Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais – FAJS
Curso de Bacharelado em Direito

DIREITO DIGITAL E PROTEÇÃO LEGAL: O aumento de crimes digitais e a falta de normas consolidadas no ordenamento jurídico

BRASÍLIA
2024
LUÍZA JÚLIA FERREIRA LIMA

DIREITO DIGITAL E PROTEÇÃO LEGAL: O aumento de crimes digitais e a falta de normas consolidadas no ordenamento jurídico

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Leonardo Gomes de Aquino

BRASÍLIA

2024

LUÍZA JÚLIA FERREIRA LIMA

DIREITO DIGITAL E PROTEÇÃO LEGAL: O aumento de crimes digitais e a falta de normas consolidadas no ordenamento jurídico

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Leonardo Gomes de Aquino

BRASÍLIA, DE DE 2024

BANCA AVALIADORA

_____

Leonardo Gomes de Aquino
Professor Orientador

_____

Professor(a) Avaliador(a)

Título do artigo: Direito digital e proteção legal: O aumento de crimes digitais e a falta de normas consolidadas no ordenamento jurídico.

Autora: Luíza Júlia Ferreira Lima

Resumo: O presente artigo trata dos desdobramentos do direito digital e sua relação com a ciência da computação, objetivando abordar esse ramo e a fragilidade da proteção legal decorrente do aumento de crimes digitais e a falta de normas consolidadas no ordenamento jurídico brasileiro quanto ao assunto, assim como os principais problemas envolvendo o anonimato e o direito à privacidade. Na era globalizada, o direito digital é um ramo do direito que regulamenta as condutas dentro do ambiente digital, com o maior e crescente uso de tecnologias e redes sociais nas relações sociais, econômicas, políticas e culturais e nas tarefas diárias. Nesse sentido, essa pesquisa sociojurídica descritiva aborda as principais teses de alguns autores para concluir as problemáticas relacionadas à incompletude e inconsistência do direito penal no ambiente virtual.
Palavras-chave: Direito digital. Proteção legal. Crimes digitais.

Sumário: Introdução. 1 – O Direito Digital. 1.1 – Contexto histórico e surgimento do direito digital. 1.2. Cibercultura. 1.3 – Direito digital no Brasil. 2 – Crimes digitais. 2.1 – Classificação dos crimes digitais. 2.2 – Fraudes e golpes. 2.3 – Crimes contra a honra. 2.4 – Responsabilidade civil e penal. 2.5 – Direito ao anonimato. 3 – Competência territorial para analisar os crimes cibernéticos. 4 – A inércia do Estado. Considerações finais.

INTRODUÇÃO

O direito digital trata-se de um ramo relativamente novo no direito, e somente surgiu pela necessidade de regular as relações dentro do ambiente digital, que se expandiu e modificou-se consideravelmente nos últimos anos. Ao invés de uma nova forma de direito, o direito digital em si não é um novo direito, mas sim a forma como será aplicado o próprio direito – que rege o ordenamento jurídico – no plano virtual, para regular as relações e ações que ocorrem nesse meio.

A reflexão acerca da falta de normas no ordenamento jurídico brasileiro para lidar com a criminalidade digital é de urgente e extrema importância, e vem sendo foco de discussões e debates há anos por estudiosos e doutrinadores de diversas áreas, principalmente a jurídica.

Nos últimos anos o número de vítimas de crimes digitais vem crescendo exponencialmente no Brasil. Essa realidade decorre da grande impunibilidade existente na prática de crimes no meio cibernético, da linha tênue entre anonimato (direito à privacidade) e liberdade de expressão, das poucas providências para punir ou responsabilizar os infratores, e das precárias normas de Direito Penal para combater esses crimes e reger a aplicação desse direito no âmbito virtual.

O objetivo geral de tratar desse tema é analisar as questões envolvendo os crimes ocorridos no meio digital e investigar, por meio das pesquisas e estudos de diversos autores, as providências necessárias no ordenamento jurídico brasileiro para lidar com a crescente onda de delitos cibernéticos, decorrente da revolução tecnológica ocorrendo dentro da sociedade informacional e do conhecimento. Ademais, neste artigo pretende-se (1) conceituar direito digital e explicitar seu contexto histórico, (2) esclarecer as peculiaridades dos crimes digitais e suas ramificações, (3) abordar a competência territorial para julgar e processar crimes cibernéticos e (4) mostrar as consequências e problemas advindos da negligência e inércia governamental quanto aos seus cidadãos dentro do ambiente virtual.

A presente pesquisa sociojurídica foi feita a partir de uma abordagem qualitativa de estudos e pesquisas de autores e estudiosos da área, por meio de uma revisão literária dos conceitos de Leonardo Zanatta, além da interpretação dos dispositivos do Código Penal de 1940 e do Código de Processo Penal de 1941.

Nesse contexto, o artigo tratará do que é o direito digital em si, como ele surgiu e o que ele abrange, e como ele afeta a realidade social. Segundamente, será feita uma exposição sobre crimes digitais – ou seja, que ocorrem no ambiente virtual –, os principais crimes desse meio, sua incidência e problemas de competência, para que seja possível pensar, de forma lógica, sobre as consequências jurídicas e penais decorrentes dessas infrações no direito brasileiro. Por fim, será tratada a forma como a sociedade, o Estado e os estudiosos de direito estão lidando com esse tema mediante as constantes mudanças sociais e culturais.

1. O DIREITO DIGITAL

O direito digital é um "ramo" relativamente novo no direito, advindo do intenso processo de globalização do século XXI. Tratar desse tema não é pensar em uma nova forma de direito, ou um novo ramo propriamente dito, mas um âmbito distinto do direito já aplicado no ordenamento jurídico, o qual regula as relações e fluxos sociais dentro da Internet. É a atuação do setor jurídico no mundo digital, sem, necessariamente, criar novas regras, mas adaptar os princípios que regem a Carta Magna ao mundo da informação. As formas de aplicação do Direito Digital são baseadas no direito natural, codificado, comparado, positivista, costumeiro, na jurisprudência e na analogia e arbitragem. Apesar disso, ainda há baixo número de leis direcionadas ao direito digital e grande negligência governamental.

1.1 CONTEXTO HISTÓRICO E SURGIMENTO DO DIREITO DIGITAL

A organização humana, tanto para produção quanto para o consumo, passou por muitas mudanças até chegar à sociedade atual, que é uma sociedade informacional e do conhecimento. A Revolução Técnico-Científico-Informacional entrou em vigor na segunda metade do século XX, principalmente a partir da década de 1970, quando houve uma série de descobertas e evoluções no campo tecnológico. Nesse contexto, trata-se de, além de tudo, uma economia do conhecimento.

