Centro Universitário de Brasília - UniCEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

GABRIEL MAGALHÃES GALVÃO BORGES

DIREITO CIBERNÉTICO: As mídias sociais e a relevância das legislações no âmbito virtual

BRASÍLIA
2023

GABRIEL MAGALHÃES GALVÃO BORGES

DIREITO CIBERNÉTICO: As mídias sociais e a relevância das legislações no âmbito virtual

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).

Professor(a) Carlos Orlando Pinto

BRASÍLIA
2023

GABRIEL MAGALHÃES GALVÃO BORGES

DIREITO CIBERNÉTICO: As mídias sociais e a relevância das legislações no âmbito virtual

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 (a): M.e Carlos Orlando Pinto

BRASÍLIA, ____,_____ de 2023.

BANCA AVALIADORA

_____

Professor Carlos Orlando Pinto

_____

Professor(a) Avaliador(a)

DIREITO CIBERNÉTICO: As mídias sociais e a relevância das legislações no âmbito virtual

Gabriel Magalhães Galvão Borges[1]

Resumo: O objetivo desta pesquisa consiste em investigar aspectos complementares relacionados à inovação tecnológica da internet na sociedade contemporânea, examinando os campos do direito digital e do direito cibernético, a fim de aprofundar o conhecimento das leis aplicadas ao ciberespaço, com especial ênfase na relevância da privacidade nesse ambiente. Um maior entendimento do direito cibernético se evidencia benéfico para a sociedade atual, na qual a maioria das pessoas, pelo que se verifica, até mesmo pelo senso comum, possui acesso à internet. Esse conhecimento pode contribuir para reduzir o número de casos de crimes virtuais. Além disso, utilizar o direito cibernético de maneira eficaz pode garantir a paz social no ambiente digital. Para conduzir esse estudo, a metodologia adotada envolveu uma revisão bibliográfica e a aplicação de métodos de investigação científica, com base nas legislações pertinentes.

Palavras-chave: direito cibernético e direito digital; internet; redes sociais; crime cibernético.

Sumário: Introdução. 1. A interação virtual alcançou a realidade virtual. 2. Crimes cibernéticos e a relevância das legislações virtuais. 3. Diretrizes das comunidades e a importância da privacidade no âmbito virtual. Considerações finais. Referências.

[1] Bacharelando em Direito pela Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília. E-mail: gabriel.magalhaes@sempreceub.com

INTRODUÇÃO

A revolução tecnológica trouxe transformações positivas em vários campos da vida humana, auxiliando, muitas vezes, a suprir as deficiências da sociedade. A tecnologia visa atender as necessidades globais, mas, também, criar necessidades através de estímulos que estão presentes na economia, vida profissional, informação e comunicação. Isso também ocorre no direito, que vive hoje uma fase de grandes aperfeiçoamentos e renovações.

Na segunda metade do século XXI a humanidade experimentou um avanço tecnológico inimaginável: os novos meios de comunicação e a manipulação de dados, popularmente conhecida como internet, ganhando espaços nas interações sociais.

Não obstante, as implicações das tecnologias digitais e recursos disponibilizados pela internet, sendo mais específico, nas redes sociais, podem motivar sérios problemas em razão do seu mal uso e ao não preparo do judiciário, acerca do modo ilícito com que a internet está sendo utilizada: a prática de delitos, como crimes contra a imagem, honra e liberdade pessoal, o crime de invasão ao dispositivo informático, extorsão, furto qualificado mediante fraude ou confiança, estelionato, dentre outros.

Essas condutas praticadas por pessoas de má índole lesionam direitos de terceiros. Diante disso, restou evidente demonstrar, que atualmente, a legislação brasileira já apresenta um aparato legal no ordenamento jurídico pátrio, mas implica em um desafio aos operadores do direito, em suma, na sua tipificação penal. E que, por conta de alguns fatores, como a privacidade e anonimato, criminosos virtuais utilizam da tecnologia para se manterem em práticas delitivas e que passaram comumente a serem chamados de crimes cibernéticos.

O objetivo deste artigo é, inicialmente, explicar que a internet é uma propulsora de mudança e que transformou a forma de se comunicar, aprimorando o que conhecemos hoje como direito digital.

Da mesma forma, surge o grande desafio da atualidade, restando analisar e responder ao seguinte problema: em que âmbito do direito digital e as redes sociais podem impactar no cotidiano social? Tendo em vista que atualmente os próprios indivíduos optam por manter seus laços sociais de maneira virtual,

consequentemente estão mais propensos aos crimes cibernéticos em um ambiente virtual e à violação da privacidade, sendo esse considerado um direito fundamental e da dignidade humana.

Por fim, além de demonstrar a importância dos avanços da internet na sociedade e o uso das redes sociais, busca-se verificar a forma de uma relação tênue entre a dignidade e os direitos fundamentais. Justificando a tutela pelo Estado e a mudança cotidiana de crimes cibernéticos dos usuários na rede, mostrando a prática de alguns crimes comuns que acontecem rotineiramente. Por último, busca compreender a necessidade de os direitos também serem resguardados no ambiente virtual, a partir da legislação e das diretrizes das redes sociais.

A metodologia de abordagem aplicada para este estudo utilizou o procedimento de levantamento bibliográfico, leituras de artigos que esclarecem e apresentam as peculiaridades quanto à privacidade na internet e suas fundamentais renovações nas esferas do mundo jurídico.

1. A INTERAÇÃO VIRTUAL ALCANÇOU A REALIDADE VIRTUAL

A revolução tecnológica na sociedade contemporânea causou transformações positivas em vários campos da vida humana, auxiliando, muitas vezes, a suprir as deficiências da sociedade.

