-se violentamente" e a julgar pela redação do novel artigo, somente se configuraria o crime se o agente acessasse o sistema de informática à força.

A possível solução para tal redação equivocada, seria substituir o verbo invadir pelo verbo acessar, tendo em vista que a definição desse, segundo o dicionário Aurélio (2010) é "obter acesso a". Dessa maneira, apenas a ação de acessar o dispositivo alheio configuraria crime, independentemente de ter ou não dispositivo de segurança.

Para finalizar a análise da Lei Carolina Dieckmann, vale ressaltar também que o legislador pecou ao empregar no art. 154-A o verbo ‘obter’, uma vez que, dessa forma, não deixa claro se o crime é configurado apenas por quem rouba, retira, faz cópia de dados alheios ou, também por quem apenas invade com a intenção de consulta, sem roubar nada.

É necessário, portanto, ressaltar que apesar de representar uma grande conquista, a Lei 12.737/2012 nasceu com lacunas que dão lugar a várias interpretações. Tal fato é determinante para a ineficácia da lei perante a proteção do direito fundamental à intimidade e à vida privada da vítima.

3.2 LEI 12.965, 23 DE ABRIL DE 2014 (LEI DO MARCO CIVIL DA INTERNET)

Tendo em vista que as relações humanas evoluem e que junto a elas surgem novas realidades e problemas, o Marco Civil da internet surgiu através da necessidade de se adaptar, bem como de regulamentar essas relações intrínsecas ao mundo virtual.

Assim como expõe o marco civil comentado por Vitor Hugo Gonçalves (2016), a Lei 12.965/2014 estabelece princípios, garantias, direitos e deveres na internet e a princípio não teve a intenção de regular criminalmente ações delituosas. Nesse sentindo, o marco civil foi criado com a intenção de promover a liberdade de expressão, a neutralidade da rede, a privacidade, o direito de acesso à internet entre outros pontos não menos importantes. Soares (2014, s.p), completa afirmando que “o grande intuito da lei é a garantia dos direitos humanos como principal fundamento o respeito à liberdade de expressão na rede mundial de computadores, no qual seja essencial ao exercício da cidadania”.

O marco civil ganhou força após o escândalo provocado pelas informações divulgadas por Edward Snowden, ex-técnico da CIA, acusado de espionagem pelo governo norte-americano. Em 2014, Edward revelou detalhes de programas de vigilância que o país usava para monitorar a população americana, bem como outros países, incluindo o Brasil. Nesse episódio, ele declarou o monitoramento, inclusive,

de ações da presidente Dilma Rousseff. A reportagem publicada no jornal G1 exemplifica:

> O ex-técnico da CIA Edward Snowden, de 29 anos, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana, utilizando servidores de empresas como a Google, Apple e Facebook e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores. Com os dados coletados por Snowden, mostrou-se que milhões de e-mails e ligações de brasileiros e estrangeiros em trânsito no país foram monitorados. Ainda segundo os documentos, uma estação de espionagem da NSA funcionou em Brasília pelo menos até 2002. Os dados 41 apontam ainda que a embaixada do Brasil em Washington e a representação na ONU, em Nova York, também podem ter sido monitoradas (G1, 2014).

Assim, o governo brasileiro agilmente pressionou o Congresso Nacional para a aprovação de uma lei que apurasse o comportamento virtual. Vale ressaltar que, o marco civil foi a primeira lei do mundo a estabelecer direitos e deveres aos usuários e, por isso, foi bastante esperado e comemorado.

Dessa forma, com a crença errônea de que o ordenamento pátrio supostamente não tinha normas que pudessem ser aplicadas às relações virtuais, o marco civil surgiu como a tentativa de estabelecer tais normas. No entanto, se configurou repetições e reafirmações descontextualizadas de princípios e garantias já existentes e, o pior, sem acrescentar praticamente nada a legislação vigente e sem relacioná-las de maneira profunda e efetiva às questões e problemas que envolvem ao ciberespaço. Tal fato é bem expresso por Vitor Hugo Gonçalves (2016, p. 8):

> O Marco Civil inicia-se com o comando legal de que nele se estabelecem os princípios, garantias, direitos e deveres para o uso da internet no Brasil. Primeiramente, há que se ressaltar que tal comando pressupõe um equívoco do legislador e uma total dissonância do sistema jurídico em que se insere o Marco Civil. Quem estabelece princípios, garantias, direitos e deveres para quaisquer usos e tecnologias é a Constituição Federal do Brasil. O Marco Civil é uma legislação infraconstitucional que deveria implementar e regulamentar a Constituição. Contudo, não é isso que ocorre. Muitas linhas se seguirão abaixo para constatar que o Marco Civil repete descontextualizadamente princípios, garantias, direitos e deveres constitucionais sem aprofundá-los para as questões e problemas existentes de suas inserções nas tecnologias de informação e comunicação.

Além disso, devemos ressaltar que outro ponto crítico da lei, o art. 2º ao tratar da liberdade de expressão ao invés da liberdade de pensamento. Nesse sentido, a interpretação equivocada desses conceitos traz consigo diversas limitações que não são enfrentadas devidamente pelo Marco Civil.

Nesse viés, seguindo a lógica de Vitor Hugo Gonçalves (2016), a liberdade de expressão se traduz pelas liberdades de comunicação, religião, artística e cultural. Enquanto a liberdade de pensamento se traduz através da liberdade de formar pensamentos sem a necessidade de externa-los à sociedade, isto é, da liberdade de resguardá-los apenas para si, longe do acesso de outros indivíduos, empresas ou autoridades governamentais.

