PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIRETO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO AJUNTA DE TRABALHO DE CURSO

ARTÍGO CIENTÍFICO

DIREITO DIGITAL

CRIMES CIBERNÉTICOS E MARCO CIVL DA INTERNET

ORIENTANDO: MATEUS RAMOS DE MELO

ORIENTADORA: PROFª. Mª. ROBERTA CRISTINA DE M.SIQUEIRA

GOIÂNIA
2020

MATEUS RAMOS DE MELO

DIREITO DIGITAL

CRIMES CIBERNÉTICOS E MARCO CIVIL DA INTERNET

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Profª Orientadora. Mª. Roberta de Cristina de M. Siqueira

GOIÂNIA
2020

MATEUS RAMOS DE MELO

DIREITO DIGITAL

CRIMES CIBERNÉTICOS E MARCO CIVIL DA INTERNET

Data da Defesa: 02 de dezembro de 2020

BANCA EXAMINADORA

_____

Orientadora: Prof. Mª. Roberta Cristina de M. Siqueira Nota

_____

Examinadora Convidada: Prof. Millene Baldy De Sant Anna Braga Grifford Nota

Dedicatória

Este trabalho é dedicado primeiramente a Deus, que me concedeu estar vivo e bem neste momento para continuar esse caminho da vida. A minha família que me ajudou por toda essa jornada, os períodos adversos que passei durante esses anos na faculdade de direito, meu pai Amir Vieira de Melo, minha mãe Vera Lara Ramos de Melo e minha irmã Maísa Ramos de Melo foram os pivôs por eu seguir firme e forte com desejo e sede de vencer essa batalha que é a vida.

Agradecimentos

Quero também agradecer a todos os professores que com muito amor e carinho pela profissão de professor e da área do direito brilhantemente lecionaram aulas de muito aprendizado e inspiraram muitos alunos como eu a amar mais ainda o direito, e que continuarão a inspirar muitos outros que terão a honra de serem seus alunos e meu destaque vai para a orientadora Roberta Cristina De Morais Siqueira pela complacência e esmero na elaboração deste TCC.

SUMÁRIO

DIREITO DIGITAL

CRIMES CIBERNÉTICOS E MARCO CIVIL DA INTERNET

Mateus Ramos de Melo[1]

RESUMO

O presente artigo científico tem o objetivo do debate do crescimento do direito digital no Brasil e no mundo que é o ramo do direito que rege as relações no âmbito virtual. Com o crescimento do uso da internet naturalmente crimes são cometidos diariamente e a tendência é só aumentar devido ao uso diário de praticamente todas as pessoas e empresas ao redor do mundo. Mostrando a evolução desse direito em nossa vidas, dos crimes cibernéticos que fazem milhões de vítimas diariamente e como está sendo o lado legislativo, pois muitas pessoas que usam seus celulares e computadores na área da informática não é para fins legais. Existem pessoas que estão ali para apenas invadir contas bancárias, roubar informações sigilosas de empresas, ou exclusivamente, usar inadequadamente informações pessoais de outros Nosso intuito é demonstrar a importância desse novo ramo do direito e como ele tem impactado as relações sociais.

Palavras-chave: Direito digital, marco civil da internet, crimes cibernéticos.

INTRODUÇÃO

A evolução humana é marcada por avanços em incontáveis áreas, A tecnologia permitiu a facilitação da vida em inúmeros aspectos para as pessoas, em ambiente de trabalho, no lazer e relação com os outros. Nessa questão se faz necessário, conhecer e adiantar os próximos passos dessas mesmas tecnologias.

Apesar de inúmeros benefícios que esse avanço do mesmo modo trazendo certas inconveniências para seus usuários, que acabam colocando em risco seus direitos e sua dignidade. Desse modo o direito digital surgiu, sendo uma forma de tentar punir os responsáveis e garantir a segurança no ambiente digital.

O direito digital decorre da união e relação de outras duas disciplinas de conhecimento. Direito e ciência da computação, essa última abordando as diversas regras, aplicações e relações em âmbito jurídico proveniente do mundo virtual.

No âmbito digital é disponibilizado acesso a uma enorme gama de informações e possibilidades de desenvolvimento, mas ao mesmo tempo podem acarretar na ocorrência de inúmeros delitos onde os agentes que os praticam contam com certo anonimato. Assim, surge o questionamento de até que o ponto se pode demandar a identificação de quem utiliza o ambiente digital e como resolver e punir crimes que ocorrem no âmbito digital.