Desde a década de 1990, com o surgimento da internet, a facilidade de conectar pessoas ficou ainda mais tangível com o seu aprimoramento. Por intermédio da chegada da internet, novas tecnologias também ganharam espaço, possuindo características particulares que a distinguem uma das outras.

O mundo moderno já tem aplicações interessantes para a realidade virtual, tudo isso possível graças aos avanços tecnológicos em *hardwares*[2] e conectividade que consolidaram no século XXI, as principais delas, a internet.Com a internet, é verificado o aumento dos recursos para as mais diversas realidades, como ferramentas voltadas para diversas funcionalidades, mas, todas fundamentais para a conhecimento da sociedade da informação. (TORQUATO, 2008)

[2] Hardwares: são os componentes físicos de um sistema computacional. Eles são as partes tangíveis e palpáveis do computador, que incluem dispositivos como processadores, memória RAM, discos rígidos, placas de vídeo, placas-mãe, teclados, mouses, monitores, entre outros.

As redes de computadores parecem complexas porque, com o seu desenvolvimento, as novas tecnologias podem ser usadas e combinadas de muitas maneiras, sem precedentes, conforme acompanhamos nos tempos atuais. Mas há de se imaginar que ligações telefônicas discadas evoluíram para diálogos instantâneos com a evolução da tecnologia. Isso prova o porquê do mundo digital ser, sim, o futuro da comunicação.

Com início da popularização da internet, em meados dos anos 2000, boa parte da sociedade não entendia do que isso se tratava. Com essa grande chegada, uma nova forma de se comunicar ganhou força. Outro tipo de serviço de comunicação e entretenimento começou a crescer cada vez mais e conhecemos hoje como as redes sociais.

Com o surgimento das redes sociais as pessoas têm se relacionado de acordo com suas preferências e individualidades. Toda essa ligação social, conexão e a interação entre os grupos diante das redes sociais foram se tornando mais frequentes.

A tecnologia visa atender às necessidades globais mas, também, criar necessidades através de estímulos que estão presentes na economia, vida profissional, informação e comunicação. Isso também ocorre no direito, que vive hoje uma fase de grandes aperfeiçoamentos e renovações. Com a nova realidade da internet, o direito começou a apresentar grandes obstáculos, de forma que acompanhou essa possível evolução, possuindo diversos desafios para sanar a complexidade do direito no ciberespaço[3].

O conjunto de normas, aplicações, conhecimentos e regulação das relações jurídicas realizadas no meio digital são imprescindíveis para conceituar o que é o direito digital.

O aprimoramento do direito digital, adveio visando apresentar normas e regulamentações do uso desses ambientes digitais pelas pessoas, além de garantir a esses usuários, informações presentes nesses espaços.

Na mesma temática, para apresentar o contexto no qual o direito digital está inserido, Antônio Jeová Santos também elucida que:

---

[3]O ciberespaço como "espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores" (LÉVY, 1999, p. 92), na qual é considerada uma plataforma de uma nova realidade humana.

> A Internet tornou-se mais uma forma de extensão do homem. Extensão que é coroada pelo fato de estar em determinados lugares ao mesmo tempo, que dando imóvel. Pode-se conversar com alguém que esteja além-mar. Com o Oriente, com a América e, até, com um vizinho. Vizinho no aspecto físico corporal, porque no mundo mítico da Internet há como que uma aproximação do Oriente com o Ocidente, estendendo as possibilidades do ser humano que é a deslocação rápida,eficaz e sem maiores traumas, pois basta um click para a viagem começar. (SANTOS, 2001, p.22)

Portanto, observa-se que a busca da sociedade por informações está intrinsecamente ligada às inovações tecnológicas. Ao compararmos com a sociedade da informação, percebemos que conceitos estão sendo aprimorados e desafiando nossa compreensão sobre presença física, revolução, conexão, habilidades, inovação e muitos outros que agora fazem parte do nosso dia a dia e, além disso, estão modificando a maneira como percebemos o mundo e atribuímos significado às informações e conhecimentos que elas contêm. O próprio tema "tecnologia", de forma inconsciente, leva as pessoas a se submeterem às tecnologias digitais, como computadores, smartphones e smartwatches, entre outros.

Segundo Mosé (2013), a sociedade da informação vem passando por modificaçõese já caminha para a sociedade do conhecimento.

> [...] A cada dia essas mudanças são mais significativas, que é a democratização do acesso ao conhecimento. A internet em algumas sociedades é chamada de sociedade da informação, mas logo, logo, ela vira sociedade do conhecimento. A sociedade da informação é quando ainda não tinha rede social, com a rede social, você não apenas tem um banco de dados disponível nas novas mídias, mas você tem pessoas ao vivo, em tempo real, discutindo questões, que vão do meio ambiente, a questões da física ou da medicina, da engenharia. Então hoje nós temos a sociedade do conhecimento, que é uma sociedade que produz conhecimento em tempo real, que pode ser acessada por qualquer aparelho móvel. Claro que eu posso ter internet e não ter acesso àquela rede social que me interessa. Então, além de ter a rede, eu tenho que ter algo que me faça ser aceita nessa rede, para que eu possa partilhar esse conteúdo. Então o que que é exigido hoje de um ser humano, de um homem, de uma mulher hoje, independentemente da idade? É preciso que essa pessoa tenha uma capacidade de fazer acordos, que ela tenha algo a partilhar e que ela tenha uma capacidade de análise e interpretação de dados. (MOSÉ, 2013, n. p.).

Então, surge a pergunta, em que âmbito do direito digital e as redes sociais podem impactar no cotidiano social? A chance de tais fatores procederem na realidade é correspondente a de ter ocorrido em âmbito cibernético, tendo em vista que opiniões existem em diversos contextos, portanto, a definição dada pelas redes sociais, ocasionada pela possibilidade da colaboração de terceiros, concebe em danos psicológicos acentuados em maior proporção, vigente a interpretação ali existente, de tal modo que supera o simples contratempo.