Sendo assim, frente à falta da liberdade de pensamento, teoricamente, os pensamentos não exteriorizados na rede, isto é, os registros e dados sigilosos que são construídos através do acesso dos cidadãos à rede, não estão efetivamente protegidos e resguardados. Consoante Vitor Hugo Gonçalves (2016, p. 12):

> A liberdade de pensamento, em tempos de internet, está ligada a registros e dados que são construídos nas tecnologias de informação e comunicação. São informações, dados, metadados, registros de conexões, registros de geolocalização, atrelados a cada um inserido nessas redes de comunicação. Aquilo que pode ser representado por essas tecnologias são pensamentos que devem ser resguardados e protegidos pela lei. O Marco Civil, ao se omitir em relação à liberdade de pensamento, restringe a complexidade que a liberdade de expressão, em sua dimensão intrínseca, protege do vigilantismo estatal e do tratamento de dados por empresas, bem como antecipa em relação a uma posterior lei de proteção de dados pessoais.

No Brasil, o direito à privacidade é um direito fundamental está garantido pelo art. 5º da CF que preconiza “invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação”. O artigo também garante o “sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

Dessa forma, através dos arts. 3º, 7º, 9º, 10º, 11, 12, 15, 19, 21 e 23, o Marco Civil também estabeleceu a proteção da privacidade e dos dados pessoais como princípios regulatórios do uso da internet.

O direito à privacidade e à intimidade nunca foi tão latente quanto na atual era digital, isso porque atualmente vivemos uma economia baseada na informação. Dessa forma, seguindo a linha de pensamento de Vitor Hugo Gonçalves (2016), os usuários e principalmente seus dados são as principais fontes de lucro, já que são a partir deles que empresas grandes, como o Facebook, Whatsapp e Google desenvolvem novas estratégias e produtos comercializáveis

Nesse viés, de acordo com o art. 7º, o Marco Civil deve garantir que os provedores prestem aos usuários informações claras e completas sobre a coleta de seus dados e, também, sobre os objetivos dessa coleta. Tudo isso, deve envolver uma política de privacidade e um termo de uso transparente que deixe claro o direito de consentir ou não com a transferência de seus dados a terceiros. Deve, ainda, deixar em destaque para os usuários a existência do direito ao acesso aos seus próprios dados, bem como deve disponibilizar canais de comunicação de fácil acesso que permitam aos usuários a revogação desse consentimento caso necessário. Além disso, segundo esse mesmo artigo, a coleta de dados pelo provedor justifica-se por uma necessidade processual, logo, caso os dados sejam excessivos, tal ação será considerada ilegal

Entretanto, a lei não aborda detalhadamente a proteção de dados e não soluciona efetivamente diversas questões que envolvem as empresas de telecomunicações e provedores de aplicação de internet. Essas empresas, através de recursos como a big data, analisam a privacidade, intimidade, pensamentos e hábitos para vender serviços e obter lucro (GONÇALVES, 2016).

Outro ponto do art. 7º que vale ressaltar é determinação da exclusão definitiva de dados pessoais após o término da relação entre provedor e usuário, exceto em casos de guarda obrigatória previstos em lei. Ao preconizar isso, o inciso X não enfrenta os reais problemas para colocar isso em prática, isto é, não se importa em regulamentar e fiscalizar tais ações.

Nesse sentindo, segundo Vitor Hugo Gonçalves (2016), não há como saber se os dados realmente foram excluídos de todos os servidores do provedor. Exemplo disso foi o que ocorreu em 2015 com o provedor de internet Snapchat que objetivava uma experiência de registros instantâneos aos usuários. Segundo a revista digital EXAME, ao ser invadido, foi descoberto que as fotos e vídeos dele não eram excluídas e trafegavam em seus servidores indefinidamente. Tal fato foi motivo

de forte repreensão pela Federal Trade Commision (FTC), órgão regulador do governo americano,

Vale ressaltar também um problema que também assola o marco civil: o uso de cookies de internet. De acordo com uma matéria publicada em 2019 no blog Intnet, tal ferramenta tem como função armazenar pequenos arquivos no navegador de internet quando o usuário acessa um site pela primeira vez, bem como notificar o site quando o usuário volta a acessá-lo. Entretanto, além de registrarem a visita de usuários podem também guardar informações importantes sobre eles.

Através da diretiva n º 95/96, o Marco Civil disciplinou o uso de cookies, estabelecendo que o provedor de aplicação informe de forma clara ao usuário que seus dados serão coletados e como eles serão utilizados, exigindo o consentimento do usuário para tal ação. Entretanto, a lei não chegou nem perto de surtir efeito nos sites brasileiros. Desde 2016, inspirada no projeto “Who has your back”? realizado pelos EUA, a instituição brasileira promove anualmente o projeto “Quem defende seus dados?” O estudo tem o objetivo avaliar como os provedores de internet protegem os dados de seus usuários, bem como promover boas práticas relacionadas a proteção da privacidade e de dados.

Figura 1- Índice de estabelecimento de proteção de dados pelas operadoras de telecomunicação no Brasil em 2016

Fonte: disponível em http://quemdefendeseusdados.org.br/pt/. Acesso em 21 set. 2021

Dessa forma, tendo em vista a tabela, embora já existisse uma lei que determinasse tal transparência, as empresas ainda não acatavam tais demandas, deixando assim os usuários à beira da vulnerabilidade. Tais índices só mostram consideráveis melhoras após a Lei de Proteção de Dados que será tema do próximo tópico.

