CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

PEDRO LUCAS DOS SANTOS SILVA

O IMPACTO DA ERA DIGITAL NOS CRIMES CIBERNÉTICOS E A INFLUÊNCIA DO CORONAVÍRUS COMO FATOR AGRAVANTE

JUAZEIRO DO NORTE-CE
2023

PEDRO LUCAS DOS SANTOS SILVA

O IMPACTO DA ERA DIGITAL NOS CRIMES CIBERNÉTICOS E A INFLUÊNCIA DO CORONAVÍRUS COMO FATOR AGRAVANTE

Trabalho de Conclusão de Curso – *Artigo Científico*, apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Francisco Gledison de Lima Araújo.

JUAZEIRO DO NORTE-CE
2023

PEDRO LUCAS DOS SANTOS SILVA

O IMPACTO DA ERA DIGITAL NOS CRIMES CIBERNÉTICOS E A INFLUÊNCIA DO CORONAVÍRUS COMO FATOR AGRAVANTE

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de PEDRO LUCAS DOS SANTOS SILVA.

Data da Apresentação 06/12/2023

BANCA EXAMINADORA

Orientador: PROF. ESP. FRANCISCO GLEDISON DE LIMA ARAÚJO

Membro: PROF. ME. FRANCISCO THIAGO DA SILVA MENDES

Membro: PROF. ME. OTTO RODRIGO CRUZ

JUAZEIRO DO NORTE-CE
2023

O IMPACTO DA ERA DIGITAL NOS CRIMES CIBERNÉTICOS E A INFLUÊNCIA DO CORONAVÍRUS COMO FATOR AGRAVANTE

Pedro Lucas dos Santos Silva[1]
Francisco Gledison de Lima Araújo[2]

RESUMO

A Era Digital tem revolucionado inúmeros aspectos da sociedade contemporânea, e os crimes informáticos não é uma exceção. Este artigo aborda o impacto da Era Digital na criminalidade cibernética, com um enfoque particular na influência exacerbada do isolamento ocasioando pela chegada do vírus da Covid-19. O isolamento social e as medidas restritivas implementadas para conter a disseminação do vírus proporcionaram um ambiente favorável para o surgimento de novas modalidades de criminalidade e para o fortalecimento de grupos criminosos já estabelecidos. A escassez de recursos e a vulnerabilidade econômica de muitos indivíduos durante a crise sanitária os tornaram alvos propícios para golpes financeiros, fraudes online e extorsões. A digitalização das atividades criminosas introduziu desafios adicionais para as autoridades responsáveis pelo combate à criminalidade digital. A natureza transnacional desses grupos complica a aplicação da lei e a cooperação entre países. Ademais, a criptografia e outras técnicas de segurança empregadas nas comunicações digitais dificultam a interceptação e a investigação de suas operações. Diante deste cenário, é imprescindível que os governos e as agências de segurança intensifiquem suas estratégias de combate aos crimes cibernéticos na Era Digital. Isso implica a adoção de medidas legais, tecnológicas e de cooperação internacional para prevenir e investigar crimes cibernéticos, bem como promover a conscientização e a educação digital da população. Em suma, o coronavírus fez com que este cenário se tornasse mais inflacionado, criando um ambiente propício para o surgimento de novos delitos e fortalecendo grupos criminosos já existentes.

Palavras-Chave: Covid-19. Cybersegurança. Internet. Crimes.

ABSTRACT

The Digital Era has revolutionized several aspects of the contemporaneous society, and the organized crime is not an exception. This article argues about the impact of Digital Era on the organized crime, with emphasis on the aggravating influence of Corona virus. During the Corona virus pandemic, it has been observed a significant increase of organized crime in multiple parts of the world. Social isolation and the restriction measures imposed to contain the virus propagation have created a conducive environment to the emergence of new forms of crime and to strengthen already formed groups. The scarcity of resources and economic vulnerability of many individuals during the sanitary crisis had turned us into easy targets to financial scams, online frauds and extortion. The digitization of criminal activity has brought extra challenges to the authorities in charge of fight organized crime. The transnational nature

[1] Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão. E-mail: pedrolucasss12@hotmail.com
[2] Professor Orientador. E-mail: franciscogledison@leãosampaio.edu.br

of these groups hinders law enforcement and the cooperation between countries. Beyond that, cryptography and other security techniques used on digital communication make interception difficult as well as the investigation of operations. In front of the landscape, it is essential that the governments and their security agencies reinforce your fighting strategies against organized crime on Digital Era. This involves the adoption of legal, technological and cooperation international measures to prevent and investigate cybernetic crimes, in addition to promoting the awareness and digital education of the population. In short, the Corona virus pandemic worsened even more this scenario creating a favorable environment to the emergence of new crimes and strengthening already existing groups.

Keywords: Covid-19. Cybersecurity. Internet. Crimes.

1 INTRODUÇÃO

Atualmente, há um debate significativo sobre a influência da internet no comportamento humano. Com a disseminação da internet, surgiram novas formas de expressão e pensamento, resultando em uma mudança no comportamento social. Portanto, tornou-se necessário um novo estudo baseado nas mudanças provocadas pela internet.

Embora esse avanço tecnológico tenha gerado inúmeros benefícios para a sociedade, também é evidente os prejuízos que a internet causou com sua evolução ao longo do tempo. Conforme mencionado anteriormente, o ambiente virtual oferece oportunidades para relacionamentos pessoais, trabalho e lazer, proporcionando uma melhor experiência de vida para o indivíduo.

No entanto, juntamente com esses aspectos, o progresso da internet também aumenta a probabilidade de ocorrência de crimes virtuais, como roubo de dados financeiros, fraudes de identidade, extorsão cibernética e, principalmente, discriminação e propagação de ódio através das redes sociais.

Como é de conhecimento geral, um estado de calamidade pública assolou o mundo nos últimos anos. Assim, com a chegada da pandemia do coronavírus, a população brasileira se viu em confinamento por um determinado período. Como resultado, houve um aumento no uso da internet e, consequentemente, os crimes digitais também aumentaram consideravelmente, pois os cidadãos estavam confinados, sem poder sair para socializar e fazer compras.

Nesse contexto, de acordo com uma pesquisa realizada pela Confederação Nacional de Dirigentes Lojistas (CNDL) em conjunto com o Serviço de Proteção ao Crédito (SPC) em junho de 2021, 59% dos participantes desse ambiente sofreram algum tipo de fraude financeira nos últimos 12 meses, em contraste com 46% em 2019.

Em resumo, essa diferença corresponde a 16,7 milhões de brasileiros e, de acordo com a mesma pesquisa, a fraude mais comum está associada à compra de produtos que nunca chegam aos seus compradores. Portanto, é importante reconhecer que, após o crescimento exacerbado e inevitável da rede mundial de computadores, surgiram mecanismos capazes de proteger os dados e a integridade moral dos indivíduos nesse ambiente.

A relação entre o recente confinamento e a evolução dos recursos digitais é a principal causa do aumento dos crimes digitais ocorridos nos últimos anos. Assim, é necessário entender quais são os desafios enfrentados pelas autoridades na contenção e combate eficaz do crescente impacto da criminalidade organizada na Era Digital, especialmente durante a pandemia do coronavírus, e como mitigar suas consequências agravantes.

Acima de tudo, é de extrema importância traçar diretrizes para que, ao final da pesquisa, a pergunta supracitada seja respondida de maneira fundamentada e coerente. Portanto, o objetivo principal deste artigo é investigar e analisar a eficácia do atual ordenamento jurídico diante das mudanças, principalmente da pandemia, que resultaram em um aumento nos crimes virtuais.

