UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE DIREITO-DDI

ROSANGELA DOS SANTOS

CRIMINALIDADE DIGITAL EM TEMPOS DE PANDEMIA: PRINCIPAIS OCORRÊNCIAS EM SERGIPE NO ANO DE 2020

SÃO CRISTÓVÃO-SE
2021

ROSANGELA DOS SANTOS

CRIMINALIDADE DIGITAL EM TEMPOS DE PANDEMIA: PRINCIPAIS OCORRÊNCIAS EM SERGIPE NO ANO DE 2020

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito-DDI da Universidade Federal de Sergipe, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Profa. Dra. Analice Nogueira Santos Cunha

SÃO CRISTÓVÃO-SE
2021

ROSANGELA DOS SANTOS

CRIMINALIDADE DIGITAL EM TEMPOS DE PANDEMIA: PRINCIPAIS OCORRÊNCIAS EM SERGIPE NO ANO DE 2020

Trabalho de Conclusão de Curso apresentado ao Departamento de Direito-DDI da Universidade Federal de Sergipe, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Cidade, __ de _____ de ____

BANCA EXAMINADORA

_____

Profa. Dra. Analice Nogueira Santos Cunha
Universidade Federal de Sergipe

_____

Prof. Vitor Oliveira
Universidade Federal de Sergipe

_____

Prof. Raphael Leal
Membro Externo

Dedico esta pesquisa aos familiares e amigos, joias raras que Deus nos presenteia para repartirmos as conquistas e experiências da nossa incrível e maravilhosa jornada que é a vida.

AGRADECIMENTOS

Aos professores do Departamento de Direito da UFS que tanto serviram e servem de exemplo para aqueles que almejam algo além do diploma, ou seja, o conhecimento de quão importante é colocar o Direito a serviço daqueles que mais precisam; principalmente os sensivelmente mais carentes, que compõem parte fundamental do nosso contexto social.

À professora Analice Cunha pela sempre gentil atenção e preocupação com minha trajetória de pesquisa que culminou neste momento.

Durante o percurso da vida temos pilares fundamentais que nos lembram de que não estamos sós e que, por vezes, a vida pode e deve ser leve. Aos meus familiares, com todo carinho possível, agradeço.

Em especial a meu companheiro Júnior, que tanto me ajudou nas horas de desespero e cansaço. Obrigada de coração!

À minha mãe (Mainha), Maria Rosa, exemplo de luta e coragem, a primeira e mais importante educadora da minha vida!

À Ana Maria, irmã maravilhosa, melhor não há! Ajuda imprescindível durante todos os momentos da minha vida.

Aos meus irmãos queridos, Marcos e Clécio, que ajudam e torcem pelo meu crescimento incondicionalmente.

Enfim, a todos que de alguma forma ajudaram na consecução desta pesquisa, muito obrigada!

"Criei meu website
Lancei minha homepage
Com 5 gigabytes
Já dava pra fazer um barco que veleje
Meu novo website
Minha nova fanpage
Agora é terabyte
Que não acaba mais
Por mais que se deseje
Que o desejo agora garimpar
Nas terras das serras peladas virtuais
As criptomoedas, bitcoins e tais
Novas economias, novos capitais
Se é música o desejo a se considerar
É só clicar que a loja digital já tem
Anitta, Arnaldo Antunes, e não sei mais quem
[...]
Estou preso na rede
Que nem peixe pescado
É zapzap, é like
É Instagram, é tudo muito bem bolado
O pensamento é nuvem
O movimento é drone
O monge no convento
Aguarda o advento de Deus pelo iPhone
Cada dia nova invenção
É tanto aplicativo que eu não sei mais não
What's app, what's down, what's new
Mil pratos sugestivos num novo menu
É Facebook, é Facetime, é google maps
[...]" (Gilberto Gil-Pela internet 2)

RESUMO

A presente pesquisa abordou a criminalidade digital abarcando as principais ocorrências em Sergipe, durante o período de março a dezembro de 2020, em que foi imposto a boa parte da população o isolamento social por causa da pandemia da covid-19. O objetivo geral da pesquisa foi analisar os crimes digitais ocorridos nesse referido período a fim de verificar se houve aumento em relação ao ano anterior. Como objetivos específicos buscou-se compreender esses crimes digitais a partir de suas terminologias e classificações; examinar as legislações existentes relativas aos crimes digitais e à proteção no meio digital; bem como identificar quais crimes digitais ocorreram em Sergipe, no citado período, a partir das informações coletadas na Coordenadoria de Estatística e Análise Criminal-CEACrim, órgão da SSP-SE. Essa coleta teve a finalidade de permitir a análise de quais crimes ocorreram durante os anos de 2019 em relação a março a dezembro de 2020; o que permitiu elaborar uma relação comparativa e constatar um aumento significativo nas ocorrências dos crimes digitais. Em seguida, os crimes foram categorizados em 7(sete) tipos penais que mais tiveram relevância numérica, a saber, estelionato, invasão de dispositivo informático, ameaça, difamação, injúria, furto e calúnia. Constatou-se que houve um aumento dos crimes digitais, de uma forma geral, em torno de 260% (duzentos e sessenta porcento) em 2020, comparativamente ao ano de 2019, possivelmente decorrente de uma interação maior das pessoas no meio digital, ou seja, na internet; originada pela pandemia da covid-19 e suas restrições. Além disso, verificou-se que o estelionato permaneceu à frente dos demais delitos, em ambos os períodos estudados e que os demais crimes a exemplo da invasão de dispositivo informático, ameaça, difamação, injúria, furto e calúnia permaneceram também nessas mesma posições nos dois períodos de análise.

Palavras-chave: Crimes digitais. Internet. Pandemia. Covid-19. Sergipe.

ABSTRACT

This research has investigated cybercrimes encompassing the most frequent occurrences in Sergipe, during the period of March to December of 2020 in which a social isolation was imposed to most of the state's population because of COVID-19 pandemic. The general goal of the research was the analysis of the cybercrimes which occurred at this isolation period to verify a possible increase in their numbers as compared to the previous year. As specific goals, it has been attempted to comprehend these cybercrimes from the perspective of their terminologies and classifications; as well as to examine the existing legislation regarding cybercrimes and the protection on digital environment, and to identify which cybercrimes occurred in Sergipe in the aforementioned period having as sources the data collected from the Coordination of Statistics and Criminal Analysis – CEACrim -, a department of Sergipe's Public Security Secretary. The data collection had as its goal the analysis of the crimes that occured in 2019 and their comparison with those that occured in the period of March to December 2020, which enabled a comparative analysis and verification of a significant increase in cybercrimes occurrences. Afterwards, the crimes were categorized in 7 (seven) criminal types whose numbers were most significant, and those were digital fraud, invasion of digital devices, threat, defamation, slander, theft and calumny. It has been revealed an increase of cybercrimes of, as a rule, nearly 260% (two hundred percent) in 2020 as compared to 2019, possibly as a consequence of an increased interaction among people in digital environment, namely, the Internet, caused by the COVID-19 pandemic and its restrictions. Besides, it has been verified that digital fraud has maintained itself at the forefront if compared to the other crimes in both 2019 and 2020 periods and the other crimes, namely, the invasion of digital devices, threat, defamation, slander, theft and calumny have ranked the same in both 2019 and 2020 analyzed periods.

Keywords: Cybercrimes. Internet. Pandemic. Covid-19. Sergipe.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CEACrim	Coordenadoria de Estatística e Análise Criminal
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidente de Segurança no Brasil
CGI.br	Comitê Gestor da Internet no Brasil
DEPATRI	Departamento de Crimes Contra o Patrimônio
DRCC	Delegacia de Repressão a Crimes Cibernéticos
LGPD	Lei Geral de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
TIC	Tecnologias de Informação de Comunicação

SUMÁRIO

1 **INTRODUÇÃO**

No panorama contemporâneo, o progressivo uso das Tecnologias de Informação e Comunicação (TIC)[1] incrementou sobremaneira o fluxo de informações promovendo uma maior interação entre as pessoas, principalmente, no mundo digital. Tal interação possui diversas origens, a saber, pessoais, educacionais, profissionais, ligadas ao lazer e a serviços públicos, negociais, entre outras. Todo esse contexto acaba por suscitar uma constante vulnerabilidade dos cidadãos que utilizam o espaço digital, muitas vezes, de forma incauta; possibilitando a ação de agentes que visam à obtenção de informações pessoais, financeiras, entre outras finalidades, contribuindo para o cometimento dos crimes digitais.

A internet propiciou a criação de um novo perfil de criminoso que possui um conhecimento técnico em informática relevante e que consegue direcionar a maneira de execução dos delitos convencionais dentro dos moldes mais tecnológicos, ou seja, alterando o seu *modus operandi* inclusive favorecendo o surgimento de “novas figuras delitivas” (ALVES, 2020, p. 15). Dessa maneira, até mesmo os crimes comuns que já faziam parte da realidade social brasileira, antes de todo o advento do universo digital, passaram a ser executados com uma estratégia tecnológica mais sofisticada, ocultadora e complicada, obstando a devida persecução penal (VIANNA, MACHADO, 2013).

O tema da presente pesquisa tem relevância por estar profundamente ligado à nossa sociedade globalizada e conectada, que cotidianizou o uso das tecnologias de uma forma tal que acaba por convergir o desempenho das suas atividades quase que integralmente no mundo digital. Essa condição propicia a exposição das pessoas aos ataques frequentes de agentes que encontram nesse ambiente um terreno fértil para a prática de delitos. Tal convergência social está intimamente ligada com a interatividade das pessoas e significa “[...] a possibilidade de participação humana em um nível de inter-relação global”(PINHEIRO, 2016, p. 68).

A motivação para a escolha desse objeto de pesquisa foi decorrente da percepção de como os criminosos vêm executando, com uma significativa facilidade, inúmeras ações, a exemplo de golpes, vazamentos de dados, etc. que fragilizam a interação no meio digital; promovendo uma sensação constante de insegurança. A tudo isso, acrescenta-se o possível agravamento das incidências desses delitos, tendo em vista as consequências causadas pela pandemia da covid-19, que impactou profundamente o cotidiano da sociedade, impondo uma nova realidade marcada pelo isolamento e distanciamento social.

---

1 Como o próprio nome diz, as Tecnologias de Informação e Comunicação consistem em dispositivos produzidos pelo engenho humano com a finalidade de obter, armazenar e processar informações, bem como estabelecer comunicação entre diferentes dispositivos, possibilitando que tais informações sejam disseminadas ou compartilhadas.

As pessoas, desde que a pandemia da covid-19 teve início, passaram a desempenhar quase todas as suas atividades sociais, laborais de forma remota, através da conexão de dados, ou seja, da internet. Em consequência desse acontecimento, a prática delitiva ocorrida nesse meio tende a se intensificar ocasionando uma série de danos aos cidadãos que se encontram numa posição de vulnerabilidade.

Sendo assim, a presente pesquisa tem como objetivo geral a análise dos crimes digitais e suas ocorrências em Sergipe, no período de março a dezembro de 2020, com base no contexto do isolamento social causado pela Pandemia da COVID-19; a fim de verificar se houve aumento dessas ocorrências em relação ao ano anterior.

Para tanto, os objetivos específicos abrangem compreender os crimes digitais e suas especificidades alcançando suas terminologias e classificações; examinar as principais legislações existentes relativas aos crimes digitais e à segurança no meio digital; e Identificar os tipos de crimes digitais registrados no período de isolamento social em 2020 e um possível aumento de ocorrências em relação ao ano de 2019. Este último foi efetivado a partir de dados coletados na Coordenadoria de Estatística e Análise Criminal-CEACrim da Secretaria de Estado da Segurança Pública-SSP/SE e na Delegacia de Repressão a Crimes Cibernéticos-DRCC.

A hipótese levantada é a de que durante a Pandemia da COVID-19 é possível associar o aumento de crimes digitais em Sergipe ao período de isolamento social imposto à coletividade, no ano de 2020, como medida de conter a disseminação da doença.

1.1 METODOLOGIA

A metodologia aplicada quanto à abordagem foi predominantemente qualitativa, com viés subjetivo; tendo em vista que as análises foram feitas a partir da leitura de legislações pertinentes e de doutrina, bem como de informações retiradas em sites oficiais ou nos próprios órgãos públicos responsáveis, a saber, Secretaria de Segurança Pública de Sergipe e Delegacia de Repressão a Crimes Cibernéticos-DRCC, em que constam subsídios a respeito dos delitos digitais no período especificado no objetivo geral. Eventualmente, após a coleta de dados relativos aos delitos digitais em Sergipe, algumas considerações foram feitas com base na abordagem quantitativa.

Cabe aqui ressaltar que, em casos de investigações científicas, o rigor metodológico aplicado em toda pesquisa, seja ela qualitativa ou quantitativa, demonstra o compromisso irrefutável com a confiabilidade do tratamento dos dados

coletados. Assim, corroborando com o tema da importância da pesquisa científica, Lakatos e Marconi (2012, p. 43) discorrem que,

> A pesquisa pode ser considerada um procedimento formal com método de pensamento reflexivo que requer um tratamento científico e se constitui no caminho para se conhecer a realidade ou para descobrir verdades parciais. Significa muito mais do que apenas procurar a verdade: é encontrar respostas para questões propostas, utilizando métodos científicos.

Em relação aos procedimentos, a nossa pesquisa é majoritariamente bibliográfica e documental, tendo por base textos de lei, livros, artigos, relatórios, notícias publicadas e demais documentos oficiais que abordam o tema proposto; incluindo as dados estatísticos da Coordenadoria de Estatística e Análise Criminal da Secretaria de Segurança Pública de Sergipe e da Delegacia de Crimes Cibernéticos.

Os dados coletados na Secretaria de Segurança Pública de Sergipe relativos ao cometimento de crimes digitais, no período de março a dezembro de 2020, foram detalhados e analisados. Além disso, foram feitas algumas entrevistas com os agentes que acompanham os registros nas delegacias a fim de adicionar elementos para possíveis análises.

O presente trabalho de pesquisa está estruturado, além da Introdução e conclusões, em três capítulos; no segundo são apresentados alguns conceitos dos delitos digitais a partir do entendimento das possíveis controvérsias doutrinárias a respeito da classificação e nomenclatura, bem como o posicionamento desta pesquisadora acerca da questão. No terceiro capítulo são abordadas, de forma geral, as legislações criadas, a partir de uma necessidade de adequação às mudanças que a tecnologia impôs ao Direito à medida que os delitos, sejam eles tradicionalmente previstos ou novos, foram sucedendo no cotidiano das relações no meio digital.

No quarto capítulo são apresentados os dados estatísticos oriundos da coleta realizada na CEACrim/SSP/SE, bem como trechos da entrevista realizada na DRCC. Com a consecução dos referidos dados foram feitas as possíveis análises dos delitos digitais cometidos no período do isolamento social decorrente da pandemia da Covid-19; apresentando as categorias mais recorrentes e o aumento de sua incidência em relação ao ano de 2019. Por fim, nas Conclusões é feito um apanhado de toda a pesquisa evidenciando aspectos mais relevantes do seu resultado.

2 **CRIMES DIGITAIS: CONTROVÉRSIAS TERMINOLÓGICAS E OCORRÊNCIAS**

É perceptível o impacto das transformações tecnológicas, nos últimos tempos, principalmente aquelas que tratam das Tecnologias de Informação e Comunicação, comumente conhecidas como TIC, e aqui cabe destacar a criação e desenvolvimento da internet. Esta propiciou a conexão de dados, causando o consequente e inevitável aumento das interações pessoais, comerciais, de serviços públicos, entre outras, nesse meio virtual.

Assim, de acordo com Crespo (2015) da mesma forma que esse avanço da tecnologia impactou inúmeras áreas da vida humana, o Direito Penal não permaneceu incólume a essa influência, visto que é instrumento da sociedade e como consequência é também alvo de suas mudanças. A partir de tais constatações, é possível corroborar com Alves (2020, p. 21) de que "[...] a rede passa a ser cada vez mais, alvo de uma cultura delinquente em que não se consegue medir a dimensão do perigo em que se está exposto. A sociedade conectada está sob um constante risco".

É fato que as condutas delitivas incidentes no chamado mundo real são previstas na nossa legislação penal e atingem bens jurídicos reconhecidamente palpáveis, tangíveis; bem como aqueles considerados intangíveis. No entanto, a partir do referido avanço tecnológico, a maneira como essas condutas são efetivadas pelos agentes criminosos foi submetida a uma transformação a fim de se moldar a esse novo meio, ou seja, ao mundo digital.

Essa inevitável adaptação do *modus operandi* dos crimes digitais trouxe à baila, também, as controvérsias existentes sobre a terminologia, conceito e classificação, que são empregados com frequência nesse profícuo campo de estudo que se apresenta. Além dessas relevantes questões, importa ressaltar aquelas relativas ao bem jurídico a ser tutelado, se há ou não a necessidade de ampliação do alcance da tutela, ou seja, da instituição de novos bens jurídicos advindos do atual processo de cometimento desses delitos digitais.

Sendo assim, torna-se premente promover uma discussão acerca das aludidas controvérsias presentes entre algumas nomenclaturas, porquanto não é intento desta pesquisa acadêmica esgotar todas as terminologias e classificações existentes no panorama teórico-prático brasileiro. A proposta, nesta etapa, é abordar algumas terminologias que merecem destaque pelo seu uso nos escritos da área, nas notícias em vários canais de comunicação, em artigos na internet, inclusive na prática cotidiana da delegacia especializada de Sergipe, a Delegacia de Repressão a Crimes Cibernéticos-DRCC, cuja própria denominação destaca o uso de um desses termos aqui tratados.

Ao iniciar um debate com um teor tão intenso, necessário se faz destacar e compreender a classificação do que usualmente é chamado de bem jurídico tutelado pelo Direito Penal. Assim, esclarece (TOLEDO, 1994, p. 15;17),

> Bem, em um sentido muito amplo, é tudo o que se nos apresenta como digno, útil, necessário, valioso. [...] Os bens são, pois, coisas reais ou objetos ideais dotados de "valor", isto é, coisas materiais e objetos imateriais que, além de serem o que são, "valem". Por isso são, em geral, apetecidos, procurados, disputados, defendidos, e, pela mesma razão, expostos a certos perigos de ataques ou sujeitos a determinadas lesões. [...] Do ângulo penalístico, portanto, bem jurídico é aquele que esteja a exigir uma proteção especial, no âmbito das normas de direito penal, por se revelarem insuficientes, em relação a ele, as garantias oferecidas pelo ordenamento jurídico, em outras áreas extrapenais.

O citado autor destaca acuradamente nesse trecho, além das características inerentes ao bem jurídico que é objeto da legislação penalística, o caráter fragmentário e a aplicação da *ultima ratio regum* do Direito Penal ao tutelar os bens jurídicos considerados relevantes para sua esfera de atuação. Tais condições são aplicáveis uma vez que não se apresenta de forma suficiente a execução da referida proteção a partir de outras esferas do Direito, a saber, Direito Administrativo, Direito do Consumidor etc.

Todo esse cuidado visa à intervenção mínima do poder/dever, ou seja, do *ius puniendi* na esfera da liberdade individual, pois de acordo com Toledo (1994) as condutas que podem ser consideradas reprováveis, em muitos casos, não devem ser necessariamente criminalizadas, pois podem não ser relevantes do ponto de vista jurídico-penal. Dessa maneira, abriga-se, quando for o caso, a concepção da adequada aplicação de outros dispositivos legais, que não sejam obviamente jurídico-penais, disponíveis no nosso ordenamento jurídico.

Acrescentando-se do mesmo modo questões relevantes ao debate em tela, Roxin (2018, p. 17-18) explicita aquilo que entende por bens jurídicos e algumas de suas implicações,

> [...] Por isso, o Estado deve garantir, com os instrumentos jurídico-penais, não somente as condições individuais necessárias para uma coexistência semelhante (isto é, a proteção da vida e do corpo, da liberdade de atuação voluntária, da propriedade etc.), mas também as instituições estatais adequadas para este fim[...] sempre e quando isto não se possa alcançar de outra forma melhor. Todos esses objetos legítimos de proteção das normas que subjazem a estas condições eu os denomino bens jurídicos.

O citado autor revela a importância fundamental da chamada função social do Direito Penal em que a sua ação precípua deve ser norteada pela garantia aos indivíduos de uma existência em que estejam presentes a paz, segurança social e liberdade, desde que não seja possível tal meta por intermédio de outras medidas

político-sociais que causem menor afetação na liberdade dos cidadãos em questão (ROXIN, 2018).

Em vista dessa discussão sobre bens jurídicos e, principalmente, diante das novas tendências e mudanças nos meios de interação e comunicação na sociedade, advindos dos avanços decorrentes do uso das modernas Tecnologias de Informação e Comunicação, especificamente no caso ora estudado a internet; a concepção de bem jurídico a ser protegido tem uma relevância crucial, pois a ele se direciona a legislação penal pela qual a referida tutela se perfaz. Tal discussão tende a conciliar os bens jurídicos que já são tradicionalmente tutelados com os que possam advir de todo esse processo de transformação do Direito, diante desse cenário da criminalidade na era digital.

O que se verifica ao adentrar na seara dos crimes digitais é que surgem controvérsias doutrinárias acerca da nomenclatura e classificação a serem utilizadas em relação a esses delitos que têm como característica a ofensa às informações e dados automatizados, bem como a alguns bens jurídicos já estabelecidos. Tendo como instrumentos para sua consecução computadores, *tablets,* celulares com utilização ou não da internet.

A partir da leitura dos autores que tratam do tema, a exemplo de Pinheiro (2016), Tupinambá (2021), Crespo (2015), Alves (2020), Gimenes (2013), Vianna e Machado (2013) Lotufo (2021b), Silva (2018), torna-se possível compreender que até a presente data não há uma harmonização, nem corrente doutrinária considerada majoritária acerca da utilização de terminologia e classificação específicas. Em vista disso, a exposição de algumas abordagens consideradas, nesta pesquisa, com maior significância será efetivada no decorrer deste capítulo.

No atual percurso científico a respeito da referida temática, vários estudiosos e profissionais utilizam terminologias, tais como: crimes digitais (CRESPO, 2015), (ALVES, 2020)e Lotufo (2021b) , crimes informáticos(VIANNA; MACHADO, 2013) e (JESUS; MILAGRE, 2016) , crimes cibernéticos (WENDT; JORGE, 2013) e (SILVA, 2018) , crimes virtuais (GIMENES, 2013) e (RAMALHO TERCEIRO, 2002) entre outras. Neste estudo, optou-se por destacar essas expressões por serem muito utilizadas pelos autores, em tela, e demais veículos de informação, sejam na internet (POLÍCIA CIVIL DO ESTADO DE SERGIPE, 2021) ou nos programas televisivos (CRESCE..., 2021).

Assim é possível conceber que todas essas nomenclaturas dos crimes digitais estão ligadas fundamentalmente por características similares. Tais características são consideradas similares, a partir da compreensão de que todos os termos convergem para o uso de tecnologias, envolvendo mais precisamente dados informáticos como objeto e/ou internet como meio.

Compreende-se que, no decorrer desse processo de incremento tecnológico e da conexão de dados, outras modalidades de delitos foram desenvolvidas, inclusive abarcando bens jurídicos ditos novos (VIANNA; MACHADO, 2013), a exemplo da “inviolabilidade de informações e dados automatizados”, fruto de sucessivas discussões que culminaram na Lei nº 12.737 /2012, que instituiu os crimes informáticos e é popularmente conhecida como Lei Carolina Dieckmann[2]. Da mesma forma, pode-se ponderar que muitos dos bens jurídicos já presentes no nosso ordenamento jurídico, que com frequência são atacados nos meios digitais, são devidamente protegidos por meio do uso dos dispositivos penais já estabelecidos.

Inicialmente, no universo das várias expressões sobre a matéria, tem-se o exemplo de Alves (2020) que se filia à terminologia crimes digitais e à chamada criminalidade digital. Tal filiação a respeito da referida denominação é compartilhada também por Crespo (2015, p. 2-3) que afirma ser essa a melhor terminologia,

> Assim, a expressão que adotamos como a mais adequada é “crimes digitais” em razão do que se pretende referir: os dados que decorrem da eletrônica digital. Note-se que “digital” deriva do inglês digit, que, por seu turno, deriva do latim, digitus e que significa a forma mais primitiva de exprimir os número [*sic*] (com os dedos da mãos). A eletrônica digital é aquela em que os dados são convertidos nos números “0” e “1”, que formam o sistema binário, base para o armazenamento de dados, mais moderna e atualizada que a eletrônica analógica.