É necessário também falar sobre o sigilo e a inviolabilidade das comunicações, preconizados no art. 10 do marco civil que em consonância com o art. 5º da Constituição federal, estabelece:

> A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Nesse viés, o §1º do art. 10 estipulou como princípio que o acesso de dados pelas autoridades estatais deve ocorrer somente com ordem judicial. Sendo que tal ordem é necessária apenas para o "conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (Lei 12.965/14, art. 4º, VI). Entretanto, o §3º desse mesmo artigo estabelece que:

> O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

Logo, o Marco Civil retirou os dados cadastrais do âmbito da proteção das ordens judicias. Além disso, entende-se como dados cadastrais dos usuários os dados: qualificação pessoal, filiação, endereço. Por serem dados não sensíveis, o marco civil determinou que qualquer autoridade administrativa legalmente competente pode ter acesso a eles sem a necessidade de ordem judicial. Tal fato é de grande preocupação para os usuários, já que as autoridades policiais, o Ministério público, a Receita federal pode requisitar facilmente tais dados.

Outro ponto que foi alvo de críticas, foi o fato do marco civil não ter deixado claro se o IP é ou não um dado cadastral, isto é, um dado não sensível e, logo, desprovido da necessidade de ordem judicial. Em tese, o endereço de IP, assim

como o telefone é apenas um elemento necessário para o usuário se conectar e navegar na internet. Entretanto, entende-se que ele é muito mais do que isso. Vitor Hugo Gonçalves (2016, p. 69) traz essa expõe esse problema:

> Se o usuário estiver num dispositivo móvel, o endereço IP informa onde ele está em todos os momentos. É com base no endereço IP que o usuário troca dados com servidores no mundo todo. E com base no endereço IP que padrões de comportamento (cookies) são traçados e personalizados. Será que, em tempos de big data, o endereço IP é somente um dado cadastral não sensível?

É fato que ao determinar a ordem judicial como medida essencial ao acesso do conteúdo de comunicações privadas, o legislador visa a proteção da privacidade e da intimidade. Logo, tentando assegurar efetivamente, tais direitos, o marco civil também estabeleceu em seu art.12 sansões às empresas que não sigam o determinado nos art. 10 e 11, isto é, que não forneçam tratamento correto aos dados de seus usuários. Os incisos II, III e IV estabelecem respectivamente: multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício, suspensão temporária das atividades e proibição do exercício das atividades.

Entretanto, ainda sim tais incisos são falhos, pois apesar do alto rigor das sanções, o marco civil não esclarece quem será o órgão regulador e fiscalizador, além disso, não se atentou para possíveis conflitos gerados com empresas internacionais que possuem suas próprias diretrizes.

Nesse viés, as decisões judiciais determinadas ao longo desses anos, fundamentadas no art.12, estabeleceram a suspensão temporária em território nacional aplicativo Whatsapp, em decorrência do descumprimento de ordens judiciais que exigiam a apresentação de determinadas informações. Uma das suspensões que mais chamou a atenção da comunidade acadêmica e jurídica foi a proferida pelo juízo da 2º Vara Criminal da Comarca de Duque de Caxias/RJ. Nesse contexto, a juíza fez o requerimento de uma alternativa tecnológica que permitisse o acesso das autoridades competentes às mensagens dos investigados em tempo real. Além disso, determinou a suspensão do aplicativo em todo o território até que a ordem fosse atendida:

> Esta magistrada, no bojo dos autos da investigação criminal em epígrafe, determinou o cumprimento da quebra do sigilo e interceptação telemática das mensagens compartilhadas no aplicativo Whatsapp em relação aos terminais salvos indicados no ofício encaminhado pela d. autoridade policial

> ao Facebook do Brasil, sob pena de aplicação de multa coercitiva diária no valor de R$50.000,00, além de eventual configuração de crime de obstrução à Justiça e suspensão dos serviços até cumprimento da ordem judicial. (...) Em verdade, o Juízo requer, apenas, a desabilitação da chave de criptografia, com a interceptação do fluxo de dados, com o desvio em tempo real em uma das formas sugeridas pelo MP, além do encaminhamento das mensagens já recebidas pelo usuário e ainda não criptografadas, ou seja, as mensagens trocadas deverão ser desviadas em tempo real (na forma que se dá com a interceptação de conversações telefônicas), antes de implementada a criptografia. (RIVAS, 2016)

Em contrapartida, a empresa afirmou como todas as outras vezes, a impossibilidade de cumprir ordens dessa natureza, alegando que tais medidas podem comprometer a própria segurança do sistema. Seu principal argumento é que, com a implementação da criptografia ponta-a-ponta, a empresa não possuiria uma chave mestra para decifrar o conteúdo das mensagens e entregar as informações buscadas pelas autoridades. Quando os usuários estão em comunicação pelo aplicativo, apenas eles mesmos possuiriam as chaves que decifram suas mensagens, o que serve para proteger sua confidencialidade e garantir que a criptografia seja "forte", isto é, inquebrável (ANTONIALLI, CRUZ, et al., 2016).