Assim como pode vir a criar aspectos futuros prejudiciais, não obrigatoriamente necessitamos dar ênfase no meio em que se encontra o direito criminal para tratar dos assuntos em detrimento do direito digital e sua atuação no cotidiano social. As vítimas que se encontram no meio cibernético, nem sempre são vítimas de crimes cibernéticos de forma designada, existem aspectos prejudiciais em quase todos os meios de relações.

2. CRIMES CIBERNÉTICOS E A RELEVÂNCIA DAS LEGISLAÇÕES VIRTUAIS

No que concerne ao direito digital para a população, a internet ainda se encontra em uma realidade paralela, na qual as pessoas se exibem de forma idealizada, no intuito de que sejam notadas por amigos, familiares e até desconhecidos como detentores de demasiadas perfeições, valores e experiências.

A popularização da internet nos últimos anos causou um amplo crescimento e facilitação na prática de crimes no âmbito digital, também conhecido como crime cibernético. Este acontece dentro da rede de computadores ou em um dispositivo conectado em rede, com o intuito de obter determinada finalidade.

Por ser considerado diligente e em constante aperfeiçoamento, o crime cibernético é um crime econômico com amplitude global, de complexa identificação e rastreamento, com impactos variados, cujos riscos e recompensas diferem do crime convencional. (BENSON; MCALANEY; FRUMKIN, 2018)

Segundo Burden, o crime cibernético pode ser compreendido pela prática de atividades ilegais realizadas mediante o uso da tecnologia, com objetivo de acessar ou comprometer sistemas computacionais. Constitui-se, dessa forma, em condutas maliciosas ou desonestas, originados no ambiente virtual ou herdados do mundo real, e são executados na internet. Os criminosos têm a sensação de facilidade, anonimidade, velocidade de operação e uma enorme quantidade de alvos. (BURDEN; PALMER, 2003)

Em qualquer plano, ainda nessa condição, o âmbito jurídico mundial contempla uma enorme necessidade de proteção, de tutela de dados e de garantias. No Brasil, mais de 35 milhões de famílias dispõem de uma conexão com a internet, conforme dados divulgados pelo IBGE em 2014, ou seja, sem uma legislação

apropriada todos esses indivíduos estavam sujeitos a serem vítimas de crimes e não conseguirem recorrer ao auxílio da Justiça.

O *modus operandi*[4] da realização de crimes cibernéticos é atualizado diariamente. Isso comprova que é um modo de crime de difícil investigação, precisando de autorização judicial, motivo pelo qual muitas vezes provas já se perderam e endereços de IPS[5] já foram mudados. Sendo considerado um crime que exige maior complexidade para sua apuração.

Entre as diferentes espécies de crimes virtuais que existem no âmbito digital, se encontram os crimes contra a imagem, honra e liberdade pessoal. Este último inclui a ameaça e, também, o *stalking*[6], na qual é considerado um tipo de perseguição, sendo muito mais fácil de se consumar na internet do que pessoalmente. Muitos desses crimes são plausíveis de pedido de indenização por danos morais[7].

Outros crimes também se encontram em alta no Brasil. Primordialmente, pode-se citar o crime de invasão ao dispositivo informático, sendo ele consumado quando a pessoa adentra em um aparelho ou dispositivo pessoal, rouba os dados, fotos pessoais e íntimas. Posteriormente, o invasor comete o crime de extorsão, ocasião que o mesmo ameaça a vítima a fim de obter uma vantagem financeira, na

---

[4]Modus operandi significa o modo de agir e, no mundo jurídico, é a expressão utilizada para caracterizar a forma peculiar que um criminoso (ou vários) tem de agir.

[5]Endereço IP significa “endereço do Protocolo de Internet”. O Protocolo de Internet é um conjunto de regras para comunicação pela internet para envio de e-mail, streaming de vídeo ou conexão a um site. Um endereço IP identifica uma rede ou dispositivo na internet.

[6]*Stalking* é um termo que vem do inglês e significa “caçar” ou “perseguir obsessivamente”.O *stalking* pode ser definido como a perseguição de uma pessoa por outra, seja fisicamente ou através da internet.

[7]Ensina Cristiano Chaves que: “A melhor corrente categórica é aquela que conceitua os danos morais como lesão a direitos da personalidade, sendo essa a visão que prevalece na doutrina brasileira. 35 Alerte-se que para a sua reparação não se requer a determinação de um preço para a dor ou o sofrimento, mas sim um meio para atenuar, em parte, as consequências do prejuízo imaterial, o que traz o conceito de lenitivo, derivativo ou sucedâneo. Por isso é que se utiliza a expressão reparação e não ressarcimento para os danos morais.

Além do pagamento de uma indenização em dinheiro, presente o dano moral, é viável uma compensação in natura, conforme reconhece enunciado aprovado na VII Jornada de Direito Civil (2015): “A compensação pecuniária não é o único modo de reparar o dano extrapatrimonial, sendo admitida a reparação in natura, na forma de retração pública ou outro meio” (Enunciado n. 589). Nos termos do enunciado, assim se situa o direito de resposta no caso de atentado contra a honra praticado por veículo de comunicação. Pontue-se que o direito de resposta foi recentemente regulamentado pela Lei 13.188, de 11 de novembro de 2015, que trata dos procedimentos judiciais para o seu exercício”.(Curso de direito civil: contratos. P. 503).

maioria das vezes, para devolver o acesso ou não divulgar esses dados. (art. 158 CP[8])

Também pode-se citar o crime de furto qualificado mediante fraude ou confiança[9], por outras palavras, a clonagem de cartão. Com a popularidade de compras pela internet mediante cadastro no cartão em sites, *hackers* criminosos *hackea* esses sites e pegam os dados do cartão e fazem compras e até fins ilícitos.