Diante do citado esclarecimento a respeito da origem e do porquê da expressão crimes digitais, e justificada a escolha por parte dos referidos autores, fica demonstrada a amplitude de seu alcance, pois envolve os elementos fundamentais da eletrônica digital que serviu de base para as atuais tecnologias de informação e comunicação, ou seja, para a internet. Em decorrência dessa visão mais ampla do termo, surge a motivação a fim de adotar seu uso no decorrer desta pesquisa por considerá-la a mais acertada.

Em função do exposto é que as expressões crimes digitais ou delitos digitais e até mesmo criminalidade digital tornam-se coerentes, ao nosso ver, e capazes de representar a realidade do impacto das inovações tecnológicas na vida humana e no papel do Direito. Ainda nessa linha e conceituando mais precisamente o que sejam crimes digitais, Crespo (2015, p. 3) explicita,

> [...] São todas as condutas previstas em lei que sejam punidas com pena criminal e cuja prática envolva aparatos tecnológicos, seja porque a conduta destina-se contra os sistemas informatizados e contra dados, seja porque o meio utilizado é tecnológico, embora o crime pudesse ser praticado de outra

2 A lei 12.737/2012 veio como resposta a uma polêmica envolvendo a atriz Carolina Dieckmann que foi alvo de ação de criminosos, pois teve o conteúdo do seu computador, a saber, fotos íntimas divulgadas na rede mundial de computadores; o que gerou muita comoção na sociedade e apressou a elaboração e aprovação da citada lei.

> forma. [...] os crimes digitais são tanto os crimes tradicionais, já previstos na legislação, contra os valores que tradicionalmente reconhecemos como merecedores de proteção, praticados com auxílio da mais moderna tecnologia, bem como as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados. [...]

Esse conceito representa uma compreensão mais ampla, envolvendo a categoria de delitos cujo instrumento para perpetração pode ser um computador, celular, tablet, internet, e-mail com vistas a violar bens jurídicos, a exemplo dos sistemas informáticos e as informações automatizadas; bem como certos bens jurídicos tradicionalmente conhecidos na nossa legislação penal.

Ao refletir acerca desse conceito, percebe-se que a correta subsunção de determinadas condutas delitivas executadas no meio digital, torna-se exequível tendo em vista a possibilidade do uso de tipos penais já previstos na nossa legislação relacionados a bens jurídicos também previamente tutelados. De acordo com informações coletadas no site do órgão, o Superior Tribunal de Justiça-STJ vem sendo acionado a fim de determinar com maior segurança a correta interpretação das normas infraconstitucionais presentes, com relação aos crimes digitais, a exemplo de casos de extorsão, furto, ameaça, entre outros (SUPERIOR TRIBUNAL DE JUSTIÇA-STJ, 2018).

Seguindo o conceito de Crespo (2015) os crimes digitais podem ser ordenados em próprios ou puros e impróprios ou mistos. Os crimes digitais próprios ou puros são aqueles que ao serem executados atentam para a violação de dados e de sistemas de informatização, sendo penalmente punidos e previstos em lei; podendo inclusive ser também chamados de delitos de risco informático. Esses crimes digitais destacam-se pela proteção a um bem jurídico novo, a saber, a inviolabilidade dos dados informáticos. Pode-se exemplificar tais delitos como acesso não autorizado a computador, e a sistemas informáticos a fim de danificá-lo, bem como propagação de vírus.

Seguindo a mesma linha do referido autor, os crimes digitais impróprios ou mistos são aqueles que ao ocorrerem atingem bens jurídicos já estabelecidos, ou seja, que possuem a devida tutela do Direito Penal; no entanto são executados de forma aprimorada por meio tecnológico. Já os crimes digitais impróprios ou mistos se relacionam com as condutas tipificadas em lei que ofendem a bens jurídicos tradicionais diversos, a exemplo do patrimônio, honra, etc.

Ainda na esteira da discussão sobre os delitos digitais e bens jurídicos tutelados, Lotufo (2021) também compreende os crimes cibernéticos ou crimes digitais como próprios ou puros por decorrerem do surgimento da internet. Assim como a ocorrência dos crimes digitais impróprios está vinculada ao uso de computadores e/ou dispositivos conectados à rede.

Na sua visão, o bem jurídico tutelado tem um conceito abrangente e mostra-se como “[...] valor ético-social protegido pelo Direito e que tem como objetivo a garantia da harmonia das relações, o bem-estar social e a proteção das pessoas e organizações contra ataques e lesões que podem decorrer das condutas criminais digitais.” (LOTUFO, 2021, p. 4).

Cabe aqui destacar o conceito apresentado pela delegada Lauana Guedes Carvalho, chefe da DRCC de Sergipe, em entrevista realizada para a presente pesquisa,

> Crimes digitais, virtuais, cibernéticos, informáticos ou mesmo crime eletrônico (e-crime) são terminologias sinônimas e adotadas nas atividades criminosas exercidas por meio de um computador, rede de computadores ou qualquer dispositivo. Contudo, tem sido mais utilizado o termo “crimes digitais”, inclusive, é adotado pelo Conselho Nacional de Justiça do Brasil. Esses delitos, por sua vez, podem ter como alvo o próprio computador ou uso do mesmo para o cometimento de outros crimes, como, por exemplo, roubo, extorsão e estelionato. (CARVALHO, 2021).

O referido esclarecimento da delegada atuante na área de investigação dos crimes digitais reitera a terminologia adotada para o presente trabalho acadêmico, tendo em vista as justificativas já explicitadas anteriormente.

Já na perspectiva de Gimenes (2013)e de Ramalho Terceiro (2002) esses delitos são chamados de crimes virtuais, pois uma distinção que o referido autor aponta e considera crucial é a ausência física do agente ativo infrator e de seus cúmplices. Sendo assim, na sua perspectiva, essa característica acentua a utilização do termo “crimes virtuais” ou “delitos virtuais”. O conceito de virtual constante do Dicionário Escolar da Língua Portuguesa da Academia Brasileira de Letras (2008, p. 1294) aclara o tema, ou seja, virtual é aquilo "que existe somente como representação feita por programa de computador: uma biblioteca virtual; uma realidade virtual."

Além do mais, discorre Gimenes (2013, p. 8-9) sobre o que considera ser o conceito de "crimes virtuais",

> Em outras palavras, o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores (Internet) seja o instrumento ou o objeto do delito.

Percebe-se que, além daquela característica citada que destaca a ausência física do agente criminoso, o referido autor abarca nesse conceito a possibilidade do delito ser cometido contra os dados ou contra sua transmissão ou pelo uso de ambos, no caso de conexão à rede mundial de computadores; podendo o

computador ser utilizado como instrumento para o cometimento do delito; bem como seu objeto.

Note-se que por esse conceito, tanto o processamento de dados ou sua transmissão via internet, podem ser utilizados para o cometimento desses delitos tendo o computador como instrumento, para a ofensa de determinados bens jurídicos; bastando que estejam presentes os três elementos ou requisitos formadores da teoria o crime, a saber, a tipicidade, antijuridicidade e culpabilidade.

Em certa medida e respeitadas as divergências entre Crespo (2015) e de Gimenes (2013), os conceitos especificados são semelhantes por tratarem de atos ilícitos praticados por intermédio da tecnologia, mais precisamente a informática aliada à rede mundial de computadores, a internet. O que remete a uma questão puramente de optar ou não por um determinado conceito a ser adotado nos estudos desse campo específico.

A tipicidade refere-se à descrição abstrata da conduta proibida ou da permitida, abrangendo em relação à primeira, os tipos chamados de incriminadores e em relação a segunda os tipos permissivos ou justificadores. Dessa forma, os tipos penais incriminadores são aqueles descritos e criados exclusivamente pelo legislador, aplicando o princípio *nullum crimen sine lege;* enquanto os tipos permissivos tratam das causas de justificação ou da exclusão de ilicitude (TOLEDO, 1994).

Ainda segundo Toledo (1994) , ao refletir sobre a antijuridicidade o que se aduz é que a conduta humana voluntária perpetrada é contrária à legislação; podendo causar dano ou colocar em perigo um determinado bem jurídico protegido. Continua a desemaranhar esses requisitos, esclarecendo que a culpabilidade se fundamenta na ideia de um juízo de reprovação jurídica com base na concepção de que ao homem é possível, em determinadas situações, agir de outro modo que não aquele que é alvo da aludida reprovação.

Em se tratando da abordagem que utiliza a expressão “crimes informáticos” ou “delitos informáticos”, autores como Vianna e Machado (2013) esclarecem que tal perspectiva está vinculada ao conceito específico do Código Penal Brasileiro e é tomado em um sentido mais restrito. Tal terminologia é oriunda das mudanças ocorridas em alguns de seus artigos, com o advento da Lei nº 12.737/2012(Lei Carolina Dieckmann).

Essa lei acrescentou alguns artigos, a exemplo do art. 154-A, que inseriu o crime de invasão de dispositivo informático, e o art. 154-B, que se refere à ação penal que se processa mediante representação, excetuando os casos de cometimento contra à administração pública direta ou indireta de qualquer dos poderes, nas três esferas político-administrativas e suas concessionárias.

Além disso, a Lei nº 12.737/2012 alterou o art. 266, que trata dos serviços de telegráfico, telefônico, cujo título passou a abrigar as expressões "informático, telemático ou de informação de utilidade pública" e o § 1º que descreve a conduta daquele que interrompe, impede ou dificulta o restabelecimento de tal serviço. Com o art. 298 incluiu o parágrafo único equiparando o cartão de crédito ou de débito a documento particular. Essas alterações foram realizadas a fim de adequar o Código Penal às novas condutas delitivas e com vistas, especialmente, a tutelar a inviolabilidade de informações e dados automatizados.

Vianna e Machado (2013) destacam a importância da denominação do tipo penal está fundamentalmente ligada ao bem jurídico a ser tutelado, a saber, a “inviolabilidade de informações e dados informáticos”. Esse destaque ao bem jurídico em questão tem sua origem na necessidade basilar de proteção à privacidade, à intimidade, à honra e a imagem dos indivíduos, como Direito Fundamental, conforme previsto no art. 5º, X da Constituição Federal (Brasil, 1988).

Ainda segundo Vianna e Machado (2013) os crimes informáticos podem ser qualificados como próprios, impróprios, complexos ou mistos e do tipo mediato ou indireto. Os crimes informáticos próprios são aqueles cujo bem jurídico lesado é a inviolabilidade da informação automatizada, conforme determinado no art. 154-A do Código Penal. Já os crimes informáticos impróprios se referem a condutas tipificadas na legislação penal, no entanto tento o computador como meio, instrumento para sua efetivação; não havendo ofensa ao bem jurídico "inviolabilidade da informação automatizada (dados).

Os crimes informáticos mistos acabam por proteger além da inviolabilidade da informação automatizada, bens jurídicos diversos. São delitos derivados da execução da invasão do dispositivo informático que possuem a qualificação de crimes *sui generis*, a exemplo do delito previsto da Lei nº 9.100/1995, art. 67, VII, em que se tipifica o crime eleitoral de invasão de dispositivo informático do sistema eleitoral. Por fim, os crimes informáticos mediatos ou indiretos tratam das condutas típicas em que o crime informático próprio foi utilizado como crime-meio para a efetivação de um determinado crime-fim, que não é considerado crime informático; a exemplo de invasão de sistema informático(ofensa à inviolabilidade da informação automatizada) de um banco para efetuar furto(ofensa ao patrimônio).

Vianna e Machado (2013) fazem uma crítica, com base no conteúdo da Lei 12.737/2012, acerca da denominação crimes virtuais. Na compreensão dos autores, não há que se falar em bem jurídico “virtual” protegido pelo Direito Penal, mesmo que as condutas delitivas sejam efetuadas no chamado “mundo virtual”. A perspectiva de análise desses autores é dirigida exclusivamente ao termo crimes informáticos ou delitos informáticos, pois apontam como bem jurídico tutelado aquele

exclusivamente contido na Lei 12.737/2012, ou seja, a informação automatizada (dados).

Os denominados crimes cibernéticos são aqueles compreendidos dentro do conceito de ciberespaço, conceito cunhado por alguns autores e retrata o aglomerado de redes de computadores, abrangendo todos os serviços disponíveis na internet. Esse termo ciberespaço foi originalmente criado pelo escritor Willian Gibson no seu famoso romance *Neuromancer*, publicado na primeira metade dos anos 1980 que se baseava analogicamente no espaço sideral dos exploradores astronautas. (PINHEIRO, 2016).

Na perspectiva de Wendt e Jorge (2013) tais delitos são classificados em crimes cibernéticos abertos e crimes exclusivamente cibernéticos. Os primeiros são caracterizados pela possibilidade de serem praticados da forma tradicionalmente concebida, tendo o computador como meio para sua realização, a exemplo dos crimes contra honra. Já os segundos, somente podem ser realizados com ou o uso do computador ou contra tal dispositivo, ou com a utilização de outros recursos tecnológicos que viabilizam o aceso à internet, a exemplo da captação informática ou telemática sem autorização judicial ou fazendo uso de objetivos não autorizados em lei.

Destacando também a terminologia adotada pela delegada responsável pela DRCC, Lauana Guedes Carvalho ao esclarecer que "No cotidiano da DRCC-Delegacia de Repressão aos Crimes Cibernéticos, como a própria terminologia é sugestiva, adotamos normalmente a terminologia crimes cibernéticos." (CARVALHO, 2021).

Em relação à expressão “crimes cibernéticos”, são lançadas algumas críticas por Crespo (2015) que esclarece ter a palavra "cibernético" uma relação mais ligada ao emprego no estudo do que ele chama de teoria das mensagens e dos sistemas de processamento de mensagens; comparando o funcionamento do cérebro humano com os computadores. Elucida ainda que esta terminologia encontra-se em constante desuso. Nessa esteira, Vianna e Machado (2013, p. 22) defendem a ideia de que a cibernética “busca estabelecer uma teoria geral do controle, seja ele de seres inanimados ou mesmo de organismos vivos, e até de máquinas [...]”. Deve-se destacar que o uso do referido termo se faz de maneira errônea, pois se fundamenta na ideia banalizada de que há conexão direta com as tecnologias mais atuais (VIANNA; MACHADO, 2013).

Com efeito, todas essas abordagens trazem de certa forma aspectos muito similares em cada terminologia estudada, principalmente no que se refere a adoção do bem jurídico a ser tutelado, por cada classificação, e meio utilizado para execução dos delitos. No entanto, a nosso ver, a adoção feita por Crespo (2015) ao

classificar os crimes digitais em apenas duas categorias, crimes digitais próprios ou puros e impróprios ou mistos, que contêm basicamente as características principais dos referidos crimes, foi bastante clara e ampla e de compreensão mais simplificada.

2.1 OCORRÊNCIAS: FATOS RELEVANTES

A legislação brasileira passa por uma série de demandas devido ao fenômeno dos crimes executados por intermédio das atuais tecnologias, a saber, da informática e da internet. Tal contexto decorre da intensidade do fluxo de informações trocadas pelos indivíduos por intermédio da rede mundial de computadores. Afinal, de acordo com Monteiro (2010) a humanidade atualmente se encontra na fase da denominada sociedade da informação ou sociedade do conhecimento, sendo necessárias várias reflexões sobre o efeito dessas trocas de informação com o uso intenso e inevitável das Tecnologias de Informação e Comunicação-TIC. Dessa forma, ocasionando o que Tupinambá (2021, p. 15) chama de "circulação monetária em meio digital [...] e principalmente a monetização da informação[...]".

Sendo assim, todos os domínios da vida humana sofreram transformações, inclusive o Direito, pois muitos delitos previstos na referida legislação penal tiveram sua execução estrategicamente adequada às atuais tecnologias, forçando um repensar do quadro legislativo vigente.

De certa forma, o cometimento de delitos no dito mundo real tem peculiaridades que do ponto de vista da persecução penal já estão acomodadas num sistema no qual há o agente passivo e o ativo do delito e um meio físico, que propicia certas condutas por parte dos atores responsáveis pela devida investigação. Como expressa Alves (2020, p. 30) "No meio físico, tanto autor quanto a vítima estão, na maior parte das vezes, próximos entre si quando acontece o fato típico, como no exemplo cometimento de crime de roubo, em que os sujeitos ativo e passivo não podem estar distantes."

Isso é perceptível inclusive no nosso Código de Processo Penal em seu art. 6º quando determina que a autoridade policial deverá, entre outras coisas, encaminhar-se ao "local", assim que tiver ciência da prática da infração penal a fim de garantir a "integridade das coisas" até a chegada dos peritos criminais, além de apreender "objetos relacionados" com o fato, colher provas; e iniciar o reconhecimento de "pessoas, coisas e as devidas acareações" (brasil, 1941). Diante disso, o panorama do Direito Penal e Direito Processual Penal, em tese, foi construído e amparado na ideia de mundo material, atrelada à elementos como

tempo e espaço em que os delitos acontecem e os sujeitos estão em interação. (ALVES, 2020).

Ainda na perspectiva de Alves (2020) torna-se questionável e difícil tratar com tal visão os crimes digitais que não conhecem fronteiras e que, definitivamente, não são adstritos a determinados espaços geográficos para serem executados. Essa característica fomenta questionamentos acerca da territorialidade e jurisdição, além de demandar necessariamente a cooperação jurídico-policial além fronteiras o que pode ser prejudicial, por questões burocráticas, para uma possível investigação e condenação.

Outro elemento também importante, que caracteriza os crimes digitais e que Monteiro (2010, p. 45-46) faz uma importante reflexão é que "Uma das principais características dos delitos eletrônicos é a volatilidade da materialidade desses atos. Por não se tratarem de dados estáticos ou que se encontram em lugar só, estes podem ser facilmente apagados ou alterados, mesmo sem intenção".

Acrescente-se a todos esses aspectos o fato de muito do que acontece em relação aos delitos digitais não chega a entrar nas estatísticas dos órgãos oficiais, tendo em vista certas peculiaridades a serem observadas no tocante ao comportamento das vítimas que aparentam receio de comunicar tais fatos, conforme esclarece Sydow (2015 apud ALVES, 2020, p. 32-33),

> [...] a falta de comunicação destes delitos se dá, primeiramente, pelo acanhamento do ofendido que acredita que, por ter sido lesado por meio da informática, isso implicaria uma sensação de incapacidade de operar seu dispositivo tecnológico, gerando assim uma relutância em se expor. O segundo motivo é em relação às pessoas jurídicas, principalmente as instituições financeiras e as lojas virtuais, com receio de que, se relatarem alguma violação do seu sistema de segurança digital, isso ocasionaria uma perda de confiança dos consumidores em utilizar e contratar seus serviços. [...] a falta de punibilidade dos autores de crimes digitais, somando ao fato de que a reparação da vítima raramente ocorre.

Diante de uma série de pontos instigadores de reflexão a respeito desses delitos é que se concebe a fonte copiosa de características que os fazem peculiares e dinâmicos no nosso contexto social, tecnológico e legislativo.

Nesse sentido, segundo Pinheiro (2016) o crime digital pode ser considerado, em princípio, como crime de meio, ou seja, faz uso de um determinado meio para sua ocorrência, a saber, o virtual. Todavia, não pode ser chamado de crime de fim, de acordo com sua natureza, pois nem todas as suas modalidades ocorrem exclusivamente no meio virtual/digital, a exemplo de do estelionato, extorsão, falsidade ideológica, entre outras. O que remete a compreensão de que o meio de materialização do delito digital pode ser virtual, porém nem sempre o tipo penal é considerado como tal.

Esses tipos penais já previstos no nosso ordenamento jurídico torna a persecução penal mais viável, visto que novas tipificações penais somente deverão ser acolhidas mediante lei e com a observância cuidadosa do respectivo bem jurídico a ser tutelado.

De acordo com Vianna e Machado (2013) esse aspecto foi acolhido com a previsão da Lei nº 9.983/2000, que inseriu os artigos 313-A e 313-B no Código Penal, que se referem à inserção de dados falsos e modificação ou alteração não autorizada de sistema de informações por funcionário; e a Lei nº 12.737/2012, que inseriu o 154-A que aludi ao crime de invasão de dispositivo informático. Em ambos os casos o bem jurídico considerado relevante na esfera do penal foi a inviolabilidade das informações automatizadas.

Relacionando ainda as questões referentes ao tema em pauta, surge um conceito muito relevante, a saber, de "engenharia social" que se refere segundo LOTUFO (2021a) às práticas que utilizam estratégias de persuasão, manipulação e de influência da conduta humana para obtenção de informações sigilosas ou muito valiosas. Entende-se que o uso da engenharia social não é restrito ao universo da tecnologia de informação, mas esse crescimento do mundo digital possibilitou sua constante aplicação como estratégia de consecução de informações relevantes, tanto de pessoas quanto de empresas, para os agentes delituosos.

De acordo com LOTUFO (2021a) mesmo com o avanço dos mecanismos de codificação e proteção das informações no meio digital, de forma diretamente proporcional às estratégias de decifrá-los e violá-los também se desenvolveram. Sempre está presente o que a referida autora chama de elo mais fraco dessa da cadeia de proteção, a saber, o ser humano. Isto porque sempre há a necessidade, na produção de mecanismos de defesa e segurança dos dados informáticos, de pessoas na linha de frente que são passíveis de erros e de serem corrompidas, sem uma razão lógica previsível para tal fato.

Complementando a informação, Goodchild (2011) apresenta dados de pesquisa realizada pela Empresa de Segurança Check Point Software Technologies com profissionais da área de Tecnologia da Informação de vários países, a exemplo de Estados Unidos, Canadá, Reino Unido, Alemanha, entre outros; que demonstram um percentual de 48% dos entrevistados que confirmaram que suas empresas foram alvo de de engenharia social.

Além disso, 86% dos profissionais ratificaram que esse método de ataque causa grande preocupação. Ainda de acordo com a referida pesquisa, constatou-se que em 47% dos casos de engenharia social os criminosos utilizam o e-mail *de phishing*[3] como ferramenta; e 39% utilizam as redes sociais

3 Tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Nesse sentido, o fator humano continua a ser o ponto mais frágil dessa cadeia de proteção no meio digital. A compreensão acertada dessa dimensão é destacada por Alexandria (2009, p. 48),

> Muitas organizações ignoram as questões sociais e comportamentais em seus programas de segurança da informação. É um erro imaginar que os aspectos humanos sejam menos importantes, e que o estabelecimento de políticas e a aplicação de controles técnicos sejam suficientes para garantir um ambiente seguro.

Sendo assim, diante de uma realidade de incidência de crimes digitais que fazem uso de uma cadeia de estratégias para persuadir, ludibriar e induzir as pessoas que utilizam a rede mundial de computadores para suas atividades cotidianas; faz-se necessária a atenção para o preparo desses cidadãos para condutas claras e eficazes que combatam os referidos delitos.

Corroborando com essa posição, Carvalho (2021) esclarece ser necessário que "[...] o usuário tome as precauções mínimas para que não seja mais uma vítima, como, por exemplo, fazer uso de senhas fortes, instalar um bom antivírus no computador, manter as informações pessoais bloqueadas, acessar apenas sites oficiais e não clicar em links desconhecidos".

Além disso, Pinheiro (2016) faz um alerta importante acerca das dificuldades jurídicas de se investigar as ocorrências dos crimes digitais ou eletrônicos, como a baixa procura para registrar os crimes, isto atrelado ao despreparo das equipes de polícia investigativa e de perícia. Salienta que alguns dos criminosos na internet não são especialistas e nem dispõem de muito conhecimento técnico necessário para o cometimento de alguns crimes, pois há uma série de facilidades disponíveis na rede que viabilizam a localização do chamado de código-fonte de um vírus ou um trojan[4].