Após tal episódio, a atitude da juíza foi criticada em vários âmbitos jurídicos. Segundo o criminalista Fernando Augusto Fernandes o bloqueio é uma arbitrariedade e que é necessário impedir tal abuso:

> Nenhum juiz tem o poder de impedir a comunicação de milhares de pessoas que não estão em sua jurisdição, já que não somos réus no processo que preside. O máximo que poderia era arbitrar multa financeira que pode ser revisada pelas instâncias judiciais. É mais um ato em que o Judiciário brasileiro expõe a insegurança jurídica nacional, que é hostil ao empresariado, ao mercado e aos direitos individuais. (Revista Consultor Jurídico, 2016)

Nesse sentido, vale ressaltar o que foi estabelecido no art.13 no Marco Civil: o prestador de serviço de conexão deve manter os registros de conexão dos usuários, sob sigilo, pelo prazo de um ano. Além disso, o art. 15 também estabelece que os provedores de aplicações de internet devem manter os registros de acesso pelo prazo de 6 meses. Lembrando que conforme o art. 10, em ambos os casos, os registros podem ser disponibilizados em caso de ordem judicial. Vale lembrar também, que a lei se refere a dados mínimos como data, hora e IP.

Entretanto, a referida lei, não se posiciona claramente a respeito das comunicações privadas, não impondo assim, um prazo especifico para que os provedores armazenem as mensagens trocadas por usuários. Nesse caso, entende-se que não há obrigatoriedade na guarda dessas comunicações privadas dos usuários, logo tais provedores, mesmo que por ordem judicial, não podem fornecer o que não possuem e nem serem punidos por isso.

Podemos concluir então, que a juíza naquela ocasião, agiu de forma equivocada, uma vez que o WhatsApp não pode ser obrigado a fornecer informações que ele não possui efetivamente sob sua custódia, nem tampouco ser punido por isso.

Vale ressaltar também que, infelizmente, o Brasil possui mais que juristas equivocados, como também um presidente da república que desconhece o valor das leis. De acordo com reportagem fornecida plea CNN, o presidente Jair Bolsonaro assinou no dia neste dia 06/09/2021 uma medida provisória (MP), alterando vários pontos do Marco Civil. O conteúdo da MP dificultava o trabalho de provedores como facebook, Instagram e Youtube, de remover contas, perfis e conteúdos que infrinjam as suas normas. Segundo a Secretaria Especial de Comunicação Social da Presidência da República:

> A alteração objetiva maior clareza quanto a políticas, procedimentos, medidas e instrumentos para cancelamento ou suspensão de conteúdos e contas, exige justa causa e motivação e prevê direito de restituição do conteúdo, alegando liberdade de expressão

Em nota enviada a Tilt, o Youtube (2021) declarou que essa ação do presidente "limita de forma significativa a capacidade de conter abusos nas nossas plataformas, algo fundamental para oferecer às pessoas um espaço seguro de expressão e conexão online”.

Em clara dissonância com a atual situação do país, o presidente optou pela MP após ter tido diversas postagens excluídas ou limitadas pelas redes pelo fato de espalhar desinformação médica sobre o covid-19, fazer apologia a tratamentos não eficazes, incentivar aglomerações e o não uso de máscaras. A situação fica ainda pior tendo em vista que a MP foi editada na véspera das manifestações bolsonaristas de 7 de setembro. Logo, caso aprovada, manteria conteúdos pró-

bolsonaristas de *influencers* nessas redes sociais. Felizmente, o presidente do senado, Rodrigo Pacheco, devolveu ao Planalto tal MP.

Além disso, a aplicação de tal rigor pelas redes sociais em questão, tem a ver também não apenas com o estado da saúde pública, mas também com diversos problemas envolvendo fake news, como ocorreu no ano anterior às eleições presidenciais.

Nesse sentido fica claro que além de legislações realmente eficazes é necessário a evolução da mentalidade jurídica e executiva deste país.

3.3 LEI 13.709, DE AGOSTO DE 2018 (LEI GERAL DE PROTEÇÃO DE DADOS)

A Lei Geral de Proteção de Dados surgiu no cenário a fim de complementar todas as leis setoriais de proteção de dados que já existiam, mas que não eram efetivas em uma sociedade cada vez mais movidas por dados. Segundo a norma, a LGPD tem como objetivo versar sobre o tratamento de dados pessoais (dados de pessoas naturais), independentemente de ser no âmbito digital ou físico. A Lei ampara todos os setores da economia e não somente o setor da tecnologia e de internet. Nesse sentido, setores como o da saúde, alimentação, automobilístico, varejo deverão manusear os dados de seus consumidores tendo como base a LGPD. Assim, a Lei consegue fornecer segurança jurídica ao cidadão, ao setor privado e ao setor estatal, bem como regular efetivamente o uso de dados e ser uma alavanca para o desenvolvimento econômico e tecnológico do país.

Um dos pontos cruciais para a ineficácia das legislações anteriores, assim como para a descredibilidade internacional delas, é a ausência de uma entidade reguladora e fiscalizadora, sendo assim um dos principais aspectos positivos da LGPD foi exatamente a criação desse órgão.

Em meio a várias consultas públicas e a muita polêmica entre o setor privado e público, construiu-se o art.55 cujo conteúdo determinou a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração público federal. A redação desse artigo aposta em um processo equilibrado, isto é, um meio termo entre o monopólio da fiscalização estatal ou uma regulação puramente

privada. Logo, a LGPD estabelece que a ANPD deve cooperar com outros órgãos reguladores a fim de que se atinja um sistema de fiscalização em rede, em que se tenha elementos privados e públicos. Vale ressaltar que desde seu projeto até o seu conteúdo, a lei contém aspectos multissetoriais, sendo tal estratégia, um deles.

Além disso, outro órgão criado pela LGPD, através do art.56 e que merece destaque, é o Conselho Nacional de Proteção de Dados (CNPD). Ele também obedece à teoria multissetorial e consiste em uma entidade consultiva que tem o poder de propor diretrizes, sugerir ações a serem realizadas pela ANPD, bem como elaborar relatórios anuais de ações da LGPD realizadas pela ANPD.