Outro crime amplamente difundido e que merece destaque é o estelionato, uma prática criminosa em que indivíduos têm suas identidades e informações pessoais utilizadas de maneira indevida, sem o consentimento deles, com o objetivo de obter vantagens ou realizar ações ilícitas. Nesse tipo de delito os dados das vítimas são explorados para obter benefícios fraudulentos, como obter acesso a contas bancárias, adquirir produtos ou serviços, ou cometer outras formas de fraude. Esse crime representa uma grave violação da privacidade e pode causar danos significativos aos lesados, tanto financeiros quanto emocionais.

Além do estelionato, há uma série de outros crimes cibernéticos que representam ameaças significativas na sociedade contemporânea. Um exemplo é o roubo de identidade, no qual os dados pessoais de indivíduos são obtidos sem autorização e utilizados para fins fraudulentos, como abrir contas bancárias, obter empréstimos ou realizar compras online em nome da vítima. Esse tipo de crime pode causar sérios danos financeiros e emocionais às pessoas afetadas, além de levar a consequências legais e problemas de crédito.

Outra prática criminosa comum é o phishing[10], que envolve a tentativa de obter informações confidenciais, como senhas e números de cartão de crédito, por meio de comunicações falsas, geralmente por e-mail ou mensagens de texto. Os criminosos se passam por instituições financeiras, empresas ou organizações legítimas, induzindo as vítimas a fornecerem seus dados pessoais. Essas informações são então utilizadas para realizar transações fraudulentas ou cometer outros crimes.

---

[8]Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa.

[9]Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel.
Furto qualificado: [...]II - com abuso de confiança, ou mediante fraude, escalada ou destreza.

[10] Phising: é uma forma de fraude online em que os criminosos se passam por entidades confiáveis, como bancos, empresas ou serviços populares, para obter informações pessoais sensíveis dos usuários, como senhas, números de cartões de crédito ou informações bancárias.

Além disso, existe o ransomware[11], um tipo de malware que criptografa os dados de um dispositivo ou rede, tornando-os inacessíveis ao usuário. Os criminosos exigem um resgate (geralmente em criptomoedas) para descriptografar os dados e devolvê-los ao proprietário legítimo. Esse tipo de ataque pode afetar empresas, órgãos governamentais e até mesmo usuários individuais, causando prejuízos financeiros e interrupções significativas nos negócios.

É importante ressaltar que a prevenção e a conscientização são essenciais para mitigar os riscos relacionados a crimes cibernéticos. Medidas como o uso de senhas fortes, a proteção de dispositivos com programas antivírus atualizados e a adoção de práticas seguras de navegação na internet podem ajudar a reduzir a probabilidade de se tornar uma vítima. Além disso, as autoridades e organizações governamentais têm implementado legislações e políticas para combater esses crimes e garantir a segurança dos indivíduos no ambiente digital.

Conforme Vogt, Jackson Leandro (2013, p. 24) o crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é considerado um crime de fim, por natureza, isto significa que é um crime cuja sua especificidade só ocorre em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de extorsão, estelionato, falsidade ideológica, fraude, entre outros. Ou melhor, quer dizer que o meio de materialização da conduta criminosa pode ser virtual, todavia, em certos casos, o crime não.

Com os estudos cada vez mais constantes referente ao direito cibernético, a concepção de que internet é uma “terra sem lei” transfigurou. Atualmente, já se encontram legislações e artigos em virtude do ambiente virtual, sendo que, cada uma delas contribui para amplificar a segurança na hora da utilização de uma rede social. Uma vez tipificados, os crimes cibernéticos necessitam ser combatidos e evitados. Uma vez que o combate aos crimes

[11]Ransomware: é um tipo de malware (software malicioso) que tem como objetivo criptografar arquivos e bloquear o acesso a eles, geralmente exigindo um resgate (ransom) para desbloqueá-los. Trata-se de uma forma de ataque cibernético em que os criminosos utilizam técnicas de criptografia para tornar os arquivos inacessíveis ao usuário legítimo.
Malware: é uma abreviação de "software malicioso" (malicious software). É um termo genérico usado para descrever qualquer tipo de software projetado para causar danos, roubar informações ou obter acesso não autorizado a um sistema de computador, dispositivo móvel ou rede.

cibernéticos terá um maior amparo e antagonismo pela norma jurídica estabelecida por um Estado.

No Brasil, a partir de 2012, sobreveio um Projeto de Lei de nº. 2.793/11, que foi posteriormente transformado na Lei n.º 12.737/12, mais conhecida como Lei Carolina Dieckmann. A motivação para sua elaboração e sancionamento decorreu após o caso de repercussão da atriz brasileira Carolina Dieckmann. O incidente ocorreu em maio de 2011, em que a atriz teve seu computador pessoal invadido por *hacker*, possibilitando que o anônimo tivesse acesso a 36 fotos pessoais de cunho íntimo. Conforme a denúncia, o invasor exigiu R$10 mil para não publicar as fotos, porém a atriz recusou a exigência e teve suas fotos íntimas divulgadas.

A partir do presente caso, instaurou-se uma maior preocupação com os crimes cibernéticos no Brasil. Fato este que, infelizmente, exigiu uma pessoa popular ser vítima para que as autoridades começassem a se preocupar com a temática, no qual a atriz defendeu a causa e cedeu seu nome à Lei. Somente a partir da Lei houve uma ampla apuração para ter o conhecimento de quantas pessoas eram vítimas desse crime no país, por conta dos registros da tipificação criminal (art. 154-a do CP[12]), este instruído pela Lei Carolina Dieckmann.