A economia do conhecimento tem três características principais. Primeiramente, o avanço e difusão da informática e das comunicações; hoje, não há como dissociar as telecomunicações da informática, e tanto a informática quanto a telecomunicação se popularizaram no Brasil. Há 212 milhões de habitantes e 234 milhões de telefones habilitados até dezembro de 2020, ou seja, existem mais telefones do que pessoas em no país. Segundamente, é uma geração de difusão de informações em volume, rapidez e abrangência;

há hoje uma quantidade de informações à disposição que podem ser acessadas de várias formas. Por fim, a economia do conhecimento é também parte do acelerado processo de globalização, com o desenvolvimento tanto do processo de conversação quanto o de comercialização.

Na sociedade moderna, principalmente na última década, a Internet passa a regular e reger grande parte das relações e interações sociais, principalmente com o grande número de mudanças e transformações, tendo surgido pela necessidade humana de novas tecnologias, principalmente em contextos políticos. Hoje, a internet também assume papeis sociais e culturais. Nesse contexto, existem várias redes, mas a Internet acaba sendo uma grande rede com funções específicas como troca de mensagens e conversas à distância, debates, comércio, tele emprego e projetos de voto, e todas essas modalidades trazem repercussões jurídicas e socioeconômicas, em algum nível (ZANATTA, 2010).

Segundo JÚNIOR (2001 apud ZANATTA, 2010):

> A Internet, portanto, nada mais é do que uma grande rede mundial de computadores, na qual pessoas de diversas partes do mundo, com hábitos e culturas diferentes, se comunicam e trocam informações. Ou, em uma só frase, é a mais nova e maravilhosa forma de comunicação existente entre os homens.

A escola tem sido, desde os primórdios da educação, uma possibilidade de difusão de ideias e informações, àqueles que têm acesso, sendo que os que têm mais poder, consequentemente, têm um acesso melhor ao conhecimento. Mesmo historicamente, não é novidade que a tecnologia e a informação têm sido filtradas e privadas ao acesso da população, por aqueles que detém maior poder, geralmente a classe econômica e política mais alta e privilegiada. No contexto atual, não se pode fugir dessa ideia, pois a maioria das relações encontradas na sociedade moderna é criada a partir dos meios de comunicação virtuais; tal qual funciona nas escolas, quem tem acesso a mais informação, tem acesso a mais conhecimento.

As interações virtuais devem se relacionar com o direito justamente pois o uso da Internet é feito em nível global, e qualquer indivíduo está sujeito a ser vítima de crimes que passam a não ter mais limites geográficos e políticos, e que têm pouca proteção. Desde 2010, já se enxerga o aumento dos problemas jurídicos, econômicos e sociais decorrentes das transformações da sociedade, em um conflito a modernidade e as inovações criarem novos problemas que dependem de novos institutos para serem solucionados. Nas palavras de Lévy (2007, pg 17 apud ZANATTA, 2010):

> A virtualização não é uma desrealização (a transformação de uma realidade num conjunto de possíveis), mas uma mutação de identidade, um deslocamento do centro de

> gravidade ontológico do objeto considerado: em vez de se definir principalmente por sua atualidade (uma "solução"), a entidade passa a encontrar sua consistência essencial num campo problemático. Verifica-se, portanto, que ocorre um círculo: a atualização soluciona um problema e a virtualização de uma solução gera um outro problema.

Deduz-se, portanto, que a virtualização é uma nova alternativa para interpretar um problema, e no plano virtual, o direito digital ocorre com a virtualização para adequar-se à realidade cibernética. Isso significa que para entender como solucionar os problemas virtuais – já que eles têm efeitos no mundo real – deve-se avançar institutos costumeiros (como o direito), para dentro da internet.

O direito digital não difere do direito já conhecido e normatizado por seus princípios e institutos, mas sim pelo plano virtual no qual ele se encontra. Isto é, o direito digital não precisa ser inventado ou criado do zero, mas sim ser estudado no plano real e aplicado na realidade virtual. O problema encontrado aqui, contudo, é que é impossível prever todas as situações concretas que podem ocorrer no plano virtual, principalmente pelo número de mudanças que ocorrem em pouco tempo, logo nem sempre o direito será capaz de reger e responsabilizar indivíduos pela Internet, sem precisar de normas específicas pensadas para o ambiente cibernético, e poucas são as normas específicas no ordenamento jurídico brasileiro (ZANATTA, 2010).

Percebe-se, contudo, que por tratar-se de um tema recente, que condiz com a realidade atual, ainda é uma área que carece de atenção, principalmente em meio a transformações tão rápidas e contínuas. O setor jurídico, por si, já se adaptou de várias formas à realidade virtual e às novas tecnologias, mas ainda há uma grande resistência de compreender as novas formas sociais e culturais advindas do advento da sociedade de tecnologia e informação, principalmente por estudiosos, doutrinadores e profissionais do direito.

1.2 CIBERCULTURA

Ao tratar do surgimento do direito digital, um importante fator nesse ramo é a cibercultura. A cibercultura (ou cultura da Internet) é a relação entre a informação e a evolução dos valores e conceitos dentro da sociedade; ao mesmo tempo em que as novas informações causam transformações na sociedade, seus valores e sua cultura, os próprios valores da sociedade podem modificar a forma como a informação é recebida. Trata-se do movimento das pessoas dentro do ambiente digital, fazendo com que a sociedade se adeque a partir dessa

mudança, surgindo a necessidade da presença do Estado regulando a mudança, e isso faz com que o direito possa responder a essa nova realidade.

Ao avaliar a evolução histórica das tecnologias, constata-se que elas constantemente estiveram em poder de minorias privilegiadas, tanto economicamente, quanto politicamente. Atualmente, a cibercultura resulta em um novo espaço de comunicação, que tem potencial nos planos econômico, político, social e cultural; o ciberespaço é o novo meio de comunicação navegado e alimentado pelos humanos, e a cibercultura é um conjunto de valores e pensamentos que se desenvolvem juntamente com o crescimento do ciberespaço (LÉVY, 2000).

O direito digital seria uma resposta a mudança social para dentro desse ambiente digital, não sendo um ramo totalmente novo e autônomo do direito, é uma leitura do direito a partir do meio digital em que as pessoas estão interagindo (conhecendo pessoas, praticando crimes, adquirindo patrimônio, vendendo bens etc.). Fica claro que a partir da nova realidade social e a cultura digital, surge a demanda de que o Estado regulamente as relações das pessoas nesse ambiente virtual.