Relata ainda Pinheiro (2016) que há situações em que o conhecimento do criminoso é acima do esperado, efetuando inclusive a clonagem de sites para a obtenção de dados pessoais dos cidadãos, a exemplo de Cadastro de Pessoas Físicas-CPF, data de nascimento, Registro Geral-RG, entre outros. Esses dados pessoais quando ilicitamente obtidos abrem caminho para uma série de práticas de outros delitos. A referida autora reforça a ideia de que a falta de informação dos usuários dificulta a ação da polícia, pois muitas vezes não conseguem passar todas as informações necessárias para desempenho das investigações; bem como a insuficiência de recursos nas delegacias também obstam o êxito das referidas investigações.

Diante de tudo que foi discorrido, reflete-se a respeito da maneira como o

---

4 Tipo de código malicioso. Programa normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

Direito Penal, ao ser confrontado com a ocorrência dos crimes digitais que possuem características específicas não respeitando os limites de fronteiras territoriais nem de espaços geográficos; se comporta perante os conceitos de territorialidade, lugar do crime e provas. Assim, a sucessão das diversas modalidades desses crimes faz com a discussão sobre esses importantes tópicos seja suscitada a fim de contribuir para a busca de um melhor procedimento; tornando a persecução penal em todas as suas fases mais viável.

Pinheiro (2016) salienta que dentro da abordagem dos crimes digitais, os temas relativos ao conceito de crime, delito, atos e efeitos são os mesmos; importando especificamente nesses casos os aspectos de territorialidade e a obtenção das provas; além obviamente, da necessária tipificação de algumas condutas em razão de suas características particulares. Esses crimes digitais no Brasil, segundo a referida autora, vem ganhando força como mais um braço do crime organizado, movimentando recursos financeiros de grande monta; tendo como exemplos de delitos recorrentes o estelionato em todas as suas formas, previsto no art. 171 do Código Penal, bem como a pornografia infantil.

Entende-se a territorialidade como aquele princípio fundamental previsto no art. 5º, caput, do Código Penal Brasileiro, que remete à aplicação da lei brasileira ao crime cometido em território nacional, sem prejuízo de convenções, tratados e regras de direito internacional (BRASIL, 1940).

Em regra, conforme determina o § 1º, do referido artigo são submetidos à legislação brasileira crimes cometidos nos espaços aéreo, terrestre, das águas fluviais e dos mares sobre os quais é exercida a soberania do Estado Brasileiro. Além disso, conforme prevê seu § 2º, consideram-se como extensão do território brasileiro as embarcações e aeronaves brasileiras de natureza pública ou que estejam a serviço do governo brasileiro; bem como as aeronaves, no espaço aéreo e embarcações brasileiras mercantes ou de propriedade privada que se localizam em alto-mar. (BRASIL, 1940).

Essa territorialidade refere-se basicamente sobre os limites da aplicação da jurisdição penal do Estado brasileiro ligados à sua soberania. Entretanto, a rápida e constante propagação das ocorrências dos crimes digitais suscita questionamentos diversos em relação a tais limites e parecem ganhar ainda mais força, principalmente quando o resultado desses delitos originados aqui no Brasil é efetivamente produzido em vários países.

A compreensão da dificuldade acerca dos aspectos legais envolvendo o "território digital/virtual" em que não há limites geográficos, mas quebra de fronteiras; e que conflitos gerados dentro desse espaço virtual/digital, a exemplo dos crimes digitais, demandam uma nova forma de discipliná-los; remete ao que Carvalho (2014, p. 93) discorre,

> A criação de regras para disciplinar o espaço virtual pressupõe uma nova visão de território, para além de um simples conjunto de objetos, mediante os quais as pessoas trabalham, circulam, moram, mas também um dado simbólico. A territorialidade não provém do simples fato de viver em um lugar, mas da comunhão com ele mantida, ao se passar do regime do orgânico, em que a consciência se criava a partir das trocas orgânicas diretas entre o homem e a natureza, para o império do organizacional, no qual dados externos ao orgânico se impõem[...]

Já analisando o conceito de lugar do crime, tem-se sua previsão no art. 6º do Código Penal, declarando que "considera-se praticado o crime no lugar em que ocorreu a ação ou a omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado" (BRASIL, 1940). Desse modo, os crimes digitais muitas vezes, por não respeitar fronteiras, causam resultados em vários lugares; originando assim um impasse muitas vezes burocrático em relação às etapas da persecução criminal, a saber, a obtenção de provas, por exemplo. Portanto, nas palavras de Monteiro (2010, p. 49, grifo nosso),

> Em suma, não existem critérios seguros para determinar em que medida o local da prática de um crime ou o local em que um crime se consuma deve ser considerado o local do crime. Várias teorias são adotadas por vários países, de forma diferente, e cada um tem competência para determinar se tem ou não autoridade para processar o delito em seu território. Tratados internacionais podem discorrer sobre a matéria, em nível de cooperação, para que os delitos sejam tratados onde o dano resultante for maior, ou onde possa ser encontrado melhores condições de investigação, para então colher as provas de forma mais adequada e fornecê-las para que as demais jurisdições tomem as medidas que por ventura [*sic*] entenderem necessárias.[...] A posição defendida no presente trabalho é o da cooperação a nível nacional e internacional e esta prevalece nesse ponto. Caso haja conflito de jurisdição causado pela natureza fragmentária e transnacional dos crimes eletrônicos, esta deve ser suprida por acordos de cooperação e auxílio mútuo entre os países.

A partir da destacada compreensão e observando a questão das provas, seria possível optar pela melhor localização a fim de realizar a sua coleta de maneira mais eficaz para a investigação. De acordo com Shimabukuro (2017) as provas nos crimes digitais são muitas, porém com certas peculiaridades que as fazem voláteis, pois as evidências digitais se não forem devidamente preservadas podem ser alteradas ou destruídas de forma bem célere; dificultando sobremaneira a investigação criminal.

É preciso, reforçando a posição adotada por Monteiro (2010), uma intensa e constante integração por partes dos países a fim de otimizar as investigações e a necessária consecução de provas; expandindo essa cooperação para um nível global, se praticável. Também Carvalho (2014) destaca a importância da construção de novos parâmetros jurídicos a fim de resolver questões de ordem territorial,

jurisdicional com foco nos tratados e convenções internacionais.

2.1.1 **Tipos Comuns de Crimes Digitais**

Inevitavelmente, faz-se necessário referenciar os delitos digitais próprios ou puros, que são aqueles que envolvem o acesso não autorizado a dados e a sistemas de informática regularmente tipificados em artigos do Código Penal Brasileiro. Segundo Vianna e Machado (2013) havia uma lacuna existente na nossa legislação penal acerca da tipificação da invasão de dispositivo informático.

Ficando evidente essa procrastinação dos legisladores, ao constatar que tal ação praticada pelos agentes não era considerada crime no Brasil até o ano de 2012. Assim, no nosso ordenamento jurídico havia essa ausência que demonstrava ser imperativa a elaboração de uma legislação específica que tratasse da violação/acesso de dados informáticos.

Em decorrência do exposto, com a Lei nº 12.737/2012 foram instituídos os denominados delitos informáticos, ou crimes digitais próprios ou puros na concepção de Crespo (2015). Esses crimes surgiram da necessidade de se tipificar a invasão do dispositivo informático e proteger a inviolabilidade das informações automatizadas, conforme art.154-A do Código Penal que prescreve:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita[...]. (BRASIL, 1940)

Além desse, também foram acrescidos ao Código Penal pela mencionada lei, os crimes de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, cujo bem jurídico tutelado é a incolumidade pública, conforme previsão do art. 266, §§ 1º e 2º; e o de falsificação de cartão, tipificado no art. 298, parágrafo único, permitindo a sua equiparação a documento particular. Aqui cabe destacar os artigos 313-A e 313-B que também tratam da proteção à inviolabilidade das informações automatizadas da Administração Pública, acrescentados pela Lei nº 9.983, de 14 de julho de 2000.

Igualmente no rol de crimes digitais impróprios, há a previsão no Código Penal do delito de falsa identidade (art. 307) que ocorre quando alguém atribui a si ou a terceiro falsa identidade com o objetivo de obter vantagem própria ou alheia, ou

de causar dano a alguém. (BRASIL, 1940). Importante destacar que o objeto ou bem jurídico protegido por esses tipos penais, a saber, falsificação de cartão e falsa identidade, é a fé pública. Esta é considerada como bem intangível, pois para a coletividade há pressuposição da segura credibilidade em assuntos concernentes ao Estado[5].

Ainda com base no Código Penal, há os crimes contra honra, a saber, calúnia (art.138), difamação (art.139) e injúria (art.140) que são exemplos de crimes digitais impróprios ou mistos, visto que o bem jurídico aqui tutelado é tradicionalmente conhecido; no entanto, a forma como é materializada a conduta delitiva é transformada em consequência da utilização das Tecnologias de Informação e Comunicação, mais precisamente da internet.

Esses crimes digitais contra a honra são estimulados, muitas vezes, pela sensação de anonimato que a rede mundial de computadores causa nos agentes criminosos. São utilizados chats, blogs, homepages, sites, redes sociais, de uma forma geral, entre outros meios de comunicação e divulgação no mundo digital.

Um fato interessante a se ressaltar é que esses crimes passaram a ter suas penas triplicadas ao serem cometidos ou divulgados em quaisquer modalidades das redes sociais da rede mundial de computadores, conforme previsto na Lei nº 13.964/2019, de 24 de dezembro de 2019, o denominado "pacote anticrime", que inseriu o § 2º ao art. 141 do Código Penal. A mencionada previsão de majoração da pena tinha sido anteriormente vetada pela Presidência da República, com a alegação de que violava o princípio da proporcionalidade, quando da publicação legal.

Contudo, no mês de abril deste ano, os vetos foram derrubados pelo Congresso Nacional e o referido dispositivo foi integrado ao texto da lei. O Desembargador Guilherme Nucci, concordando com a queda do veto, em entrevista concedida ao site do www.migalhas.com.br, esclarece que a referida majoração "objetiva punir mais gravemente a prática do crime contra a honra, quando cometido na presença de várias pessoas ou outro meio facilitador da divulgação". (MIGALHAS, 2021). Isto posto, em se tratando da internet e das diversas redes sociais existentes, a velocidade com que essas ofensas avançam atinge um número extremamente significativo de pessoas, podendo causar efeitos danosos muito mais graves às vítimas.

Também se enquadram como crimes digitais impróprios ou mistos, previstos no Código Penal, aqueles que atentam contra a liberdade individual, a saber, de ameaça (art.147), contra a inviolabilidade de correspondência (art. 151 e art. 152) e

5 DECISÃO: Falsa identidade agride a fé pública e não permite aplicação do princípio da insignificância. Disponível em: https://portal.trf1.jus.br/portaltrf1/comunicacao-social/imprensa/noticias/decisao-falsa-identidade-agride-a-fe-publica-e-nao-permite-aplicao-do-principio-da-insignificancia.htm. Acesso em: 01 jan 2021.

contra a inviolabilidade dos segredos previsto nos artigos 153 e 154, bem como aquele específico que trata de divulgação de segredos contidos ou não em sistemas de informação ou bancos de dados da Administração Pública (art. 153, § 1º- A). Ressalta-se que o referido § 1º-A foi incluído pela Lei nº 9.983, de 14 de julho de 2000, trazendo a adequação das ações criminosas com base nas tecnologias direcionadas à Administração Pública.

Da mesma forma, seguindo a concepção de crimes digitais impróprios na nossa codificação penal, há crimes cujo bem jurídico tutelado é o patrimônio, como é o caso , furto (art. 155), extorsão (art.158), com uma particularidade de que na extorsão há o sequestro de informações, dados que possuem valor altamente monetário para pessoas, empresas e para Administração Pública; o crime de apropriação indébita (art. 168) e por fim um dos mais recorrentes no cotidiano da população o estelionato (art. 171).

Os crimes contra o patrimônio, especialmente este último, tem grande projeção no meio digital e vem crescendo de forma intensa, por permitir a utilização de uma série de artefatos e técnicas capazes de induzir ou manter a vítima em erro. (POLÍCIA CIVIL DO ESTADO DE SERGIPE, 2021).

Também há a previsão no Estatuto da Criança e do Adolescente-ECA, nos artigos 240 ao 241-E, do crime de pornografia infantil ou infanto-juvenil[6], nos meios de comunicação de uma forma geral, inclusive no digital; destacando os tipos penais e os respectivos verbos do tipo, bem como as penas aplicadas e as situações de majoração das referidas penas.(BRASIL, 1990).

De acordo com Shimabukuro (2017) os criminosos que cometem o crime de pornografia infantil utilizam comumente a chamada *dark web* ou *darknet*[7], pois dessa forma conseguem compartilhar o material de forma anônima, dando a sensação de segurança e impunidade.

Alertam Wendt e Jorge (2013) que a pornografia infantil não deve ser confundida com a pedofilia, pois aquela compreende a divulgação e uso de imagens de conteúdo erótico e é muito difundida pela internet. Existem perfis desses criminosos, aqueles que produzem vídeos e fotos e divulgam na internet, bem como aqueles que consomem esse tipo de material; além disso atuam nesse contexto criminoso as organizações tanto nacionais quanto internacionais de pornografia infanto-juvenil. Um exemplo desse crime, por meio digital, é o aliciamento de menores previsto no art. 241-D do ECA, em que boa parte das ocorrências são

6 Expressão utilizada por Ângelo Roberto Ilha da Silva, por ser considerada mais abrangente que pornografia infantil. A pornografia infantil segundo definição da UNESCO, constitui qualquer meio de retratar ou promover o abuso de uma criança, incluindo meios impressos ou de áudio, centrados nos atos sexuais ou nos órgãos genitais das crianças.

7 Dark Web ou Darknet é uma rede fechada, usada para compartilhar conteúdo de forma anônima. Seu acesso é permitido mediante o uso de softwares específicos, como o TOR Project, o Freenet e a rede I2P (2017) ou outras dezenas de redes secretas e criptografadas.

realizadas com a utilização dos computadores e outros meios tecnológicos conectados à rede mundial de computadores.

Segundo Patrícia Peck Pinheiro, existem muitas situações a serem observadas, problematizadas numa possível discussão no Legislativo acerca das diversas formas de execução desses delitos e suas caracterizações em ambientes digitais. Diante disso a referida autora aponta que,

> Desse modo, precisamos, para a matéria de crimes eletrônicos, de uma boa atualização do Código Penal Brasileiro, do Código de Processo Penal Brasileiro e da Lei de Execuções Penais. Mas nada disso será útil sem um modelo forte de prova de autoria, de uma identidade digital obrigatória. (PINHEIRO, 2016, p. 378)

Tal discussão mostra-se importante, pois demanda cautela em toda essa problemática acerca de temas delicados relacionadas ao cometimento de delitos no meio virtual, a exemplo das provas de autoria e da identidade digital, a fim de não penalizar os inocentes ou aqueles que não detêm um conhecimento seguro acerca do uso dos recursos disponibilizados pela internet.

2.1.2 **Crimes Digitais: Algumas Técnicas Usuais**

Ao tratar dos ataques oriundos da internet, o criminoso utiliza com frequência técnicas, artefatos ou métodos específicos que permitem a concretização da conduta criminosa no meio digital.

Nesse sentido, alerta Jesus e Milagre (2016, p. 29) acerca do lapso temporal para elaboração de legislações sobre crimes digitais no Brasil e principalmente sobre a forma equivocada de se legislar sobre esses crimes,

> "[...] Tal mora pode ser atribuída ao péssimo modo de se legislar sobre o tema adotado no Brasil que, por vezes, tentou condenar técnicas informáticas (ao invés de condutas praticadas por diversas técnicas), técnicas estas que são mutantes, nascem e morrem a qualquer momento, de acordo com a evolução dos sistemas, novas vulnerabilidades e plataformas tecnológicas.[...].

Uma técnica já citada nesta pesquisa é a "Engenharia Social" que, segundo Jesus e Milagre (2016) por intermédio de ferramentas tais como e-mails falsos com anexos ou com orientações para que o indivíduo acesse determinados links maliciosos, leva a sites clonados e a páginas falsas de instituições financeiras. Todo esse procedimento tem como objetivo específico a obtenção de informações valiosas que servem de insumos para o cometimento de outros delitos, a exemplo

do estelionato e outras fraudes; visto que nossa sociedade está conectada permanentemente.

De acordo com Tupinambá (2021) a ação criminosa dentro do ambiente digital possui um *modus operandi* característico, existem técnicas além da citada engenharia social que são amplamente utilizadas para obtenção de informações que fazem parte da execução do delito. Uma das mais aplicadas é o chamado *phishing ou phishing scam* que teve seu início na década de 1990 e ainda é considerado o mais expressivo meio de ataque e fraudes digitais no ano de 2020; sendo executado na maioria das vezes por meio do endereço eletrônico, ou seja, e-mail.

Ainda na percepção de Tupinambá (2021) entende-se que nos dias atuais além do e-mail, existe uma diversidade de caminhos que são utilizados com frequência para a execução do *phishing,*a saber, SMS[8], as redes sociais, páginas da web, aplicativos maliciosos, documentos digitais e qualquer outro meio digital que permita a execução da "pescaria".

Outro exemplo que Tupinambá (2021) elenca dessa técnica delituosa utilizada pelos criminosos é o *malware* que é um software malicioso que tem como objetivo a obtenção de informações importantes, além de poder controlar a máquina, servidores, dispositivos, como também a rede vinculada de forma remota; podendo inclusive se disseminar da remotamente. Nos dias atuais, o propósito da aplicação do *malware* pode ser altamente variado causando sequestro de informações com pedidos de resgate, o que caracteriza a extorsão, entre outros.

As informações digitais são na maioria das vezes o objetivo desses criminosos, para isso existem uma infinidade de espécies que são abarcadas pelo gênero *malware,* tais como *spyware*[9], ou seja, código espião, que por sua vez pode ser identificado como *keyloggers*[10]*.* Conforme Jesus e Milagre (2016)*,* esses *keyloggers* são responsáveis por gravar dados digitados pelos usuários ao acessarem normalmente o site do *internet banking* ou sites de comércio eletrônico.

Já Tupinambá (2021) ressalta que é possível destacar um leque variado de tipos de códigos maliciosos que visam aos mais diversos alvos, a saber, a gravação de informações registradas na tela, alteração e destruição de dados, invasão de privacidade, bem como captura de imagens e de áudio com objetivo de extorsão, modificação de serviços e de domínio, captura de tráfego de dados, obtenção de de informações para acesso a e-mails e redes sociais, serviços bancários, serviços

8 Do inglês Short Message Service. Tecnologia utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas dados do tipo texto e cada mensagem e limitada em 160 caracteres alfanuméricos.
9 Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware. DIsponível em: https://cartilha.cert.br/
10 Tipo específico de spyware. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente a ativação do keylogger é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

corporativos, espionagem empresarial, governamental e pessoal, furtos de criptomoedas, entre outros.

Uma característica bastante interessante do *malware* é a capacidade de camuflar, através de compressão, criptografia de código e a mutação, a fim de não ser detectado pelos softwares de proteção da máquina, a exemplo de antivírus. (TUPINAMBÁ, 2021).

Outro exemplo interessante de um software malicioso e bastante utilizado nos ataques de criminosos é o *ransomware*[11] que é responsável pelo sequestro de informações importantes das vítimas, pessoas naturais e organizações com exigência de pagamento para a devolução das informações sequestradas. Para o referido pagamento é exigido, comumente criptomoedas[12], pois dessa maneira torna-se muito difícil localizar a origem ou rastrear o caminho percorrido até o destino final; bem como o acesso às informações sequestradas só é obtido, quando ocorre, após o pagamento e através do acesso da vítima à *deepweb.* (TUPINAMBÁ, 2021).

Além disso, Tupinambá (2021) discorre sobre a técnica de envio via internet de um falso boleto para vítima, que na verdade já era utilizada mesmo antes, através de correspondência física. Essa vítima por acreditar que o documento é verdadeiro, até mesmo por ter relação com a entidade comercial, profissional, identificada no referido documento, acaba por efetuar o pagamento; no entanto o valor é depositado na conta do criminoso, pois este configura a linha digitável e o código de barras.

Com o aprimoramento dessa técnica, advindo com o avanço das tecnologias, o criminoso instala um *malware* que consegue detectar se há boletos emitidos em sites da internet e em e-mails, alterando as características da conta de depósito com os dados do agente criminoso.

---

11 O ransomware é um malware utilizado para sequestro de dados das vítimas.

12 Normalmente os cibercriminosos têm utilizado o bitcoin (criptomoeda) para o pagamento dos resgates por dificultar o rastreamento das transações. O bitcoin trata-se de uma moeda digital descentralizada, ou seja, ela não depende de um emissor central e pode ser transacionada para qualquer pessoa em qualquer parte do planeta sem intermediários, e, inclusive, sem limite de valor.

3 **PANORAMA LEGAL ACERCA DOS CRIMES DIGITAIS NO BRASIL**

A Lei nº 12.375/2012, de 30 de novembro de 2012, é chamada popularmente de Lei Azeredo, pois recebeu o nome do seu relator; trouxe como uma das principais inovações o fomento da especialização da polícia judiciária em relação aos crimes digitais. O texto legal traz no seu artigo 4º:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. (Brasil, 2012).

Sendo assim, a partir desse instrumento legal buscou-se estimular mecanismos a fim de se equipar a polícia judiciária de forma adequada com o principal objetivo de combater, a contento, os crimes efetuados na rede mundial de computadores e aqueles que afetam dispositivos de comunicação e sistemas informatizados.

Além disso, a Lei 12.375/2012 alterou o art. 20, § 3º, incluindo nova redação ao inciso II, da Lei nº 7.716/1989, a Lei do Racismo. Tal alteração incluiu a necessidade de "cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio, que contribuam para a prática dos crimes de racismo divulgados por intermédio dos meios de comunicação social ou da publicação por qualquer natureza (BRASIL, 1989).

Essa mudança na Lei do Racismo, ao incluir no referido inciso a expressão "eletrônicas ou da publicação por qualquer meio" atendeu a transformação ocorrida com o crescimento do uso de Tecnologias de Informação e Comunicação-TIC, que intensificou o fluxo de interações sociais na internet, decorrendo daí a possibilidade desse fluxo ser um meio, em potencial, de indução ou incitação ao racismo; principalmente com uso das redes sociais em todas as suas modalidades.

No Estado de Sergipe, há a atuação da Delegacia de Repressão a Crimes Cibernéticos-DRCC com funcionamento junto ao Departamento de Crimes contra o Patrimônio-DEPATRI, criado no ano de 2017, a fim de centralizar as ações de combate a esses delitos (POLÍCIA CIVIL DO ESTADO DE SERGIPE, 2021). De acordo com Wendt (2020) o Brasil se encontra atualmente com 20 estados que possuem unidades especializadas com o objetivo de combater os crimes praticados no meio digital, seja uma divisão ou uma delegacia propriamente dita.

Nesse sentido, assevera Barreto (2018) ao analisar a Lei Azeredo levantando a importante contribuição dessa especialização da polícia judiciária a fim de dar mais efetividade naquilo que alude à configuração da autoria e da materialidade dos delitos digitais. Esclarece ainda o referido autor que, à medida que esse processo se

perfaz, as possibilidades de solução dos casos se tornam mais viáveis por terem as condições técnicas adequadas.

Igualmente, a Lei 12.737/2012, de 30 de novembro de 2012, comumente conhecida como Lei Carolina Dieckmann, foi responsável pela inclusão no Código Penal Brasileiro, de dispositivos que abarcam ofensa à inviolabilidade das informações e dados informáticos, a exemplo do previsto no art. 154-A que trata do tipo penal "invasão de dispositivo informático", especificamente considerado crime digital próprio ou puro; e do art. 154-B que se refere à ação penal relativa a esses casos.

Além do mais, com a Lei 12.737/2012 foram incluídas pequenas alterações no texto do art. 266 do Código Penal, em que foi inserido o § 1º que discorre sobre a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; bem como foi alterado seu título para inclusão das expressões "informático, telemático ou de informação de utilidade pública" (Brasil, 2012). E, por fim, foi alterado parcialmente o art. 298 do Código Penal, que trata de falsificação de documento particular; passando seu conteúdo a ter um parágrafo único, em que consta a equiparação a documento particular do cartão de crédito ou de débito.