1 DIREITO DIGITAL

1.1 EVOLUÇÃO DO DIREITO DIGITAL NO MUNDO

Em um mundo cada dia mais conectado, o direito digital é uma necessidade para os advogados.

> O Direito Digital ou Direito Informático é o conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador - como meio e como fim - que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do *software*; o comércio eletrônico e as relações humanas estabelecidas viam Internet (PAIVA, 2019, p 18).

Afinal, todos nós já ouvimos falar em “mundo digital”. Às vezes, o termo é utilizado apenas para fazer objeção ao “mundo real”. É claro que as interações *online* e *offline* acontecem todas no mesmo local. Mas chamar o ambiente virtual de “mundo” é bastante necessário.

> O virtual permite a existência legítima do estar “não-presente”. Do manifestar-se por intermédio de sistemas de comunicação telemática através de encontros móveis e transitórios de mensagens, com a desconexão em relação a um meio particular, com diversos meios de registro e transmissão oral, escrita e audiovisual em redes digitais. (PECK, Patrícia 2009, p 17).

O uso dessa palavra advém porque, na internet, as coisas sucedem de maneira diferente, e na maioria das vezes o direito convencional não é suficiente. Conforme o avanço da tecnologia, surgem novos questionamentos morais que precisam ser resolvidos nas áreas legislativa e judiciária. A área do direito digital decorre da relação e união de outras duas disciplinas de conhecimento: Direito

e a Ciência da Computação. Versam as diversas regras, aplicações e relações em âmbito jurídico proveniente do mundo virtual.

> A palavra virtual vem do latim medieval virtualis, derivado por sua vez de virtus, força, potência. Na filosofia escolástica, é virtual o que existe em potência e não em ato. O virtual tende a atualizar-se, sem ter passado, no entanto, à concretização efetiva ou formal. A árvore está virtualmente presente na semente. O virtual é o real, em sua característica potencial de ser atual. Em termos rigorosamente filosóficos, o virtual não se opõe ao real, mas ao atual: virtualidade e atualidade são apenas duas maneiras de ser diferente. (LEVY, Pierre 1996, p 15).

Essas mudanças acontecem de maneira rápida, outras áreas também têm influência e até necessidade da situação atuais do mundo que vivemos, em que quanto mais cedo as coisas acontecerem melhor é. Isso é evidente para os especialista no âmbito do direito e da computação.

O direito digital abrange todas essa áreas do direito.

> O Direito Digital possui todas as características para ser considerado uma disciplina autônoma, justificando a sua posição através de três argumentos: possui um objeto delimitado, qual seja a própria tecnologia, dividido em duas partes, sendo a primeira o objeto mediato, ou seja, a informação, e o segundo o objeto imediato, ou a tecnologia; a existência de uma metodologia própria, a qual visa possibilitar uma melhor compreensão dos problemas derivados da constante utilização das novas tecnologias da informação (informática) e da comunicação (telemática); tal tarefa se realiza mediante o uso de um conjunto de conceitos e normas que possibilitam a resolução dos problemas emanados da aplicação das novas tecnologias às atividades humanas; a existência de fontes próprias, ou seja, fontes legislativas, jurisprudenciais e doutrinárias; não havendo como negar a existência dessas fontes no âmbito do Direito Digital; foi justamente a existência de ditas fontes que possibilitaram, em um grande número de 8 países, principalmente os mais desenvolvidos, a criação da disciplina do Direito Digital nos meios acadêmicos (ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009. p, 9-10).

Essa velocidade de metamorfose, existe uma contínua defendendo o direito digital com sendo um ramo de direito autossuficiente, soberano, tanto quanto as outras áreas do direito que estão presentes no nosso cotidiano como o direito penal, direito civil, direito tributário, direito do trabalho, entre outros.

O alerta com questões relacionadas com crimes na tecnologia da informação e sua classificação no âmbito jurídico vem sendo monitorados a muitos anos. O primeiro país a punir penalmente crimes de rede de computadores foram os Estados Unidos da América.