1.3 DIREITO DIGITAL NO BRASIL

A Constituição Federal de 1988 é a carta que rege as relações jurídicas e as garantias fundamentais dos cidadãos, as quais devem ser respeitadas em todas as esferas, inclusive no meio digital. Dentre liberdade de expressão, direito à privacidade e à honra, e igualdade entre todos (princípios constitucionais no ordenamento jurídico brasileiro), o direito digital deve observar a relação entre as pessoas e o uso que fazem das tecnologias, para saber como lidar e desenvolver normas que atendam às necessidades e os problemas atuais.

No Brasil, a necessidade de proteger os direitos individuais dentro das relações e atividades cibernéticas, fez com que surgissem algumas leis de proteção digital, como a Lei Carolina Dieckmann de 2012 (focou nas invasões a dispositivos que acontecem sem a permissão de seu proprietário), o Marco Civil da Internet de 2014 (estabelece princípios, garantias, direitos e deveres para o uso da internet), a Lei Geral de Proteção de Dados (regulação no tratamento de dados no meio físico e digital) e a Lei de *stalking* e *cyberstalking* de 2021 (tipifica o stalking e o cyberstalking como crime).

As análises jurisprudenciais do Supremo Tribunal Federal sobre o tema de Internet têm como base os direitos e garantias fundamentais do artigo 5º da Carta Magna que, dentre outros

assuntos, assegura aos cidadãos as garantias relativas ao acesso à informação pública (Art. 5º, XXXIII), liberdade de manifestação de pensamento (Art. 5º, IV), liberdade de expressão (Art. 5º, IX), além de prerrogativas contra formas de censura (Art. 220, § 1º). Apesar disso, muitos reguladores do direito se recusam a adaptar-se à aplicação do direito nos meios cibernéticos e, por isso, mesmo havendo algumas leis que tratam – exaustivamente ou não – do assunto, pouco é o interesse de editar mais leis e levar mais casos concretos à frente.

Vale ressaltar, no entanto, que a maioria das leis de proteção digital são focadas nos direitos e deveres para o uso da internet, tutelando diversas relações que são mantidas dentro desse meio, mas não contemplam as regras que envolvem a atuação do direito penal, como, principalmente, a territorialidade, o lugar do crime e a competência para processar e julgar crimes cometidos na internet, mesmo que os delitos ocorridos na internet estejam em grande crescimento. Da mesma forma, existem poucas iniciativas para combater a criminalidade digital e proteger os cidadãos dentro desse ambiente.

2. CRIMES DIGITAIS

Os crimes digitais cresceram exponencialmente com a utilização da Internet e da evolução da tecnologia. A sociedade se digitalizou e, dessa forma, a criminalidade seguiu o mesmo caminho, ou seja, adotou o ambiente digital, acompanhando a sociedade. Crime digital, crime virtual e crime eletrônico são a mesma modalidade de cometimento de crimes.

Crimes digitais são condutas previstas em lei (Código Penal ou leis específicas) e punidas criminalmente, envolvendo, de alguma forma, dispositivos tecnológicos. Seja porque o crime foi cometido com o uso de um, seja visando algum sistema informático. Portanto, para que ocorra um crime digital não é necessário que o meio utilizado para a prática do crime seja um computador ou equivalente, mas qualquer dispositivo tecnológico.

Se o agente estiver, pessoal e fisicamente na frente do computador que ele está invadindo, ou seja, o agente não utilizou outro meio tecnológico, ele está utilizando o próprio objeto que contém os dados que deseja invadir, nesse caso, estamos diante de um crime digital. Se o agente estiver em outro continente, utilizando um computador ou um celular como meio para invadir um sistema, ou seja, o computador é o meio para atingir um fim específico, nesse caso, estamos diante também de um crime digital.

De acordo com Zanatta (2010), ainda existe uma problemática com relação ao tempo para o direito digital com relação à validade, pois a demora em resposta ou até mesmo a burocracia faz com que os indivíduos (principalmente consumidores) percam o seu direito de pleitear algo ou exigir responsabilidade civil. Nesse contexto, a prática de crimes é muito recorrente pelos infratores saberem que provavelmente sua infração não vai resultar em nada, justamente pelo tempo limitado em que a parte lesada tem para interpor algo, e a falta de proteção jurídica dentro do ambiente virtual, que ao invés de impedir que o crime venha acontecer, só se preocupa com a responsabilização que tem a possibilidade de ocorrer posteriormente. Não só isso, mas o autor traz outros exemplos e possibilidades de consequências e efeitos decorrentes da perda de "tempo".

Por conseguinte, encontrar os ofensores, em alguns crimes, também está suscetível a dificuldades. A busca pela autoria dos ofensores cibernéticos está sujeita à proteção da privacidade e do anonimato, já que a questão da vigilância e guarda de dados específicos é autorizada aos provedores de serviços na Internet, justamente pela falta de legislação específica sobre o tema.

Para FARAH (2016, apud COSTA, 2018):

> Conteúdos disponibilizados na Internet são rastreáveis e a captura de telas dos equipamentos tecnológicos, como computadores, celulares e tablets devem ser feitas com o fito de comprovar o crime e sirvam de testemunha sobre os conteúdos abusivos publicados." Deve-se registrar por meio de ata notarial ou através de telas gravadas. Porém, a guarda de evidências eletrônicas (logs) configura o registro dos fatos no ambiente virtual, associado a autoria (login) de quem postou os arquivos online, torna-se relevante; ao passo que somente vestígios de fatos, mas sem prova, não configuram a autoria do crime. (FARAH, 2016)

Outro elemento importante a considerar aqui é o território. No direito digital, há uma complicação a mais relacionada à falta de limites geográficos e políticos, já que por ser uma rede global é muito difícil delimitar as localidades em que os crimes estão acontecendo, ou se ao menos podem ser punidos pelos seus Estados com tantas incertezas com relação à liberdade e ao anonimato (ZANATTA, 2010). Apesar de essa ser uma preocupação do autor, no ano presente muito já se tem avançado em relação ao alcance das leis internacionais e às tecnologias capazes de identificar e lidar com localizações na internet e determinar a autoria desses crimes (como a identificação do IP, por exemplo).

Quanto aos delitos cometidos por via eletrônica, já há classificações que dividem esses crimes, seja por serem considerados "novos" crimes, seja por serem considerados crimes

comuns. Atualmente, já se tem uma visão melhor dessas classificações, sendo de relevância a diferenciação de crimes digitais próprios e crimes digitais impróprios (puros e impuros), software e hardware; os tipos de autores e as técnicas utilizadas também são tópicos já diferenciados e categorizados.