Nesse ponto do trabalho, deve-se destacar a criação do decreto 9.854/19 que instituiu o Plano Nacional de Internet das Coisas (IoT) que tem o objetivo de implementar e desenvolver a Internet das Coisas no país. Segundo a Oracle, empresa gerenciadora de cadeia de suprimentos:

> A Internet das Coisas (IoT) descreve a rede de - “objetos físicos” - incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas [...] Por meio da computação de baixo custo, nuvem, big data, análise avançada e tecnologias móveis, coisas físicas podem compartilhar e coletar dados com o mínimo de intervenção humana. Nesse mundo hiperconectado, os sistemas digitais podem gravar, monitorar e ajustar cada interação entre itens conectados. O mundo físico encontra o mundo digital - e eles cooperam.

Segundo muitos estudiosos do meio jurídico e econômico, a IoT é uma estratégia certeira para o desenvolvimento econômico do país. Sendo que a estratégia é que os objetos ao nosso redor se tornem sensores que monitoram todas as nossas atividades para a elas agregar inteligência. Entretanto, falando assim, a preocupação com relação a privacidade e a intimidade, tão discutidas no tópico anterior, é latente e inevitável. Principalmente, tendo em vista que um grande índice de cybercrimes se configuram através do aproveitamento de falhas de segurança em dispositivos de IoT.

Nesse sentido, a uso generalizado das tecnologias de IoT potencializam os riscos de violação de dados pessoais sensíveis. Logo, para Bruno Bioni, a proteção de dados pessoais é uma questão estratégica e indissociável do Plano Nacional de IoT. Para ele, o Plano Nacional de IoT, ao contrário de arriscado, é uma

oportunidade para o Brasil encapar uma nova estratégia regulatória e firme através da LGPD.

O autor também afirma que no Brasil permanece com uma mentalidade regulatória meramente punitiva para a proteção de dados pessoais. Um exemplo disso seria a multa de R$3,5 milhões aplicada a empresa “Oi” por não informar de forma adequada os dados pessoais de seus consumidores. É claro que a punição deve existir, porém uma alternativa anos luz mais eficaz seria prevenir, incentivando práticas responsáveis do uso de dados.

> Por que não combinar medidas de incentivo a comportamentos desejáveis, ao invés de somente punir práticas reprováveis? Isso seria capaz de desencadear um movimento de regulação de baixo para cima (bottow-up) e não só de cima para baixo (top-down). O direito ambiental já tem feito isso ao incentivar tecnologias menos poluentes, as quais têm isenções ou benefícios tributários. É o que o jurista italiano Noberto Bobbio professava ao dizer que o direito deve incentivar boas práticas por meio de normas premiais. O mesmo poderia ser feito com tecnologias que tivessem como valor de concepção a proteção à privacidade, metodologia comumente chamada de “privacy by design”, em que o projeto de um produto ou serviço é orientado por soluções tecnológicas que sejam pró-privacidade. Por que também não conceder vantagens fiscais para aqueles sensores de IoT concebidos com esse tipo de preocupação? Não seria o caso da privacy by design ser uma condicionante imposta pelo BNDES para o financiamento de empresas nascentes de tecnologia? Essa estratégia regulatória poderia ter vários desencadeamentos. Um deles, talvez o principal, é que a proteção de dados pessoais passaria a ser encarada como um elemento de competividade e vantagem econômica. Os atores regulados seriam induzidos a cooperarem com o órgão regulador, dando ensejo a um movimento de corregulação (BRUNO BIONI, 2019)

Vale ressaltar que LGPD estabelece que toda empresa deve conhecer os dados que armazena, bem como, convertê-los em informações úteis para o progresso de atividades econômicas e para as relações sociais. Logo, a lei determina que qualquer atividade que envolva tratamento de dados deve ter uma finalidade, sendo que após o objetivo ter siso alcançado, tais dados devem ser descartados.

A lei estabelece, ainda, que o titular dos dados coletados, deve ter conhecimento da finalidade do uso de seus dados. Dessa forma, se estabelece a autodeterminação informativa, ou seja, o direito de o titular dos dados pessoais ter controle sobre como, quando e onde serão tratados seus dados, bem como ter o conhecimento de quem será o responsável pelo tratamento. Assim, as organizações

devem informar adequadamente e obter o consentimento do usuário para o tratamento de seus dados.

Vale ressaltar que a LGPD, no art. 5º também deu atenção especial ao os dados sensíveis, isto é, aqueles relacionados a preferências políticas e sexuais, religião, hábitos, raça ou etnia, entre outros. Tais dados devem ser tratados com ainda mais cautela e cuidado pelas empresas.

A LGPD também define o que são controladores e processadores. O processador, ou seja, o terceirizado, deve realizar o tratamento de dados de acordo com as instruções do controlador, ou seja, do gestor da cadeia de tratamento de dados. O controlador deve indicar o encarregado pelo tratamento de dados. Nesse caso, se houver algum problema causado pelo processador, o gestor pode ser acionado diretamente para fazer o reparo. Logo, obriga-se que controladores contratem apenas processadores que seguiam à risca as normas de proteção de dados. Tal estratégia, segundo Bruno Bioni (2020), cria um vínculo de solidariedade entre o controlador e o processador, fazendo com que tais agentes automaticamente fiscalizem uns aos outros e excluam aqueles que não se adaptaram. Dessa forma, quem estiver de acordo com as regras, obtém uma vantagem competitiva frente aos outros e, consequentemente, a valorização de seus serviços e produtos.