2 CRIMES CIBERNÉTICOS

2.1 CONCEITO DE CRIME CIBERNÉTICO

Crime cibernético é uma atividade criminosa que o alvo usa ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Na maioria desses crimes cibernéticos são *ciber* criminosos ou *hackers* que buscam adquirir dinheiro. O crime cibernético é realizado por pessoas ou organizações. Para Feliciano crime cibernético é:

> Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que tem por objeto material ou meio de execução o objeto tecnológico informático (2000 p, 13).

Os crimes cibernéticos são, assim como os crimes comuns, condutar típicas, antijurídicas e culpáveis, porém praticadas contra ou com a utilização dos sistemas de informática. Para a OECD – *Organization for Economic Cooperation and Development* (Organização para a cooperação Econômica e Desenvolvimento) da ONU crime de computador é qualquer comportamento ilegal, aético, ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados.

> O conceito de delito informático poderia ser tralhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele,

> e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI 2004, p 110).

Essas organizações usam técnicas avançadas e são muito bem preparadas em termos técnicos. São raros os casos em que o objetivo é danificar os computadores que não seja o lucro. Os motivos nesses casos são pessoais ou políticos.

Os crimes cibernéticos são praticados das mais diversas formas, é importante destacar que os crimes e contravenções penais são compreendidos tanto pelas práticas na internet, quanto pelos sistemas informáticos, pois estes se difundem em ambiente virtual, o qual está repleto de usuários mal-intencionados, que seu objetivo é ter uma oportunidade para o cometimento de atos ilícitos.

> Crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através de computador. Inclui-se nesse conceito os delitos praticados através da internet, pois pressuposto para acessar a rede é a utilização de um computador (Castro 2001, p 9)

Há diversas formas e espécies de cometimento de um crime cibernético, Colares nos ensina que:

> Crime contra a segurança nacional, preconceito, discriminação de raça-cor e etnias, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, dano, apropriação indébita, estelionato, violação de direito autora, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso. Falsa identidade, inserção de dados em sistema de informações. Falso testemunho, exercício arbitrário da próprias razões e jogo de azar (2002, p 02).

Os crimes cibernéticos cometidos em ambiente virtual possuem uma lista extensa e com a universalização da internet, sua prática aumentou em proporções nunca antes vista.

2.2 PRINCIPAIS CONDUTAS CRIMINOSAS CIBERNÉTICAS

Os crimes mais comuns que acontecem diariamente são por fraude de e-mail; pela internet; fraude de identidades; quando informações pessoais são roubadas e usadas. Roubo de dados financeiros ou relacionados a pagamento de cartões; roubo e venda de dados corporativos; extorsão cibernética que exige dinheiro para impedir o ataque ameaçado. Ataques de *ransomware*; um tipo de extorsão cibernética. Espionagem cibernética, é quando hackers acessam dados do governo ou de uma empresa.

A maioria desses crimes são enquadrados em duas categorias. Atividade criminosa que visa computadores e atividade criminosa que usa computadores para cometer outros crimes. Esse último visa na grande parte das vezes infectar computadores com vírus e *malware* para danificar serviços ou impedi-los de funcionar. Também são usados para roubar e excluir dados.

O anonimato é um dos principais pontos dos crimes cibernéticos, tendo em vista que o meio virtual possibilita que o sujeito crie ou transforme sua identidade conforme bem quiser. As formas mais comuns de chegar a esse infrator é pelo número do IP (*Internet Protocol*) seria algo parecido como o R.G do computador. Para a instauração de um inquérito policial é necessário evidência concreta de autoria. Com relação desse assunto, Malaquias entende que:

> O Estado não pode estigmatizar o indivíduo alcançar pessoas abstratas com meras inferências. A perfeita identificação do autor e a correta delimitação da infração cometida são essenciais para se punir o criminoso virtual principalmente, quando se considera o ambiente virtual em que o crime foi praticado, caracterizado pela ausência da presença física do infrator (MALAQUIAS, Roberto Antônio Darós, 2015 p 12).

A identidade virtual constitui um tema de suma importância. Entretanto, a ausência de normas especificas abre precedentes para diversos posicionamentos sobre o assunto por parte do judiciário. Cabe ao legislador especificar formas eficientes e eficazes na procura pelo sujeito infrator, resultando, na mesma análise sobre a insuficiência de uma legislação própria para tratar dos crimes cibernéticos.