2.1 CLASSIFICAÇÃO DOS CRIMES DIGITAIS

Para Marco Aurélio Rodrigues da Costa (2010 apud ZANATTA, 2010):

> Crime de informática Puro: São aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõem a informática o "software", o "hardware" (computador e periféricos), os dados e sistemas contidos no computador, os meios de armazenamento externo, tais como fitas, disquetes, etc. Portanto são aquelas condutas que visam exclusivamente a violar o sistema de informática do agente passivo. As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador. Portanto, é crime de informática puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

A partir do estudo de Zanatta (2010), é possível inferir que quando o crime é praticado contra um sistema (objetivando a invasão do sistema) ou com o objetivo de acesso a dados de um sistema, ou seja, trata-se de uma invasão hacker. O que se quer é, de fato, entrar na máquina para obter acesso a um sistema específico, a um banco de dados ou a uma base de informação. O autor ainda define:

> Crime de informática Misto: são todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação. Quando o agente objetiva, por exemplo, realizar operações de transferência ilícita de valores de outrem, em uma determinada instituição financeira utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial, defrontamo-nos com um crime de informática misto. É crime de informática misto porque incidiriam normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 17137 do Código Penal combinado com uma norma de mau uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas (art. 70, CP)
>
> Crime de informática Comum: são todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outra ferramenta. Como exemplo, os casos de estelionato (art. 171, CP), e as suas mais amplas formas de fraude. Quando o computador é ferramenta escolhida pelo agente ativo, que poderia escolher outros meios diversos da informática. Porém, é de se pensar na possibilidade de qualificadora para o delito de estelionato o uso do sistema de informática. Despiciendo aclarar a aplicabilidade aos crimes comuns das normas penais vigentes, porém, poder-se-ia, atendendo a essa classificação, incorporar ao Código Penal agravantes pelo uso de sistema de informática, vez que é meio que necessita de capacitação profissional e a

> ação delituosa por esta via reduz a capacidade da vítima em evitar o delito. Posto isto, entendemos ser a presente classificação apta a elaboração de legislação que possa alcançar os delitos de informática, sem, contudo, correr-se o risco de sobreposição de normas, e, assim, também entendemos que é meio hábil à formação de um eficaz Direito Penal de Informática.

Trata-se, portanto, de quando o crime é praticado contra bens jurídicos não tecnológicos tutelados pelo ordenamento, como por exemplo utilizar da tecnologia para prejudicar alguém e comprometer a honra de terceiros ou violar a propriedade de alguém e o direito patrimonial de terceiros. Ou seja, utiliza-se de instrumentos digitais para violar bens não tecnológicos, como a vida, a liberdade, a propriedade, a honra e a própria integridade física, dentre outros bens, ou seja, qualquer bem previamente tutelado pelo ordenamento jurídico brasileiro.

A partir dessas definições, compreende-se que o direito digital e a vertente de crimes digitais estão muito além da mera utilização do computador propriamente dito, podendo ocorrer a utilização da tecnologia de forma incidental para o cometimento de crimes, e seus principais atores podem ser desde indivíduos que trabalham com sistemas de informação, até pessoas comuns que comete crimes, mesmo sem o dolo de infringir a lei.

2.2 FRAUDES E GOLPES

Fabio Assolini, analista sênior de segurança da empresa Kaspersky, especializada em segurança para a internet, enfatizou que o Brasil é o quinto país mais afetado por ataques cibernéticos no mundo em 2021, de acordo com o relatório de Ameaças Cibernéticas da *SonicWall*. Dentre os principais crimes digitais, estão as fraudes e os golpes. Parece haver um universo gigante de possibilidades que os autores desses crimes têm para criar e reinventar métodos de praticar tais delitos. Os golpes aparecem de todas as formas possíveis, e geralmente resultam no furto de identidade e de dados pessoais, principalmente dados financeiros.

De acordo com a Federação Brasileira dos Bancos, cerca de 70% das fraudes na internet estão relacionadas à chamada engenharia social, que é um método de manipulação psicológica da vítima para conseguir algo dela. As fraudes mais comuns são: furto de identidade (se passar por outra pessoa), antecipação de recurso (envio de dados ou dinheiro devido a histórias comoventes ou fraudulentas), *phishing* (obtenção de dados sensíveis com o uso de e-mails e sites fraudulentos), *hoax* (mensagens com conteúdos apelativos que incitam o leitor a fazer alguma atividade maliciosa), entre outros.

Durante a pandemia da COVID-19, esses golpes foram ainda mais atualizados, envolvendo principalmente pagamento de vacinas falsas e golpes em compras e serviços pela internet. Para muitas pessoas, essas atividades delituosas são facilmente detectadas e prevenidas, mas outras pessoas não têm qualquer tipo de experiência com esse tópico e acabam tornando-se ainda mais vulneráveis a isso.

O preocupante é que, quanto mais a sociedade evoluí, mais esses crimes pioram, logo a repressão e prevenção do Estado deve aumentar, para impossibilitar a perpetuação desses delitos. Atualmente, as formas de se prevenir são mais intuitivas e lógicas do que propriamente preventivas do Estado e da Lei. Entende-se, nesse contexto, que o Estado deve ser mais proativo em aumentar a segurança dos usuários da rede, e incentivar uma educação mais efetiva sobre esse assunto.

2.3 CRIMES CONTRA A HONRA

Estes são os crimes mais comuns praticados na internet, em decorrência da falsa noção de que a internet é uma terra sem lei. Ele pode ocorrer em diversas modalidades, como a difamação, a calúnia e a injúria, sempre ofendendo a honra de alguém, seja objetiva ou subjetiva, seja afetando a dignidade pessoal ou profissional. A internet possui as mesmas regras que o mundo físico, sendo inclusive muito mais regulamentada e vigiada. Parte-se da compreensão de que não há direito absoluto, já que o direito de um termina quando tem início o direito do outro. Mais a frente, será exposto a forma como esses crimes são tratados na legislação brasileira, principalmente no que tange a sua prática na Internet.