Do mesmo modo, a inserção de dados falsos em sistema de informações, conforme art. 313-A e a modificação/alteração não autorizada de sistema de informações disposta no art. 313-B do Código Penal, possuem como bem tutelado os dados informatizados; uma vez que se pretende proteger a sua inviolabilidade. Estes dispositivos foram inseridos no texto penal por intermédio da lei nº 9.983, de 14 de julho de 2000. Esta lei objetiva a tutela da Administração Pública naquilo que se refere aos sistemas informatizados, banco de dados e programas de informática geridos pela esfera pública e que são praticados por funcionários públicos "autorizados", ou seja, são seus sujeitos ativos.

Além dessas alterações originadas das referidas leis em comento, ainda existem no Código Penal Brasileiro, conforme exposto nesta pesquisa, alguns artigos relacionados a tipos penais que já são normalmente cometidos fora do meio digital. No entanto, há a possibilidade desses delitos serem perpetrados pelo meio virtual, adequando-se, dessa forma, aos chamados crimes digitais impróprios ou mistos.

Portanto, podem ser enquadrados na referida condição os crimes contra a honra, que vão do art. 138 ao art. 140, abarcando a calúnia, difamação e a injúria, respectivamente. O crime de ameaça previsto no art.147; o furto com previsão no art. 155, a extorsão conforme art. 158, apropriação indébita descrita no art. 168, o estelionato descrito no art. 171; bem como a falsa identidade consolidada no art. 307; todos artigos com Código Penal.

Soma-se a esse cenário o Estatuto da Criança e do Adolescente-ECA (Lei nº 8.069/1990) que teve alguns de seus artigos do texto original alterados e outros foram inseridos, no ano de 2008, por intermédio da Lei nº 11.829, de 25 de novembro de 2008, a fim de se adequarem de forma mais rígida acerca da proteção da criança e do adolescente em relação aos crimes contra sua dignidade sexual.

Os artigos que se referem a proteção da criança e do adolescente, inclusive no meio digital, vão do art. 240 a art. 241-D que tratam da pornografia infantil; proibindo entre outros atos a apresentação, produção, venda, fornecimento, divulgação, distribuição ou publicação por qualquer meio de comunicação, incluindo a rede mundial de computadores ou Internet (BRASIL, 1990).

Conforme Wolff (2018) discorre, uma questão interessante deve ser observada em relação à vigência da Lei nº 13.441/2017, de 08 de maio de 2017; que alterou o ECA para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente, de forma pioneira. Os tipos penais abarcados pela Lei nº 13.441/2017 na ação de agentes virtuais infiltrados estão descritos no Código Penal, a exemplo do art. 217-A (estupro de vulnerável) e dos artigos referenciados no citado Estatuto, ou seja, do Art. 240 ao 241-D(Brasil, 2017).

Também há que se pontuar a chamada Lei de Proteção à Propriedade Intelectual de Programas de Computador, ou seja, a Lei nº 9.609, de 19 de fevereiro de 1998, que trata do conceito de programa de computador abarcando sua comercialização, previsão de direitos do autor, e elencando, inclusive, algumas penalidades no seu capítulo V, a exemplo do tipo penal previsto no at. 12 que trata da violação dos direitos do autor do programa.

As penas previstas no art. 12 da Lei de Proteção à Propriedade Intelectual de Programas de Computador possuem qualificadoras, de acordo com seu § 1º, como no caso da reprodução, por qualquer meio, do referido programa, mesmo que em parte, para fins comerciais, sem autorização; passando a pena a ser mais severa, ou seja, de reclusão de um a quatro anos, incluindo multa (Brasil, 1998). Tal instrumento legal confere proteção aos autores de softwares, tendo em vista aos ataques constantes da famosa pirataria digital que é uma realidade em nossos dias.

De acordo com Brugioni (2006) O aludido texto legal traz a orientação da possibilidade de proteção independentemente do registro dos programas no Instituto Nacional da Propriedade Industrial-INPI. No entanto, recomenda-se que seja feito o devido registro para que o autor/inventor possa ter garantida a proteção ampla reservada pela lei.

Da mesma forma, a Lei nº 9.296, de 24 de julho de 1996, que trata da interceptação de comunicações telefônicas, informática e telemática traz no seu

corpo, precisamente no seu art. 10, a constituição de crime ao se efetuar a interceptação de comunicações, telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem a devida autorização judicial ou com objetivos não autorizados em lei; prevendo uma pena de reclusão de dois a quatro anos e multa (brasil, 1996).

Ressalta-se que a Lei nº 9.926/1996 também foi alterada pela Lei nº 13.869, de 05 de setembro de 2019, que trata dos crimes de abuso de autoridade, que acabou introduzindo algumas inovações, a exemplo da inclusão da expressão "promover escuta ambiental" no citado artigo, a fim de se amoldar às atuais demandas do legislação penal e processual penal, entre outras.

Prosseguindo na análise, há que de se relatar um importante acontecimento do ponto de vista de segurança nos meios digitais, a exemplo do Marco Civil da Internet, ou seja, a Lei nº 12.965, de abril de 2014, que trata da regulamentação do acesso e uso da Internet no Brasil visando garantir o direito à informação, à proteção e à liberdade de expressão. Nas palavras de Pinheiro (2016, p. 91),

> A análise desse recente marco legal demonstra a difícil missão de legislar sobre a matéria. Com pouco mais de 30 artigos, tentou-se estabelecer uma carta de princípios para uma Internet mais inclusiva e justa para os brasileiros. São eles: neutralidade, acesso à internet como direito essencial para o exercício da cidadania, liberdade de expressão e permanência do conteúdo e sua remoção só em casos excepcionais e com ordem judicial, privacidade (com vedação para monitoração não acordada de forma prévia e expressa com o internauta), proteção de dados pessoais, transparência com exigência de regras claras de provedores de conexão e de aplicações na *web*, segurança na rede, educação em ética digital, uso preferencial de códigos abertos e responsabilidade dos agentes.

A citada lei reflete a preocupação do legislador com os direitos e deveres envolvendo a utilização da internet no nosso país. As empresas responsáveis pela fornecimento de tais serviços, ou seja, os provedores de conexão[13] à internet e de aplicação[14] da rede mundial de computadores ficam obrigadas a guardar informações dos usuários, além da data e hora dos acessos, para que seja possível permitir a sua correta identificação.

Na visão de Shimabukuro (2017) tais provedores passam a ser agentes na investigação criminal, ainda que haja os direitos relativos à privacidade, pois a obtenção dessas informações é fundamental para o devido rastreio da conduta criminosa e, somente pode ser realizada mediante autorização judicial.

Do mesmo ponto de vista, Barreto e Brasil (2016) destacam o papel importante do Marco Civil para o Direito Penal e Processual Penal, embora tenha

---

13 Provedor de conexão é a pessoa jurídica fornecedora de serviços que possibilitam o acesso dos consumidores à Internet. Exemplo: Tim, Claro, Vivo, etc.
14 Provedor de aplicação é a pessoa natural ou jurídica que se utiliza do acesso à Internet para prestar serviços. Exemplos: provedores de conteúdo, de e-mail, de hospedagem, etc.

suas origens atreladas à tutela de direitos civis, traz no seu arcabouço elementos cruciais para a atuação dos referidos diplomas legais penais, a saber, trata de conceitos, provas e suas formas de obtenção a fim de se chegar a autoria e materialidade do delito digital.

De acordo com Pinheiro (2016) o Marco Civil da Internet também trouxe para o âmbito da nossa jurisdição questões relacionadas a empresas no estrangeiro, conforme ciência do seu art. 11. O texto do referido artigo ressalta que, para operações que envolvam a coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou de comunicação de provedores de conexão e de aplicações da Internet, ocorridas, qualquer uma delas, em território nacional; a legislação brasileira é que prevalece, respeitando a privacidade, a proteção de dados pessoais, o sigilo das comunicações privadas e os registros.

Porém, ainda segundo Pinheiro (2016) faz-se necessário abordar alguns aspectos acerca do Marco Civil da Internet. Um dos dilemas enfrentados a respeito do que ficou determinado no seu art. 11, § 2º, a saber, quando passou a regulamentar que as empresas que de alguma forma coletam dados de brasileiros, ou seja, ofertam serviços ao público brasileiro, mesmo que tenham seus servidores situados fora do país, devam se submeter à referida lei.

Além disso, Pinheiro (2016) alerta para o fato de que o Marco Civil afeta consideravelmente segmentos de mercado, restringindo algumas práticas, tendo em vista a exigência dos princípios da neutralidade, liberdade de expressão e da privacidade dos dados dos internautas no país. A discussão que é proposta, segundo a autora em tela, é a possível intervenção estatal na livre-iniciativa e na economia. Essas empresas e pessoas naturais, inclusive as situadas fora do país, estão sujeitas, inevitavelmente, às leis brasileiras por tratarem necessariamente de dados de brasileiros, estando submetidas às penas previstas no art. 12 da aludida lei; que abrangem advertência, multa, suspensão e proibição do exercício das atividades.

A Lei nº 13.709, de 14 de agosto de 2018, a conhecida Lei Geral de Proteção de Dados-LGPD vem na esteira da proteção dos dados pessoais, inclusive nos meios digitais. Ressalta-se que a *vacatio legis* da LGPD, em relação às sanções administrativas, foi estendida até 1º de agosto de 2021; em função da pandemia da covid-19, conforme Lei nº 14.010/2020, de 10 de junho de 2020, que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19).

A LGPD chega num momento propício, em que o cometimento de delitos com a utilização dos dados, das informações dos cidadãos se torna cada vez mais crescente. Recentemente, no nosso país, foi noticiado o vazamento de dados

pessoais, a exemplo de CPF, nome, sexo, telefone, etc. de cerca de 223 milhões de cidadãos; o que facilita o cometimento de crimes digitais; pois tais informações são insumos para possíveis fraudes, entre outros. (SECRETARIA DE SEGURANÇA PÚBLICA DE SERGIPE, 2021)

As atividades no meio digital ganharam proporções incomensuráveis, movimentando uma série de informações numa velocidade espantosa. Essas transformações advindas da expansão mundial das Tecnologias de Informação e Comunicação trouxeram consigo a necessidade de proteger tais informações que circulam nesse meio digital. De acordo com Pinheiro (2020, p. 70), nesse atual mundo digitalizado a informação “[...] passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder."

Nesse panorama, a criação da Lei Geral de Proteção de Dados Pessoais/LGPD advém de um movimento crescente de valorização e proteção de dados das pessoas naturais que se originou da necessidade de garantir os direitos fundamentais, conforme determina o art. 5º, X, da CF de 1988, ou seja, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas; que são também considerados direitos humanos, conforme preceitua o art. 12 da Declaração Universal dos Direitos Humanos, a saber,

> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (DECLARAÇÃO..., 1948).

A LGPD prevê de forma rigorosa sanções administrativas diversas, compreendendo advertência, com indicação de prazo para adoção de medidas corretivas; aplicação de multas; publicização da infração; bloqueio dos dados pessoais a que se refere à infração até sua regularização, entre outras. A citada lei prevê que todas as sanções serão antecedidas de procedimento administrativo que disponibilize a ampla defesa, que poderá ser de forma gradativa, isolada ou cumulativa, conforme o caso concreto em análise. (PINHEIRO, 2020).

Interessante ressalvar que as multas contidas na LGPD podem variar de 2% (dois porcento) do faturamento bruto do último exercício da pessoa jurídica de direito privado, grupo ou conglomerado, podendo chegar ao limite de 50 milhões, por infração (SLEIMAN et al., 2021). O que de certa forma evidencia a importância da LGPD para o fomento mais que necessário de uma gestão mais responsável dos dados pessoais dos cidadãos envolvidos.

De qualquer forma, com a entrada em vigência da LGPD mais um mecanismo

de proteção dos dados dos cidadãos é criado, diante de um conjunto de legislações internacionais que já vinha trilhando esse caminho, a exemplo do *General Data Protection Regulation-GDPR*[15]; regulamento europeu aprovado em 2016, que serviu de base para a nossa legislação.

Pinheiro (2020) explica também que a LGPD surge com o intuito de resguardar os direitos fundamentais a exemplo da privacidade, intimidade, honra, direito à imagem, bem como a dignidade, tendo alcance extraterritorial, similarmente ao Marco Civil da Internet. No ano seguinte ao da sua publicação, a medida provisória nº 869 de 27, de dezembro de 2018, foi convertida na lei nº 13.853/2019 que trouxe alteração em diversos dispositivos da LGPD, bem como no seu art. 55-A que determinou a criação, sem aumento de despesa, da Autoridade Nacional de Proteção de Dados (ANPD); sendo um órgão da Administração Pública que faz parte da Presidência da República (BRASIL, 2018).

Há que se falar também a respeito da Lei nº 13.964/2019, popularmente chamada de "pacote anticrime" que trouxe à baila, com a inserção do art. 10-A na Lei nº 12.850/2013[16], a permissão de agentes da polícia infiltrados no meio virtual, através da internet para fins de investigação dos crimes tipificados na lei. Para essa infiltração são exigidos os requisitos básicos, a saber, a indicação do alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas (Brasil, 2019).

Diversas alterações foram trazidas pela citada lei em vários dispositivos legais de outras leis vigentes no país, a exemplo do Código Penal, Código de Processo Penal, Lei de Execução Penal, Lei de Interceptação das Comunicações Telefônicas, entre outras.

Paralelamente a esse contexto, a Lei nº 14.132, de 31 de março de 2021, inova ao trazer para o corpo do Código Penal o art. 147-A que trata do delito de "perseguição", tendo no caput do seu texto legal "perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade (BRASIL, 1940).

Britto e Fontainha (2021) salientam que tal perseguição ou *stalking* como é chamado em inglês, pode ser devidamente tipificada, caso sua execução seja feita por meio digital, pois o texto legislativo teve essa preocupação de abranger os dois

15 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) .

16 Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências.

meios, a saber, o físico e o virtual; inclusive podendo o infrator mesclar os dois na sua conduta. Outra modificação oriunda da lei em comento foi a revogação do art. 65 da Lei de Contravenções Penais, no qual estava prevista a contravenção de "perturbação de tranquilidade".

Cabe também destacar que, durante a elaboração da etapa final desta pesquisa, a recentíssima Lei nº 14.155, de 27 de maio de 2021, foi aprovada e devidamente sancionada pela Presidência da República. A mencionada lei torna as penas mais graves para os crimes de violação de dispositivo informático (art. 154-A), furto (art. 155) e estelionato (art.171), todos do Código Penal, cometidos pela internet; incluindo além do aumento da penas mínima e máxima, qualificadoras e majorantes.

Acredita-se que essa iniciativa tenha suas origens aos altos índices de crimes digitais ocorridos durante o período de isolamento social imposto pela Pandemia da Covid-19, em que no Brasil houve um aumento expressivo de casos, conforme relata Blum e Almeida (2021). Assim, traz o referido texto legal relativo ao art. 171 do Código Penal, que aqui recebeu destaque,

> Fraude eletrônica
> §2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> Estelionato contra idoso ou vulnerável
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso. (Brasil, 2021).

O advento de legislações que tratam do tema de forma específica, a exemplo de leis relativas à internet, aos delitos cometidos nesse meio, como é o caso do Código Penal; à proteção de dados pessoais, entre outras legislações; contribuíram para o desenvolvimento de mecanismos de proteção das organizações e da sociedade de uma forma geral. Entretanto, acredita-se que seja longo o caminho a percorrer a fim de implementar, de forma integral, estruturas legais protetivas sobre essa tão relevante pauta, principalmente de acordo com a dinâmica das atuais condutas reprováveis penalmente e com as que porventura venham a existir.

Alguns fatores devem ser levados em consideração acerca do incremento da legislação penal, diante da demanda oriunda da sociedade acerca da criminalidade digital. Dessa maneira, alertam Crespo e Sydow (2007) acerca do papel do Direito Penal ao se cogitar, diante de tais demandas, a criação de novos tipos penais;

deve-se de forma premente requerer boa dose de estudo e ponderação a fim de não abarcar condutas que poderiam ser enquadradas por outros meios, a saber, jurídico-administrativos.

A tarefa do Direito Penal acaba por ser árdua, tendo em vista seus princípios norteadores relativos a u*ltima ratio regum,* fragmentariedade, intervenção mínima, entre outros. Além desses aspectos, há a percepção da dificuldade encontrada para a correta tipificação das ações delitivas digitais, bem como a identificação mais acertada dos bens jurídicos expostos aos riscos. Assim, para iluminar essa questão delicada do Direito e especificamente do Direito Penal, Roxin (2018, p. 40) atesta,

> Querendo o Direito penal proteger bens jurídicos contra os ataques humanos, isto só será possível na medida em que o Direito penal proíba a criação de riscos não permitidos e, ademais, valore a infração na forma de uma lesão ao bem jurídico, como injusto penal. Portanto, ações típicas são sempre lesões de bens jurídicos na forma de realização de riscos não permitidos, criados pelos homens.

Dessa forma, segundo Crespo e Sydow (2007) a atividade de legislar com a função de se adequar tipos penais à nova fase dinâmica das Tecnologias de Informação e Comunicação exige que o Direito e próprio Direito Penal; regidos por princípios basilares a exemplo da Legalidade, permaneçam alertas para as dificuldades futuras. Tendo em vista que a legislação penal não pode trabalhar com tipos penais com definição muito aberta; podendo, inclusive, ocasionar a não tipificação de algumas condutas delituosas, tendo em vista opção por uma tipificação do tipo mais fechada, numa realidade de grande mutabilidade das condutas no meio tecnológico e digital.

Ainda nesse viés, Jesus e Milagre (2016) apontam para para o cuidado de não se legislar sobre as técnicas utilizadas e vulnerabilidades, sob pena de criar uma legislação demasiadamente específica com grande probabilidade de obsolescência. Sendo mais correto se debruçar sobre a o comportamento criminoso que decorre de uma ou várias das técnicas, existentes ou que possam ser criadas, combinadas. Esse comportamento identificado, caso seja relevante para o Direito Penal possivelmente passa a ser configurado como crime.

Essa seara de legislar sobre criminalidade digital envolve questões cruciais acerca da territorialidade, jurisdição, lugar do crime e a obtenção de provas que devem sempre estar em pauta. Partindo de uma ideia fundamental de cooperação entre os países, as polícias a fim de combater os criminosos digitais e tornar a persecução criminal mais ágil em relação aos diversos meios de ocultação de provas. De acordo com Domingos e Röder (2018) questões cruciais, a exemplo da obtenção de provas, tornam-se muito discutíveis em relação às jurisdições diversas, em que as informações estão armazenadas, ocasionado inevitavelmente a

interferência na soberania dos países.

Importante destacar a posição de Shimabukuro (2017, p. 19) que reforça a preocupação de "Especializar os legisladores e dar expertise à magistratura são medidas essenciais para combater esta nova onda de crimes tecnológicos, que infelizmente não parece diminuir a cada ano."

Ao concluirmos essa etapa de explanação, impossível não reporta-se à teoria indelével de Miguel Reale acerca da estrutura tridimensional do Direito. Os três elementos básicos que compõem tal sustentação, a saber, a norma que nada mais é que o Direito como Ciência Jurídica e ordenamento jurídico; o elemento fático que remete à dimensão de efetividade histórica e social do Direito e o elemento com o fulcro axiológico, o Direito visto como valor de Justiça (REALE, 2002).

A concepção de tridimensionalidade do Direito segundo (REALE, 2002), envolve a apreensão de que a ocorrência de um fenômeno jurídico está atrelada a um determinado acontecimento, a exemplo de um fato econômico, geográfico, de ordem técnica, entre outros. Somando-se a esse aspecto, aquilo que os indivíduos de uma sociedade atribuem de significado para o referido fato, e que, a partir daí, converge para a consecução e preservação de certa finalidade e objetivo. Por fim, a norma que corresponde à relação de medida entre os dois elementos de forma a integrar um ao outro.

Portanto, diante de tudo que por ora foi exposto, ainda restam muitos outros aspectos a serem discutidos e adequados a essa nova realidade, em que a ocorrência dos "fatos", mundo digital e criminalidade digital, remete a repensar sobre o que já foi feito até o presente momento, e o que se pode fazer de mais apropriado para o enfrentamento desse tipo de criminalidade; cuja característica *sui generis* é transnacionalidade.

Assim sendo, o Brasil recentemente vislumbrou a possibilidade de se tornar signatário da Convenção do Conselho da Europa contra a Criminalidade Cibernética, mais popularmente conhecida como "Convenção de Budapeste". A Presidência da República encaminhou ao Congresso Nacional para análise a mensagem nº 412, de 22/07/2020, publicada no Diário Oficial da União em 24/07/2020, contendo o texto da aludida convenção sobre crime cibernético com a finalidade de uma possível adesão brasileira ao instrumento. Esse acordo permitirá maior cooperação jurídica internacional a fim de combater os crimes na rede mundial de computadores, facilitando principalmente a obtenção de provas durante a persecução penal (PRESIDÊNCIA DA REPÚBLICA, 2020).

O processo de adesão à mencionada Convenção já se iniciou e o Brasil já tem permissão para participar das reuniões dos membros, no caráter de país observador, até a conclusão de todos os trâmites. O grupo de trabalho formado para

fins de acompanhamento abrange, os Ministérios da Justiça e Segurança Pública e das Relações Exteriores, Polícia Federal-PF, o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional-DRCI, que é vinculado ao Ministério da Justiça, como também o Gabinete de Segurança Institucional-GSI e o Ministério Público Federal-MPF (RICHTER, 2019).

De acordo com Senna e Ferrari (2020) caso o país se torne signatário, acredita-se que o arcabouço jurídico brasileiro tornar-se-á mais robusto e que se fomente a elaboração de um aparato legislativo mais condizente com a realidade tecnológica atual. Realidade que é repleta da transformação digital e que, por sua vez, implica um *deficit* protetivo, preventivo e repressivo que impulsiona ainda mais a exigência pela ratificação da referida Convenção.

4 ESTATÍSTICA E ANÁLISE DOS CRIMES DIGITAIS EM SERGIPE: PANDEMIA DA COVID-19

A pandemia da covid-19 instaurou-se no mundo oficialmente no começo de 2020; tendo seu início na cidade de Wuhan província de Hubei na República Popular da China. A Organização Mundial de Saúde-OMS recebeu a informação de uma nova cepa (tipo) de coronavírus que estava causando uma série de casos de pneumonia naquela região e que ainda não havia sido detectada em humanos. Sendo assim, em 30 de janeiro de 2020, foi determinado pela OMS o surto da covid-19 constituindo uma Emergência de Saúde Pública de Importância Internacional, cuja sigla é ESPII. (HISTÓRICO...).

A referida Emergência, ou seja, a ESPII exige, segundo previsto no Regulamento Sanitário Internacional-RSI[17], que todos os países mantenham cooperação coordenada e rápida a fim de impedir a disseminação internacional de doenças (HISTÓRICO...). Como consequência, após os devidos estudos e emissão de parecer, veio a informação no cenário mundial, em 11 de março de 2020, por intermédio da declaração feita pelo Diretor-Geral da OMS, Tedros Adhanom, após ouvir o Comitê de Emergências do RSI; de que no mundo havia a ocorrência de uma pandemia de Covid-19. Ressalta-se que a designação "pandemia" é caracterizada pela distribuição da doença em várias localidades do mundo e não diz respeito especificamente à sua gravidade.

Desde então, várias orientações foram lançadas pela OMS acerca de como efetivamente evitar o maior nível de infecção do vírus, através das chamadas medidas profiláticas e do isolamento social, que foram adotadas em muitos países para evitar aglomeração e circulação de pessoas e, como consequência, a não saturação dos sistemas de saúde, tanto público quanto particular (SILVA et al., 2020). O que passou a ser a grande preocupação dos gestores públicos tanto estaduais quanto municipais em todo nosso país.

No Brasil, o impacto da pandemia foi devastador contando atualmente com mais de 540.000 (quinhentos e quarenta mil) vítimas fatais[18], em quase um ano e meio desde seu início, datado de março de 2020. As restrições aplicadas no país como um todo foram uma alternativa para um possível controle da disseminação da doença. Tendo, obviamente, como principal expectativa, caso todos cumprissem de forma rigorosa tais medidas; o retorno, o mais breve possível, da normalidade no cotidiano da população.