2.1 APLICAÇÃO DA LEI NOS CRIMES CIBERNÉTICOS

Na Polícia Civil, já há focos especializados no combate ao ciber crime espalhados pelo Brasil. Um exemplo de aplicação do direito legal no viés legislativo é a criação da Lei nº 12.737/2012, que ficou conhecida como Lei Carolina Dieckmann.

A lei adiciona o artigo 154-A ao Código Penal, criando um tipo penal que criminaliza a invasão de dispositivo informático alheio a fim de obter, adulterar ou destruir dados ou informações sem autorização do titular. O nome da lei é de uma famosa atriz que foi vítima de crime cibernético e tornou o caso público, corroborando à aprovação da lei.

Em 2012, a atriz teve fotos íntimas furtadas por hackers, que demandaram determinada quantia em dinheiro para não as divulgar na rede. Ela não cedeu à tentativa de extorsão e as fotos se tornaram públicas.

Crimes semelhantes já vinham acontecendo há anos, e continuam acontecendo com pessoas comuns, causando prejuízos inimagináveis para os envolvidos.

> Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionavam virtualmente, além de lhes restringira capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade (NUNES, Bittencourt Rodolfo, 2016. p 18)

Repare que esse é um caso diferente de roubo ou furto padronizado, em que o meliante deve estar presente para cometer o roubo de um pertence material da vítima. Imagens de um computador ou celular não podem ser pegas na mão, mas os dispositivos podem ser invadidos à distância.

Por conta dessas peculiaridades, os legisladores acharam por bem criar uma descrição específica de delito no qual condutas desse tipo pudessem ser enquadradas.

A pena para o crime de invasão de dispositivo informático é de três meses a um ano de detenção e multa (com agravantes) ou seis meses a dois anos de reclusão e multa em situações mais graves (também com possíveis agravantes que aumentam a pena). Outro exemplo maior de lei criada para uma maior adequação da legislação brasileira à realidade de um mundo cada vez mais conectado é o Marco Civil da Internet.

Não faltam exemplos também de aplicação do direito digital pelo outro viés, da aplicação de normas já consolidadas nas leis do país. Talvez os exemplos mais comuns sejam crimes de calúnia, difamação, injúria ou ameaça, praticados em e-mails, redes sociais e aplicativos como o *WhatsApp*.

Existem questões no direito do consumidor (compras feitas online), direito do trabalho (verificação de e-mails fora do horário de trabalho), direito de família (infidelidade via sites de aplicativos de relacionamento) e outros.

> Outra vantagem importante é a redução de custos, pois quanto mais simples for a relação comercial, maior a chance de êxito, o que gera uma queda nos custos de transação e com isso, queda nos preços (FERNANDES 2012, p 19).

E há também várias situações em que se fica no meio disso, quando a ausência de uma lei específica suscita dúvidas sobre qual o enquadramento legal adequado e motiva a discussão sobre a necessidade de regulamentar a questão.

A briga dos taxistas é o melhor exemplo que temos atualmente no âmbito digital, que precisam de licença especial e obedecem a uma série de regras municipais para operarem, contra o *Uber*. Em várias cidades do país, o impasse motivou a aprovação de leis para regulamentar o funcionamento do aplicativo, incluindo dispositivo federal, como a Lei 13.640/2018.

Frequentemente, dificuldades envolvendo o direito digital chegaram a um dos órgãos máximos do sistema judiciário brasileiro: o Superior Tribunal de Justiça (STJ). Em relação aos e-mails o STJ já decidiu sobre a responsabilidade

de um provedor de correio eletrônico que não revela dados de usuários que transmitem mensagens ofensivas por e-mail, inocentando a empresa de tecnologia.

Em outro caso, decidiu que o conteúdo de e-mails pode ser usado como prova para fundamentar uma ação de cobrança de dívida.

O número de crimes perpetrados na rede e em computadores cresceu desenfreadamente com o passar do tempo, fraudes, golpes dentre diversos outros atos ilícitos se proliferaram de uma forma que podem afetar milhares de usuários, por isso surge a necessidade da criação de leis especificas para o combate dos mesmos.