Antes do surgimento da referida Lei, a ação praticada por invasores sem permissão de um ambiente virtual para subtrair dados pessoais já era considerado crime, mas não havia nenhuma norma que tratava detalhadamente sobre a matéria, tipificando essa conduta.

As preocupações com o crime cibernético vêm se tornando cada dia mais usuais. Portanto, o que paira é o questionamento se o Brasil tem condições de investigar autoria desses crimes.

Ao abordar a falta de conhecimento sobre as leis digitais, o aumento dos crimes cibernéticos não possui uma resposta simples de imediato.

Ao discutirmos os crimes que ocorrem no mundo físico é necessário que o infrator esteja fisicamente presente para realizar a ação, como um sequestro, um roubo ou qualquer outra atividade criminosa. No entanto, no caso dos crimes cibernéticos, as circunstâncias são diferentes. A natureza desses delitos ocorre no

[12]Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

ambiente virtual, onde o perpetrador pode estar localizado em qualquer parte do mundo e ainda assim realizar suas atividades criminosas. Não há a necessidade de proximidade física com a vítima, pois o crime é cometido por meio de dispositivos eletrônicos e da internet. Essa característica dos crimes cibernéticos apresenta um desafio adicional para as autoridades responsáveis pela investigação e repressão dessas atividades ilegais.

Existe uma série de programas e sistemas que o *hacker* pode invadir para se resguardar, na qual ele é capaz até de conseguir ocultar os rastros do ilícito, por exemplo, por advento de um dispositivo com IP falso ou ceder dados sequestrados em troca de criptomoedas, tendo em vista que são complicadas de serem rastreadas. Outro imenso obstáculo é a interpretação do crime digital, por ser algo relativamente recente, a penalidade para alguns crimes ainda é ampla.

Na mesma temática, VOGT, JACKSON LEANDRO (2013) que conclui o quanto segue:

> Legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente. Também importante frisar desde logo, que em computação forense as “testemunhas máquinas”, diferente do ser humano, não conseguem diferenciar “culpa” de “dolo”. Ou seja, um computador não traz informações de contexto da situação, tampouco consegue dizer se foi “sem querer”, sem intenção. Um exemplo disso é a tentativa de se tipificar o crime de envio de arquivo malicioso em e-mail. É sabido, que muitas pessoas, até por excesso de inocência, enviam e-mail com vírus para outras. Além disso, o computador pode ter se tornado uma máquina “zumbi”, sendo usada remotamente por terceiros para gerar este tipo de ação. Por isso, e tantas outras razões, devemos acompanhar esta discussão toda no Legislativo, visto que é necessária, e, de grande valida a todo o sistema jurídico do País. O crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não.

Diante da afirmação de Vogt, nota-se que a internet não é uma terra considerada sem leis, pois o perigo é iminente. Dependendo de como utilizá-la, o indivíduo pode acabar tornando-se vítima de um crime virtual, podendo perder seus dados e até ocasiões piores, causando um prejuízo enorme pela falta de conhecimento das legislações presentes no meio virtual.

No que concerne a crimes informáticos:

> [...] o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de

> princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. (DAMÁSIO, 2016, p. 49)

Conforme é abordado pelo especialista Leonardo Andrade, especializado em investigações de cibercrimes, os crimes cibernéticos chegam ao grau máximo de complexidade do direito virtual quando são provenientes da zona da internet que não pode ser localizada tão facilmente pelos tradicionais propulsores de busca, pois fica mais difícil a procura de rastros de suas ações, por conta da privacidade e anonimato. Dessa maneira, criminosos virtuais aproveitam da vulnerabilidade das leis, da ausência de fronteiras e da tecnologia para se manterem em práticas delitivas. (ANDRADE, 2015)

Consequentemente, surge a exigência de leis rigorosas e profissionais especializados na era digital, como procuradores, juízes e promotores que possuam um conhecimento adequado sobre como atuar nessa área. Quando esses profissionais não possuem um amplo entendimento da tecnologia podem se sentir inseguros e receosos de cometer atos abusivos em relação ao direito à privacidade. Portanto, é fundamental que esses operadores do direito adquiram conhecimentos especializados para lidar de forma eficaz e justa com os casos envolvendo crimes cibernéticos e garantir a proteção dos direitos individuais, ao mesmo tempo em que combatem as atividades criminosas no ambiente digital. (MELO, 2008)

Dessa forma, denota-se que o surgimento dos meios de comunicação em massa, sendo o mais considerável a internet, mas de modo geral a tecnologia de informações, provocaram um impacto relevante na sociedade contemporânea. Evidentemente apresentando pontos positivos à sua utilização e pontos negativos, principalmente se o usuário for vítima de algum crime, sendo impactado em seu cotidiano social.

É evidente que a sociedade da informação é responsável por romper as barreiras existentes e introduzir uma abordagem inovadora no que diz respeito à criação e utilização de informações. Por conseguinte, vemos que além de crimes praticados por *hackers*, a invasão de privacidade e o não respeito de diretrizes das comunidades em redes sociais, por exemplo, infringem do mesmo modo direitos amparados pela legislação.