---

17 O Regulamento Sanitário Internacional (RSI) é um instrumento jurídico internacional vinculativo para 196 países em todo o mundo, que inclui todos os Estados Membros da Organização Mundial da Saúde (OMS). Seu objetivo é ajudar a comunidade internacional a prevenir e responder a graves riscos de saúde pública que têm o potencial de atravessar fronteiras e ameaçar pessoas em todo o mundo.

18 Dados obtidos pelo site: https://covid.saude.gov.br/. Acesso em: 08 jul. 2021.

Dessa forma, a imposição do isolamento social, materializado pelas medidas restritivas oriundas dos governos federal, estadual e municipal, obrigou uma parcela significativa da população a desempenhar as mais diversas atividades no próprio ambiente doméstico. Tal mudança para o *home office*[19] tornou inevitável e mais que necessária a utilização da internet para a concretização das tarefas profissionais, sociais, educacionais, entre outras. Assim, em pesquisa elaborada pelo Comitê Gestor da Internet no Brasil-CGI.br, a citada mudança é corroborada,

> Com as medidas de restrição à circulação de pessoas adotadas no enfrentamento da COVID-19, as tecnologias digitais tornaram-se uma ferramenta crucial para lidar com o distanciamento social e mitigar os efeitos da pandemia. A Internet, em particular, tem sido indispensável para garantir a comunicação, o acesso à informação, o comércio eletrônico, a prestação de serviços públicos – incluindo aqueles relacionados ao combate ao novo coronavírus –, a telemedicina, o trabalho remoto, o ensino a distância e a fruição cultural. (COMITÊ GESTOR DA INTERNET NO BRASIL-CGI.BR, 2021, p. 17).

Durante esse período de isolamento social, que teve seu início em março de 2020 e vem perdurando até o momento atual, para muitas categorias profissionais e, por que não dizer, para a população em geral, as Tecnologias de Informação e Comunicação foram aliadas fundamentais para a manutenção do cotidiano que foi bruscamente alterado pela pandemia da covid-19.

Nesse panorama, acredita-se que a internet foi responsável pelo atendimento das mais variadas necessidades da população, viabilizando reuniões, aulas, compras, atividades culturais, obtenção de serviços públicos, lazer, entre outras. Toda essa nova realidade está bem representada no escrito integrante do Relatório Anual de Gestão-2020 da Agência Nacional de Telecomunicações,

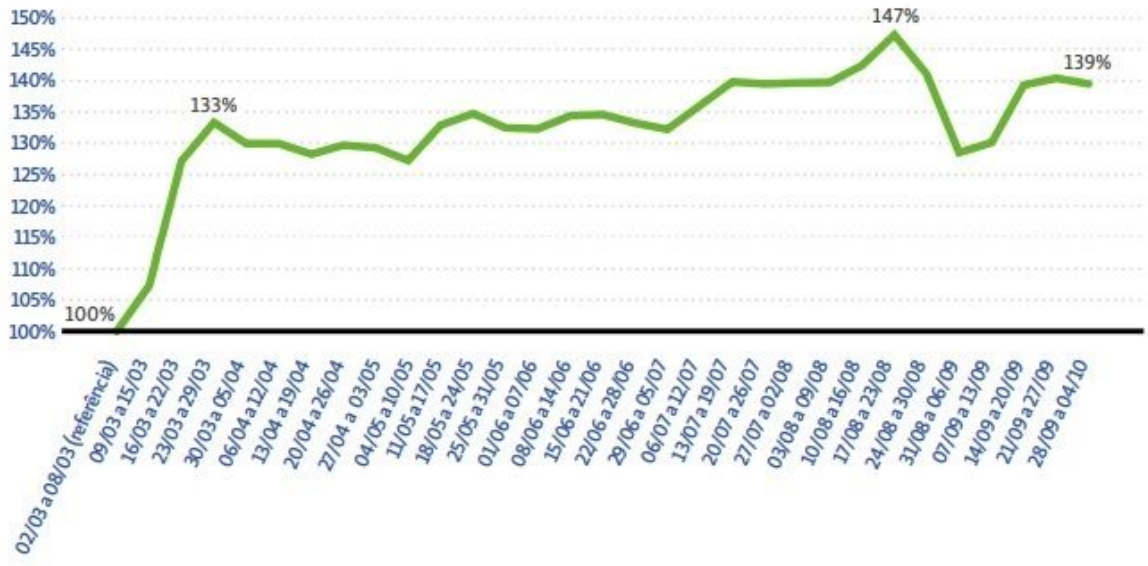
> Observou-se que o aumento do tráfego de dados iniciou nas primeiras semanas da pandemia e esteve muito relacionado à quantidade de pessoas que, distantes de suas rotinas habituais, recorreram as [*sic*] aplicações disponíveis para atendimento de necessidades de trabalho, estudo ou lazer, a exemplo de acessos a vídeos (filmes, desenhos, tutoriais, entre outros), participações em videoconferência (recurso bastante utilizado para teletrabalho), fomento à telemedicina e à educação à distância (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2020, p. 71).

Para tornar mais esclarecedor o aumento do fluxo de dados pela população brasileira no isolamento social decorrente da pandemia, apresenta-se o gráfico a seguir:

---

19 Home office não significa trabalho em casa. Apesar desta ser a tradução literal do termo, no Brasil ele define de forma genérica o trabalho que é realizado em espaço alternativo ao escritório da empresa. Este local pode ser – ou não – o escritório em casa. Uma pessoa pode trabalhar “home office” em cafés, hotéis, aeroportos, táxis, parques…ou em casa. Disponível em: https://revistapegn.globo.com/Noticias/noticia/2014/08/7-coisas-que-todo-mundo-precisa-saber-sobre-home-office.html. Acesso em: 23 maio 2021.

Gráfico 1 — TRÁFEGO TOTAL DE DADOS - NACIONAL E INTERNACIONAL (EM %)



Fonte: Adaptado da Agência Nacional de Telecomunicações (2020, p. 71)

A partir da observação do referido gráfico, a ANATEL destacou que houve um aumento médio superior a 30% (trinta porcento) do tráfego de dados que se iniciou, principalmente, nas primeiras semanas do isolamento social, perdurando aproximadamente até o final do segundo semestre do mesmo ano. Essas informações vêm referendar a ocorrência de aumento do uso das Tecnologias de Informação e Comunicação e em especial da internet, tendo em vista a necessidade de desempenho das atividades laborais, educacionais, sociais como lazer, telemedicina[20], entre outras.

Nota-se que há uma queda no tráfego de dados sentida no final de agosto e início de setembro, isto pode ser atribuído a um processo gradativo de retomada de uma parcela dos serviços, ocorrido em alguns estados brasileiros; com a principal alegação da grave crise econômica causada pela pandemia. Cada Estado, a partir de leituras acerca dos casos, internamentos e índice de mortes por covid-19, teve liberdade para decidir acerca dos critérios aceitos para uma maior ou menor flexibilização (VALENTE; SOUZA; NITAHARA, 2020).

Ao contemplar todo esse panorama, constata-se que em Sergipe não foi diferente, visto que em março de 2020, o governador do Estado, Belivaldo Chagas, por intermédio do Decreto 40.567[21], de 24 de março de 2020; determinou medidas

20 Autorizado pela Lei nº 13.989, de 15 de abril de 2020 que dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2).
21 Disponível em: https://www.pge.se.gov.br/decretos/

de combate à disseminação da Covid-19, a fim aplicar o cumprimento do isolamento social proposto pela OMS e implementado em diversos países assolados pela pandemia.

Essas medidas restritivas foram gradativamente flexibilizadas para alguns setores, incluindo o comércio, bares e restaurantes nos meses de agosto e setembro, em função da estabilização e decréscimo de casos, óbitos e internamentos pela covid-19 no Estado de Sergipe. Essas flexibilizações foram oriundas da edição do Decreto nº 40.652,[22]de 24 de agosto de 2020, que trata da retomada das atividades econômicas e também da homologação e publicação da Resolução nº 06/2020 do COGERE[23], de 27 de agosto de 2020.

O COGERE é o Comitê Gestor de Retomada Econômica que, após a análise das informações fornecidas pela Secretaria Estadual da Saúde-SES e Superintendência Especial de Planejamento, Captação de Recursos-SUPERPLAN, orientou a referida flexibilização nos meses de agosto e de setembro do ano de 2020 (Sergipe, 2020).

Salienta-se que, no decorrer do ano de 2020, uma série de outros decretos foram editados pelo Governo do Estado contendo, a depender do cenário da pandemia, proibições e restrições ou algumas flexibilizações, a exemplo do já citado Decreto nº 40.652, de 24 de agosto de 2020. Além desses, também foram expedidas portarias, resoluções e notas informativas a fim de orientar e esclarecer a população, a classe empresarial e demais segmentos da sociedade.

Após a publicação do Decreto nº 40.652, muitas atividades foram liberadas para funcionamento, a exemplo de academias, atividades de treinamento de desporto profissional, amador e demais atividades físicas e esportivas; com algumas restrições de capacidade e com exigência de atendimento do protocolo sanitário específico, elaborado pela Secretaria de Estado da Saúde-SES. Também os templos religiosos, empresas de *call-centers,* clubes, *shopping centers*, restaurantes, lanchonetes, praias, orla, áreas de lazer coletivo de praias, parques e praças públicas foram liberados sob as mesmas condições de restrição da capacidade e com a exigência dos protocolos sanitários pertinentes (Sergipe, 2020).

Salienta-se que a orientação adotada por muitos países do mundo foi o isolamento social, chegando ao extremo da utilização do chamado *lockdown*. Este termo determina um protocolo de isolamento total que impede completamente o deslocamento das pessoas e de cargas (VALENTE, 2020a). No entanto, aqui em Sergipe não se chegou a esse extremo, sendo aplicadas as restrições, a saber, fechamento de comércio por algum tempo, suspensão de aulas, etc.

A partir dessa sequência de acontecimentos, o que se presenciou foi a

22 Disponível em: https://www.pge.se.gov.br/decretos/
23 Disponível em: https://www.pge.se.gov.br/decretos/

completa modificação da rotina da maioria da população do Brasil e de Sergipe; desempenhando, dessa maneira, suas atividades, especialmente as laborais, em casa, o chamado *home office* ou trabalho remoto. Somando-se a isso as restrições que escalonavam tanto grupos de pessoas, como horários de permanência nas ruas, a exemplo da suspensão das aulas presenciais nas escolas, universidades e faculdades, tanto particulares quanto públicas; bem como o "toque de recolher". Com uma situação como essa, a interação por meio da internet tornou-se o principal caminho para a maioria das pessoas durante esse período de quarentena.

Além desse aspecto, muitos setores do comércio, como foi dito, foram fechados durante um tempo considerável por conta dessas medidas administrativas governamentais e municipais, direcionando uma boa parte da comercialização dos produtos e serviços para o esquema de *delivery* com o uso massivo da internet.

Portanto, é possível entender que o fluxo de mensagens, compras, negócios de uma forma geral, ou seja, a continuidade natural do ritmo da vida da sociedade, passou a ser realizada quase que exclusivamente pela rede mundial de computadores (LAVADO, 2020).

4.1 CRIMES DIGITAIS OCORRIDOS EM 2020

Nesta fase, é preciso esclarecer que, especificamente, o período de ocorrência dos delitos digitais analisados foi o decorrente do início do isolamento social aqui no Estado de Sergipe, conforme determinado pelo Decreto 40.567, de 24 de março de 2020; cobrindo março a dezembro de 2020. Em complementação, os dados relativos a todo o ano de 2019 também foram solicitados à Coordenadoria de Estatística e Análise Criminal-CEACrim a fim de efetuar uma análise comparativa entre esses dois períodos.

Realizou-se, também, uma entrevista com a delegada Lauana Guedes Carvalho, que é a responsável pela Delegacia de Repressão a Crimes Cibernéticos-DRCC de Sergipe, a fim de coletar informações a respeito das atividades cotidianas dos profissionais envolvidos no registro e acompanhamento de casos relativos aos crimes digitais.

Explicita-se, neste momento, que a referida entrevista foi baseada em um roteiro elaborado contendo um total de 13(treze) perguntas, e foi concedida por escrito, via e-mail, por solicitação da própria delegada; tendo em vista os protocolos sanitários aplicados em função da pandemia da covid-19. Em relação ao roteiro de perguntas que foi encaminhado à Diretoria da CEACrim, houve alegação de que a referida coordenadoria não teria respaldo para respondê-las, por estarem

especialmente vinculadas à etapa de investigação dos crimes.

A DRCC é uma delegacia especializada que foi inaugurada em 02 de novembro de 2012, por meio de uma parceria, que posteriormente se concretizou com a publicação do convênio nº 03/2013; entre a Secretaria de Estado da Segurança Pública de Sergipe e Banco do Estado de Sergipe-BANESE.

O referido convênio teve a finalidade de dar um aporte financeiro à constituição e funcionamento da unidade especializada, viabilizando a qualificação das ações de combate aos crimes cibernéticos no Estado de Sergipe. Tal unidade policial, foi inicialmente dirigida pelo então delegado Alessandro Vieira, hoje Senador da República; e veio com a proposta de agir em duas frentes, a saber, no atendimento direto ao cidadão e às instituições prejudicadas por crimes digitais.

Sabe-se que os crimes praticados nos meios digitais são diversos, abrangendo fraudes bancárias, pornografia infantil, crimes contra a honra, etc. Sendo assim, as atividades da DRCC auxiliam as demais unidades policiais do Estado, a exemplo de Grupos Vulneráveis (DAGV), Centro de Operações Policiais Especiais (COPE), tanto no nível estadual quanto federal, cooperando inclusive com outros Estados, a fim de combater os citados delitos digitais(PRIMEIRA..., 2012).

Com a publicação no Diário Oficial do Estado da Portaria nº 01 de 03 de janeiro de 2013, na gestão do Secretário da SSP de Sergipe, João Eloy de Menezes e da Superintendente da Polícia Civil, Katarina Feitoza Lima Santana, foi oficialmente criada a DRCC, que passou a ser incorporada à Coordenadoria de Polícia Civil da Capital-COPCAL, como também foram regulamentadas as suas atribuições. Essas ações voltadas ao atendimento especializado dessas condutas delitivas se deram em decorrência, também, do que foi disposto na Lei nº 12.735, de 30 de novembro de 2012 (Lei Azeredo), que determinou a devida estruturação da polícia judiciária a fim de combater os delitos ligados a rede mundial de computadores, dispositivo de comunicação ou sistema informatizado.

Atualmente a DRCC faz parte do Departamento de Crimes Contra o Patrimônio-DEPATRI, criado no ano de 2017, que é dirigido pela delegada Viviane Pessoa; e é estruturada com três delegadas de polícia que possuem as suas respectivas equipes, atuando nas situações em que o proveito ilícito for igual ou superior a 10 (dez) salários-mínimos, à época do fato (CARVALHO, 2021).

Após o recebimento das informações encaminhadas pela Coordenadoria de Estatística e Análise Criminal da SSP-SE, que é dirigida pelo Escrivão de Polícia, senhor Sidney Santos Teles, iniciaram-se as primeiras análises com o intuito de buscar compreender as ocorrências dos crimes digitais, nos respectivos períodos selecionados. Inicialmente, realizou-se a análise de forma descritiva dos quantitativos obtidos para cada delito, com pontuais observações.

O levantamento fornecido pela CEACrim, conforme Quadro 1 a seguir, destacou os 15 (quinze) delitos principais cometidos de forma mais significativa no ambiente virtual/digital, seguindo a ordem decrescente, e devidamente registrados pela DRCC. O que se constatou foi o aumento considerável dos delitos digitais durante o ano de 2020, em relação ao mesmo período de 2019.

Ao efetuar a soma de todos os delitos cometidos em ambos os anos e compará-las, tem-se um valor total de 1.377 (mil trezentos e setenta e sete) delitos digitais cometidos em 2019 contra 4.954 (quatro mil novecentos e cinquenta e quatro) registros de ocorrências no ano de 2020; correspondendo a mais que o triplo do quantitativo relativo ao ano imediatamente anterior ao isolamento social.

Para facilitar o reconhecimento da amplitude desse aumento, o total de delitos perpetrados em 2019, ou seja, 1.377(mil trezentos de setenta e sete) foi suplantado somente pelo quantitativo dos casos de estelionato no ano de 2020, qual seja, 2.847(dois mil oitocentos e quarenta e sete).

Esse mencionado aumento, em valores percentuais, corresponde a aproximadamente 260% (duzentos e sessenta porcento); o que demonstra o nível alto de ocorrências da criminalidade digital nesse período de 2020, possivelmente em decorrência do isolamento social advindo da pandemia da covid-19 e de todos os seus desdobramentos.

Acerca desse acréscimo de crimes digitais durante o ano de 2020, a delegada Launa Guedes Carvalho explicita,

> Durante a pandemia da Covid-19, que assola a humanidade, observou-se um aumento acentuado no número de crimes dessa espécie, tendo em vista que as pessoas passaram a ficar mais tempo em casa e por conseguinte ficaram conectadas por mais tempo na internet, seja para acesso a e-mails, mensagens, telefone, redes sociais, operações bancárias ou outros recursos. Então, valendo-se da fragilidade e vulnerabilidade das pessoas, os criminosos se aproveitaram e passaram a "investir" em práticas criminosas[...] (CARVALHO, 2021, p. 1, grifo nosso).

A partir da explanações acima, torna-se admissível creditar esse avanço dos crimes digitais, ao menos em boa parte, à permanência das pessoas de um forma mais intensa na internet a fim de realizar uma miríade de atividades afeitas ao seu cotidiano, a exemplo de teletrabalho[24], estudos, comércio, lazer, obtenção de serviços públicos, entre outras.

Logo abaixo, tem-se o quadro 1 fornecido pela CEACrim que traz as listas de crimes digitais cometidos no ano de 2019 em comparação com o ano de 2020.

24 A Reforma Trabalhista (Lei 13.467/2017) introduziu um novo capítulo na CLT dedicado especialmente ao tema: é o Capítulo II-A, "Do Teletrabalho", com os artigos 75-A a 75-E). Os dispositivos definem o teletrabalho como "a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo". Assim, operações externas, como as de vendedor, motorista, ajudante de viagem e outros que não têm um local fixo de trabalho não são consideradas teletrabalho. Fonte: https://www.tst.jus.br/teletrabalho.

Quadro 1 — AS 15 MAIORES OCORRÊNCIAS EM 2020 COMPARATIVO COM 2019

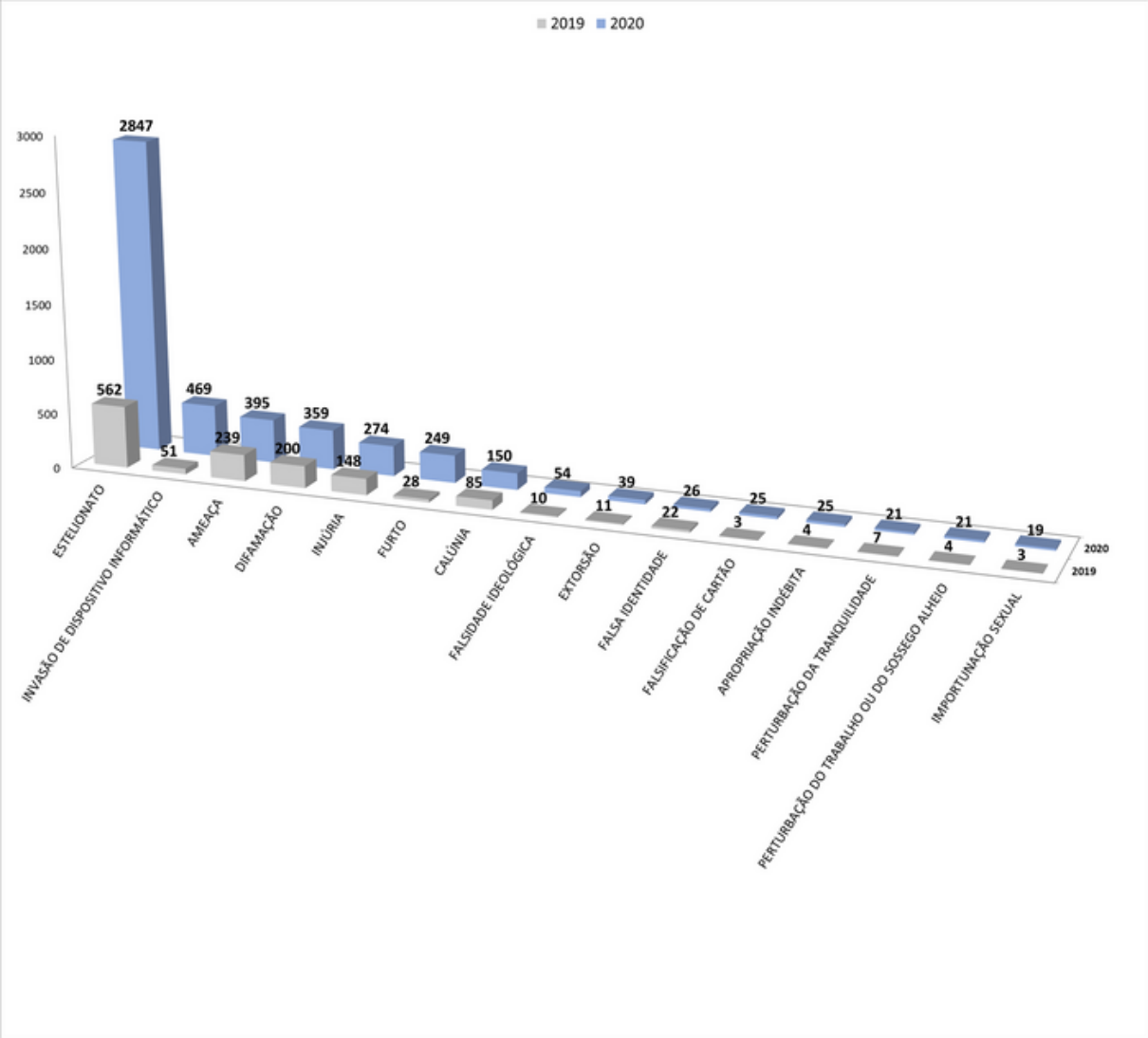
	2019	2020
ESTELIONATO	562	2847
INVASÃO DE DISPOSITIVO INFORMÁTICO	51	469
AMEAÇA	239	395
DIFAMAÇÃO	200	359
INJÚRIA	148	274
FURTO	28	249
CALÚNIA	85	150
FALSIDADE IDEOLÓGICA	10	54
EXTORSÃO	11	39
FALSA IDENTIDADE	22	26
FALSIFICAÇÃO DE CARTÃO	3	25
APROPRIAÇÃO INDÉBITA	4	25
PERTURBAÇÃO DA TRANQUILIDADE (REVOGADO PELA LEI Nº 14.132/2021)	7	21
PERTURBAÇÃO DO TRABALHO OU DO SOSSEGO ALHEIO	4	21
IMPORTUNAÇÃO SEXUAL	3	19

Fonte: Adaptado da CEACrim/SSP/PC/SE-PPE

Dentre os tipos listados, pela referida ordem, tanto em 2019 quanto em 2020, destaca-se encabeçando a lista, o estelionato com um total de 562(quinhentos e sessenta e dois) casos em 2019 versus 2.847(duas mil oitocentas e quarenta e sete) ocorrências no ano de 2020. Em seguida, vem a invasão de dispositivo informático com um registro de 51 casos durante o ano todo de 2019, emplacando em relação a 2020 um aumento representado num quantitativo de 469 registros.

Na representação, conforme Gráfico 2 abaixo, tem-se uma visão facilitada das diversas ocorrências dos delitos e das suas variações e índices de crescimento.

Gráfico 2 — CRIMES DIGITAIS-COMPARATIVO 2019/2020



Fonte: Adaptado da CEACrim/SSP/PC/SE-PPE

Conforme o referido gráfico aponta, o delito de ameaça contabilizou no ano de 2020, 395 ocorrências contra 239 no ano de 2019, o que o coloca na terceira posição do levantamento apresentado. Já os crimes contra honra, a saber, difamação, injúria e calúnia, que aqui analisa-se como grupo, obtiveram registro de ocorrências em patamares de 359, 274 e 150 casos, respectivamente. Esses citados quantitativos fizeram com que esses delitos se mantivessem em 4º, 5º e 7º lugares, respectivamente.