3 MARCO CIVIL NA INTERNET

3.1 CONCEITUAÇÃO E LEGISLAÇÃO DO MARCO CIVIL DA INTERNET

É uma legislação que inovou vários aspectos da regulamentação das práticas das empresas relacionadas ao ambiente digital. A partir do crescimento dos *e-commerces* e do crescimento e da existência virtual nas empresas.

A lei que regula o uso da internet no Brasil por princípios e previsão e garantias, direitos e deveres para quem usa a rede, bem como da determinação de indicação para a atuação do Estado.

> O caráter global da internet e a ausência de um domínio único sobre suas dimensões impõem acerca dos efeitos do mundo virtual na vida real de usuários. Nesse sentido, ressalta-se o equívoco da afirmação de que a internet seria o meio livre e irrestrita circulação de informações, onde qualquer espécie de restrição ou censura seria vedada (GREENBERG 2016, p 21).

A ideia do Marco Civil surgiu a partir da concepção do professor Ronaldo Lemos, expressa em artigo publicado em 22 de maio de 2007. Partindo

de debates e sugestões, foi formular a minuta do anteprojeto que voltou a ser debatida, numa segunda fase, em um processo de construção colaborativo com participação da sociedade. O Marco Civil foi descrito pelo então Ministro da Justiça, Luiz Paulo Barreto, como ´´A Constituição da internet``. Também foi descrito pelo site *Techdirt* como uma lei ´´anti-ACTA``, fazendo referência ao Acordo Comercial Anticontrafação, muito criticado por restringir a liberdade na internet e que acabou rejeitado pela União Europeia. Foi também muito criticado sob a alcunha de AI-5 digital. Após ser desenvolvido colaborativamente em um debate aberto por meio de um blog.

Atualmente a principal lei que regulamente o âmbito jurídico no Brasil é o marco civil da internet (Lei nº 12.965/2014). Sancionada em 2014, foi o primeiro a regulamentar e tratar sobre o uso da informática no Brasil. Também trouxe garantias aos internautas, O Marco Civil da internet regulamenta a responsabilidade civil de usuários e provedores. O processo do qual o texto é resultado ao ano de 2009. Naquela época existiam 26 propostas para a regulamentação da internet no Congresso Nacional. Mas a reação da sociedade civil ao Projeto de Lei nº 84/1999, conhecida como AI-5 Digital, foi o motivo do Ministério da justiça a iniciar um processo de consulta pública através da internet para a construção de uma lei.

Em frente a importância que foi adquirido pela internet e sua complexidade que foi restabelecida pelas relações estabelecidas, cada vez mais deveres e direitos virão a ser garantidos aos sujeitos envolvidos. Foi proposto elaborar novas normas para a proteção não só da pessoa física mas também no âmbito digital. Na internet assim como todas as outras ações desenvolvidas, se submetem estritamente aos princípios constitucionais.

3.2 OS PRINCÍPIOS FUNDAMENTAIS DO MARCO CIVIL DA INTERNET

O art. 3º do Marco civil da internet prevê que no Brasil ela se encontra alicerçada em um tripé axiológico formado pelos princípios da neutralidade de rede, da privacidade e da liberdade de expressão, que estão ligados entre si. Enquanto a neutralidade de rede reforça a liberdade de expressão, a privacidade representa seu limite.

O princípio da neutralidade da rede, determina que a rede deve tratar da mesma forma tudo aquilo que transportar, sem fazer discriminações quanto a natureza do conteúdo ou identidade do usuário.

> Garantir uma experiência integral da rede a seus usuários, um tratamento isonômico dos dados, sem distinção de conteúdo, origem, destino, serviço, terminal ou aplicação, havendo expressa vedação de bloqueio (WU, 2012, p. 244).

O princípio impõe que a filtragem ou os privilégios de tráfego devam respeitar apenas motivos políticos, comerciais, religiosos ou culturais que criem forma de discriminação ou favorecimento.

Em relação a privacidade, sua configuração de maior destaque é o controle da circulação das informações pessoais. Afirma-se que a configuração atual da privacidade ultrapassa o eixo ´´pessoa-informação-segredo`` para se estruturar naquele da ´´pessoa-informação-controle``.