Além disso, seguindo a mesma linha de pensamento, este trabalho também busca conhecer a evolução histórica da tecnologia até a chegada da indústria 4.0, compreender a história do direito digital ao longo do tempo, entender os impactos causados pela pandemia do COVID-19 no comportamento das pessoas e analisar a eficácia da legislação digital durante o período mencionado.

É inegável que o campo tecnológico não é completamente conhecido e compreendido por uma parcela da sociedade, tornando-se, portanto, imprescindível o estudo sobre o tema em questão. Nesse contexto, este trabalho tem a capacidade de explorar uma área que carece de proteção, especialmente considerando os fatores desencadeados pela pandemia do COVID-19. O ambiente digital tornou-se mais frequentado pela sociedade e, consequentemente, mais suscetível à má-fé dos participantes.

A título ilustrativo, uma matéria publicada por Dino no jornal Valor Econômico revelou que, segundo dados da Coordenadoria de Estatística e Análise Criminal (CEACrim) da SSP, o ano de 2020 registrou um crescimento de 265% nos crimes praticados no ambiente virtual, apenas no estado de São Paulo. Portanto, é de suma importância o estudo desta pauta para que os indivíduos possam compreender as causas e os mecanismos que auxiliam na prevenção de tais crimes.

2 A EVOLUÇÃO DA INFORMÁTICA

Conforme o site Educação Pública, em 2007, o fenômeno da globalização, aliado aos eventos das revoluções industriais, resultou em uma mecanização no comportamento da sociedade. Atualmente, nas empresas de qualquer segmento, é indispensável a contratação de um profissional da informática, seja para a utilização de recursos tecnológicos para uma melhor organização ou devido à necessidade de proteção de dados essenciais das empresas.

Portanto, destaca-se que "Não há instituições financeiras sem computadores e internet; a maioria dos serviços públicos requer uma central informatizada; grande parte das grandes empresas - se não todas - possui bancos de dados para controle orçamentário, contábil, de estoques e de clientes. Os pequenos empreendimentos certamente estagnarão ou desaparecerão se não se adequarem à realidade em estudo" (BRITO, AURINEY, 2017, p. 7).

Além de impactar o mercado de trabalho, o desenvolvimento tecnológico geracional afetou principalmente a rotina dos indivíduos, que passaram a participar mais frequentemente de ambientes virtuais. Dessa forma, também trouxe consigo malefícios inquestionáveis, tendo como principal foco da presente pesquisa, a criminalidade organizada na era digital, dentro das alterações e evoluções vivenciadas pela sociedade global.

Portanto, ressalta-se que a informática e todos os avanços tecnológicos tornaram-se ferramentas indispensáveis para a vida cotidiana dos indivíduos, seja no ambiente de trabalho, de comunicação social ou de lazer. Nessa perspectiva, é importante investigar como ocorreu esse avanço tecnológico e informático ao longo dos anos, pois, ao contrário da visão que temos nos dias atuais, no seu surgimento, a informática não era uma ferramenta acessível para toda a sociedade e, além disso, a chegada dessa ferramenta não se trata de um processo único, mas sim de diversos procedimentos que resultaram na informática atual (LIMA; ARAÚJO, 2021).

> Os estágios de evolução dos computadores são divididos em cinco gerações. A 1ª Geração (1940-1952) foi formada por computadores à base de válvulas a vácuo; na 2ª Geração (1952-1964), a substituição das válvulas por transistores; na 3ª Geração, a substituição dos transistores por circuitos integrados e a miniaturização dos grandes computadores; a 4ª Geração foi marcada pela substituição dos circuitos pelos microprocessadores; e na 5ª Geração (1981) ocorreu um grande avanço da computação com a utilização da Inteligência Artificial, assim como a massificação do uso da internet. (BRITO, 2017, p. 8).

Nessa perspectiva, ao realizar uma análise mais aprofundada, o primeiro computador surgiu no ano de 1946, sendo denominado de ENIAC (*Eletronic Numerical Integrator and Computer*). A pedido do exército norte-americano, os pesquisadores John Eckert e John Mauchly apresentaram ao mundo o primeiro computador da história. O ENIAC pesava 30 toneladas e ocupava uma área correspondente a 180 metros quadrados.

O sistema do primeiro computador visto no mundo baseava-se em um esquema de cartões perfurados, sendo que cada conjunto de furos significava uma operação ou um número, pois a principal utilidade da máquina era fazer cálculos. Assim, o substantivo “computador” aparece, já que vem do verbo computar e tem como sinônimo o verbo “calcular” (FRANZÃO, 2021).

Até a década de 70, os computadores eram de difícil manuseio, pois eram controlados através de um analógico e, com o avanço de suas atribuições, ficava cada vez mais difícil utilizar a máquina. Em virtude disso, a empresa Xerox conseguiu desenvolver dois aparelhos com o intuito de facilitar o manuseio do computador: o mouse e a interface gráfica. Sendo assim, as referidas máquinas da época se aproximavam cada vez mais das que vemos hoje em dia, pois já com a facilidade empregada no manuseio do mouse e a interface gráfica sendo novos componentes da ferramenta, temos a certeza de que houve uma evolução considerável.

É certo que a máquina passava por evoluções consideráveis, mas ainda faltavam alguns componentes para que o manuseio e a utilidade do computador fossem melhor aproveitados. Por conta disso, em 1975, a empresa Microsoft criou um sistema operacional que se baseia em um conjunto de software com o objetivo de gerenciar e administrar um sistema de um computador (MEYER, 2018).

3 INFLUÊNCIA DA INTERNET NA SOCIEDADE

Portanto, com foco na 5ª geração da informática, a internet desempenha um papel crucial para a problemática da pesquisa. A internet foi criada durante a Guerra Fria, em meados dos anos de 1960. Conforme Auriney Brito, ocorreu um experimento financiado pelo Departamento de Defesa dos Estados Unidos e desenvolvido pela *Advanced Research Projects Agency - ARPA*, por meio de um de seus departamentos, o IPTO (*Information Processing Techniques Office*) (BRITO, 2020).

Isso culminou na primeira forma de comunicação entre computadores, denominada ARPANET. Nos anos subsequentes, foram realizados vários testes e, em 1973, foi conduzido um experimento sob a liderança do acadêmico Vinton Cerf, professor da Universidade de Stanford, com o envolvimento do governo norte-americano no projeto.

> Cerf, juntamente com o engenheiro Robert Kahn, também designado para administrar o funcionamento da Arpanet, foi o responsável pela criação de um pequeno mecanismo que permitiu que dois computadores conversassem entre si, no mesmo idioma, quando ligados na rede. E, o que era melhor, possibilitou que duas ou mais redes de computadores também se comunicassem, falando a mesma língua. Esse

> mecanismo, batizado com o horrível nome de otocolo TCP/IP - sigla em inglês para Transfer Control (VIEIRA, 2003, p. 5).

Assim, foi desenvolvido o primeiro programa de navegação da história da internet, o Mosaic. Isso possibilitou o compartilhamento de textos, imagens e símbolos entre os computadores que, naquela época, já possuíam uma interface gráfica acessível a todos.

Portanto, foi o primeiro grande movimento da internet no mundo. No contexto nacional, a internet chegou ao Brasil em 1988, por meio de uma parceria com os Estados Unidos.

> O primeiro contato do Brasil com a Internet ocorreu em 1988, quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), ligada à Secretaria Estadual de Ciência e Tecnologia, realizou a primeira conexão à rede através de uma parceria com o Fermilab, um dos mais importantes centros de pesquisa científica dos Estados Unidos. A façanha coube aos professores Oscar Sala e Flávio Fava de Moraes, da Universidade de São Paulo (USP), que tocaram o projeto em conjunto e inauguraram a conexão oficialmente no ano seguinte. (VIEIRA, 2003, p. 8).