As definições propostas por diversos estudiosos como Lévy e Zanatta expõem melhor ao que esses crimes se destinam e como ocorrem, e a partir disso é mais fácil aplicar normas mais específicas para categorias diferentes. No Brasil, os crimes digitais mais comuns são o estelionato e a pedofilia, assim como a pirataria, os crimes contra a honra e principalmente as práticas de cyberbullying, mas são inúmeras as formas e possibilidade que infratores encontram para realizar essas práticas delituosas, sendo importante analisar como esses crimes já previstos se manifestam no ambiente virtual e aplicar o direito para que não haja impunidade ou negligência com as vítimas e o próprio ordenamento jurídico.

2.4 RESPONSABILIDADE CIVIL E PENAL

Atualmente, não é segredo algum o aumento e a proporção assustadora das práticas de bullying virtual, muitas vezes caracterizado como ato infracional passível de sanção. Todo ano, o número de usuários das redes sociais e de meios digitais aumenta, podendo-se inferir que cada vez mais a expectativa é que quase toda a população seja usuária das redes, algo que não se limita ao Brasil, mas percorre globalmente. O perfil do internauta se modificou de uma figura pacífica a uma figura que opina em qualquer circunstância, seja de forma crítica ou preconceituosa, sobre temas políticos, éticos, cotidianos, pessoas, entre outros.

Para Rodolfo Pamplona Filho e Pablo Stolze Gabliano, constitui requisito necessário para a configuração da responsabilidade, a conduta humana e voluntária, baseada na própria vontade de agir e na liberdade de escolha. Quanto à responsabilidade civil, entende-se que é a atividade humana que deve ser feita com responsabilidade, tendo em vista as obrigações pessoais, visando o bem e a harmonia coletiva, estando carregada de um dever de reparação patrimonial caso haja uma situação de dano causado por ato praticado pelo infrator.

De acordo com LOPES e GONÇALVES (2009, apud FRANÇA 2020):

> O termo responsabilidade deve ser entendido como restituição ou compensação de algo que foi retirado de alguém. Como já dito, a responsabilidade tem por finalidade restituir ou ressarcir algo em benefício da pessoa que sofreu o dano. Porém, se o dano atinge o patrimônio de alguém, é chamado de dano material. Imagine uma situação em que alguém envie um arquivo malicioso (o chamado malware) a outra pessoa, causando problemas no computador do destinatário, o qual será obrigado a contratar alguém para resolvê-lo. O remetente do arquivo poderá ser condenado a pagar os danos que causou à vítima.

Infere-se que, ao tratar de responsabilidade civil, há uma ligação direta com uma consequência, presente em forma de reparação econômica ou patrimonial; nesses casos, o dano pode ser material ou moral, atingindo o patrimônio ou à pessoa, o que não impossibilita que um ato possa gerar ambos danos ao mesmo tempo.

No Código Civil Brasileiro há previsão de que haverá obrigação de reparar o dano, independentemente da comprovação da culpa, quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, riscos para os direitos de outrem (parágrafo único do art. 927 do Código Civil). Estabelece ainda, que as empresas respondem pela assunção do risco, independentemente de comprovação de culpa, pelos danos que podem ser causados pelos produtos postos em circulação ou pela atividade desenvolvida, essencialmente perigosos. Ademais, há que se considerar a ótica do CDC, onde na teoria adotada existe como regra geral

a responsabilidade civil objetiva de todos os envolvidos com o fornecimento de um produto ou serviço que tenha resultado em algum dano ao consumidor

Quanto à responsabilidade penal, trata-se de ato ilícito previsto em lei, estando passível de indenização e penalidade da legislação penal, como cumprimento de pena. No Brasil, a lei penal não é exclusiva para atos praticados presencialmente, podendo ser responsabilizados aqueles que cometerem crimes pelo meio digital. Esclarece FRANÇA (2020):

> Se alguém ofende a honra de outrem e, desse modo comete crime previsto na legislação penal, é indiferente se essa conduta foi na presença da vítima, através de carta, pela imprensa, pela internet ou outro meio. Em qualquer dos casos, poderá ser responsabilizada. Em alguns países, as leis podem estabelecer diferenças a depender da forma como o crime seja cometido, mas, geralmente, as penas costumam ser as mesmas. No caso do Brasil, não há distinção para crimes praticados pela internet ou por outro meio.
>
> Diferentemente da responsabilidade civil, na responsabilidade penal, se alguém for ofendido na internet ou sofrer algum outro dano, poderá optar por ajuizar apenas ação de indenização contra o autor do fato. Para o juiz condenar alguém a pagar indenização, não é indispensável que exista condenação criminal.

Pela responsabilidade penal tratar de interesse público, o lesado é a sociedade, há tipicidade e pessoalidade; o mesmo não ocorre com a responsabilidade civil, na qual o interesse tutelado é o privado, qualquer ação ou omissão pode ensejar responsabilidade e o réu responde com seu patrimônio, nem sempre podendo a vítima ser ressarcida pelo dano causado.

Ao direito digital importa, primeiramente, entender que os crimes praticados na internet não necessariamente caracterizam crimes novos, mas geralmente são crimes já conhecidos, que ocorrem no âmbito terrestre. A problemática encontrada é a falta de regulamentação dispondo sobre o tratamento desses crimes e os limites que decorrem do ato ou fato ter ocorrido no meio virtual. Nesse contexto, há uma problemática tanto penal quanto civil.

De acordo com FRANÇA (2020):

> Embora as condutas ilícitas mais comuns em ambiente virtual sejam de ameaça, de pedofilia e de violação aos direitos da personalidade–tipificadas criminalmente como calúnia, injúria ou difamação, que geram, civilmente, o direito à indenização por danos morais à vítima – outras também previstas no Código Penal e na legislação extravagante admitem a prática em ambiente virtual, como a instigação ao suicídio, o estelionato e a fraude. Convém salientar também, o dever do Estado em apurar e proceder com a efetiva condenação dos indiciados. Neste ponto, é preciso destacar a criação de Delegacias Especializadas em crimes cibernéticos, em alguns Estados da federação. Essa iniciativa aliada às discussões sobre a possível existência de varas judiciais igualmente especializadas para a tramitação de processos decorrentes de atos ilícitos cometidos na internet, está dando resultados positivos.

Há uma constante polêmica e controvérsia jurídica no que tange às consequências desse tipo de iniciativa de criação de varas judiciais especificamente para problemáticas dentro do ambiente virtual.

Para FRANÇA (2020):

> [...] a jurisprudência ainda está bastante dividida acerca do seguinte aspecto: uma simples comunicação do fato junto ao provedor por qualquer pessoa é suficiente ou tal notificação deve ser, necessariamente, judicial? Em obediência à segurança das relações jurídicas e à própria liberdade de expressão, o que parece mais acertado e corrobora com o que está contemplada na Lei Ordinária 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil é a necessidade de a notificação ser de fato, judicial. E, em hipótese alguma essa medida significa uma judicialização no processo de comunicação dos sujeitos ou um dispositivo jurídico para impedir as pessoas de manifestarem suas opiniões abertamente, mas, tão somente uma forma de proteger essas mesmas pessoas que reclamam que estão tendo o seu direito de se comunicar cerceado.