A liberdade de expressão, considerada como liberdade de expressar ideias, juízos de valor e as mais variadas manifestações do pensamento, além de já ser amplamente protegida pelo constituinte, sendo considerada um fundamento e um princípio para a disciplina do uso da internet no Brasil e condição para o pleno exercício do direito de acesso. Ao longo do Marco Civil contata-se a preocupação do legislador com a compatibilização desses princípios a fim de garantir a pessoa possa desenvolver sua personalidade na internet.

> Por mais que seja simpático também a tal linha de entendimento, a atribuição de uma função preferencial a liberdade de expressão não parece, salvo melhor juízo, compatível com as peculiaridades do direito constitucional positivo brasileiro, que, neste particular, diverge em muito do norte-americano e mesmo do inglês. Aliás, o nosso sistema, nesse domínio, está muito mais afinado com o da Alemanha, onde a liberdade de expressão não assume uma prévia posição preferencial na arquitetura dos direitos fundamentais. Mesmo uma interpretação necessariamente amiga da liberdade de expressão (indispensável num ambiente democrático) não poderia descurar a inviolabilidade dos direitos a privacidade, intimidade, honra e imagem (artigo 5º, inciso X), além de assegurar expressamente um direito fundamental a indenização em caso de violação consagrar já no texto constitucional

> atribuir à liberdade de expressão a referida posição preferencial (SARLET 2015, p 23).

Com consequência, parece essencial compatibilizar os princípios constitucionais e nunca os colocar em atrito. É necessário entender que a liberdade de expressão é condição para que a personalidade humana possa ser totalmente desenvolvida e protegida, o próprio princípio da liberdade constitucional consolida numa perspectiva de liberdade de exercício da vida privada (RODOTÀ, 2008, P. 74-75). Assim, liberdade significa hoje, poder realizar, sem interferências de qualquer gênero, as próprias escolhas individuais, exercendo-as como melhor convier (BODIN DE MORAES, 2016, p 107).

3.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

É a lei nº 13.709/2018 que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16º do Marco Civil da internet. Aprovada em 2018 e com vigência em agosto de 2020. Ela criou uma categoria de novos conceitos jurídicos (´´dados pessoais, dados pessoais sensíveis``) demonstra as condições nas quais os dados pessoais podem ser tratados, define um conjunto de direitos para os titulares de dados, gerando obrigações especificas para os controladores dos dados e cria uma série de procedimentos e normas para que haja maior cuidado com o tratamento de dados pessoais e compartilhamento de terceiros.
Conceitua o advogado Luiz Fernando Pereira:

> Para fins de aplicação pratica, os dados pessoais coletado por estas empresas são toda e qualquer informação, como nome, CPF, RG, nacionalidade, estado civil, profissão, escolaridade, dentre outras. Dado pessoal sensível é o dado pessoal sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Distintamente de Dado anonimizado, relativo

> que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

A Lei Geral de Proteção de dados regulamenta no Brasil, em âmbito privado e público seu uso, transferência e proteção de dados pessoais, e determina quem são os agentes envolvidos e suas atribuições de responsabilidade por incidentes. O impacto da lei afeta as empresas do ramo diretamente, podendo determinar multas por não cumprir o valor acertado baseado no grupo econômico que está inserida a empresa infratora.

> Tal como exposto, os pilares da Lei Geral de Proteção de Dados são as garantias constitucionais fundamentais de privacidade e liberdade, e também o desenvolvimento econômico, tecnológico e inovação nacional. Entretanto, destaca-se em seus princípios o da transparência da finalidade, segundo o qual ´´os dados só devem ser utilizados para as finalidades especificas para as quais foram coletados previamente informados aos seus titulares, e também do princípio da necessidade, que significa limitar o uso dos dados ao mínimo necessário para que possa atingir a finalidade pretendida, do qual surge ainda a indispensável exclusão imediata de dados, após atingida tal finalidade`` (Samodossi 2018 p 27).

A lei define como dado pessoal ´´informação relacionada a pessoa natural identificada ou identificável``, e toda a operação envolvida no tratamento, sendo levantado o conceito de titular, controlador, operador, compartilhamento, transmissão, em seu artigo 5º. O texto legal determina que estão suscetíveis à aplicação da Lei Geral de Proteção de Dados Pessoais, inclusive nos meios digitais, pessoas naturais ou por pessoas jurídicas do direito público ou privado, que estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no pais, devendo a partir da lei possuir o consentimento expresso do usuário para esta operação.