O governo federal brasileiro começou a utilizar a ferramenta da internet apenas em 1992, por meio da RNP (Rede Nacional de Pesquisa). A RNP estabeleceu uma espinha dorsal baseada em uma grande estrutura para suportar os cabos da rede mundial de computadores, espalhando pontos de conexão pelas principais capitais do país. Segundo Eduardo Vieira, no mesmo ano, no Rio de Janeiro, ONGs também buscavam disseminar o serviço para que toda a população do estado tivesse acesso à mais nova ferramenta tecnológica da época. Dessa forma, a internet ganhava força no Brasil.

É certo que a chegada da rede mundial de computadores no Brasil ocorreu de maneira relativamente tardia quando comparada ao dia de seu surgimento e utilização. No entanto, quando se compara com o resto do mundo, observa-se que, até nos dias atuais, a internet ainda é um privilégio em alguns países, como, por exemplo, a população da Coreia do Norte, a população rural da China e do Paquistão.

A título exemplificativo, em uma pesquisa realizada pelo portal DataReportal em agosto de 2020, a população norte-coreana é a que menos possui acesso à internet, pois sua rede global é bloqueada e, sendo assim, a população não tem acesso à internet de fato, uma vez que utilizam apenas a rede doméstica. Em termos de porcentagem, países como Sudão do Sul, Eritreia, Burundi e Somália têm mais de 90% de sua população sem acesso à rede mundial de computadores.

No que se refere à quantidade de pessoas em um só país, verifica-se que as regiões mais afetadas pela falta de internet são a Ásia e a África, segundo dados da mesma pesquisa. Portanto,

é importante ter em mente que, apesar de o Brasil ter adotado o uso da internet um pouco tarde, trata-se, até hoje, de um privilégio quando comparado aos países supracitados.

3.1 SOCIEDADE DA INFORMAÇÃO

O termo “sociedade da informação” se manifestou ainda no século XX, mais precisamente por volta dos anos 70, período em que houve a evolução e o surgimento de vários artefatos tecnológicos, aumentando a produção e a quantidade de pessoas que passaram a utilizar a tecnologia (NOVO, 2023).

Conceitualmente, a sociedade da informação busca proporcionar aos indivíduos um processo de comunicação mais rápido, prático e eficiente por meio da inovação tecnológica ocasionada pela globalização. Assim, a sociedade da informação oferece novas possibilidades de obter fontes de conhecimento e de comunicação em qualquer lugar ou horário. Diante disso, o mundo digital e a evolução da sociedade da informação apresentam desafios para o mundo jurídico, uma vez que a legislação não consegue acompanhar (NOVO, 2023).

Segundo Alvin Toffler (PINHEIRO, 2008, p. 6), três ondas caracterizam a evolução da humanidade. A primeira onda representa a era agrícola, fundamentada na propriedade da terra como instrumento de riqueza e poder. A segunda onda coincide com a denominada revolução industrial, com seu ápice no tempo da Segunda Grande Guerra. Nesta, a riqueza consiste na combinação da propriedade, do trabalho e do capital.

A terceira onda é a da informação. Suas primeiras manifestações ocorreram ainda antes do apogeu da segunda onda, com o surgimento de grandes invenções no campo das comunicações, como o telefone, o cinema, o rádio e a TV (séc. XX). Com o avanço tecnológico, a difusão dos meios de informação e a transformação dessas fontes de informação em mecanismos mais rápidos, práticos e de fácil acesso, houve um aumento significativo de pessoas que acessavam a internet, modificando completamente o ambiente digital.

Assim como a sociedade natural, o campo da internet torna-se carente de atenção e regulamentação para ser mais seguro para os usuários, pois também existem pessoas mal-intencionadas no ambiente virtual. Desse modo, o que se tem em mente é que esse ambiente digital, nos dias atuais, precisa de muito mais colaboração e transparência entre os usuários para que possa seguir de uma maneira saudável e que possa viabilizar as punições daqueles que não seguem a ética e a boa-fé dentro da rede mundial de computadores.

4 DIREITO DIGITAL

O Direito Digital é um ramo jurídico que surgiu em resposta às significativas atualizações tecnológicas que ocorreram ao longo do tempo. Assim, emergiu a necessidade de fiscalizar e regulamentar o uso dessas ferramentas dentro da sociedade da informação. A disciplina do Direito Digital não tem uma origem antiga. De fato, é considerada uma matéria recém-nascida quando comparada às demais áreas do direito, pois estima-se que sua idade não ultrapasse 20 anos.

> O Direito Digital vem sendo considerado uma nova disciplina jurídica. Sua idade é estimada em duas décadas. Costuma-se dizer que a Portaria Interministerial 147, de 31 de maio de 1995, editada pelos ministros da Comunicação e da Ciência e Tecnologia, que regulou o uso de meios da rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet, foi o primeiro diploma legal desse ramo (ARAÚJO, 2017, p. 17).

Consequentemente, destaca-se que o Direito Digital é um ramo que ainda não foi completamente explorado, dado que é recente a sua criação. Quando se trata de uma disciplina tão atual e de difícil regulamentação como o Direito Digital, é necessário um prazo maior para que tenha sua eficácia plena, permitindo que a sociedade conheça suas normas e as aplicações destas. Tendo em mente o que foi citado, é de grande relevância mencionar os primeiros registros concretos acerca do Direito Digital.

> A pesquisa do Prof. João Marcello de Araújo Jr., apresentada no Congresso de Würzburg (Alemanha), em outubro de 1992, demonstrou, entretanto, que, pelo menos desde 1976, a Câmara dos Deputados e o Senado tramitaram projetos de lei que tratavam de informática. São exemplos: o projeto de lei nº 3.279, de 1976, do Deputado Siqueira Campos, que dispunha "sobre a programação viciada de computador" (arquivado em 1979); o projeto de lei nº 96, de 1977, do Senador Nélson Carneiro, que dispunha "sobre a proteção das informações computadorizadas" (REIS, 1997, p. 50).

Conceitualmente, Patrícia Peck traz em sua bibliografia a seguinte definição:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicadas até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional, etc. (PECK, 2007.)

Portanto, com base no que foi mencionado, entende-se que o Direito Digital representa apenas uma nova área de prática, pois grande parte dos direitos debatidos por ele também são regulados por outros ramos do direito. Os crimes, de certa forma, podem ser punidos de acordo com o Código Penal, as indenizações cabíveis podem encontrar fundamento e amparo no Código Civil e de Processo Civil. Além disso, o Direito Digital também pode se fundamentar

no disposto em outras leis, como por exemplo, o Código de Defesa do Consumidor, que serve de embasamento para relações também pertencentes ao Direito Digital.

Em contrapartida, é importante mencionar que não podemos sobrecarregar nosso ordenamento jurídico com leis específicas para todos os casos. Já que as questões de direito autoral podem ser resolvidas pelo Direito Civil, os crimes pelo Direito Penal e outras questões por demais áreas, podemos nos fundamentar no que já existe, proporcionando uma segurança jurídica para o usuário da internet, desde que o direito também acompanhe a sociedade de acordo com a sua evolução. Dessa maneira, neste aspecto, não se trata de criar um "Direito da Internet", mas sim de manter nossas leis referentes a esse ambiente sempre atualizadas para garantir a eficácia de sua aplicação.

Neste tópico, temos em mente que o principal desafio para o Direito Digital não é a sua especialidade no que diz respeito à sua matéria, e sim, a dificuldade do legislativo em acompanhar as evoluções tecnológicas. Isso não significa que o legislativo tenha se omitido da regulamentação da área, de fato, no Brasil tivemos um atraso em todo o campo de atuação do Direito Cibernético, mas em qualquer lugar do mundo seria difícil regulamentar algo que está em constante evolução e mudança de uma maneira tão rápida.