No que concerne a crimes cibernéticos, confira-se o seguinte julgado:

> AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. REPRESENTAÇÃO POLICIAL. INVESTIGAÇÃO DE HOMICÍDIO. ORDEM DE QUEBRA DE SIGILO TELEMÁTICO DE USUÁRIOS NÃO IDENTIFICADOS EM ÁREAS ESPECÍFICAS. GEOLOCALIZAÇÃO. VIABILIDADE. AGRAVO REGIMENTAL DESPROVIDO. 1. Há diferenciação na proteção dada pela legislação ao conteúdo das comunicações mantidas entre indivíduos e às informações de conexão e de acesso às aplicações da internet. O tratamento desta última hipótese encontra-se no art. 22, e seus incisos, da Lei n. 12.965/2014, a qual exige para o seu deferimento a necessidade da medida para o prosseguimento das investigações; e, finalmente, a limitação da área e do período de tempo dos registros dos dados necessários. 2. "A Terceira Seção desta Corte no julgamento do RMS n. 61.302/RJ e do RMS n. 62.143/RJ, ambos de Relatoria do Min. ROGERIO SCHIETTI CRUZ, em sessão de 26/08/2020 (DJe de 04/09/2020), reconheceu, por maioria, a legalidade da ordem judicial que determina quebra de sigilo de dados informáticos estáticos relativos a dados pessoais e registros de conexão ou acesso a servidores, navegadores ou aplicativos de internet, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, desde que, presentes circunstâncias que denotem a existência de interesse público relevante, a decisão seja proferida por autoridade judicial competente, com fundamentação suficiente, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios mínimos que indiquem a configuração de suposta ocorrência de crime sujeito à ação penal pública" (AgRg no RMS n. 66.791/CE, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, DJe de 13/12/2021). 3. Agravo regimental desprovido. (AgRg no RMS n. 67.104/MA, relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 27/3/2023, DJe de 31/3/2023.)

A jurisprudência apresentada trata da quebra de sigilo telemático de usuários não identificados em áreas específicas, mediante a utilização de técnicas de geolocalização, em investigações de homicídio. O tema é relevante no âmbito do direito digital, pois envolve questões relacionadas à proteção de dados pessoais e à privacidade dos usuários da internet, bem como aos limites da atuação das autoridades em casos de investigação criminal. Nesse sentido, a jurisprudência apresenta um importante precedente para a aplicação da legislação brasileira no que diz respeito à quebra de sigilo telemático em investigações criminais envolvendo o uso da internet.

Considerando o que foi mencionado anteriormente, nota-se que a jurisprudência é de extrema importância para o Direito Digital, já que é através dela que se constrói a interpretação das leis e normas que regem o ambiente virtual, além de ser recente e se encaixar perfeitamente com o tema retratado no âmbito de crimes cibernéticos. No caso apresentado, o julgado trata da legalidade da ordem judicial que determina a quebra de sigilo de dados informáticos estáticos relativos a dados pessoais e registros de conexão ou acesso a servidores, navegadores ou aplicativos de internet, delimitada por parâmetros de pesquisa em determinada

região e por período de tempo, desde que presentes circunstâncias que denotem a existência de interesse público relevante.

A decisão destaca a diferenciação na proteção dada pela legislação ao conteúdo das comunicações mantidas entre indivíduos e às informações de conexão e de acesso às aplicações da internet. Além disso, exige que a ordem judicial seja proferida por autoridade judicial competente, com fundamentação suficiente, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios mínimos que indiquem a configuração de suposta ocorrência de crime sujeito à ação penal pública.

Assim, a jurisprudência se relaciona com o Direito Digital ao estabelecer diretrizes e limites para a atuação do poder público na investigação de crimes que envolvem o ambiente virtual, garantindo a proteção dos direitos fundamentais dos usuários da internet.

Na mesma temática, temos o caso recente:

> Suspeito de divulgar fotos de Marília Mendonça, Cristiano Araújo e Gabriel Diniz após a morte é preso no DF
>
> Jovem, de 22 anos, usou uma rede social para propagar imagens dos artistas feitas para laudo pericial do IML. 'Imagens foram obtidas de forma ilegal e distribuídas de forma indiscriminada na internet', diz Polícia Civil (CINTRA, 2023).

Na segunda-feira (17/04/2023), a Polícia Civil do Distrito .... prendeu um jovem de 22 anos suspeito de divulgar fotos dos artistas Marília Mendonça, Cristiano Araújo e Gabriel Diniz após suas mortes, por meio de redes sociais. As investigações apontaram que as imagens foram obtidas ilegalmente e distribuídas indiscriminadamente na internet. A prisão ocorreu durante a Operação Fenrir, realizada pela Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC) para combater crimes praticados na internet. O suspeito confessou o crime e está à disposição da Justiça, aguardando audiência de custódia. A ação tem como objetivo identificar administradores de perfis em redes sociais que divulgaram e compartilharam fotos e vídeos do corpo dos artistas, feitas para o laudo pericial no Instituto de Medicina Legal (IML). O nome do suspeito não foi divulgado.

Conforme estabelecido no artigo 212[13] do Código Penal brasileiro, a punição para aqueles que cometem o crime de vilipêndio de cadáver pode variar de 1 a 3 anos de detenção, além do pagamento de multa.

3. DIRETRIZES DAS COMUNIDADES E A IMPORTÂNCIA DA PRIVACIDADE NO ÂMBITO VIRTUAL

A internet, apesar de transmitir para alguns uma impressão diferente, não é um ambiente típico para quem busca privacidade. Seu usuário deve levar essa realidade em consideração. Fato este que a maioria dos dados da rede mundial de computadores transita sem qualquer tecnologia de segurança da informação.

De certa forma, com o surgimento da internet, além de revolucionar a comunicação em massa, facilitou sobremaneira a exposição da vida privada.

A capacidade de comunicação direta entre usuários, sem intermediários, apesar de apresentar pontos positivos que contribuem para sociedade da informação, expõe, também, pontos negativos quanto à insegurança e violação de direito e da liberdade, impactando de forma negativa em seu cotidiano social. Hoje, restam evidentes notícias de vazamentos de informações, dados, imagens, que ocasionam repercussões evasivas, como danos a vida dessas pessoas. Portanto, nota-se que o preponderante risco pertinente às redes sociais é a invasão de privacidade e a ofensa à dignidade de seus utilizadores.