O autor complementa fazendo uma analogia:

> Em resumo, usando um exemplo mais próximo do leitor em geral e que costumo recorrer em sala de aula, é o da arrumação de um guarda-roupa. Enquanto essa atividade era executada apenas em virtude da pressão de um castigo a ser imposto pelos nossos pais e mães, a arrumação era algo burocrático e que raramente se extraía valor dela. Diferentemente por parte de quem, a curto, médio ou longo prazo, internalizou a tarefa de forma engajada e organizou cuidadosamente as roupas – os dados, transformando-as em informações que otimizaram o processo de tomada de decisão – se preferir os custos de transação – quanto à vestimenta mais apropriada para as diversas ocasiões do dia a dia. Uma organização que não enxerga valor no processo de conformidade regulatória da LGPD, é como se fosse uma pessoa adulta com um armário desorganizado que, cedo ou tarde, se atrasará para uma reunião ou nela chegará malvestida e terá perdas financeiras e reputacionais (BRUNO BIONI, 2020).

É importante salientar também, que para justificar e autorizar as empresas a utilizarem dados pessoais, deve-se considerar determinadas bases legais.

A LGPD prevê dez bases legais: consentimento, cumprimento de obrigação legal ou regulatória, execução de políticas públicas, estudos e pesquisa, execução de contrato, exercício regular de direitos, proteção da vida, tutela da saúde, legítimo interesse e proteção de crédito.

Uma das principais bases legais abordadas pelo âmbito acadêmico e jurídico é o legítimo interesse, já que de acordo com ele, os dados pessoais podem ser tratados quando necessários para atender aos interesses legítimos do controlador ou de terceiros, desde que tal prática não exceda os direitos e liberdades fundamentais do usuário titular.

Dessa forma, as empresas devem estar aptas para justificar a qualquer momento para as autoridades fiscalizadoras a utilização de dados. Logo, há o consequente aumento da responsabilidade no uso desses dados pelas empresas.

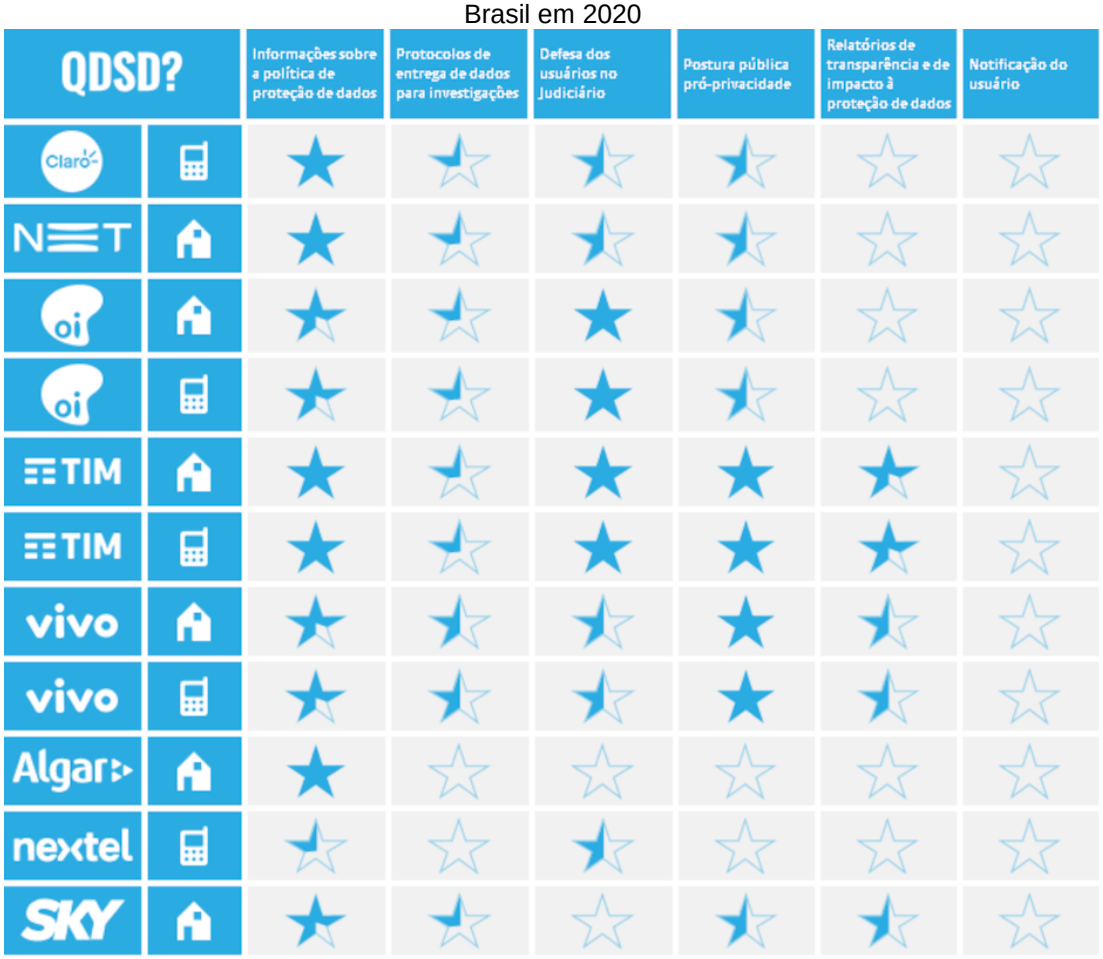
Vale ressaltar também que a ANPD pode requisitar ao controlador o relatório de impacto à proteção de dados pessoais, tornando assim, cada vez mais difícil o uso abusivo de tais dados pelas organizações.