Portanto, é importante que neste ramo jurídico os princípios possuam a mesma força ou até mais em comparação às normas. Como consequência, o princípio da autorregulamentação torna-se de extrema relevância.

> No Direito Digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa. Por isso, a disciplina jurídica tende à autorregulamentação, pela qual o conjunto de regras é criado pelos próprios participantes diretos do assunto em questão com soluções práticas que atendem ao dinamismo que as relações de Direito Digital exigem. (PECK, 2007).

Outro desafio do Direito Digital é o paradigma existente entre a liberdade e o anonimato na internet. Com o passar dos anos, o surgimento de novas redes sociais, novas ferramentas tecnológicas e formas de interação, as pessoas conseguem, atualmente, esconder-se atrás do anonimato para, por meio da internet, praticar crimes digitais que infringem a honra, a dignidade e a privacidade de outras pessoas.

O anonimato, quando ligado à manifestação de pensamento, é vedado, de acordo com o art. 5°, inciso IV da Constituição Federal. Entretanto, a Lei Geral de Proteção de Dados, em seu artigo 18, inciso IV, assegura que o titular das informações pode requerer a anonimização, bloqueio e eliminação de dados pessoais desnecessários que não estejam em conformidade com a lei. De fato, trata-se de um assunto polêmico, pois as pessoas se utilizam desse artifício para

o cometimento de crimes de ódio e disseminação de *fake news*. É uma questão a ser resolvida ou amenizada principalmente pela conscientização de toda a população usuária da rede mundial de computadores.

A privacidade, embora seja um direito garantido a todos, não é o principal debate, pois existem outros pontos a serem mencionados. Por exemplo, nos casos de empresas que compartilham formulários na internet para os clientes preencherem com seus dados, reflete claramente uma falta de informação por parte da população.

Logicamente, é um crime utilizar os dados de pessoas para outros fins sem o seu consentimento, além de infringir princípios do Direito Digital, mas à medida que cresce o número de empresas se valendo de ações ilegais para obter vantagem, também é necessário que cresça o número de informações para a sociedade. Esse argumento se torna válido pois a proteção à privacidade já está regulamentada, por isso é relevante mencionar uma lição de Patrícia Peck:

> Logo, não há lacuna jurídica no tocante à solução da privacidade na Internet. Há, sim, falta de entendimento quanto à aplicação de leis em vigor para questões relativamente novas, que exigem uma interpretação da norma e sua adequação ao caso concreto. Este é um princípio fundamental para a aplicação do Direito, o qual, consequentemente, deve ser adotado também no Direito Digital. (PECK, 2007).

5 CRIMES DIGITAIS

Ao conceituar crimes digitais, entende-se que se trata de delitos cometidos por meio da informática, visando prejudicar tanto os bens já tutelados no ordenamento jurídico atual, quanto aqueles bens jurídicos particulares ao Direito Digital. Segundo Rocha (2017, p. 13), os crimes cibernéticos são “condutas ilícitas realizadas por algum tipo de dispositivo tecnológico (…) por entender-se que as realizações das condutas são dadas em um ambiente virtual”.

Na mesma linha de raciocínio, o conceito analítico de crime definido pelo Direito Penal também pode se estender à área do Direito Digital. Dessa forma, crime é uma ação humana, antijurídica, típica, culpável e punível. No entanto, esse conceito deve ser adaptado para o ambiente virtual, pois, como já foi mencionado, certos conceitos presentes no Direito Digital já se encontram positivados em outros ramos jurídicos.

Portanto, os crimes digitais podem sim ter uma definição com base no Direito Penal, contudo, acrescentando uma nova característica a esse conceito que nada mais é do que o local da sua prática. Em razão disso, os crimes digitais precisam dos requisitos cumulativos presentes

no conceito analítico de crime, mas também precisam, necessariamente, serem efetuados por meio de algum artifício tecnológico.

Ainda no conceito de crime virtual, tem-se:

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o anonimato é possível na Web e que a Internet é um "mundo sem lei (BRASIL, p.23, 2008).
> (...)
> Os primeiros crimes relacionados à informática foram praticados na década de 1960, nos Estados Unidos. Na época, começaram a aparecer na imprensa e na literatura científica norte-americana os primeiros casos de uso de computadores para cometer delitos como sabotagens e espionagem. Somente na década seguinte, foram iniciados estudos sistemáticos e científicos sobre o tema. A partir de 1980, as ações criminosas intensificaram-se, envolvendo principalmente manipulação de dados bancários, pirataria de programas de computador, abusos nas telecomunicações e pornografia infantil (BARROS, 2006).

Segundo Marcelo Xavier Crespo (2011), o termo "crimes digitais" pode abranger diversas condutas, apresentando uma grande amplitude. Por isso, uma das primeiras questões que deve ser observada ao discorrer sobre tais ilícitos reside na nomenclatura. É necessário apresentar claramente o que se busca discutir para evitar ambiguidades.

Apesar do Direito Digital possuir grande parte de seus conteúdos já regulados em outras áreas do direito, o Direito Cibernético também possui particularidades em sua matéria. Um exemplo disso são os bens jurídicos tutelados apenas nessa área do direito. Segundo Marcelo Xavier Crespo (2011), ao considerar as condutas ilícitas por meio da informática, verifica-se a possibilidade de lesão a outros bens jurídicos.

Assim, pode-se falar em condutas dirigidas a atingir não só aqueles valores que já são protegidos juridicamente, como a vida, a integridade física, o patrimônio, a fé pública, mas também as informações armazenadas (dados) e a segurança dos sistemas de redes informáticas ou de telecomunicações.

As particularidades do Direito Digital evidenciam os principais bens jurídicos tutelados por esse ramo. De acordo com Rovira del Canto, entende-se a informação como sendo o bem jurídico principal nos crimes digitais e, secundariamente, os dados ou os sistemas. Essa ideia parte do princípio de que os dados constituem nada mais que a representação eletrônica ou digital da informação, ainda que com valores variáveis, ao passo que os sistemas nada mais são que os mecanismos materiais de funções automáticas de armazenamento, tratamento e transferência.

No entanto, o debate acerca dos bens jurídicos protegidos pelo Direito Digital ainda não se exauriu. Nessa perspectiva, surge uma dúvida comum daqueles que não têm informações sobre esse ramo do direito: a utilização de um computador para a prática de um estelionato é um crime virtual?

Com efeito, alguns autores e a própria mídia utilizam o termo “crime digital” para esse tipo de conduta. Assim, tem-se a ideia de que qualquer ação do indivíduo, desde que tenha como meio para a prática do ilícito algum aparelho tecnológico, é um crime digital. No entanto, segundo Marcelo Xavier, o mais correto é considerar como crime informático apenas a ação que tenha como objetivo atingir sistema informático ou de telecomunicações ou, ainda, a informação. A mera utilização de um computador para a efetuação de um delito como um estelionato não deve ser, com precisão técnica, considerada um crime informático.

Partindo desse pressuposto, Marcelo Xavier divide os crimes informáticos em duas espécies: crimes digitais próprios e impróprios. Os crimes digitais próprios são aqueles cujas condutas praticadas são contra bens jurídicos informáticos (sistemas, dados). Já os delitos informáticos impróprios são condutas que se dirigem contra bens jurídicos tradicionais (não relativos à tecnologia).