Por fim, entende-se a necessidade de uma legislação atualizada para lidar com as novas tecnologias. A responsabilidade pode ocorrer em mais de um nível, podendo ser penal ou civil, e um mesmo ato pode aderir a essas duas circunstâncias, mas é necessário que haja um maior combate às transgressões criminais que ocorrem na internet, sem que a tecnologia aja sozinha, mas com o auxílio de uma legislação mais específica.

2.5 DIREITO AO ANONIMATO

O autor William Tashiro, em diversos de seus artigos, trata do tema de direito ao anonimato, direito à privacidade e direito à liberdade de expressão. Ao tratar de direito ao anonimato, o autor define o anonimato como uma condição na qual o nome de uma pessoa é desconhecido e ela é não identificável, localizável ou alcançável. Essa condição está ligada ao direito à privacidade, e por isso acaba tornando-se tão problemática, já que o anonimato facilita e incentiva a prática de crimes na internet.

O autor trata principalmente da área e ciência da informática, que está em constante conflito com o direito no que tange ao ambiente virtual, e dos grupos de defesa aos direitos digitais, os chamados *cypherpunks*, que são grupos de informáticos extremistas que defendem fortemente a importância do anonimato para o bem da sociedade digital, gerando um extremismo tão grande que foge e impede a proteção legal dos indivíduos na internet.

De acordo com TASHIRO (2015),

> Os ativistas *cypherpunks* defendem o uso da criptografia como fio condutor de transformações sociais e políticas, acreditam que a privacidade é necessária na era digital, e que ela deve ser conquistada (e não esperada) por meio da criptografia. São contrários a qualquer tipo de regulação criptográfica, e são dedicados a construir sistemas anônimos. O meio para isso é a redação de código, publicados internacional e gratuitamente, independente da aprovação de terceiros (HUGHES, 1993).

Para TASHIRO (2015):

> A relevância deste ramo do direito tem se provado gritante tanto no cotidiano do cidadão comum quanto no âmbito político, com a dicotomia entre dois projetos de lei: a Lei Azeredo e o Marco Civil. O primeiro restringe a liberdade em favor da regulação, e o segundo tem a neutralidade de rede como princípio disciplinador da Internet. O Marco Civil foi aprovado no Senado e sancionado pela Presidenta Dilma Rousseff em abril de 2014, enquanto o projeto da Lei Azeredo foi aprovado após ter sido alterado para conter principalmente a tipificação de delitos informáticos de invasão, muito menos polêmicos.

O direito informático sofreu um "desenvolvimento retardado" na academia brasileira. As questões de direito digital continuam crescendo e se tornando mais polêmicas, pois sua própria origem traz uma dicotomia muito grande aos cidadãos e ao regulamento normativo. Entende-se que é uma questão polêmica que afeta a população no geral, pois tem presença na vida de qualquer cidadão, já que todos têm possibilidade de acesso aos meios digitais.

Para HABERMAS (1964, apud TASHIRO 2015),

> [...] a esfera pública é essa dimensão social que se situa entre a sociedade e o Estado, na qual todos os cidadãos têm potencial de acesso, e onde a opinião pública pode ser formada livre de interesses econômicos ou estatais. O corpo público toma forma quando os cidadãos conversam irrestritamente sobre qualquer assunto de seus interesses, com a garantia de liberdade de associação e de expressão.

De acordo com o autor, o anonimato pode, positivamente, proteger a identidade, aumentar a eficiência de grupos de trabalho e empoderar indivíduos marginalizados, mas traz consequências como o comportamento predatório, intensificação de ódio racial, religioso ou de outra espécie, e até mesmo encorajamento de comportamentos ilegais ou anti-normativos, tudo pelo disfarce de identidade.

Quanto à possibilidade ou não do anonimato, ainda é um assunto muito polêmico. Ele é altamente restringido, tanto pelo entendimento jurisprudencial, quanto pela própria Constituição, mas no que tange à livre manifestação de pensamento, ao invés de privação do direito à privacidade. Pelo anonimato estar de uma forma ligado ao direito à privacidade, há uma controversa no que tange ao conceito de anonimato e a expectativa de privacidade dentro da internet.

O problema considerado é que a comunidade jurídica ainda não tem uma posição estabelecida sobre até que ponto o anonimato vai para proteger a privacidade, mesmo causando comportamentos ilegais ou ofensivos, e a lei pouco dispõe sobre o que deve ou não ser considerado, o que divide a doutrina entre dois modelos de desindividualização, dependendo do cenário concreto apresentado, já que no Brasil há uma certa proibição do anonimato, o que gera conflitos em discussões tratando de liberdade de expressão e pensamento.

Segundo TASHIRO (2015):

> [...] fica claro como a vedação do anonimato possui suas origens na Constituição de 1891 e na Lei de Imprensa, ambas preocupadas em inibir abusos da liberdade de expressão de pensamento. Percebe-se, com evidência, que a tradição civil do direito brasileiro não prioriza a livre manifestação de pensamento no ordenamento jurídico, relativizando-a em favor da facilidade em responsabilizar, diferente de países como os Estados Unidos, no qual é permitido, inclusive, o discurso do ódio (contanto que não provoque violência iminente) sob a proteção da Primeira Emenda.

Ainda assim, para Tashiro, o direito ao anonimato não é mitigado na sua totalidade, tanto pelo dispositivo constitucional em defesa à privacidade, tanto com a interpretação jurisprudencial de que a vedação ao anonimato não é interpretada como forma de nulificação das liberdades do pensamento. Esses entendimentos geram, em si, uma confusão e dúvida maior dentro da comunidade jurídica.

3. COMPETÊNCIA TERRITORIAL PARA ANALISAR OS CRIMES CIBERNÉTICOS

Ao tratar de jurisdição e territorialidade no ambiente digital, há uma grande dificuldade para determinar onde ocorrerá o processamento e julgamento de crimes, já que não existem limites territoriais na internet. Na teoria, o lugar do crime é onde ocorreu a ação ou omissão, bem como onde se produziu ou deveria produzir-se o resultado, conforme artigo 6º do Código Penal de 1940.