O crime de furto que teve um relevante crescimento em relação ao ano pré-pandemia, apresentou 28 registros em 2019 e marcou 249 ocorrências no primeiro ano pandêmico. Também nesse rol está o crime de falsidade ideológica que ficou em 8º lugar com um quantitativo de 10 casos registrados em 2019 contra os 54 casos existentes no ano de 2020.

O crime de extorsão, que sustentou o 9º lugar, teve um registro em 2019 de 11 casos, tendo atingido em 2020 o número de 39 casos. Logo em seguida vem o delito de falsa identidade, com 22 ocorrências em 2019 comparadas as 26 no ano de 2020, ficando em 10º e apresentando uma variação relativamente baixa em relação aos dados de 2019.

O crime de falsificação de cartão, ocupou 11º lugar do ranking, obtendo um quantitativo de 3 casos registrados no ano de 2019 em comparação com as 25 ocorrências de 2020. Em se tratando do crime de apropriação indébita, 12º colocado, foram contabilizadas 4 ocorrências em 2019 comparativamente ao quantum de 25 casos em 2020.

Há que se destacar que a infração penal prevista no art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941, a conhecida Lei de Contravenções Penais-LCP, que estipulava a indicação do tipo "perturbação de tranquilidade", foi revogado pela Lei nº 14.132, de 31 de março de 2021. No entanto, foram contabilizadas 21 ocorrências no ano de 2020, em relação aos 7 casos registrados durante todo ano de 2019; ficando esta contravenção em 13º lugar.

A contravenção penal de perturbação do trabalho e do sossego, conforme art. 42 da Lei e Contravenções Penais, ficou na 14ª posição, atingindo o registro de 4 ocorrências em 2019, em relação ao patamar de 21 casos em 2020. Seguida finalmente pelo crime de importunação sexual, que quantificou 3 casos registrados em 2019, comparativamente ao número de 19 casos ocorridos no primeiro ano da pandemia.

Na etapa seguinte, adentra-se nas questões mais específicas da análise dos delitos digitais obtidos a fim realizar possíveis conexões entre os objetivos propostos e a hipótese levantada durante a realização da presente pesquisa.

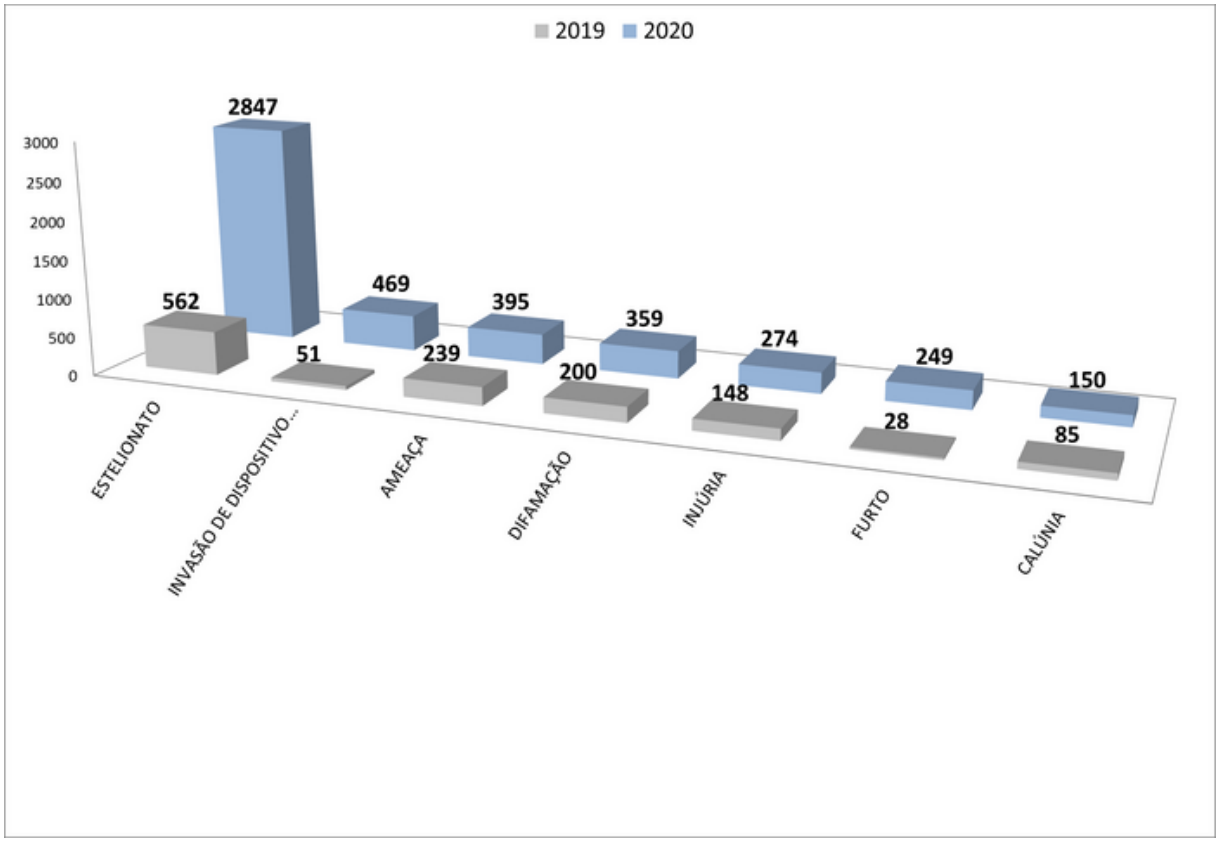
4.2 ANÁLISE DAS INFORMAÇÕES ENCONTRADAS

Após a exposição e alguns comentários pontuados acerca dos quantitativos dos delitos digitais ocorridos no período de 2020, durante o cumprimento das medidas de isolamento social; iniciam-se as reflexões acerca das informações alcançadas. Elucida-se que a citada análise não se efetivou para todos os delitos integrantes das informações fornecidas pela SSP-SE. Essa seleção foi feita de acordo com critérios considerados de relevância para esta pesquisa com a finalidade de sintetizar melhor os possíveis resultados; tendo como crimes escolhidos para apreciação os que atentam contra o patrimônio, inviolabilidade dos dados informáticos, liberdade individual e honra que por sua vez tiveram maior destaque do ponto de vista numérico.

A opção por tais delitos efetivou-se a partir do critério julgado mais acentuado, a saber, o grau de ocorrência atingido, a partir das informações da CEACrim. Portanto, foi feita a seleção dos 7 tipos mais expressivos numericamente dentre os 15 levantados pelo referido órgão da SSP, a fim de efetuar um recorte e otimizar seu exame e, assim, atender melhor os fins desta pesquisa. A citada seleção abrangeu, nessa ordem, o estelionato, a invasão de dispositivo informático, ameaça, difamação, injúria, furto e calúnia.

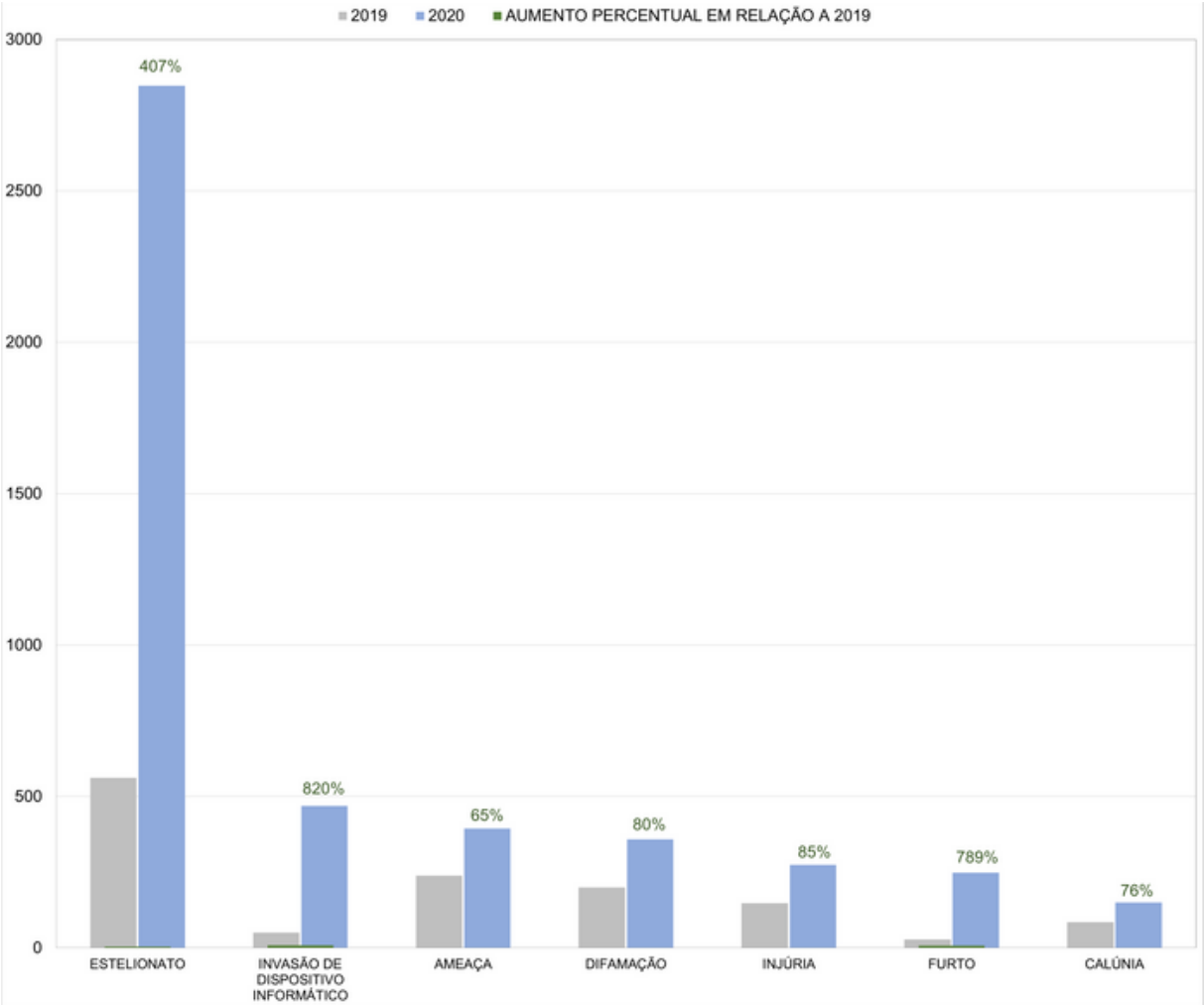
Em primeiro lugar, com o objetivo de facilitar o entendimento, elaborou-se o gráficos 3 , 4 e 5 a fim de compreender quão expressivo foi o aumento dos crimes digitais em 2020, constantes do recorte selecionado, comparativamente ao ano de 2019.

Gráfico 3 — CRIMES DIGITAIS-PRINCIPAIS OCORRÊNCIAS-2019 E 2020



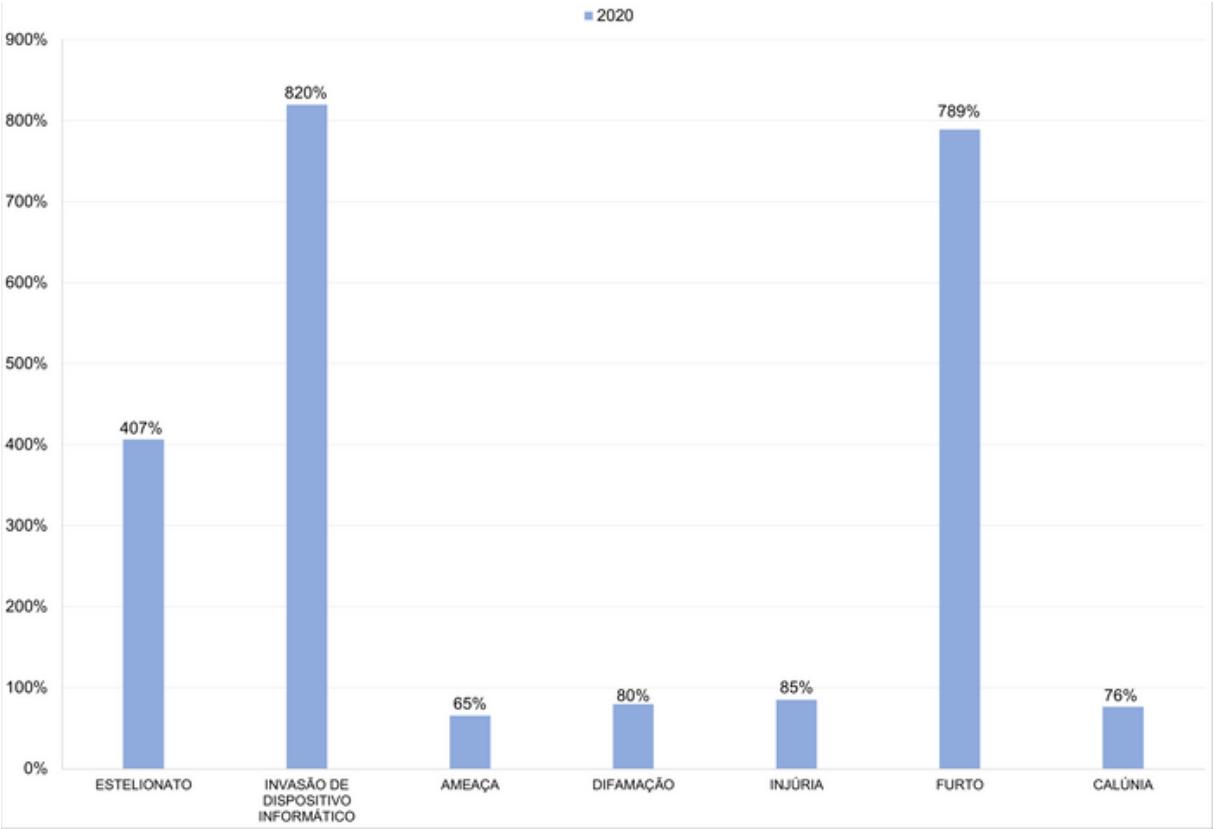
Fonte: Adaptado da CEACrim/SSP/PC/SE-PPE

Gráfico 4 — CRIMES DIGITAIS: AUMENTO PERCENTUAL EM RELAÇÃO A 2019



Fonte: Adaptado da CEACrim/SSP/PC/SE-PPE

Gráfico 5 — ACRÉSCIMO PERCENTUAL POR CRIME DIGITAL EM 2020



Fonte: Adaptado da CEACrim/SSP/PC/SE-PPE

Observando a ocorrência dos chamados crimes contra o patrimônio, a saber, estelionato e furto, é possível depreender a marca significativa atingida principalmente pelo estelionato, em relação aos demais crimes. O tipo estelionato tem sua previsão legal no art. 171, caput, do Código Penal e expressa a forma de obter, para si ou para outrem, algum tipo de vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante uso de artifício, ardil, ou qualquer outro meio fraudulento; tendo como pena a reclusão, de um a cinco anos, e multa. (BRASIL, 1940)

Tendo esse cenário de escalada, não é sem propósito que o estelionato teve suas penas aumentadas pela Lei nº 14.155, de 27 de maio de 2021, com a inclusão no art. 171 do Código Penal dos parágrafos 2º-A e 2º-B, que trazem situações de qualificadoras e majorantes, respectivamente. A qualificadora do § 2º-A, explicita a situação de que a pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, caso a fraude seja cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Já a majorante do § 2º-B trata da pena prevista no § 2º-A , caso seja

considerada a relevância do resultado gravoso, a pena é aumentada de 1/3 (um terço) a 2/3 (dois terços), na situação do crime ser cometido mediante a utilização de servidor mantido fora do território nacional (BRASIL, 1940).

Analisando as modalidades específicas dessa fraude, segundo Carvalho (2021) o estelionato, bem como outros crimes digitais acontecem através de técnicas específicas a exemplo do já mencionado, *phishing* a fim de que a vítima seja levada a informar seus dados pessoais e bancários. Suas modalidades abarcam o sequestro do WhatsApp, em que o criminoso busca em sites de venda e em redes sociais e efetua a reconfiguração do WhatsApp do número verdadeiro disponível nos referidos sites. Infelizmente, a vítima recebe um determinado código de SMS e repassa para o golpista que, rapidamente, envia uma série de mensagens para diversos contatos da vítima, com o fim de obter retorno financeiro.

Ainda na concepção de Carvalho (2021) outra modalidade de estelionato também muito recorrente é o do falso intermediador, comumente conhecido como "golpe da OLX", em que o criminoso elabora um anúncio falso e passa a manter contato com vendedor e comprador, fazendo uso de artifícios faz com que ambos se encontrem com o objetivo de finalizar o acordo de compra e venda, solicitando, inclusive que ambos omitam alguma situação e ao final da transação comercial o dinheiro acaba indo para conta de algum “laranja”. Já o golpe do perfil falso ou simulado, por sua vez, ocorre quando o criminoso cria uma conta a partir de um número, fazendo uso de uma fotografia da vítima, e passando-se por ela, pede dinheiro aos contatos da vítima.

Em entrevista realizada com a delegada responsável pela DRCC de Sergipe, quando questionada acerca do porquê desse tão expressivo número de estelionatos perpetrados na rede mundial de computadores, esclareceu que no caso específico do estelionato, os agentes criminosos normalmente fazem uso de sites falsos, para dessa forma induzir a vítima em erro, a exemplo do acesso a e-mails em que ingenuamente a vítima fornece seus dados, viabilizando para o referido agente criminoso a consecução de lucro indevido. Além desse exemplo, há também os conhecidos sites de leilões falsos que levam a vítima a depositar valor na conta de algum membro do grupo criminoso (CARVALHO, 2021).

O delito de furto previsto no art. 155, caput, do Código Penal é caracterizado pelos mesmos mecanismos usualmente tradicionais com uso dos artifícios oriundos da tecnologia; sendo a conduta do criminoso descrita como a de subtrair, para si ou para outrem, coisa alheia móvel, prevendo uma pena de reclusão, de um a quatro anos, e multa (BRASIL, 1940). O mencionado crime teve, em relação ao ano anterior estudado, um crescimento considerável, de acordo com o gráfico 3; passando de 28 casos para 248. Esse crescimento em termos percentuais chega a marca de 789%

(setecentos e oitenta e nove porcento) de acordo com os gráficos 4 e 5. Um fato muito importante é que esse crime, assim como o estelionato, teve suas penas aumentadas em virtude da publicação da nova da Lei nº 14.155, de 21 de maio de 2021; que inseriu no art. 155 os parágrafos 4º-B e 4º-C trazendo qualificadoras e majorantes, respectivamente.

No § 4-B, do citado artigo, tem-se a qualificadora que discorre sobre a situação de o delito ser cometido por meio de dispositivo eletrônico ou informático, com conexão ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo; prevendo uma pena de reclusão de 4(quatro) a 8(oito) anos ou multa. Também no § 4-C, inciso I e II, é prevista a majorante de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável (BRASIL, 1940).

O crime de invasão de dispositivo informático, que tem a inviolabilidade de informações automatizadas como bem jurídico tutelado, obteve um crescimento relevante no ano de 2020, ficando logo atrás do estelionato. Apresentando um crescimento de 820% (oitocentos e vinte porcento) em comparação ao ano de 2019; conforme leitura dos gráficos, 3, 4 e 5 . Tal delito está tipificado no art. 154-A do Código Penal e seu texto esclarece a conduta típica a invasão de 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; prevendo uma pena de reclusão, de 1 (um) a 4 (quatro) anos, e multa.(BRASIL, 1940).

O art. 154-A do Código Penal teve o texto do seu caput alterado com a Lei nº 14.155/2012 que retirou a expressão "mediante violação indevida de mecanismo de segurança" e trocou também a expressão "do titular do dispositivo" para "usuário do dispositivo"; bem como aumentou a pena prevista no caput, trazendo uma situação de majorante no parágrafo § 2º; e um aumento na pena decorrente de uma qualificadora prevista no § 3º. (BRASIL, 1940).

Cabe neste momento salientar que a Lei 14.155/2021 advém de uma necessidade presente, enfrentada pela sociedade que constantemente é subjugada por ataques oriundos de criminosos que agem no mundo virtual/digital. Seu escopo foi abarcar alguns dos principais delitos cometidos em 2020, a saber, invasão de dispositivo Informático, furto e estelionato ocorridos com maior intensidade nesses tempos de pandemia da covid-19.

O crime de ameaça, que ofende a liberdade individual, está inserido no

Código Penal n art. 147, caput, que informa a conduta típica, qual seja, "Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940). Tal delito ficou logo atrás da invasão de dispositivo informático, registrando 395 casos no ano de 2020, em comparação aos 239 registros no ano de 2019. Contudo, sua atuação do ponto de vista percentual não foi tão significativa, sendo a menor em relação aos demais delitos digitais analisados; atingindo 65% (sessenta e cinco porcento) de crescimento, conforme gráficos, 3, 4 e 5.

Além desses, os crimes contra honra, a saber, difamação, injúria e calúnia tiveram destaque e são muito conhecidos e disseminados, principalmente depois da maior interação entre as pessoas por intermédio da diversas modalidades de redes sociais, estando previstos no art. 138, art. 139 e art.140 do Código Penal. Analisando os gráficos 3, 4 e 5 é possível perceber que esses três delitos tiveram crescimento razoável em 2020, comparativamente a 2019. A difamação atingiu numericamente no primeiro ano da pandemia 359 casos em relação aos 200 registros em 2019; ficando com a representação percentual de crescimento de 80% (oitenta porcento).

A injúria teve em 2020 um registro de 274 casos em relação aos 148 ocorridos em 2019. Apresentando, assim, um crescimento percentual de 85% (oitenta e cinco porcento). Já a calúnia obteve um registro de 150 casos em 2020, em comparação aos 85 no ano de 2019. Perfazendo um valor 76%(setenta e seis porcento) de crescimento. Nota-se que os percentuais de crescimento relativo aos três tipos penais foram parecidos, apresentando pouca variação.

Inclusive, cabe aqui reiterar que as penas aplicadas para os delitos contra honra que sejam cometidos na rede mundial de computadores foram triplicadas conforme Lei nº 13.964/2019(pacote anticrime) que inicialmente foi vetado pelo Presidente da República, porém tal veto foi derrubado pelo Congresso Nacional (INSTITUTO BRASILEIRO DE DIREITO DE FAMÍLIA-IBDFAM, 2021).

Importante destacar que com a observação dos três gráficos desta seção e, principalmente, os gráficos 4 e 5, tomando por base o enfoque de valores com a utilização de porcentagem, o crime que teve maior crescimento em 2020 em relação a 2019, foi a invasão de dispositivo informático com 820% (oitocentos e vinte porcento), seguido do furto com 789% (setecentos e oitenta e nove porcento) e em terceiro lugar o estelionato, que numericamente teve maior relevância, porém percentualmente atingiu 407% (quatrocentos e sete porcento) de aumento.

Assim, a partir do analisado, percebe-se que o suposto anonimato, por intermédio dos recursos disponíveis na internet para camuflar identidade, bem como do contato com um número indescritível de pessoas a fim de obter a vantagem

ilícita; contribuem para a prática dos crimes cujo bem jurídico tutelado é o patrimônio, bem como para os de invasão de dispositivo informático. Os criminosos, por sua vez, aproveitam-se desse novo caminho digital, a partir de certas fragilidades dos cidadãos, a saber, "[...] erros de desenvolvimento e concepção de produtos e aplicações, o uso de técnicas avançadas de engenharia social pelos criminosos aliado à inabilidade de alguns usuários (TUPINAMBÁ, 2021, p. 15).

Tais crimes executados no meio digital utilizam, como foi dito, artifícios, ardis, a exemplo das técnicas de *phishing, malware, keylogger*s, engenharia social, falsos e-mails que foram amplamente facilitadas com o desenvolvimento das Tecnologias de Informação e Comunicação-TIC e, fundamentalmente, com a advento da rede mundial de computadores e seu avanço no dia a dia das pessoas ao redor do mundo.