Ainda seguindo a mesma linha de raciocínio de Marcelo Xavier Crespo, é necessário elencar quais são os sujeitos dos crimes digitais. Segundo ele, os hackers são aqueles que invadem sistemas em benefício próprio, obtendo dados e informações alheias (documentos, programas, músicas etc.), mas sem danificar nada. No entanto, nem todo hacker age com intuito de causar prejuízo alheio. Já os crackers podem ser considerados os verdadeiros criminosos da rede. São ladrões, valendo-se da internet para roubar dinheiro e informações, invadindo sites quebrando o seu sistema de segurança.

Nessa perspectiva, os mais comuns e que são mais vistos na vida cotidiana atual das pessoas são os carders que nada mais são do que estelionatários típicos. São assim chamados por fazerem compras pela rede com cartões de crédito alheios ou gerados por programas de computador. Portanto, esses três sujeitos ativos são, no mundo atual, os principais praticantes de crimes na internet.

5.1 RESPONSABILIDADE CIVIL NOS CRIMES DIGITAIS

Neste tópico, é imperativo realizar uma análise da legislação vigente relacionada ao tema. A responsabilidade civil está intrinsecamente ligada ao nexo causal entre o ato praticado

e o dano resultante. Portanto, mais crucial do que a existência do nexo causal, é o dever de reparação ou punição do agente causador do ato.

O direito digital tem promovido alterações significativas na responsabilidade civil, um conceito fundamental no direito tradicional. Conforme Patrícia Peck, no âmbito do Direito tradicional, o conceito de Responsabilidade Civil é fundamentado em duas teorias: a teoria da culpa e a teoria do risco. A distinção primordial entre ambas reside na obrigatoriedade, ou não, da presença de culpa, mesmo que mínima, para caracterizar a responsabilidade e o consequente dever de indenizar (PECK, 2021).

No entanto, no contexto do direito digital, Patrícia Peck esclarece que:

> Para o Direito Digital, a teoria do risco tem maior aplicabilidade, uma vez que, nascida na era da industrialização, vem resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações, em virtude do princípio de equilíbrio de interesses e genérica equidade. (PECK, 2021, p. 181).

Em conclusão, considerando que a internet é um poderoso meio de disseminação de informações, onde dados corretos ou incorretos são compartilhados com extrema rapidez, os danos resultantes desse instrumento tendem a ser mais indiretos do que diretos. Isso amplia a possibilidade de alguém causar danos a terceiros sem necessariamente ter culpa.

Nesse contexto, Patrícia Peck argumenta que a teoria do risco é mais adequada para lidar com questões virtuais, pois oferece uma solução mais apropriada. Essa teoria deve estar fortemente associada à determinação legal de quem tem o ônus da prova em cada caso.
Portanto, devemos considerar que:

> Um dos pontos mais importantes é o da responsabilidade pelo conteúdo. Considerando que é o conteúdo o principal fator que atrai as pessoas para a Internet e que ele deve estar submetido aos valores morais da sociedade e atender aos critérios de veracidade, é importante determinar os limites de responsabilidade dos provedores, dos donos de websites, das produtoras de conteúdo, dos usuários de e mail e de todos os que tenham de algum modo participação, seja em sua produção, seja em sua publicação ou compartilhamento (PECK, 2021, p. 182).

Portanto, surge a seguinte questão: os provedores responsáveis pela conexão deveriam ser responsabilizados por crimes e pelos conteúdos que circulam em suas redes? A Lei do Marco Civil da Internet estabelece regulamentações pertinentes a essa problemática.

Até o presente momento, o que se tem de concreto é a regulamentação que exclui a responsabilidade total dos provedores de conexão e abjura a responsabilidade solidária dos provedores de aplicação. Dessa forma, estes últimos apenas incorrem em responsabilidade

subsidiária na eventualidade de, após notificação por ordem judicial, permanecerem omissos ou inertes.

6 O AGRAVANTE DO CORONAVÍRUS

Como elemento determinante para esta pesquisa, a pandemia do novo Coronavírus (COVID-19) impôs diversas medidas com o objetivo de atenuar o impacto do vírus na sociedade, entre as quais se destaca o isolamento. Embora o isolamento tenha sido adotado como uma política de proteção à saúde pública, essa medida também revelou uma problemática já existente, mas que não era amplamente divulgada ao público.

A recente pandemia evidenciou à comunidade, não apenas da internet, que o ambiente virtual requer atenção e proteção, pois se tornou um grande foco para a ocorrência de crimes.

Isso ocorre porque, segundo uma pesquisa realizada por Raquel Ribeiro e Tayanne Silva e publicada na revista Correio, as pessoas que se encontravam em situação de isolamento acabaram se inserindo cada vez mais no mundo digital. Ou seja, indivíduos que não estavam habituados a esse ambiente tiveram que se adaptar a ele (SILVA, 2022).

> Segundo a pesquisa feita pelo FortiGuard Labs (laboratório da Fortguard), no ano de 2020 o Brasil sofreu 8,5 bilhões de tentativas de ataques informáticos, sendo que, 5 bilhões ocorreram somente nos últimos três meses do ano. No ano de 2021 o Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos, tendo um aumento de mais de 950% com relação ao ano anterior. (com 8,5 bi), o Brasil ocupou o segundo lugar em número de ataques na América Latina e Caribe, atrás somente do México (com 156 bi). A alta nos números foi constante durante o ano e ocorreu em toda a região, que chegou a registrar 289 bilhões de ataques no total, um crescimento de mais de 600% com relação ao ano anterior (com 41 bi). (SILVA; MARINHO, 2022, p. 13).

Portanto, a presente pesquisa se faz necessária, uma vez que os crimes virtuais têm se tornado cada vez mais presentes na sociedade brasileira. Busca-se, assim, conhecer os tipos penais envolvidos nessa realidade e todos os mecanismos que poderão ser utilizados para o devido combate.

É evidente que o aumento do número de acessos, transações via internet e o maior tempo de utilização das redes sociais resultaram em um aumento no número de usuários vítimas de golpes, como a clonagem do aplicativo de mensagens WhatsApp. Apenas em 2020, mais de 5 milhões de contas foram clonadas e, no Brasil, já são mais de 150 milhões de vítimas apenas em 2021, vítimas de phishing, um golpe que engana as vítimas com sites e aplicativos falsos, conforme mostra a estimativa do DFNDR - LAB, Laboratório Especializado em Cibersegurança da Psafe (SILVA, 2022).

Segundo Corrêa (2002, p. 42), a rede mundial de computadores é um campo altamente abastecido de informações valiosas, o que atrai ataques e, por ser um ambiente de fácil acesso, proporciona uma maior concretização de crimes nos dias atuais. Além disso, a internet é utilizada para transações financeiras, como nunca antes visto, devido ao período da pandemia da Covid-19, onde milhões de brasileiros se isolaram e começaram a usar os meios remotos de atendimento de todas as esferas, com envio de informações pessoais e compartilhamento de dados. Isso possibilitou que criminosos investissem mais tempo e desenvolvessem novas estratégias para aplicar golpes, pois há uma enorme quantidade de informações sendo transitadas na internet.

De acordo com os dados da Central Nacional de Denúncias de Crimes Cibernéticos, somente em relação a condutas específicas, como, LGBTFobia, Neo Nazismo, Pornografia Infantil, Intolerância Religiosa, Xenofobia, Racismo, Violência ou Discriminação contra mulheres, Tráfico de Pessoas e Apologia e Incitação a crimes contra a Vida, foram recebidas e processadas um grande número de denúncias anônimas envolvendo páginas distintas e escritas em diversas línguas diferentes. (SILVA; MARINHO, 2022).

Portanto, a presente pesquisa se faz necessária, uma vez que os crimes virtuais têm se tornado cada vez mais presentes na sociedade brasileira. Busca-se, assim, conhecer os tipos penais envolvidos nessa realidade e todos os mecanismos que poderão ser utilizados para o devido combate.