O Código de Processo Penal brasileiro, em seu artigo 70, firmou a competência para processamento de crimes, de regra, no lugar em que se consumar a infração, ou, tratando-se de tentativa, no lugar em que for praticado o último ato de execução, com algumas regras de territorialidade e, excepcionalmente, a competência pode ser determinada pelo domicílio ou residência do réu, quando o local da infração não é conhecido.

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

> § 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção.
> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

O critério utilizado no art. 70 do Código de Processo Penal advém da intenção do legislador de que os juízes estejam localizados estrategicamente, para julgar atos que se relacionem com suas localidades (MOUGENOT, 2012).

No entanto, não há, no ordenamento jurídico brasileiro, leis que expressem a competência para julgar os crimes cibernéticos, já que o Código Penal de 1940 não previu essas situações, mesmo após tantos anos da revolução digital.

Não obstante, a Terceira Seção do Superior Tribunal de Justiça, seguindo as regras do Código de Processo Penal, firmou entendimento, no CC (Conflito de Competência) 97201, no sentido de que a competência para julgar os crimes virtuais deve ser do local de onde foi praticado o delito, que nessa situação equivale ao local da sede do provedor do site.

Tal entendimento resolve as principais questões para firmar a competência territorial, mas não abrange as diversas possibilidades de atuação criminosa no meio digital, como por exemplo quando os provedores estão localizados fora do Brasil. Nesta hipótese, ainda não há respostas para a competência territorial, se seria no Brasil ou no local do provedor, se o Brasil teria competência para julgar, ou até mesmo se o autor seria processado e julgado pela Justiça estrangeira.

O próprio artigo 88 do Código de Processo Penal prevê a competência para processar e julgar crimes praticados fora do território brasileiro. Contudo, se o autor do crime está no Brasil, então teoricamente praticou o crime dentro do território brasileiro, mas usa um provedor internacional, então o local da consumação seria fora do Brasil.

> Art. 88 . No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República.

De tal modo, a competência territorial nos casos de crimes virtuais pode tentar acompanhar as normas de competência já existentes nos Códigos Penal e de Processo Penal brasileiros, mas ainda há uma lacuna para tratar de casos mais complexos, devido à omissão legislativa quanto ao tema dentro do universo cibernético. Inevitavelmente, enquanto não houver leis sobre o tema, essas situações continuarão gerando dúvidas e sendo tratadas de forma individual.

4. A INÉRCIA DO ESTADO

É de clareza solar que os principais problemas envolvendo o aumento de crimes, sejam eles relacionados à violação de privacidade ou à ofensa à honra das pessoas, continuam sem solução. Atualmente, o Poder Judiciário se limita a analisar os casos singularmente para encontrar soluções individuais para o julgamento de crimes no meio virtual, enquanto isso há uma dupla falha em pacificar normas de aplicação do direito penal no âmbito virtual, e proteger os cidadãos brasileiros usuários da internet.

A ideia que o ordenamento tenta resguardar é de que a privacidade é inviolável, mas que a liberdade de expressão não pode ser abusada para causar dano ou cometer abusos. Há ainda um desafio constante de como o direito pode regulamentar e supervisionar o abuso da liberdade de expressão. É difícil interpretar ou saber os limites disso, pois trata-se de um direito de todos. Ademais, essa divergência decorre, também, da inconsistência e falta de regulamentação na lei, e resulta no aumento de práticas previstas como delito no meio digital de forma desenfreada.

A Internet deve ser capaz de garantir a liberdade de expressão para que todos da sociedade tenham sua possibilidade e atuação no espaço público, sendo o Estado responsável por não permitir abusos. Nesse contexto, as normas e políticas públicas são muito fracas no incentivo às discussões e comunicações saudáveis e enriquecedoras, e por isso pouco ajudam na conscientização dos usuários por meio de mediação, algo extremamente necessário em ambientes com tanta abundância de conteúdo e divergência de ideias; nesse quesito, o Estado parece pouco se preocupar com a presença social nos espaços informáticos, tratando muitas vezes o que é dito na internet como tópicos e discussões banais.

Há, entretanto, uma grande dúvida sobre quem deve ser responsabilizado por danos causados no âmbito digital, pois falta legislação específica que discorra sobre essa matéria e facilite a compreensão de juízes e outros profissionais do direito, o que muitas vezes traz

impunidade aos ofensores e acaba incentivando a continuidade dessas práticas. Além disso, a falta de legislação específica também traz muitos posicionamentos contraditórios entre os próprios tribunais, envolvendo políticas de uso e maior regulação dos conteúdos que são compartilhados nas redes.

O aumento da impunidade e dos crimes cibernéticos deveria ser uma evidência clara do que carece ao Estado como protetor. É dever do Estado garantir a todos os princípios fundamentais, dentre eles a dignidade da pessoa humana. A falta de segurança cibernética, junto da alta leviandade com a qual o ordenamento trata os crimes digitais, vai contra a obrigação do Estado de proteger os direitos individuais. Nesse contexto, o próprio Estado deve ser responsabilizado pelo dano que está causando aos indivíduos.

CONSIDERAÇÕES FINAIS

A partir dos estudos e análises realizadas neste artigo, foi possível perceber a complexidade das relações sociais e da aplicação do direito penal dentro da era globalizada. As grandes distinções existentes em conceitos e percepções geram polêmica dentro e fora da comunidade jurídica, principalmente quanto às questões envolvendo a proteção dos cidadãos e a aplicabilidade da matéria penal nos casos concretos.

O processo civilizatório da humanidade trouxe consigo a ideia aos seres humanos de que as liberdades e os direitos são absolutos, mas pouco se consideram as consequências. Diversos são os desafios para delinear normas e argumentos jurídicos que regulam o convívio social e acompanhem as inevitáveis mudanças que ocorrem no tempo. O direito é, portanto, essencial para que haja um progresso ético, social, cultural e informacional.

Ainda há uma incompletude e inconsistência do direito em face dos crimes digitais, no que tange ao pouco interesse que o Estado tem de se mostrar capaz de resolver os problemas jurídicos que surgem dentro do ambiente virtual. Muitos profissionais ainda se mostram relutantes em tratar do direito digital como uma outra modalidade, e pouco se interessam em tentar compreender a realidade virtual, o que gera um grande impasse dentro da própria comunidade jurídica. A sociedade, além de tudo, também não está regida por uma legislação protetora, principalmente aqueles em situação mais vulnerável.