Esse fato reforça a ideia de que, com o avanço das referidas tecnologias, necessariamente, boa parcela da população no mundo, no Brasil e em Sergipe, tendem a utilizar mais intensamente a internet para execução das múltiplas tarefas diárias. Sendo assim, as ocorrências de criminalidade digital são disseminadas na rede mundial de computadores, tendo em vista o maior alcance das vítimas, a lucratividade, a falsa sensação de anonimato e de impunidade, entre outros aspectos. Há cada vez mais o que Lotufo (2021b, p. 5) chama de "uma consequência da digitalização das relações" , ou seja, na atualidade não tem como fugir deste caminho de avanço das modernas tecnologias.

5 **CONCLUSÕES**

O que a humanidade tem vivido nos tempos atuais é o movimento progressivo de "cotidianizar" as tecnologias, a exemplo da conhecida internet, que é responsável pela efetivação de um sem número de atividades das mais variadas espécies. Em vista dos dois últimos anos em que a humanidade se viu atingida pela pandemia da covid-19 e, consequentemente, submetida ao isolamento social, em que suas rotinas habituais de trabalho, estudo, de consumo de bens e de serviços variados, inclusive serviços públicos, de produção acadêmica e comercial, todas passaram a ser desenvolvidas, quase que integralmente, no meio digital.

Esse processo tecnológico no cotidiano dos sujeitos trouxe aspectos muito importantes a serem considerados, a exemplo dos meios de proteção legais existentes que possam viabilizar um certo nível de segurança, como também combater às ações dos agentes criminosos no meio virtual. Diante de todo esse contexto tecnológico constante e intenso da "circulação monetária digital", é que se percebe a importância da adoção de tais medidas, sejam elas educativas, legais que envolvam o Direito nessa esfera digital, bem como outras áreas do saber.

Dessa forma, analisou-se na presente pesquisa, dentro desse contexto da pandemia da covid-19, no Estado de Sergipe, a ocorrência ou não de crescimento dos crimes digitais durante o período de isolamento social imposto à população, no ano de 2020

O período de coleta de dados abrangeu março a dezembro do ano de 2020; bem como o ano de 2019 para que se pudesse estabelecer a devida relação comparativa. Foram identificados, a partir da análise dos dados obtidos da CEACrim, órgão vinculado à Secretaria de Estado da Segurança Pública de Sergipe, 15 tipos de crimes digitais ocorridos durante a Pandemia da covid-19. Destacando-se que os delitos digitais estelionato, ameaça, invasão de dispositivo informático, furto e os crimes contra honra foram os mais comuns e que tiveram maior expressividade numérica durante o período estudado; bem como apresentaram um aumento relevante em relação ao ano de 2019. De maneira geral, houve um aumento dos crimes digitais em torno de 260% (duzentos e sessenta porcento) no ano de 2020 durante o período de isolamento social, em relação ao ano anterior. E acrescenta-se que, individualmente, todos os tipos de crimes tiveram crescimento significativo, conforme capítulo 4 desta pesquisa.

Apreendeu-se que o crime digital de estelionato foi o mais relevante em aumento de ocorrências, enquadrando-se no conceito de crime digital impróprio ou misto visto que é uma categoria de tipo penal que já existia tradicionalmente no

nosso ordenamento jurídico. Sendo que a forma de sua execução, ou seja, seu *modus operandi,* que foi modificado devido ao avanço das Tecnologias de Informação e Comunicação-TIC. Isso decorre das facilidades encontradas pelos criminosos para perpetrar os mais diversos delitos, pois encontram, com certa frequência, um terreno fecundo de fragilidades diversas.

A constatação decorrente do presente estudo acerca dos conceitos de crimes digitais ou delitos digitais é que há controvérsias a respeito das nomenclaturas e classificação a serem utilizadas. São vários as terminologias para a mesma situação, ou seja, a denominação dos delitos praticados com uso ou não da internet e/ou que visem aos dados informáticos e sistemas informatizados. A concepção utilizada inclusive na pesquisa como todo foi o termo "delitos digitais" ou "crimes digitais" visto terem, a nosso ver, mais identidade com esses delitos em questão.

A terminologia que apregoa os delitos digitais, encampada por Crespo (2015), (LOTUFO, 2021b), (PINHEIRO, 2016) abarca a concepção dos delitos digitais chamados puros ou próprios e os impuros ou mistos. Os primeiros se referem aos delitos praticados contra os bens jurídicos advindos da própria digitalização das relações, os novos bens jurídicos tutelados, a exemplo da inviolabilidade dos dados informáticos. Os segundos são decorrentes de violação aos bens jurídicos tradicionalmente protegidos. Com essa terminologia e classificação, torna-se possível enquadrar vários tipos penais que se encontram determinados no Próprio Código Penal e em algumas legislações esparsas que foram estudadas nesta pesquisa.

Ao analisar as legislações atualmente vigentes no nosso país, tornou-se claro que ainda há uma lacuna que poderá ser ou não suprida, a depender da forma como nossos legisladores e especialistas da área penal e demais áreas pertinentes atuarem. No caso da atuação ser de forma unívoca contribuirá para o melhor entendimento do referido assunto dentro de um contexto maior e mais complexo.

Um acréscimo positivo ocorrido durante a elaboração desta pesquisa foi a Lei nº 14.132, de 31 de março de 2021, que adicionou o art. 147-A ao nosso Código Penal, trazendo o tipo penal "perseguição"; e a Lei nº 14.155/2021, de 27 de maio de 2021, que tornou as penas dos delitos de invasão de dispositivo informático estelionato, furto mais gravosas. Essas alterações surgem num momento oportuno em que as pessoas passaram a utilizar a internet de forma quase que integral nas suas vidas, tendo em vista o isolamento social oriundo da pandemia da covid-19.

Nesta pesquisa buscou-se uma metodologia que favorecesse o estudo de forma que os 7(sete) delitos selecionados para análise foram categorizados conforme o bem jurídico tutelado correspondente e seu maior grau de incidência

numérica; bem como seu aumento do ponto de vista percentual, no ano de 2020. Esse processo metodológico facilitou a compreensão dos resultados alcançados durante a pesquisa, apontando os crimes digitais mais relevantes e, a partir daí, as possíveis ligações com as teorias abordadas.

O fato é que há uma dinâmica veloz dos meios tecnológicos de informação e de comunicação, a exemplo da internet, que atende atualmente no Brasil um quantitativo de 134 milhões de brasileiros[25] e projeta-se uma demanda ainda maior tendo em vista que o país conta hoje com um contingente populacional total em torno de 213 milhões[26]. Todos esses fatos exigirão muito dos profissionais de todas as áreas e, sob o enfoque aqui presente, fundamentalmente dos profissionais do Direito a fim de adequarem a atuação desta matéria aos contornos dos bens jurídicos tradicionais e dos novos a serem tutelados.

Todo esse caminho é permeado de dificuldades diversas, pois a mutabilidade constante da aplicação tecnológica pode se configurar grande empecilho para as possíveis tipificações no âmbito do Direito Penal. Há que se alertar para a devida cautela na busca desenfreada pela tipificação penal a qualquer preço, visto que o Direito Penal enfrenta um período intenso de inflação o que exige muito estudo e reflexão a serem exercidos pelos legisladores e doutrinadores.

Relevante para a discussão de todas essas questões são elementos como a territorialidade e a soberania, visto que os crimes digitais têm característica *sui generis,* que é a transnacionalidade; o que acaba por exigir de todos os países um incremento à cooperação entre as polícias a fim de equiparar a agilidade do combate e da investigação criminal aos níveis utilizados pelos agentes criminosos.

Essa pesquisa buscou a compreensão do que sejam crimes digitais ou delitos digitais e se deparou com questões que, consideravelmente, ainda estão em construção, a exemplo da própria discussão acerca do que sejam os crimes digitais e a maneira de tipificá-los no nosso ordenamento jurídico; tendo em vista uma dinâmica intensa de ações criminosas cada vez mais inovadoras e que, inclusive, abarcam bens jurídicos novos.

Por isso, a partir de tais constatações o que se propõe de forma relevante é uma possível continuidade dos estudos a fim de consolidar e aprimorar o conhecimento de tema tão relevante nos nossos dias.

---

25 Três em cada quatro brasileiros acessam a internet, o que equivale a 134 milhões de pessoas. Embora a quantidade de usuários e os serviços online utilizados tenham aumentado, ainda persistem diferenças de renda, gênero, raça e regiões.
26 Disponível em: https://www.ibge.gov.br/apps/populacao/projecao/index.html.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE LETRAS. **Dicionário Escolar da Língua Portuguesa**. 2 ed. São Paulo: Companhia Editora Nacional, 2008. 1312 p.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Estratégia e Desempenho*. In:* AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Relatório Anual de Gestão 2020**. Brasília/DF, 2020. cap. 2, p. 50-74. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?eEP-wqk1skrd8hSlk5Z3rN4EVg9uLJqrLYJw_9INcO7WGrElvTz1_rj8nrMF-QM9oN9YJznGAw7n0RtP46wrHKG9JxftAZtduI1twGiTCE97imTxROoxD5Z4y36esrlt. Acesso em: 25 mai. 2021.

ALEXANDRIA, João Carlos Soares de. **Gestão da segurança da informação**: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. São Paulo, 2009 Tese (Doutorado em Ciências na área de Tecnologia Nuclear) - Instituto de Pesquisas Energéticas e Nucleares Associado À Universidade de São Paulo, São Paulo, 2009. Disponível em: https://teses.usp.br/teses/disponiveis/85/85131/tde-22092011-095831/pt-br.php. Acesso em: 6 mai. 2021.

ALVES, Matheus de Araújo. **Crimes Digitais**: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. Editora Dialética, 2020. 148 p.

ARAÚJO, Fábio Lucena. Aspectos jurídicos no combate e prevenção do ransomware*. In:* MINISTÉRIO PÚBLICO FEDERAL. **Crimes cibernéticos** . Brasília: MPF, v. 3, 2018. cap. 5, p. 92-115. (Coletânea de Artigos). Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 17 mai. 2021.

BARRETO, Alesandro Gonçalves. **Análise da lei azeredo**: necessidade de criação de delegacias e setores especializados na repreensão aos crimes informáticos. www.migalhas.com.br. 2018. Disponível em: https://www.migalhas.com.br/depeso/278027/analise-da-lei-azeredo--necessidade-de-criacao-de-delegacias-e-setores-especializados-na-repreensao-aos-crimes-informaticos. Acesso em: 5 mai. 2021.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética**: à luz do Marco Civil da Internet. Rio de Janeiro: Brasport, 2016. 222 p.

BLUM, Renato Opice ; ALMEIDA, Ana Rita Bibá Gomes de. **Sancionada a lei 14.155/21, que altera o Código Penal Brasileiro, materializando a resposta do Direito à elevação do número de crimes praticados com o uso de dispositivos eletrônicos**. www.migalhas.com.br. 2021. Disponível em: https://www.migalhas.com.br/depeso/346485/lei-14-155-21-que-altera-o-codigo-penal-brasileiro. Acesso em: 27 jun. 2021.

BRASIL. Conselho Nacional de Justiça. Portaria n° 242, de 10 de novembro de 2020. Institui o Comitê de Segurança Cibernética do Poder Judiciário. DJe/CNJ:

DJe/CNJ nº 358/2020, p. 9-11, 11 nov. 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3566. Acesso em: 30 jun. 2021.

BRASIL. **Constituição**. República Federativa do Brasil de 1988. Brasília, DF. Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 10 jan. 2021.

BRASIL. Presidência da República. Decreto-Lei n. 2.848, de 06 de dezembro de 1940. Código Penal. **Diário Oficial da União**. Rio de Janeiro, 31 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 24 mai. 2021.

BRASIL. Presidência da República. Decreto-Lei n. 3.688, de 03 de outubro de 1941. Lei das Contravenções Penais. **Diário Oficial da União**. Rio de Janeiro, 03 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3688.htm. Acesso em: 19 mai. 2021.

BRASIL. Presidência da República. Decreto-Lei n. 3.689, de 02 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**. Rio de Janeiro, 24 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 4 mai. 2021.

BRASIL. Presidência da República. Lei n. 11.829, de 24 de novembro de 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet . **Diário Oficial da União**. Brasília, 25 de novembro de 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm. Acesso em: 25 mai. 2021.

BRASIL. Presidência da República. Lei n. 12.735, de 29 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 -Código Penal, [...], e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.. **Diário Oficial da União**. Brasília, 02 de dezembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 10 jan. 2021.

BRASIL. Presidência da República. Lei n. 12.737, de 29 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. **Diário Oficial da União**. Brasília, 02 de dezembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 5 jan. 2021.

BRASIL. Presidência da República. Lei n. 12.965, de 22 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, DF, 24 de abril de 2014. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 jan. 2021.

BRASIL. Presidência da República. Lei n. 13.441, de 08 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. **Diário Oficial da União**. Brasília, 09 de maio de 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm. Acesso em: 14 abr. 2021.

BRASIL. Presidência da República. Lei n. 13.709, de 13 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**. Brasília, DF, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 jan. 2021.

BRASIL. Presidência da República. Lei n. 13.718, de 23 de setembro de 2018. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, [...], estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais).. **Diário Oficial da União**. Brasília, 25 de setembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 6 mai. 2021.

BRASIL. Presidência da República. Lei n. 13.869, de 05 de setembro de 2019. Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).. **Diário Oficial da União**. Brasília, 18 de setembro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13869.htm#art41. Acesso em: 27 abr. 2021.

BRASIL. Presidência da República. Lei n. 13.964, de 23 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. **Diário Oficial da União**. Brasília/DF, 24 de dezembro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 26 mai. 2021.

BRASIL. Presidência da República. Lei n. 13.989, de 15 de abril de 2020. **Diário Oficial da União**. Brasília/DF, 16 de abril de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L13989.htm#view. Acesso em: 6 mai. 2021.

BRASIL. Presidência da República. Lei n. 14.132, de 30 de março de 2021. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). **Diário**

Oficial da União. Brasília/DF, 01 de abril de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm. Acesso em: 22 abr. 2021.

BRASIL. Presidência da República. Lei n. 14.155, de 23 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. **Diário Oficial da União**. Brasília, 28 de maio de 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 31 mai. 2021.

BRASIL. Presidência da República. Lei n. 7.716, de 04 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor. **Diário Oficial da União**. Brasília, 08 de janeiro de 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 3 mai. 2021.

BRASIL. Presidência da República. Lei n. 8.069, de 12 de julho de 1990. **Diário Oficial da União**. Brasília, 27 de agosto de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 7 jan. 2021.

BRASIL. Presidência da República. lei n. 9.296, de 23 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**. Brasília, 25 de julho de 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 4 mai. 2021.

BRASIL. Presidência da República. Lei n. 9.609, de 18 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.. **Diário Oficial da União**. Brasília, DF, 24 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 7 jan. 2021.

BRASIL. Presidência da República. lei n. 9.983, de 13 de julho de 2000. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. **Diário Oficial da União**. Brasília, 17 de julho de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9983.htm. Acesso em: 25 mai. 2021.

BRITTO, Cláudia Aguiar Silva ; FONTAINHA, Gabriela Araújo . **O novo crime de perseguição** : Stalking. www.migalhas.com.br. 2021. Disponível em: https://www.migalhas.com.br/depeso/343381/o-novo-crime-de-perseguicao--stalking. Acesso em: 26 mai. 2021.

BRUGIONI, Franco Mauro Russo . **O direito autoral e a proteção ao programa de computador**. www.migalhas.com.br. 2006. Disponível em: https://www.migalhas.com.br/depeso/20101/o-direito-autoral-e-a-protecao-ao-programa-de-computador. Acesso em: 8 jun. 2021.

CARVALHO, Ana Cristina Azevedo P. **Marco civil da internet no Brasil**: análise da lei 12.965/14 e do direito de informação. Rio de Janeiro: Alta Books, 2014. 272 p.

CARVALHO, Lauana Guedes. **Entrevista [jun. 2021]. Entrevistadora: Rosangela**

dos Santos. São Cristóvão: Universidade Federal de Sergipe, 2021. (Roteiro de Entrevista (13 perguntas). Entrevista concedida para pesquisa sobre Criminalidade Digital em Tempos de Pandemia: Principais Ocorrências em Sergipe no Ano de 2020).

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **Cartilha de segurança para Internet**: versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, f. 48, 2012. 142 p. Disponível em: https://cartilha.cert.br/. Acesso em: 9 mar. 2021.

COMITÊ GESTOR DA INTERNET NO BRASIL-CGI.BR. **Pesquisa web sobre o uso da internet no Brasil durante a pandemia do novo coronavírus**: painel tic covid-19 [livro eletrônico]. Tradução de vários tradutores . 1 ed. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2021. Tradução de: Web survey on the use of Internet in Brazil during the new coronavirus pandemic: ict panel covid-19. Disponível em: https://cetic.br/pt/publicacao/painel-tic-covid-19/. Acesso em: 5 mai. 2021.

CRESCE O NÚMERO DE CRIMES EM AMBIENTES VIRTUAIS. Jornal do Estado. TV Atalaia. https://a8se.com/. Aracaju, 2021. Disponível em: https://a8se.com/tv-atalaia/jornal-do-estado/cresce-numero-de-crimes-em-ambientes-virtuais/. Acesso em: 4 fev. 2021.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**: do que estamos falando?. canalcienciascriminais.jusbrasil.com.br. 2015. 4 p. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/noticias/199340959/crimes-digitais-do-que-estamos-falando. Acesso em: 4 mar. 2021.

CRESPO, Marcelo Xavier de Freitas; SYDOW, Spencer Toth. **Novas tendências da criminalidade telemática**. http://bibliotecadigital.fgv.br/. 2007. 29 p. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/41656. Acesso em: 3 mai. 2021.

DECLARAÇÃO Universal dos Direitos Humanos. Paris, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 12 jan. 2021.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na internet. *In:* MINISTÉRIO PÚBLICO FEDERAL-MPF. **Crimes cibernéticos**. Brasília/DF: MPF, v. 3, 2018. 276 p. cap. 2, p. 26-50. (Coletânea de Arquivos). Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 4 mai. 2021.

DUARTE, Rosália . **Entrevistas em pesquisa qualitativa**. www.scielo.br. Curitiba, 2004. 13 p. Disponível em: https://www.scielo.br/j/er/a/QPr8CLhy4XhdJsChj7YW7jh/abstract/?lang=pt#. Acesso em: 14 abr. 2021.

DUARTE, Rosália. **Pesquisa qualitativa**: reflexões sobre o trabalho de campo. www.scielo.br. São Paulo, 2002. 16 p. Disponível em: https://www.scielo.br/j/cp/a/PmPzwqMxQsvQwH5bkrhrDKm/abstract/?lang=pt.

Acesso em: 13 abr. 2021.

GILBERTO Gil: pela internet 21 anos. Youtube, 2018. Vídeo (57min19s). Disponível em: https://www.youtube.com/watch?v=pGONgrm3mEU. Acesso em: 5 mai. 2021.

GIMENES, Emanuel Alberto Sperandio Garcia . **Crimes virtuais**. Revista de Doutrina TRF 4. Porto Alegre , 2013. 19 p. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm? https://revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html. Acesso em: 4 mar. 2021.

GOODCHILD, John. **Novos funcionários estão mais propensos a ataques de engenharia social**. https://egov.ufsc.br/portal/. 2011. Disponível em: https://egov.ufsc.br/portal/conteudo/not%C3%ADcia-novos-funcion%C3%A1rios-est%C3%A3o-mais-propensos-ataques-de-engenharia-social. Acesso em: 5 mai. 2021.

HISTÓRICO da pandemia de COVID-19. Organização Pan-Americaca da Saúde. Brasília. Disponível em: https://www.paho.org/pt/covid19/historico-da-pandemia-covid-19. Acesso em: 3 mai. 2021.

INSTITUTO BRASILEIRO DE DIREITO DE FAMÍLIA-IBDFAM. **Crimes contra a honra cometidos na internet terão pena triplicada; para especialista, medida coíbe noção de impunidade**. https://ibdfam.org.br/. Belo Horizonte, 2021. Disponível em: https://ibdfam.org.br/noticias/8423/. Acesso em: 27 abr. 2021.

JESUS, Damásio de ; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva , 2016. 208 p.

LAKATOS, Eva Maria; MARCONI, MARINA DE ANDRADE MARCONI. **Fundamentos de metodologia científica**. 7 ed. São Paulo: Atlas, 2012.

LAVADO, Thiago. **Com maior uso da internet durante pandemia, número de reclamações aumenta; especialistas apontam problemas mais comuns**. https://g1.globo.com/. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/06/11/com-maior-uso-da-internet-durante-pandemia-numero-de-reclamacoes-aumenta-especialistas-apontam-problemas-mais-comuns.ghtml. Acesso em: 10 mai. 2021.

LOTUFO, Larissa. Engenharia Social*. In:* SLEIMAN, Cristina *et al*. **Segurança digital**: proteção de dados nas empresas. São Paulo, 2021a. 247 p. cap. 7, p. 95-101.

LOTUFO, Larissa. Introdução*. In:* SLEIMAN, Cristina *et al*. **Segurança digital**: proteção de dados nas empresas. São Paulo : Atlas, 2021b. 274 p, p. 1-10.

MELO, Renato Dolabella ; OLIVEIRA, Lívia Costa de. **Direito de software e critérios para indenização judicial**. www.migalhas.com.br. 2021. Disponível em: https://www.migalhas.com.br/depeso/345783/direito-de-software-e-criterios-para-indenizacao-judicial. Acesso em: 2 jun. 2021.

MIGALHAS. **Desembargador Nucci avalia pontos da lei anticrime que voltam a**

valer. www.migalhas.com.br. 2021. Disponível em: https://www.migalhas.com.br/quentes/344322/desembargador-nucci-avalia-pontos-da-lei-anticrime-que-voltam-a-valer. Acesso em: 23 jun. 2021.

MONTEIRO, Renato Leite. **Crimes eletrônicos**: uma análise econômica e constitucional. Fortaleza, 2010. 192 p Dissertação (Mestrado em Direito) - Universidade Federal do Ceará, Fortaleza, 2010. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp142465.pdf. Acesso em: 7 mai. 2021.

PAINEL do Corona Vírus. CORONAVÍRUS BRASIL. 2021. Disponível em: https://covid.saude.gov.br/. Acesso em: 25 mai. 2021.

PINHEIRO, Patricia Peck. **Direito digital**. 6 ed. São Paulo: Saraiva, 2016. 781 p.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2020. 152 p.

POLÍCIA CIVIL DO ESTADO DE SERGIPE. **Departamentos/ Órgãos**. www.policiacivil.se.gov.br. Aracaju, 2021. Disponível em: https://www.policiacivil.se.gov.br/departamentos-orgaos/. Acesso em: 23 mar. 2021.

POLÍCIA CIVIL DO ESTADO DE SERGIPE. **Internet**: estelionatos na internet crescem 421% e Polícia Civil orienta população para não cair em golpes no ambiente virtual. www.policiacivil.se.gov.br. Aracaju, 2021. Disponível em: https://www.policiacivil.se.gov.br/internet-estelionatos-na-internet-crescem-421-e-policia-civil-orienta-populacao-para-nao-cair-em-golpes-no-ambiente-virtual/. Acesso em: 3 mar. 2021.

POLÍCIA CIVIL DO ESTADO DE SERGIPE. **Polícia civil orienta como evitar ser vítima de golpes na internet**. www.se.gov.br. Aracaju, 2021. Disponível em: https://www.se.gov.br/noticias/seguranca-publica/policia_civil_orienta_como_evitar_ser_vitima_de_golpes_na_internet. Acesso em: 22 abr. 2021.

PRESIDÊNCIA DA REPÚBLICA. **Brasil é convidado a aderir à convenção do conselho da europa contra a criminalidade cibernética** . www.gov.br. Brasília, 2020. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso em: 23 jun. 2021.

PRIMEIRA delegacia especializada em crimes virtuais é inaugurada em SE. g1.globo.com/se/sergipe. Aracaju, 2012. Disponível em: http://g1.globo.com/se/sergipe/noticia/2012/11/primeira-delegacia-especializada-em-crimes-virtuais-e-inaugurada-em-se.html. Acesso em: 10 mai. 2021.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. https://jus.com.br/. 2002. Disponível em: https://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais. Acesso em: 11 mai. 2021.

REALE, Miguel. **Lições preliminares de direito**. 27 ed. São Paulo: Saraiva, 2002.