O entendimento de consentimento demonstrada na lei é a livre manifestação. Inequívoca informada pelo titular dos dados.

A Lei garante e prevê o direito dos usuários ao acesso e obtenção, mediante recurso, retificação de informações de todos os dados tratados e o correto tratamento e retificação, mantendo os agente sempre adaptados.

As mudanças causando impactando alteração na atual forma de tratamento de dados, a Lei foi estabelecida com a vacância de 18 meses, sendo sua vigência estabelecida para 16 de fevereiro de 2020. E desde essa época os investimentos em cibersegurança e *complicance* tem crescido com precedentes nunca antes visto, sendo afetado também pela pandemia que estamos enfrentando para assim agir ativamente na prevenção e detectação de crimes cibernéticos e remediar violações.

CONCLUSÃO

O direito digital é bastante complexo. São inúmeros os empecilhos legais que estão envolvidos o mundo virtual das tecnologias. Com a necessidade de cada vez mais a digitalização em qualquer área e trabalhar em rede para ter mais produtividade e eficiência todos estão aderindo a esse tipo de questão. Então disso vem a necessidade de ter proteção contra possíveis casos de roubo de propriedade intelectual, vazamento de informações, De forma geral o direito digital foi criado para adequar os fundamentos do direito para a sociedade nos dias atuais.

Contudo nem tudo é um mar de rosas e com isso vieram adversidade para as pessoas no âmbito virtual, sendo prejudicados na sua vida em todos os aspectos. O direito digital advém da junção do direito e o estudo da computação, abordando variadas ideias, execuções, vínculos no meio legal do direito e os crimes se tornam cada vez mais comuns.

Crimes contra propriedades intelectuais são os que mais crescem, o acesso ilimitado a qualquer conteúdo a qualquer momento dominam esses conteúdos de particulares sem autorização influenciando o âmbito digital.

A influência do ambiente digital impactou nas relações todas as áreas do direito: direito constitucional (nova visão sobre privacidade); direito penal (crimes virtuais); direito tributário (impostos sobre transações online); direito do consumidor (com o e-commerce e bancos de dados) etc.

O fato é que o direito digital é uma realidade que não se pode ignorar.

É cada dia mais recorrente os comportamentos humanos acontecendo no meio digital. Essa tendência é reforçada pela abrangência da área, que é a contemplação da relação dos mais diversos ramos do direito.

Se o poder público se abster da criação de leis para por exemplo o que os bancos fazem de divulgar os dados pessoais de seus clientes, qualquer indivíduo tem acesso a essas informações. Essas empresas tem der ser responsabilizados por essa exposição de informações de seus clientes.

O próximo passo seria na elaboração de instrumentos mais eficazes que possam ser usados para proteger a pessoa humana nas relações desenvolvidas na internet.

ABSTRAT

This scientific article aims to debate the growth of digital law in Brazil and in the world, which is the branch of law that governs relationships in the virtual sphere. With the growth in the use of the internet, naturally crimes are committed on a daily basis and the trend is only increasing due to the daily use of practically all people and companies around the world. Showing the evolution of this right in our lives, of cyber crimes that make millions of victims daily and how the legislative side is being. Because many people who use their cell phones and computers in the computer area are not for purposes within the law. There are people who are just there to break into bank accounts, steal sensitive information from companies, or exclusively, improperly use other people's personal information. The methodology used will be a pilgrimage for digital law, the civil framework of the internet the application of laws and what will be the next to be given in relation to this area that will be the most used in a few years in the legal scope of Brazil and around the world.

Keywords: Digital law, civil framework of the internet, cyber crimes

REFERÊNCIAS

ALMEIDA FILHO, José Carlos de Araújo*. Direito Eletrônico ou Direito da Informática*? Informática Pública vol. 7 (2): 11-18, 2005. Disponível em: http://www.ip.pbh.gov.br/ANO7 N2 PDF/IP7N2 almeida.pdf. Acesso em 25 de ago. 2020.

ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009

Ambitojuridico.com/cadernos/direito-penal/crimes-ciberneticos-consideraçoes-sobre-a-criminalidade-na-internet/ Acesso 18 nov. 2020.