É certo afirmar que, na internet, todos os tipos de interações praticadas deixam rastros nas redes sociais às quais o indivíduo está conectado, seja pelas postagens que realiza, compras, serviços utilizados, pesquisas. Diante disso, Vieira (2007, p.155) leciona que “O avanço tecnológico, ao propiciar o cruzamento de dados pessoais e o monitoramento eletrônico de indivíduos e empresas, agiganta-se como uma ameaça ao direito à privacidade”.

Empresas têm constantemente o hábito de controlar seus usuários, buscando regularmente informações por meio da coleta de dados e utilizando-as para obter vantagens comerciais ou de controle, muitas vezes sem autorização. No entanto, surge um problema na sociedade digital em que a privacidade é violada, o que tem um impacto direto na proteção da dignidade pessoal.

---

[13] Art. 212 - Vilipendiar cadáver ou suas cinzas: Pena - detenção, de um a três anos, e multa. Todos os direitos reservados.

Ao citar o grande escândalo de comercialização de dados motivado pela rede social Facebook, percebe-se um exemplo de descumprimento de diretrizes da rede social quanto à privacidade de seus utilizadores. No caso, uma empresa parceira captou informações confidenciais de mais de cinquenta milhões de usuários e os manipulou para o direcionamento personalizado de mensagens e propagandas políticas nas últimas eleições dos Estados Unidos. A intenção específica da empresa parceira era de “compilar perfis psicométricos que classificam as pessoas por tipo de personalidade, de modo a que pudesse encaminhar a elas mensagens políticas com maior probabilidade de influenciar suas decisões”. (KUCHLER, 2018)

O Google, ferramenta que apresenta uma variedade de serviços, onde muitos deles são interligados, está em constantes observações sobre o comportamento adotado pelos seus usufrutuários na internet. É verificado o que se pesquisa no site, localização de pessoas, comentários, compras, e outras formas de captação de informações que sejam capazes de melhor traçar a formação de um perfil acerca da personalidade da pessoa. E, não só como o modelo adotado pelo Facebook, o Google igualmente direciona a publicidade de seus clientes anunciantes. Nesses dois casos, a privacidade foi totalmente desrespeitada.

Para isso, é necessário que cada rede social em suas comunidades tenha suas diretrizes. Cada comunidade adotará as diretrizes como regras de comportamento. Como, por exemplo, no Youtube que estabelece preceitos. Caso o conteúdo do usuário viole os princípios que regem a rede social receberá um aviso e, posteriormente, poderá remover o conteúdo por demais motivos além de violações das diretrizes da comunidade. Por exemplo, um mandado ou uma denúncia de violação de privacidade da parte envolvida.

Com esses exemplos é possível perceber que a aplicabilidade de Leis ligadas ao âmbito tecnológico, intrinsecamente, não representa de maneira eficiente a garantia do direito à privacidade nas redes sociais. Porquanto, quanto a temática, está inserida sobre o contexto virtual. A complexidade é uma proposição.

Todas eventualidades e encadeamentos que se desenvolvem no universo da internet “não exigem apenas novas soluções jurídicas para os novos problemas, como também afetam a maneira como os problemas e as soluções jurídicas devem ser analisadas”. (LEONARDI, 2012, p. 39)

Na esfera da sociedade da informação, embora haja o espaço livre para exposição de opinião, estas atribuições do mesmo modo são asseguradas. O que se verifica, inclusive, nas disposições preliminares da Lei 13.709, de 14 de agosto de 2018. Lei esta alusiva à proteção de dados pessoais, a qual tem o "[...] objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". (BRASIL, 2018)

Esta Lei altera alguns pontos do Marco Civil da Internet, na qual seu objetivo é zelar pela manutenção dos dados pessoais. Em seu artigo 2º[14] tutela sobre o respeito à privacidade. Assim como em seu artigo 7º[15] é alegado que os dados pessoais são restritos, precisando da autorização do titular.

Comunidades virtuais pressupõe o conjunto de normas e conduta, regras que são comuns em cada rede social, observando principalmente a privacidade dentro das mesmas. Fato este que induz o princípio do respeito à privacidade e confidencialidade, na qual está relacionada com o campo da ética desde as últimas décadas do século passado.

Para compreender a privacidade como um direito humano fundamental e de personalidade, a Constituição Federal do Brasil de 1988 (BRASIL, 1988) abrange um amplo rol de direitos fundamentais. Dos artigos 5º ao 17º, a Constituição expressa os direitos inerentes ao ser humano que merecem a máxima tutela. O respeito à privacidade no que lhe concerne encontra-se nesse rol no art. 5º, inciso X que dispõe que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988)

Culminando com a promulgação da Declaração Universal sobre Bioética e Direitos Humanos da Unesco 11 (Organização das Nações Unidas para a Educação, Ciência e Cultura), em 2005, da qual faz parte como seu artigo 9, que diz:

> A privacidade dos indivíduos envolvidos e a confidencialidade de suas informações devem ser respeitadas. Com esforço máximo possível de proteção, tais informações não devem ser usadas ou reveladas para outros propósitos que não aqueles para os quais foram coletadas ou consentidas, em consonância com o direito internacional, em particular com a legislação internacional sobre direitos humanos. (ONU, 2005, p. 8)

[14]Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade; I - o respeito à privacidade; [...] IV - a inviolabilidade da intimidade, da honra e da imagem. [...]
[15]Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular. [...]