É evidente que o aumento do número de acessos, transações via internet e o maior tempo de utilização das redes sociais resultaram em um aumento no número de usuários vítimas de golpes, como a clonagem do aplicativo de mensagens WhatsApp. Apenas em 2020, mais de 5 milhões de contas foram clonadas e, no Brasil, já são mais de 150 milhões de vítimas apenas em 2021, vítimas de phishing, um golpe que engana as vítimas com sites e aplicativos falsos, conforme mostra a estimativa do DFNDR - LAB, Laboratório Especializado em Cibersegurança da Psafe (SILVA, 2022).

Em relação a essas condutas, em 2019, foram recebidas e processadas 75.671 denúncias anônimas envolvendo 39.864 páginas (URLs) distintas, escritas em 9 idiomas e hospedadas em 8.015 domínios diferentes, conectados à Internet através de 7.258 números IPs distintos, atribuídos para 65 países em 6 continentes. Em 2020, foram recebidas e processadas 156.692 denúncias anônimas de 74.011 páginas (URLs) distintas, escritas em 10 idiomas e hospedadas em 9.236 domínios diferentes, conectados à Internet através de 8.524 números IPs distintos, atribuídos para 63 países em 6 continentes (SILVA; MARINHO, 2022).

Em 2021, foram recebidas e processadas 150.095 denúncias anônimas envolvendo 71.095 páginas (URLs) distintas, escritas em 10 idiomas e hospedadas em 8.926 domínios diferentes, conectados à Internet através de 9.900 números IPs distintos atribuídos para 68

países em 6 continentes (SILVA; MARINHO, 2022).

No período da pandemia do Coronavírus, alguns crimes se tornaram muito comuns. Inicialmente, cita-se o sequestro de dados através de Malware. Nesse tipo de crime, utilizam-se sites e propagandas enganosas de qualquer natureza por e-mail ou páginas na internet, com o intuito de roubar informações para atos criminosos ou até mesmo para vender essas informações para outros criminosos. De fato, esse tipo de crime foi o mais comum durante a pandemia, pois se traduz basicamente em um vírus de resgate. Logo após, o criminoso pode utilizar os dados da vítima ou até mesmo chantageá-la (SILVA; MARINHO, 2022).

Em segundo lugar, tem-se a figura do Phishing. Trata-se de crimes que mantêm a vítima em erro. O agente compartilha links, e-mails e SMS com mensagens curtas que redirecionam as pessoas para sites criados pelo próprio criminoso. Geralmente, trata-se de sites falsos com certa semelhança com o site original. Dessa forma, a vítima, em erro, fornece seus dados econômicos acreditando estar em um site de compras confiável, já que possui a mesma identidade visual (SILVA; MARINHO, 2022).

Além disso, a clonagem de WhatsApp também é uma forma de Phishing. Com o mesmo modus operandi, o criminoso encaminha mensagens curtas com códigos para a vítima e acaba clonando o WhatsApp do indivíduo. Sendo assim, os agentes passam a ter acesso a todo conteúdo do App da vítima, consequentemente, facilitando o "golpe do pix" (INFOMONEY, 2023).

Com isso em mente, é importante notar que os crimes comuns também aumentaram durante esse período. Crimes como calúnia, difamação, injúria e ameaça tiveram um aumento considerável devido à internet. Atualmente, o senso comum denomina esses tipos penais como crimes de ódio. Outros tipos penais, como o estelionato, também tiveram um aumento em seus números devido a esse fenômeno prejudicial (SILVA; MARINHO, 2022).

O estelionato se tornou mais comum devido à facilidade de sua prática com a evolução da tecnologia. Além disso, o crime de perseguição obsessiva, ou "stalking", que se tornou um dispositivo legal no ordenamento jurídico do país em função dos acontecimentos supracitados. Indivíduos que invadem repetidamente a esfera da vida privada da vítima, por meio de atos que restringem a liberdade da vítima ou que atacam diretamente sua privacidade ou reputação, resultando em um dano temporário ou mesmo permanente à integridade psicológica e emocional do indivíduo, podem ser punidos criminalmente (SENADO FEDERAL, 2021).

7 LEGISLAÇÃO PÁTRIA NO COMBATE AOS CRIMES CIBERNÉTICOS NO BRASIL

Conforme afirmado pelo Ministro Humberto Martins durante uma entrevista ao seminário virtual "Criminalidade em tempos de Covid-19", é incumbência do Estado brasileiro aperfeiçoar seu arcabouço normativo a fim de prevenir a prática desses crimes, evitando assim prejuízos financeiros e patrimoniais às pessoas, empresas e ao próprio poder público. Ele destacou que os criminosos começaram a cometer fraudes eletrônicas ao perceberem o uso intensivo da internet durante a pandemia.

7.1 LEI CAROLINA DIECKMANN

Em 2011, um grupo de hackers invadiu o computador da atriz brasileira Carolina Dieckmann, violando sua privacidade. Cerca de 36 fotos íntimas foram roubadas, além de ameaças e extorsões para evitar a exposição. Diante disso, a necessidade de uma regulamentação rigorosa para esse tipo de crime tornou-se cada vez mais imprescindível. Idealmente, essa necessidade deveria ter sido atendida nos anos anteriores, pois com o avanço da tecnologia, é obrigatório haver uma fiscalização no ambiente virtual.

Afinal, a atriz Carolina não foi a primeira e certamente não será a última a ter sua privacidade violada. Como resultado, a Lei Nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi sancionada em 30 de novembro de 2012.

O novo texto altera os artigos 154-A e 154-B do Código Penal, incluindo pela primeira vez a tipificação de crimes virtuais e delitos informáticos, como a invasão de dispositivos informáticos com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do proprietário (DEFENSORIA PÚBLICA DO ESTADO DO CEARÁ, 2022).

Segundo o defensor público Aldemar Monteiro, supervisor das Defensorias Criminais em Fortaleza, “A lei trouxe uma ferramenta a mais para a punição dos crimes informáticos, porque antes o mecanismo que tínhamos tratava-os apenas como atos preparatórios. Antes, só o fato de você ter acesso ao dispositivo não era considerado crime. Com o advento da lei, isso passou a ser crime” (DEFENSORIA PÚBLICA DO ESTADO DO CEARÁ, 2022).

7.2 MARCO CIVIL DA INTERNET

A internet oferece inúmeras possibilidades, incluindo a capacidade do usuário de criar múltiplas contas em uma única plataforma e de compartilhar suas opiniões com o mundo inteiro. O fenômeno da internet evidenciou que todas as esferas necessitam de leis para garantir uma convivência saudável e harmoniosa entre seus participantes.

Nesse sentido, a Lei do Marco Civil da Internet, no Brasil, veio para desmistificar a ideia de que a internet é uma terra sem lei. A Lei 12695/14 foi criada com o objetivo de proteger a privacidade de todos os usuários e garantir o acesso de toda a população à rede mundial de computadores, conforme estabelecido no art. 5°, X (RAMOS, 2021).

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à

> vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - 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, 1998).

A mencionada lei incorpora todos os princípios inerentes ao direito digital, regulamenta a atuação dos provedores de internet, restringindo seu acesso aos dados e transações da vida privada das pessoas, assegurando a inviolabilidade dos mesmos, exceto mediante consentimento ou ordem judicial. A lei também estabelece a possibilidade de responsabilização civil dos provedores em caso de descumprimento de ordem judicial.