ATHENIENSE, Alexandre. *Informatização e Prática da Advocacia no Mundo Contemporâneo*. Dezembro, 2006. Disponível em: http://www.dnt.adv.br/noticias/cibercultura/informatizacao-e-pratica-da-advocacia-nomundo-contemporaneo-3/. Acesso em 02 de ago. 2020.

BITTENCOURT, Rodolfo Pacheco Paula. O anonimato, a liberdade, a publicidade e o direito eletrônico. 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico> Acesso em: 10 nov. 2020.

BODIN DE MORAES, Maria Celina. Danos à pessoa humana. Uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2020.

CASTRO. Carla Rodrigues Araújo. Crime de informática e seus aspectos processuais. 2. Ed. Rio de Janeiro: Lumen Juris 2001.

COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informáticahttps://jus.com.br/artigos/3271/cybercrime-os-crimes-na-era-da-informática Revista Jus Navigandi, ISSN 1518-4862, Teresins, ano 7. Acesso em 18 nov. 2020.

FELICIANO, Guilherme Guimarães, Informática e Criminalidade: parte I, Lineamentos e Definições. Boletim do Instituto Pedro Pimentel, São Paulo, v 13, n 2, 2000.

FERNANDES, José. Tipos de comércios eletrônico. 2012. Disponível em:https://bloomidea.com/blog/tipos-comercio-eletronico. Acesso em 19 nov. 2020.

GALO, Carlos Henrique. Lei nº 12.965/11: O Marco Civil da Internet – Análise Crítica. Disponível em: http://henriquegalo.jusbrasil.com.br/artigos/118296790/lei-n-12965- 11-o-marco-civil-da-internet-analise-critica. Acesso em 10 jul. 2020.

GREENBERG, Andy. Its Been 20 Years since This Man Declared Cyberspace Independece. Wird. Disponível em: https://www.wired.indepedence/. Acesso em 14 nov. 2020.

LÉVY, Pierre. Disponível em: https://books.google.com.br/books?id=IeNw_sOADVEC&printsec=frontcover&dq=PI ERRE+LEVY&hl=pt BR&sa=X&ved=0ahUKEwji35jEyv3LAhWHQpAKHcpkBNsQ6AEINzAD#v=onepage&q=PIERRE%20LEVY&f=false. Acesso em 21 de jul. 2020.

MALAQUIAS, Roberto Antonio Darós. CRIME CIBERNÉTICO e Prova – A Investigação Criminal em Busca da Verdade. 2 ed. São Paulo: Juruá Editora, 2015.

PAIVA, Mário Antônio Lobato de*. Os institutos do direito informático*. Maio, 2002. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf. Acesso em 17 de nov. 2020.

RODOTÀ, Stefano. A vida na sociedade de vigilância. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004. Acesso em 15 nov. 2020.

SARLET, Ingo. Liberdade de expressão e biografias não autorizadas. Consulto jurídico. 19 de junho de 2015. Disponível em:http://www.conjur.com.br/2015-jun-19/direitos-fundamentais-liberdade-expressao-biografias-nao-autorizadas. Acesso em 11 nov. 2020.

SOMADOSSI, Henrique. O que muda com a Lei Geral de Proteção de Dados (LGPD). Migalhas nº 4.478 24 de agosto de 2018. Disponível em:<https://www.migalhas.com.br/dePeso/16,MI286235,31047O+que+muda+com+a+Lei+Geral+de+Proteção de Dados. Acesso em 19 nov. 2020.

Wu, Tim. Impérios da comunicação. Do telefone a internet, da AT&t AO Google. Traz. De C. Carina. Rio de Janeiro: Zhahar,2012.

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

RESOLUÇÃO n°038/2020 – CEPE

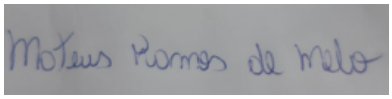
ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante MATEUS RAMOS DE MELO do Curso de Direito, matrícula 2011.2.0001.0796-3, telefone: (62) 98236.5884, e-mail mateus4108@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado DIREITO DIGITAL: CRIMES CIBERNÉTICOS E MARCO CIVIL DA INTERNET, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 02 de dezembro de 2020.

Assinatura do(s) autor(es): 

Nome completo do autor: MATEUS RAMOS DE MELO

Assinatura do professor-orientador: 

Nome completo do professor-orientador: ROBERTA CRISTINA DE MORAIS SIQUEIRA