De fato, toda aplicação da legislação com a privacidade representa hoje um componente primordial das pessoas e da sociedade. Mostra-se uma pressuposição da busca de uma sociedade livre com o fator predominante para solidificação da própria liberdade de expressão. De outra forma, a eficácia dos ordenamentos jurídicos, apesar de demonstrar uma evolução nas questões inerentes a internet, esbarra na dificuldade de se acompanhar a frenética mudança do cenário digital e das novas tecnologias. (LIMA, 2016, p. 84)

Diante do desenvolvimento tecnológico hoje presente, a falta de controle nesses ambientes consegue propiciar condutas ilícitas, além de ser um risco à dignidade, à privacidade e à intimidade. Estas devem ser cessadas com a implantação de limites que projetem pontos aos quais os usuários podem atingir sem desrespeitar o direito alheio.

E sob esse entendimento, acha-se necessário que para a preservação da privacidade nesse cenário é fundamental ir além da aplicação pura e simples do que se está previsto na legislação, assim como, a busca de garantias se algum direito de terceiro for lesionado e impor limites às atuações virtuais, utilizando e aperfeiçoando a legislação vigente. Com o intuito de amenizar que o direito digital e as redes sociais possam impactar de forma negativa o cotidiano social dos usuários.

CONSIDERAÇÕES FINAIS

Nos últimos anos, discussões quanto ao direito digital têm alcançado destaque e curiosidade crescente por parte das pessoas. Por conseguinte, têm gerado debates, críticas e pesquisas.

As questões jurídicas que irão surgindo pelo uso de tecnologias inovadoras têm comprovado que o atual modo de solução de conflitos, método jurisdicional tradicional, está se adaptando em lidar com algo novo e diferente. Também é identificado que o sistema habitual apresenta desafios e atrasos para lidar e resolver essas novas disputas. Necessitando de rígidas leis, e maior preparação aos operadores da era digital, como procuradores, juízes e promotores.

O trabalho buscou demonstrar de que forma atualmente, no cenário do direito digital, as redes sociais podem impactar o cotidiano social. Apesar dos pontos positivos, há também maior probabilidade para o cometimento de violações de

direitos e liberdades, sendo abordado a violação do direto à privacidade. Direito este que, por ser considerado um direito fundamental e de personalidade, é digno de maior proteção.

Proteção percebida em tutelas legais que dialogam com a privacidade, mas que, por sua vez, sua aplicabilidade também é vista como falha por não conseguir abranger todos os casos e garantir plenamente o direito à privacidade nas redes sociais online, representando um obstáculo.

Dessa forma, entende-se que todas as leis que amparam os crimes cibernéticos e as que resguardam a privacidade e liberdade do usuário representam uma conquista da sociedade, na medida em que seus textos coincidem com os direitos fundamentais previstos na Constituição.

REFERÊNCIAS

ANDRADE, Leonardo. Cybercrimes na deep web: as dificuldades de determinação de autoria nos crimes virtuais.**Jus.com.br**, 2015. Disponível em: https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais. Acesso em: 10 set. 2022.

BENSON, V.; MCALANEY, J.; FRUMKIN, L.A. Ameaças emergentes para o elemento humano e contra medidas no cenário atual de segurança cibernética. Em Exames psicológicos e comportamentais em segurança cibernética. **IGGlobal**,p. 266-271, 2018.

BURDEN, K.; PALMER, C. Crime na Internet.**Computer Law & Security Review**, v. 19, n. 3, p. 222-227, 2003.

BRASIL. Superior Tribunal de Justiça. **AgRg no RMS n. 67.104/MA**. Relator: Ministro Joel Ilan Paciornik. Quinta Turma. Julgado em 27/3/2023. DJe de 31/3/2023. Acesso em: 1 jun. 2023.

CINTRA, Caroline. Suspeito de divulgar fotos de Marília Mendonça, Cristiano Araújo e Gabriel Diniz após a morte é preso no DF. **G1**, 17 abr. 2023. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2023/04/17/suspeito-de-divulgar-fotos-de-marilia-mendonca-cristiano-araujo-e-gabriel-diniz-apos-a-morte-e-preso-no-df.ghtml. Acesso em: 17 maio 2023.

JESUS, Damásio de. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. *E-book.*

KUCHLER, Hannah. Escândalo ameaça modelo do Facebook. **Folha de São Paulo**, 2018. Disponível em:https://www1.folha.uol.com.br/mercado/2018/03/escandalo-ameaca-modelo-do-facebook.shtml. Acesso em: 7 set. 2022.

LEONARDI, M. **A tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.

LÉVY, P. **Cibercultura**. São Paulo: Ed. 34, 1999.

LIMA, L. A. **O direito à privacidade nas redes sociais na internet**. 2016. Dissertação (Mestrado em Direitos Humanos) – Universidade Regional do Noroeste do Estado do Rio Grande do Sul,Ijuí,2016.

MELO, Leonardo Bueno de. Entrevista: Leonardo Bueno de Melo, perito da Polícia Federal**. Consultor Jurídico**, jul. 2008. Disponível em: https://www.conjur.com.br/2008-jul-20/falta_lei_informacao_beneficiam_cibercrime. Acesso em: 25 set. 2022.

MOSÉ, V. Os desafios da educação na Sociedade do Conhecimento.**Canal UNA TV**, 29 abr. 2013. 1 vídeo (15min.). Disponível em: http://www.youtube.com/watch?v=Zlr1VmBBOP s. Acesso em: 19 set. 2022.

SANTOS, Antonio Jeová. **Dano moral na Internet**. São Paulo: Método, 2001.

TORQUATO, C. Prefácio. *In:* POLIZELLI, D. L.; OZAKI, A. M. (org.). **Sociedade da informação:** os desafios da era da colaboração e da gestão do conhecimento. São Paulo: Saraiva, 2008.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Fabris, 2007.