É evidente, portanto, que a LGPD trouxe maior e rigor à proteção de dados pessoais, da privacidade e da intimidade, sendo também não apenas uma norma reguladora do tratamento de dados, mas também uma janela de oportunidade econômica e tecnológica para o Brasil.

Tudo isso pode ser observado através da comparação entre a pesquisa realizada pela InternetLab em 2016, exposta no subcapítulo anterior, e o levantamento realizado em 2020, 2 meses após a entrada em vigor da LGPD.

A quinta edição do projeto “Quem defende seus dados?” (2021) deixou claro a evolução das empresas em relação às políticas de privacidade de seus clientes e à adoção de práticas transparentes. Segue a tabela:

Figura 2 - Índice de estabelecimento de proteção de dados pelas operadoras de telecomunicação no Brasil em 2020



Fonte: disponível em: http://quemdefendeseusdados.org.br/pt/. Acesso em 21 set 2021.

Segundo Nathalie Fragoso (2020), coordenadora da área de Privacidade e Segurança do InternetLab:

> Os pesquisadores envolvidos no estudo observaram também o engajamento de algumas operadoras no judiciário em defesa da privacidade de usuários, seja diante de pedidos abusivos ou genéricos de dados, ou contestando normas que fragilizam a proteção à privacidade no Brasil. Uma tendência geral é a melhora no conteúdo e na forma das políticas de proteção de dados e privacidade. Estão mais completas, mais claras, mais acessíveis. Isso, certamente, está relacionado à entrada em vigor da Lei Geral de Proteção de Dados há poucos meses. (InternetLab, 2020)

Nesse sentido, é evidente que a LGPD trouxe diversos avanços e preencheu diversos espaços, tendo assim, um papel importante tanto no âmbito jurídico, quanto econômico.

CONCLUSÃO

A internet, indubitavelmente, surgiu com a finalidade de proporcionar comunicações e relações interpessoais mais seguras. Entretanto, ao longo dos anos, além de um grande avanço também se tornou uma grande ameaça à privacidade e à intimidade de seus usuários que passaram a ser vítimas dos famosos cybercrimes.

A globalização tecnológica foi e ainda é um fenômeno de crescimento imensurável, onde a sistematização dos serviços e dados tanto da iniciativa privada, quanto da iniciativa pública estão transigindo para o meio digital, tendo em vista o fornecimento de um serviço prático e a rápido aos usuários, principalmente no cenário atual de pandemia, na qual houve uma necessidade ainda maior de tal transição ao uso da internet e dos sistemas eletrônicos.

Com isso, uma infinidade de dados e informações pessoais estão armazenadas nos “HD’s” do meio digital, muitas vezes em sites e banco de dados de prestadores de serviços que não estabelecem nenhum plano de ação ou diretriz de proteção de dados, facilitando a coleta ilegal dessas informações pelos cybercriminosos.

Logo, surgiu a necessidade de tipificar penalmente tais crimes, já que os criminosos quase sempre estavam protegidos pelo anonimato e quase nunca eram identificados e quando eram, o judiciário pecava na demora ao punir tais condutas.

Nesse viés, ao analisar a evolução das legislações que amparam tais crimes, percebemos a dificuldade do âmbito jurídico em se adaptar a essa nova era. Várias lacunas e omissões foram identificadas em tais Leis, principalmente na definição das redações das condutas típicas, não deixando claro quais os atos, meios e bens jurídicos protegidos, consumam e caracterizam tal cibernético.

Além dos crimes, as Legislações deixaram de se atentar a regulamentação dos meios de segurança de tais dados, onde há previsão de princípios e garantias. Assim, deixam de apresentar normas infralegais explicativas, para dirimir tais dúvidas daqueles que aplicam as medidas punitivas. Além disso, a previsão de um Órgão Fiscalizador só veio com a vigência da LGPG/2018, prevendo a modulação de efeitos somente para 2021.

Ou seja, levaram 3 anos para a instauração de um órgão fiscalizador e para definição de condutas de proteção de dados as empresas detentoras de dados pessoais coletados, e suas respectivas sanções. De certa forma, foram 3 longos anos de dados indiretamente divulgados, em virtude da não observação das diretrizes de segurança.

REFERÊNCIAS

A HISTÓRIA DOS COMPUTADORES E DA COMPUTAÇÃO. TECMUNDO, 2009. Disponível em: https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm Acesso em: 02/09/2021.

BARROS, Marco Antonio. *Tutela Punitiva Tecnológica*. In: O Direito na Sociedade da Informação, São Paulo: Atlas, 2007.

BRASIL É O SEGUNDO PAÍS NO MUNDO COM O MAIOR NÚMERO DE CRIMES CIBERNÉTICOS. UOL. 2018. Disponível em https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 13/09/202

CARDOSO, André Guskrow. IoT – Internet das Coisas – O Decreto 9.854 e o Plano Nacional IoT. Migalhas, 2019.