A partir dessas descobertas, compreende-se que o universo dos crimes ainda é imaturo quanto ao direito digital, e que ele passará por muitas mudanças e reflexões para alcançar o que é adequado à sociedade. A internet não deixará de existir e, portanto, o ordenamento jurídico brasileiro continuará sofrendo as consequências dos crimes digitais e de sua própria negligência enquanto não se adaptar à nova realidade.

As discussões mais atuais em relação ao direito digital envolvem o abuso do direito ao anonimato, à privacidade, e à liberdade de expressão, as reprimendas que as outras ciências demonstram à rigorosidade do direito, e o problema da responsabilidade. No que tange a essas problemáticas, ainda há um longo caminho a ser seguido, mas há uma clara e imediata necessidade do Estado tomar providências, antes que a criminalidade seja completamente banalizada e a impunidade seja uma regra, não uma exceção.

A presente realidade de indivíduos com acesso desmedido às informações e às redes de conhecimento perpetua e solidifica a preocupação sobre os valores da sociedade em meio à complexidade dos tempos atuais. É relevante, portanto, que não só a sociedade identifique os caminhos sólidos a percorrer, em épocas de riscos, excessos e incertezas, mas que as bases jurídicas sobre o direito penal no meio digital se consolidem no Brasil.

Cabe, ao direito, adaptar-se a resolver os novos conflitos, problemas e exposições que ocorrem nos ambientes virtuais, para proteger os cidadãos do ordenamento brasileiro, e acompanhar as transformações sociais advindas da era tecnológica.

REFERÊNCIAS

ABRUSIO, Juliana Canha; BLUM, Renato Ópice. *Crimes eletrônicos*. Disponível em: https://buscalegis.ufsc.br/arquivos/crimes_eletronicos.htm. Acesso em: 15 out. 2022.

ADJUNTO, GRAÇA. Caminhos da Reportagem: fraudes na internet foram atualizadas. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-04/caminhos-da-reportagem-fraudes-na-internet-foram-atualizadas. Acesso em: 16 nov. 2023.

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 19 out. 2022.

AMARAL, S. A. do. *Gestão da informação e do conhecimento nas organizações e a orientação de marketing. Informação & Informação*. Londrina, 2008;13 (seção especial): 52-70.

ATHENIENSE, Alexandre. *Internet e o Direito.* Belo Horizonte: Inédita, 2000. 285p.

BONFIM, Edilson Mougenot. *Código de Processo Penal Anotado.* 4. Ed. São Paulo: Saraiva, 2012. P. 214-281.

CELLA, José Renato Gaziero; MORAES, Marco Tulio Braga. *Direito na Era Digital: Informação, interação e sociedade do conhecimento.* Disponível em: http://www.publicadireito.com.br/artigos/?cod=e1360bb1174a56e6. Acesso em 11 nov. 2023.

COSTA, Lucas Ferreira; SILVA, Bruna Camila da; SOARES, Fernanda Heloisa Macedo; VIEIRA, Sara Moraes. *Perspectivas da Responsabilidade Civil na Era Digital: V Congresso Interdisciplinar: Ciência para Redução das Desigualdades.* Goianésia, 2018.

COSTA, Marco Aurélio. *Crimes de Informática*. Disponível em: https://jus.com.br/artigos/1826/crimes-de-informatica. Acesso em 13 out. 2022.

COSTA, Matheus Souza. *O ciberterrorismo diante do atual ordenamento jurídico brasileiro.* Lavras, 2017.

COSTA, Roberto Renato Strauhs da; PENDIUK, Fabio. *Direito digital: O marco civil da internet e as inovações jurídicas no ciberespaço.* Faculdade de Educação Superior do Paraná, 2018.

FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gamba Prata de (Coord.). *Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia - 2017.* Belo Horizonte: Fórum, 2018. 485 p. ISBN 978-85-450-0453-0.

FRANÇA, Marlene Helena. *A Responsabilidade Civil e Criminal na Internet: O Papel do Judiciário Brasileiro*. In: Quaestio Iuris. Vol. 13, nº 01, Rio de Janeiro, 2020. Pp. 480-507.

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 03 out. 2022.

HALÉVY, Marc. A era do conhecimento: princípios e reflexões sobre a noética no século XXI. São Paulo: Editora Unesp, 2010.

HUGHES, E. A Cypherpunk's Manifesto. (1993). Acesso em: 27 de junho de 2015, disponível em: https://medium.com/medium-brasil/manifesto-de-um-cypherpunk-3c678c4898c5. Acesso em 05 dez. 2023.

LIMBERGER, Temis. *O Direito À Intimidade na Era da Informática*. Rio de Janeiro: Temis, 2007, 250p.

MONTEIRO, Vilbégina. *Cibernética, Direito, ciberespaço. Ciberdireito?* Disponível em: http://www.datavenia.net/entrevistas/00001092001.htm. Acesso em 12 out. 2022.

MOUGENOT, Edilson. Curso de Processo Penal. São Paulo: Saraiva, 2012.

PECK, Patrícia Pinheiro. *Direito Digital: em defesa do mundo virtual*. Fevereiro, 2009. Disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2901. Acesso em 23 out. 2022.

PINHEIRO, Patrícia Peck; HAIKAL, Victor. *Nova lei de crimes digitais.* In: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2. ed. São Paulo: Thomson Reuters, 2016.

PINHEIRO, Patrícia Peck. *Guerra digital e ciberterrorismo*. In: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2. ed. São Paulo: Thomson Reuters, 2016.

QUEIRÓZ, Regis Magalhães Soares de. *Assinatura Digital e o tabelião virtual*. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.) et al. Direito e Internet – aspectos jurídicos relevantes. São Paulo: EDIPRO, 2000.

REINALDO FILHO, *Demócrito. Direito da Informática: Temas Polêmicos*. São Paulo: Edipro, 2002. 432p.

TASHIRO, William. *Direito ao anonimato na Intern*et. Jusbrasil, 2015.

VIANNA, Rafael. Fraudes na Internet. Disponível em: https://cra-pr.org.br/fraudes-na-internet/ . Acesso em 17 nov. 2023.

WEBER, Sandra Paula Tomaz. *A utilização da assinatura eletrônica biométrica na formação dos contratos*. In: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2. ed. São Paulo: Thomson Reuters, 2016.

ZANATTA, Leonardo. *O Direito Digital e as implicações cíveis decorrentes das relações virtuais*. Trabalho de Conclusão de Curso para obtenção do grau de Bacharel em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul. 2010. Disponível em: http://35.238.111.86:8080/jspui/bitstream/123456789/241/1/Zanatta_Leonardo_O%20direito%20digital.pdf. Acesso em 20 out. 2022.