7.3 LEI GERAL DE PROTEÇÃO DE DADOS

De acordo com o site do governo “gov.br”, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi promulgada com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, bem como a livre formação da personalidade de cada indivíduo. Esta lei aborda o tratamento de dados pessoais, que podem estar em meio físico ou digital, realizado por pessoa física ou jurídica de direito público ou privado. Ela engloba um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

A LGPD assegura que os dados do usuário sejam tratados apenas para o fim previamente designado ou acordado, sem desvio de finalidade ou função. Além disso, a lei lista os sujeitos que podem realizar esse tratamento de dados: o controlador, o operador e o encarregado.
Portanto, a LGPD foi criada como uma ferramenta para prevenir abusos em relação à privacidade e intimidade de pessoas físicas e jurídicas. Assim, as entidades públicas e privadas designadas devem garantir o tratamento de dados com base legal na LGPD (GOVERNO DO BRASIL, 2023).

8 METODOLOGIA

Com base nos pressupostos definidos pelo título deste trabalho, é necessária a realização de uma pesquisa básica estratégica. Segundo o professor André Fontenelle, na pesquisa básica estratégica, não se parte de uma situação específica que se pretende resolver na prática. No entanto, busca-se desenvolver conhecimentos que possam eventualmente ser utilizados para a solução de problemas conhecidos.

Em uma segunda análise, trata-se de uma pesquisa descritiva. Ainda segundo o conceito de Fontenelle, essa pesquisa objetiva retratar as características do objeto estudado, expondo com precisão os fatos ou fenômenos, a fim de estabelecer a natureza das relações entre as variáveis delimitadas no tema.

Outro aspecto a ser mensurado refere-se ao tipo de abordagem utilizada na pesquisa. Dessa forma, observando todos os pontos apresentados, é certo que se trata de uma abordagem qualitativa. De acordo com Fontenelle, essa é uma ferramenta essencial, pois é através dela que se realiza a análise dos dados coletados, buscando os conceitos, princípios, relações e significados das coisas.

As fontes utilizadas nesta pesquisa serão inteiramente de cunho bibliográfico e documental, fazendo menção ao estudo de caso como procedimento para embasar a pesquisa.

9 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Em uma análise inicial, este artigo busca contribuir para o aprofundamento da pesquisa sobre a temática, com o objetivo de envolver cada vez mais a população usuária de ambientes digitais, conscientizando-a sobre os riscos e os cuidados necessários para a prevenção de crimes digitais.

O trabalho produzido se mostra cada vez mais necessário devido às formas de criminalidade que surgem diariamente pelo intenso acesso à internet. Assim, procurou-se explicitar a importância do tema no decorrer do artigo.

Nesse sentido, foram utilizados métodos mistos para uma melhor abordagem da nova realidade enfrentada após a pandemia do coronavírus. Além disso, a presente pesquisa tem o propósito de enriquecer pessoalmente o autor e servir como base de conhecimento para trabalhos futuros, com o objetivo de aprofundar cada vez mais a pesquisa sobre o tema, buscando melhorar o ambiente de navegação, tornando-o mais seguro e evitando o aumento da criminalidade digital.

10 CONSIDERAÇÕES FINAIS

Em decorrência dos avanços tecnológicos, toda a comunidade buscou se readaptar aos novos meios de comportamento e convivência social. Nesse contexto, os criminosos também migraram para o ambiente virtual, resultando no aumento dos crimes nesse local e em uma mudança nas técnicas para a prática de delitos.

Adicionalmente, como objetivo principal da pesquisa, a pandemia causada pelo Coronavírus também agravou a problemática. De certa forma, o caos enfrentado por toda a população auxiliou os agentes a aprimorarem seu modus operandi com o intuito de lucrar em cima das pessoas que não têm tanta afinidade com a internet.

Por conta desse argumento, torna-se extremamente necessário o aprofundamento e a leitura mais frequentes de artigos, revistas e jornais sobre o mundo digital, pois o movimento migratório de atividades essenciais e não essenciais se fortalece com o passar dos anos, fazendo com que a vida das pessoas estejam cada vez mais presente na internet.

Com o fator pandemia, a migração das atividades físicas para as digitais tornou-se ainda mais intensa em virtude da necessidade de proteção em relação ao vírus. Como medida assecuratória de saúde, foi adotado o confinamento, obrigando os indivíduos a permanecerem em casa e, como alternativa, resolverem suas vidas por meio da tecnologia.

A presente pesquisa foi realizada trazendo referências bibliográficas, estudos recentes e dados estáticos como sinal de alerta para que essa área carente ganhe mais importância daqui para frente, uma vez que o futuro da sociedade tende a ser mais digital do que nos dias atuais. Portanto, é evidente que há um grande desafio para a legislação brasileira, pois é necessário que a evolução social caminhe lado a lado com o ordenamento jurídico.

No entanto, ainda estamos passando por atualizações referentes à legislação, como por exemplo, o crime de *stalkin*g recentemente criado. Atualmente, além de leis que acompanhem o desenvolvimento, o que mais se precisa para evitar ou atenuar esse tipo de crime é o conhecimento dos recursos tecnológicos. Dessa forma, mais do que o conhecimento de qualquer lei, é importante saber utilizar a internet da forma mais segura possível, já que os hackers têm possibilidades infinitas.

Em suma, a tarefa principal é conhecer mais sobre os recursos tecnológicos para poder praticar o uso saudável e dentro dos limites legais observados em lei, observando também o direito de terceiros. Ademais, é extremamente importante que o ordenamento jurídico continue acompanhando as evoluções sociais, pois o direito nada mais é do que um reflexo da sociedade.

REFERÊNCIAS

ANDRION, Roseli**. História da segurança virtual: a origem do cibercrime**. CanalTech, 2021. Disponível em: <https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-cibercrime-203073/>. Acesso em 15 de outubro de 2023.

BRASIL ESCOLA. **A Sociedade da informação**. Disponível em: <https://meuartigo.brasilescola.uol.com.br/educacao/a-sociedade-da-informacao.htm>. Acesso em 07 de setembro de 2023.

BARBOSA, Marina. **Seis em cada dez consumidores sofreram algum tipo de fraude financeira nos últimos 12 meses, aponta CNDL/SPC Brasil**. CNDL Brasil, 2021. Disponível em: <https://site.cndl.org.br/seis-em-cada-dez-consumidores-sofreram-algum-tipo-de-fraude-financeira-nos-ultimos-12-meses-aponta-cndlspc-brasil/>. Acesso em 07 de setembro de 2023.

BARROS, Antonio**. Conheça a evolução dos crimes cibernéticos.** Agência Câmara de Notícias, 2006. Disponível em: <https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-doscrimesciberneticos#:~:text=Os%20primeiros%20crimes%20relacionados%20%C3%A0,delitos%20como%20sabotagens%20e%20espionagem>. Acesso em 07 de setembro de 2023.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2017.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2002.

CRESPO, Marcelo Xavier. **CRIMES DIGITAIS**. São Paulo: Saraiva, 2011.

CNN BRASIL. **Do ENIAC ao notebook: confira a evolução dos computadores nas últimas décadas**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/do-eniac-ao-notebook-confira-a-evolucao-dos-computadores-nas-ultimas-decadas/>. Acesso em: 22 de outubro de 2023.

DEFENSORIA DO CEARÁ. **Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual.** Disponível em: <https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/>. Acesso em 03 de novembro de 2023.

DINO. **Crimes digitais crescem pós-pandemia e provocam corrida por ciberseguros**. Valor Econômico, 2022. Disponível em: <https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml>. Acesso em 07 de setembro de 2023.

E-GLOBAL. **Quais países com menos acesso à internet?** Disponível em: <https://e-global.pt/noticia/vida/tecnologia/quais-os-paises-com-menos-acesso-a-internet/>. Acesso em 06 de outubro de 2023.