CARNEIRO, Adeneele Garcia. Crimes Virtuais: Elementos para uma reflexão sobre o problema na Tipificação. Postado em 2012. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-elementos-para-umareflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o>

Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'. G1 GLOBO. 2012. Disponível em: http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html. Acesso em 05/09/2021.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e seus Aspectos Processuais*. 2. ed. Rio de Janeiro: Lumen Juris, 2003. https://www.migalhas.com.br/depeso/306003/iot---internet-das-coisas---o-decreto-9-854-e-o-plano-nacional-de-iot Acesso em: 18/09/2021

FERREIRA, Érica Lourenço de Lima. *Internet: macrocriminalidade e jurisdição internacional*. 1. ed. (ano 2007), 1ª reimpr. Curitiba: Juruá, 2010.

FILHO, Eduardo Tomasevicius. Marco Civil da Internet: uma lei sem conteúdo normativo. Disponível em:< https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=html&lang=pt > Acesso em: 14 set. 2021

FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos Relevantes.2 v. São Paulo: Quartier Latin, 2008.

FRANÇA, Misael Neto Bispo da. **Crimes informáticos e lei "Carolina Dieckmann": mais do mesmo no direito penal contemporâneo.** In: Revista Jurídica Consulex, v. 27, n. 39, p.3-5, set./2013.

LISBOA, Roberto Senise. *Quebra da Inviolabilidade de Correspondência Eletrônica por Violação da Boa-fé Objetiva*. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.) Direito & Internet: Aspectos Jurídicos Relevantes. São Paulo: Quartier Latin, 2005.

LIRA, Leide de Almeida. **Lei Carolina Dieckmann: (in)eficácia na proteção dos direitos fundamentais à intimidade e à vida privada em face da pena cominada aos delitos informáticos.** Conteúdo Jurídico, Brasília- DF: 01 jul.2014. Disponível em: < file:///C:/Users/Usu%C3%A1rio/OneDrive/%C3%81rea%20de%20Trabalho/Lei%20Carolina%20Dieckmann%20(Leide%20de%20Almeida).pdf > Acesso em: 13 set.2021

MACHADO, Lucyana A. *A consciência digital, independente de idade, é o caminho mais seguro para o bom uso da internet, sujeita às mesmas regras de ética, educação e respeito ao próximo.* 2014. Disponível em: https://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos Acessado em: 28/09/2020.

MAIA, Mateus. Pacheco devolve ao Planalto MP que alterava Marco Civil da Internet. Poder 360, 2021. Disponível em: https://www.poder360.com.br/congresso/pacheco-devolve-mp-que-alterou-marco-civil-da-internet-ao-planalto/. Acesso em: 22/09/2021.

Mari, João de. Pacheco devolve ao Planalto MP de Bolsonaro que alterou Marco Civil da Internet. CNN, 2021. Disponível em : https://www.cnnbrasil.com.br/politica/pacheco-devolve-ao-planalto-mp-de-bolsonaro-que-alterava-marco-civil-da-internet/ Acesso em: 22/09/2021.

MENDES, Maria Eugênia Gonçalves. VIEIRA, Natália Borges. *Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade da legislação específica*. 2012. Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2"2. Acessado em: 28/09/2020.

MORAIS, Carlos Tadeu Queiroz de; LIMA, José Valdeni de; FRANCO Sérgio R. K. Conceitos sobre Internet e Web – Porto Alegre: Editora da UFRGS, 2012.

NETO, Pedro Américo de Souza. *Crimes de Informática*. 2009. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro de Ciências Sociais e Jurídicas - CEJURPS, Universidade do Vale do Itajaí, Itajaí, 2009. Disponível em:http://siaibib01.univali.br/pdf/Pedro%20Americo%20de%20Souza%20Neto.pdf Acessado em: 29/09/2020.

O que é o IOT. Oracle, 2020.Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/ Acesso em: 22/09/2020.

Relatório mostra melhor desempenho de operadoras em proteção de dados de usuários em 2020. InternetLab, 2020. Disponível em: internetlab.org.br/pt/privacidade-e-vigilancia/quem-defende-seus-dados-relatorio-aponta-avanco-de-operadoras-em-transparencia/ Acesso em 20/09/2020.

ROSA, Fabrízio. *Crimes de Informática*. 2.ed. Campinas: Bookseller, 2006.

ROHR, ALTIERES. Localização de endereço de IP: entenda como pode ser feito o rastreamento e o que é mito. G1 GLOBO. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/03/02/localizacao-de-endereco-de-ip-entenda-como-pode-ser-feito-o-rastreamento-e-o-que-e-mito.ghtml Acesso em: 10/09/2021

SCHMIDT, Guilherme. CRIMES CIBERNÉTICOS. JUSBRASIL.2016. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em 13/09/2021.

SÓ PEDAGOGIA. *Ciberespaço e Cibercultura: Definições e Realidades Virtuais Inseridas na Práxis do Homem Moderno*. Virtuous Tecnologia da Informação, 2008-2020. Disponível em <http://www.pedagogia.com.br/artigos/ciberespaco_cibercultura/?pagina=1>. Acessado em 29/11/2020.

TECMUNDO. *A história dos computadores e da computação.* 2009. Disponível em<https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>*.* Acessado em 29/11/2020.

UGALDE, Júlio Cesar Rodrigues. Crimes Cibernéticos: Considerações sobre a criminalidade na internet. Âmbito Jurídico. 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/amp/. Acesso em: 15/08/202

ZANINI, Leonardo Estevam. **Responsabilidade civil dos provedores de Internet e a proteção da imagem.** Revista de Doutrina TRF4, 2017. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao080/Leonardo_Zanini.html

ZAPAROLI, Rodrigo Alves. **Comentários à Lei nº12.737/12**. Disponível em: < https://www.jurisway.org.br/v2/dhall.asp?id_dh=10576 > . Acesso em: 13 set. 2021