FONTENELLE, André. **TIPOS DE PESQUISA**. Disponível em: <https://andrefontenelle.com.br/tipos-de-pesquisa/>. Acesso em 06 de novembro de 2023.

FORTIGUARD LABS. **FortiGuard Labs apresenta relatório sobre ciberataques no Brasil**. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/pressreleases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em 02 de agosto de 2023.

G1. **29 países restringiram conexão com a internet durante 2020, aponta relatório**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/03/05/29-paises-restringiram-conexao-com-a-internet-durante-2020-aponta-relatorio.ghtml>. Acesso em 15 de outubro de 2023.
GOVERNO DO BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd>. Acesso em 09 de setembro de 2023.

INFOMONEY. **Novo golpe utiliza sites falsos para emitir segunda via de contas de Sabesp, CPFL, Copasa e Light**. 2023. Disponível em: <https://www.infomoney.com.br/consumo/novo-golpe-utiliza-sites-falsos-para-emitir-segunda-via-de-contas-de-sabesp-cpfl-copasa-e-light/>. Acesso em 07 de setembro de 2023.

LIMA, Marilia Freires de; ARAÚJO, Jefferson Flora Santos de. **A utilização das tecnologias de informação e comunicação como recurso didático-pedagógico no processo de ensino e aprendizagem.** Revista Educação Pública, v. 21, nº 23, 22 de junho de 2021. Disponível em: <https://educacaopublica.cecierj.edu.br/artigos/21/23/a-utilizacao-das-tecnologias-de-informacao-e-comunicacao-como-recurso-didatico-pedagogico-no-processo-de-ensino-aprendizagem>. Acesso em 07 de setembro de 2023

NOVO, Benigno. **A Sociedade da informação**. Disponível em: <https://meuartigo.brasilescola.uol.com.br/educacao/a-sociedade-da-informacao.htm>. Acesso em 07 de setembro de 2023.

OUVIDOR DIGITAL. **Anonimato Digital: quais as vantagens e desvantagens?** Disponível em: <https://ouvidordigital.com.br/blog/anonimato-digital-vantagens-e-desvantagens/#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,em%20conformidade%20com%20a%20lei>. Acesso em 07 de setembro de 2023.

PECK, Patrícia. **DIREITO DIGITAL**. São Paulo: Saraiva, 2021.

PIMENTEL, Eduardo de Souza. **INTRODUÇÃO AO DIREITO DIGITAL**. São Paulo.

RAMOS, Rahellen. **O que é o Marco Civil da Internet? Politize, 2021**. Disponível em: <https://www.politize.com.br/marco-civil-da-internet/>. Acesso em 07 de setembro de 2023.

REDIVO, Joslaine. **Crimes cibernéticos: no mundo durante a pandemia covid-19 e seus impactos.** Conteúdo jurídico, 2022. Disponível em: <https://conteudojuridico.com.br/consulta/Artigos/58541/crimes-cibernticos-no-mundodurante-a-pandemia-covid-19-e-seusimpactos#:~:text=Crime%20virtual%20ou%20crime%20digital,ou%20como%20meio%20de%20crime>. Acesso em 07 de setembro de 2023.

RIBEIRO, Raquel; Silva Tayanne. **Isolamento social potencializa dependência tecnológica**. Revista do Correio, 2021. Disponível em: <https://www.correiobraziliense.com.br/revista-do-correio/2021/02/4905199-isolamento-social-potencializa-dependencia-tecnologica.html>. Acesso em 07 de setembro de 2023.

SENADO FEDERAL. **Lei que criminaliza Stalking é sancionada.** 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/04/05/lei-que-criminaliza-stalking-e-sancionada>. Acesso em 07 de setembro de 2023.

SILVA, Gilsimar Pinheiro. **CRIMES DIGITAIS: EVOLUÇÃO DOS CRIMES E A APLICAÇÃO DO DIREITO**. Repositório Universitário de Ânima, Guanambi/BA. 2022.

SILVA, T. A. João; MARINHO, A. Luiz. **O AUMENTO DOS CRIMES VIRTUAIS NA PANDEMIA E OS LIMITES DA LIBERDADE DE EXPRESSÃO**. Universidade Potiguar, Natal/RN. 2022.

STJ. **Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins.** 2020. Disponível em <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-ciberneticotomou-lugar-de-roubos-e-furtos-na-pandemia–diz-o-ministro-Humberto-Martins.aspx>. Acesso em: 17 maio 2023.

PARECER DE REVISÃO ORTOGRÁFICA E GRAMATICAL

Eu, **ALINE RODRIGUES FERREIRA**, graduada em Biblioteconomia pela Universidade Federal do Cariri, atesto que realizei a revisão ortográfica e gramatical do trabalho intitulado "**O IMPACTO DA ERA DIGITAL NA CRIMINALIDADE ORGANIZADA E A INFLUÊNCIA DO CORONAVÍRUS COMO FATOR AGRAVANTE**", de autoria de **PEDRO LUCAS DOS SANTOS SILVA**, sob orientação do(a) Prof.(a) **FRANCISCO GLEDISON DE LIMA ARAÚJO**. Declaro que este TCC está em conformidade com as normas da ABNT e apto para ser submetido à avaliação da banca examinadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 03/12/2023

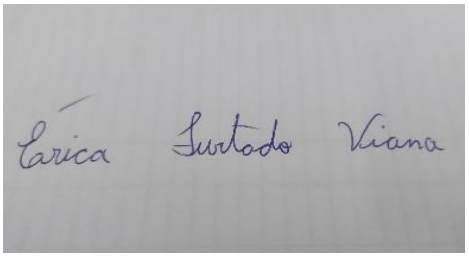
gov.br
Documento assinado digitalmente
ALINE RODRIGUES FERREIRA
Data: 04/12/2023 00:20:57-0300
Verifique em https://validar.iti.gov.br

ALINE RODRIGUES FERREIRA

PARECER DE TRADUÇÃO DO RESUMO PARA LINGUA INGLESA

Eu, **ÉRICA FURTADO VIANA**, professor (a) com formação Pedagógica em Letras: Língua Inglesa-Licenciatura, pela Instituição de Ensino Superior **Estácio de Sá**, realizei a tradução do resumo do trabalho intitulado O IMPACTO DA **CRIMINALIDADE ORGANIZADA E A INFLUÊNCIA DO CORONAVÍRUS COMO FATOR AGRAVANTE**, do (a) aluno (a) **PEDRO LUCAS DOS SANTOS** SILVA e orientador (a) **FRANCISCO GLEDISON DE LIMA ARAÚJO**. Declaro que o ABSTRACT inserido neste TCC está apto à entrega e análise da banca avaliadora de Trabalho de Conclusão de Curso do Centro Universitário Doutor Leão Sampaio/Unileão.

Juazeiro do Norte, 02/11/2023



Assinatura do professor

TERMO DE AUTORIZAÇÃO PARA ENTREGA DA VERSÃO FINAL DO TRABALHO DE CONCLUSÃO DE CURSO (TCC II) DO CURSO DE DIREITO

Eu,_____, professor(a) titular do **Centro Universitário Dr. Leão Sampaio - UNILEÃO**, orientador(a) do Trabalho do aluno(a)_____, do Curso de Direito, **AUTORIZO** a **ENTREGA** da versão final do Trabalho de Conclusão de Curso (Artigo) do aluno supracitado, para análise da Banca Avaliadora, uma vez que o mesmo foi por mim acompanhado e orientado, sob o título_____

_____

_____.

Informo ainda que o mesmo não possui plágio, uma vez que eu mesmo passei em um antiplágio.

Juazeiro do Norte,____/___/____

_____

Assinatura do professor