391 p.

REGULAMENTO Geral sobre Proteção de Dados. Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 10 jan. 2021.

RICHTER, André. **Brasil inicia adesão a tratado contra crimes cibernéticos**. https://agenciabrasil.ebc.com.br/. Brasília, 2019. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2019-12/brasil-inicia-adesao-tratado-contra-crimes-ciberneticos. Acesso em: 23 jun. 2021.

ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal**. Tradução André Luís Callegari, Nereu José Giacomolli. 2 ed. Porto Alegre: Livraria do Advogado Editora, 2018. 64 p.

SANTOS, Clodogil Fabiano Ribeiro dos. **Tecnologias da informação e comunicação**. Paraná: UNICENTRO, 2017. Disponível em: http://repositorio.unicentro.br:8080/jspui/handle/123456789/543. Acesso em: 1 jun. 2021.

SECRETARIA DE SEGURANÇA PÚBLICA DE SERGIPE. **Com vazamento de dados de 223 milhões de brasileiros, Polícia Civil orienta como evitar ser vítima de golpes na internet**. https://www.ssp.se.gov.br/. Aracaju, 2021. Disponível em: https://www.ssp.se.gov.br/Noticias/Detalhes?idNoticia=18073. Acesso em: 7 abr. 2021.

SENNA, Felipe ; FERRARI, Daniella . **Convenção de Budapeste e crimes cibernéticos no Brasil**. www.migalhas.com.br. 2020. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil. Acesso em: 23 jun. 2021.

SERGIPE. Governo do Estado. Decreto n. 40652, de 26 de agosto de 2020. Homologa a Resolução n.º 06/2020, de 27 de agosto de 2020, do Comitê Gestor de Retomada Econômica - COGERE, altera o Anexo V do Decreto n.º 40.615, de 15 de junho de 2020 e dá outras providências. **Diário Oficial**. Aracaju, 28 de agosto de 2020. Disponível em: https://www.pge.se.gov.br/wp-content/uploads/2020/08/HOMOLOGA-06-COVID-SES.pdf. Acesso em: 26 mai. 2021.

SERGIPE. Governo do Estado. Decreto n. 40.567, de 24 de março de 2020. Atualiza, consolida e estabelece novas medidas de enfrentamento e prevenção à epidemia causada pelo COVID-19 (novo Coronavírus) no Estado de Sergipe, e dá outras providências. **Diário Oficial**. Aracaju, 25 de março de 2020. Disponível em: https://www.legisweb.com.br/legislacao/?id=391536. Acesso em: 2 mar. 2021.

SERGIPE. Governo do Estado. Resolução n. 6, de 27 de agosto de 2020. Aprova o enquadramento das Regiões de Território de Planejamento na Terceira Fase - Bandeira Verde de retomada econômica prevista no art. 7º do Decreto nº 40.615 , de 15 de junho de 2020, e dá outras providências. **Diário Oficial**. Aracaju, 28 de agosto de 2020. Disponível em: https://www.legisweb.com.br/legislacao/?id=400574. Acesso em: 21 abr. 2021.

SHIMABUKURO, Adriana *et al*. **Crimes Cibernéticos**: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. 2 ed. Porto Alegre: Livraria do Advogado, 2018. 270 p.

SHIMABUKURO, Adriana. Cibercrime: quando a tecnologia é aliada da lei*. In:* TRIBUNAL REGIONAL FEDERAL DA 3º REGIÃO. **Investigação e prova nos crimes cibernéticos**. 1 ed. São Paulo: EMAG, 2017. 352 p. cap. 1, p. 17-31. Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 24 mai. 2021.

SILVA, Carlos Eduardo Menezes *et al*. **Influência das condições de bem-estar domiciliar na prática do isolamento social durante a Pandemia da Covid-19**. https://docs.bvsalud.org/. 2020. 7 p. Disponível em: https://periodicos.unichristus.edu.br/jhbs/article/view/3410/1179. Acesso em: 4 mai. 2021.

SILVA, Ângelo Roberto Ilha da. Pedofilia, pornografia infantojuvenil e os tipos penais previstos no Estatuto da Criança e do Adolescente*. In:* SILVA, Ângelo Roberto Ilha da (Org.). **Crimes Cibernéticos**: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas . Porto Alegre: Livraria do Advogado, 2018. 270 p. cap. 4, p. 87-104.

SLEIMAN, Cristina *et al*. **Segurança digital**: proteção de dados nas empresas. São Paulo: Atlas, 2021. 247 p.

SUPERIOR TRIBUNAL DE JUSTIÇA-STJ. **Crimes pela internet, novos desafios para a jurisprudência**. www.stj.jus.br. 2018. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx. Acesso em: 26 mai. 2021.

SUPERIOR TRIBUNAL DE JUSTIÇA-STJ. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma**. www.stj.jus.br. Brasília, 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021-Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decide-Quinta-Turma.aspx. Acesso em: 25 jun. 2021.

SUPREMO TRIBUNAL FEDERAL-STF. **Coletânea temática de jurisprudência**: direito penal e direito processual penal. 3 ed. Brasília : STF: Secretaria de Documentação, 2017. 910 p. Disponível em: http://www.stf.jus.br/arquivo/cms/publicacaoPublicacaoTematica/anexo/CTJ_Direito_Penal.pdf. Acesso em: 3 fev. 2021.

TOLEDO, Francisco de Assis. **Princípios básicos do direito penal**: de acordo com a lei nº 7.209, de 11-7-1984 e com a constituição federal de 1988. 5 ed. São Paulo: Saraiva, 1994. 362 p.

TRIBUNAL REGIONAL FEDERAL DA 3º REGIÃO. **Investigação e provas nos crimes cibernéticos**. 1 ed. São Paulo: EMAG, 2017. 352 p. (Cadernos de estudos). Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 24 mai. 2021.

TUPINAMBÁ, Marcos. Ataques e crimes cibernéticos*. In:* SLEIMAN , Cristina *et al*. **Segurança Digital**: proteção de dados nas empresas. São Paulo : Atlas, 2021. 247 p. cap. 3, p. 15-30.

VALENTE, Jonas. **Agência Brasil explica: entenda o que é o lockdown**. https://agenciabrasil.ebc.com.br/. Brasília, 2020a. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/agencia-brasil-explica-entenda-o-que-e-o-lockdown. Acesso em: 5 mai. 2021.

VALENTE, Jonas. **Brasil tem 134 milhões de usuários de internet, aponta pesquisa**: a maioria acessa a internet pelo celular. https://agenciabrasil.ebc.com.br. 2020b. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa. Acesso em: 4 mai. 2021.

VALENTE, Jonas; SOUZA, Ludmilla; NITAHARA, Akemi. **Covid-19: estados flexibilizam, mas adiam retomada de aulas**. https://agenciabrasil.ebc.com.br/. Brasília, 2020. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2020-08/estados-flexibilizam-distanciamento-mas-adiam-retomada-das-aulas. Acesso em: 25 mai. 2021.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a lei nº 12.737/2012. Belo Horizonte: Fórum, 2013. 112 p.

WENDT, Emerson. **Lista dos Estados que possuem Delegacias de Polícia de combate aos Crimes Cibernéticos**. Delegado Emerson Wendt. Canoas-Rio Grande do Sul, 2020. Disponível em: http://www.emersonwendt.com.br/2010/07/lista-dos-estados-com-possuem.html. Acesso em: 29 abr. 2021.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2 ed. Rio de Janeiro: Brasport, 2013. 369 p.

WOLFF, Rafael. Infiltração de agentes por meio virtual*. In:* SILVA, Ângelo Roberto Ilha da (Org.). **Crimes Cibernéticos** : racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. 2 ed. Porto Alegre : Livraria do Advogado, 2018. 270 p. cap. 9, p. 217-234.

GLOSSÁRIO

Bring Your On Device-BYOD	Fenômeno em que os próprios funcionários levam seus próprios dispositivos particulares para uso profissional.
Código Malicioso	Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.
Criptografia	Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.
Cyberspace ou Ciberespaço	Assim se designa habitualmente o conjunto das redes de computadores e serviços existentes na Internet. É uma espécie de planeta virtual, no qual as pessoas se relacionam virtualmente, por meios eletrônicos.
Deepweb	Denominação genérica de uma rede que tem como principal recurso o anonimato, funcionando estruturalmente de forma voluntária e em camadas, o que oculta a verdadeira origem dos dados, geralmente relacionada à rede TOR.
Deepweb	Denominação genérica de uma rede que tem como principal recurso o anonimato, funcionando estruturalmente de forma voluntária e em camadas, o que oculta a verdadeira origem dos dados, geralmente relacionada à rede THOR.
Endereço de IP	É o endereço real de uma máquina na Internet. Consiste em uma série de números separados por pontos. Cada máquina conectada à rede tem um endereço de IP.
Malware	Do inglês Malicious Software-Código Malicioso.
SMS	Do inglês Short Message Service. Tecnologia utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas

	dados do tipo texto e cada mensagem e limitada em 160 caracteres alfanuméricos.
Spyware	Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware.
TIC	Como o próprio nome diz, as Tecnologias de Informação e Comunicação consistem em dispositivos produzidos pelo engenho humano com a finalidade de obter, armazenar e processar informações, bem como estabelecer comunicação entre diferentes dispositivos, possibilitando que tais informações sejam disseminadas ou compartilhadas.
Vírus	Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

APÊNDICE A — ROTEIRO PARA ENTREVISTAS

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE GRADUAÇÃO–PROGRAD
DEPARTAMENTO DE DIREITO-DDI

DISCENTE: Rosangela dos Santos DATA: 18/06/ 2021
ENTREVISTADA: Lauana Guedes Carvalho
OCUPAÇÃO: Delegada de Polícia Civil e responsável pela Delegacia de Repressão a Crimes Cibernéticos-DRCC/SSP/SE

ROTEIRO PARA ENTREVISTA COM AS DELEGADAS

1. O que se entende por crimes digitais, virtuais, cibernéticos, informáticos, visto que há uma série de terminologias utilizadas em diversos meios, a exemplo de artigos, livros de doutrina e nas mídias em geral, que geram certa controvérsia?

2. Tendo em vista a pergunta anterior, normalmente na prática cotidiana da DRCC como são chamados (terminologia utilizada comumente) esses crimes que são efetivados com o uso ou não da internet ou que sejam relacionados a dados e sistemas informatizados?

3. Após analisar os dados da CEACrim, foi possível constatar que a ocorrência desses delitos digitais durante a Pandemia da Covid-19 ficou mais intensa, a que é possível se atribuir esse fenômeno?

4. Em relação aos crimes contra o patrimônio perpetrados em 2020, a exemplo do estelionato, furto, apropriação indébita e extorsão que tiveram quantitativos bastante expressivos em relação ao ano de 2019, em sua opinião existe uma facilidade maior no meio digital para o cometimento desses delitos? Se possível explanar mais sobre a dinâmica do cometimento dos crimes de furto, apropriação indébita e extorsão a fim de fornecer esclarecimentos para a pesquisa.

5. E no caso específico do estelionato que já apresentava em 2019 um quantitativo mais significativo em relação aos outros crimes e manteve esse posicionamento em 2020, a que se atribui esse fenômeno?

6. Ainda em relação ao estelionato, quais foram as modalidades aplicadas pelos criminosos? É possível detalhar as principais ocorrências?

7. As legislações atuais que tratam de alguma forma dos delitos digitais, a saber, Código Penal, Marco Civil da Internet, ECA, LGPD, entre outras, são hoje suficientes para abarcar a proteção aos cidadãos em relação aos riscos no meio virtual?

8. Em sua opinião, quais as perspectivas futuras para o Direito e em especial para o Direito Penal diante do avanço tecnológico intenso, que por sua vez gera a necessidade de entendimento e ação no combate à crescente disseminação dos crimes digitais?

9. Atualmente no Brasil há algum grupo de trabalho ou sistema que interliga as ações das delegacias especializadas em crimes digitais em todo território nacional?

10. O que fazer para conscientizar a população que é preciso denunciar esses tipos de delitos?

11. Em relação às repercussões dos crimes digitais aqui apresentados e tendo em vista o nível de dificuldade na persecução criminal, existe algum levantamento acerca dos crimes investigados e sua consecutiva punibilidade?

12. Como é estruturada a DRCC? A equipe é formada por quantos membros? Quais as especialidades?

13. Há alguma dificuldade encontrada, caso queira relatar, no cotidiano das atividades desenvolvidas na delegacia? De ordem tecnológica, pessoal ou qualquer outra?

ANEXO A - PORTARIA Nº 01, DE 03 DE JANEIRO DE 2013 (CRIAÇÃO DA DRCC EM SERGIPE).

Segunda-feira, 25 de Fevereiro de 2013 Aracaju - Sergipe

Diário Oficial

Nº 26672

SECRETARIAS

Fazenda

GOVERNO DE SERGIPE
PORTARIA SEFAZ Nº 083
DE 21 DE FEVEREIRO DE 2013

Cria a Comissão de Apuração do Sorteio de prêmios no âmbito do Programa de Estímulo à Cidadania Fiscal e Tributária do Estado de Sergipe

O SECRETÁRIO DE ESTADO DA FAZENDA DE SERGIPE, no uso das atribuições que lhe são conferidas nos termos do art. 90, inciso II, da Constituição Estadual; Considerando a necessidade de garantir a transparência no processo dos sorteios a serem realizados pelo Programa de Estímulo à Cidadania Fiscal e Tributária do Estado de Sergipe,

RESOLVE:

Art. 1º Fica constituída a Comissão de Apuração do Sorteio de prêmios no âmbito do Programa de Estímulo à Cidadania Fiscal e Tributária do Estado de Sergipe, com o objetivo de acompanhar, aferir e certificar o processo de apuração do sorteio de prêmios do Programa de Estímulo à Cidadania Fiscal e Tributária do Estado de Sergipe.

§ 1º A comissão a que se refere o caput deste artigo é composta pelos seguintes servidores públicos, no exercício de suas funções:

I- Tarcisio Valois Galvão (SEFAZ), CPF: 503.519.905-34;

II- Kleber Henrique de Jesus Prado (SEFAZ), CPF: 963.489.415-15;

III- Silvana Maria Lisboa Lima (SEFAZ), CPF: 276.324.315-00;

IV- Sandra Santos Alves Silva (SEFAZ), CPF: 366.191.755-20;

V- Helber Andrade Sousa (SEFAZ), CPF: 590.941.845-91;

VI- Pablo Moreno Andrade dos Santos (CGE), CPF: 002.839.545-07;

VII- Silvar Pereira dos Anjos Júnior (CGE), CPF: 983.119.565-53.

§ 2º A referida comissão de apuração, composta nos termos deste artigo, tem como Presidente o Sr. Tarcisio Valois Galvão.

§ 3º Os servidores elencados no § 1º não farão jus a adicional de participação nesta comissão de trabalho.

Art. 2º A Comissão de que trata o art. 1º desta Portaria conduzirá os trabalhos para o quinto sorteio de prêmios do Programa de Estímulo à Cidadania Fiscal e Tributária do Estado de Sergipe.

Art. 3º Esta Portaria entrará em vigor na data de sua publicação.

PUBLIQUE-SE E CUMPRA-SE.
Aracaju, 21 de fevereiro de 2013.
JOÃO ANDRADE VIEIRA DA SILVA
SECRETÁRIO DE ESTADO DA FAZENDA

EXTRATO DO TERMO DE CONTRATO No 01/2013
PROCESSO Nº: 016.000-13265/2012-5 – PE nº 414/2012
OBJETO: Aquisição Parcelada de Água Mineral potável sem gás, garrafões de 20 litros, para atender as unidades da SEFAZ no interior do Estado.
CONTRATADA: AKBAR COMÉRCIO EXPORTAÇÃO E IMPORTAÇÃO LTDA
VALOR CONTRATADO: R$ 6.510,50 (valor mensal estimado)
R$ 78.126,00 (valor total estimado)
VIGÊNCIA DO CONTRATO: 02/01/2013 a 31/12/2013
DOTAÇÃO ORÇAMENTÁRIA: 16.101.04.122.0036-0457 –SEFAZ
ELEMENTO DE DESPESA: 339030 – **FR** – 0101
NOTA DE EMPENHO: 2013NE000120, 02/01/2013.
AUTORIZAÇÃO SECRETÁRIO : Pedido de Licitação 006/2012-23/10/2012
PARECER PGE Nº: 5816/2012 – PGE- 12/11/2012

EXTRATO DO 5º TERMO ADITIVO AO CONTRATO No 005/2009
PE Nº 510/2008
PROCESSO Nº: 016.000.13836/2012-5
ESPÉCIE: Quinto Termo Aditivo ao Contrato nº 005/2009, que entre si firmam o Estado de Sergipe, através da Secretaria de Estado da Fazenda, e ***ELIFRIOS COMÉRCIO, REFRIGERAÇÃO E SERVIÇOS LTDA.***
OBJETIVO: Prorrogar a vigência do mencionado Contrato, de 02/02/2013 a 01/02/2014, sem prejuízo do limite máximo estabelecido no Art. 57,II, da Lei 8.666/93.
PRAZO CONTRATUAL: INICIAL – 02/02/2009 a 01/02/2010,.
1º T.A. - 02/02/2010 a 01/01/2011 - prorrogação
2º T.A. - 02/02/2011 a 01/1/2012 - prorrogação
3º T.A. - 02/02/2012 a 01/02/2013 – prorrogação
4º T.A. - reajuste mensal - retroativo a janeiro/2012
BASE LEGAL: - Art. 57, II, da Lei 8.666/93, Cláusula Quarta do citado contrato.
AUTORIZAÇÃO DO SECRETÁRIO: Data: 13/11/2012
PARECER: Nº 6592/2012 – PGE –Data: 18/12/2012

Segurança Pública

GOVERNO DE SERGIPE
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
SUPERINTENDÊNCIA DA POLÍCIA CIVIL

PORTARIA N.º 01,
DE 03 DE JANEIRO DE 2013

Cria e Regulamenta as atribuições da Delegacia Especial de Repressão a Crimes Cibernéticos – DRCC, e estabelece providências correlatas.

A **SUPERINTENDENTE DA POLÍCIA CIVIL**, no exercício de suas atribuições institucionais e legais que lhe confere o Art. 12, da Lei nº 4.133, de 13 de Outubro de 1999, e

Considerando a crescente demanda por repressão qualificada aos crimes praticados na rede mundial de computadores ou por meios eletrônicos;

Considerando a necessidade de capacitação, qualificação e especialização dos servidores policiais civis que atuem na investigação destas modalidades criminosas;

Considerando a necessidade de suporte especializado e apoio às ações investigativas das demais unidades da Polícia Civil; e, por fim,

Considerando a necessidade de regulamentação administrativa e legal das unidades e atividades policiais;

R E S O L V E:

Art. 1.º Fica criada, no âmbito da Coordenadoria de Polícia Civil da Capital - COPCAL, a Delegacia Especial de Repressão a Crimes Cibernéticos – DRCC.

Art. 2.º A apuração dos fatos enquadrados como condutas típicas, antijurídicas e culpáveis contra sistemas de informática ou praticadas com a utilização destes, desde que com autoria desconhecida e ocorrido nos limites da circunscrição da COPCAL, serão da atribuição investigativa da DRCC.

§ 1º. A Superintendência da Polícia Civil poderá determinar à DRCC que atue na apuração de fatos que extrapolem a definição do *caput*, inclusive nos casos de autoria conhecida, quando a comprovação da mesma seja complexa.

§ 2º. As dúvidas com relação à atribuição para apuração deverão ser dirimidas pela Superintendência da Polícia Civil.

§ 3º. No caso de fato típico em que a vítima seja criança ou adolescente, a apuração será realizada pela Delegacia de Atendimento à Criança e ao Adolescente Vítima – DEACAV, com apoio da DRCC, quando demandada.

Art. 3.º A DRCC prestará apoio especializado às demais unidades da Polícia Civil, quando se tratar de fato típico cuja apuração não seja de sua atribuição, inclusive às unidades do interior do estado.

Art. 4.º Fica estabelecido o prazo máximo de 60 (sessenta) dias após a publicação desta Portaria para que a equipe da DRCC elabore e apresente:

I - Ementa de curso básico de apuração de crimes cibernéticos, a ser ministrado, por servidores lotados na própria DRCC, bem como por qualquer profissional com conhecimento específico sobre o tema, objetivando capacitar servidores policiais civis lotados em outras unidades da Polícia Civil.

II - Manual de procedimentos básicos para registro de ocorrências e apuração de crimes cibernéticos, a fim de ser distribuído para todas as unidades da Polícia Civil, após referendo do Conselho Superior de Polícia Civil.

Art. 5.º Esta portaria entrará em vigor a partir da data de sua publicação, ficando revogadas as disposições em contrário.

PUBLIQUE-SE, DÊ-SE CIÊNCIA E CUMPRA-SE.

KATARINA FEITOZA LIMA SANTANA
Superintendente da Polícia Civil

Estado de Sergipe
Secretaria de Estado da Segurança Pública
Gabinete do Secretário de Estado

PORTARIA N.º 002/2013
DE 11 DE JANEIRO DE 2013

Proíbe a custódia de presos nas Unidades Policiais Civis e nos Centros Integrados de Segurança Pública - CISP localizados no interior do Estado.

O SECRETÁRIO DE ESTADO DA SSP, juntamente com a **SUPERINTENDENTE DA POLÍCIA CIVIL DE SERGIPE**, ambos no uso das suas atribuições legais e visando preservar e exaltar os princípios da Integridade Física e Psíquica, da Razoabilidade, Proporcionalidade e Dignidade da Pessoa Humana, e, ainda,

CONSIDERANDO o dever legal dos gestores em manter a incolumidade física e psíquica dos servidores policiais civis, potencialmente afetadas em razão do excesso de serviço, reduzido número de servidores e tensão constante derivada da presença de custodiados em unidades policiais;

CONSIDERANDO a necessidade de otimizar as atividades desenvolvidas pelos policiais civis lotados no interior do Estado, comprometida em razão do baixo efetivo existente em todo o Estado e acúmulo inafastável das funções de custódia e policiamento investigativo;

CONSIDERANDO que a atividade policial civil é essencialmente investigativa, e que a manutenção de presos em unidades policiais é passível de causar prejuízos ao andamento dos inquéritos, investigações e demais operações policiais realizadas nas cidades do interior, e, finalmente,

CONSIDERANDO a possibilidade de ocorrer fugas, rebeliões e outras ações criminosas em razão da permanência de presos em delegacias localizadas em municípios distantes da capital;

CONSIDERANDO que a atividade fim da Polícia Militar é o policiamento ostensivo, que, em razão do baixo efetivo e da necessidade de custódia de presos em delegacias do Interior e CISP's, acaba sendo prejudicado.

R E S O L V EM:

Art. 1º. É vedada a custódia de presos em qualquer unidade policial civil ou Centro Integrado de Segurança Pública do Interior, salvo pelo período em que durar o flagrante ou na impossibilidade motivada da remoção imediata.

Art. 2º. Uma vez efetivada a prisão em flagrante, decorrente de mandado de prisão ou de qualquer outra modalidade prevista em lei, a Autoridade Policial responsável pelo ato deverá entrar em contato com o Coordenador Operacional da Diretoria de Polícia Civil do Interior – COPCI, informando acerca dos motivos da prisão, do número de presos e demais dados julgados necessários.

Art. 3º. Caberá obrigatoriamente à Unidade Policial responsável pela prisão o transporte do custodiado até uma das unidades policiais existentes na Capital com atribuições de custódia.

§ único. Em casos excepcionais e fundamentados, a Coordenadoria de Polícia Civil do Interior poderá, subsidiariamente, efetivar a remoção.

Art. 4º. Caberá à Superintendência de Polícia Civil de Sergipe, em razão da dinâmica apresentada e das condições físicas dos estabelecimentos policiais civis encarregados da custódia de presos oriundos do Interior, encaminhar à COPCI relação atualizada das unidades policiais aptas a receber presos.

Art. 5º. Esta Portaria entre em vigor na data da sua publicação revogando-se todas as disposições em contrário existentes.

Publique-se.

Aracaju, 11 de janeiro de 2013.

João Eloy de Menezes
Secretário de Estado da SSP

Katarina Feitoza Lima Santana
Superintendente da Polícia Civil

Educação

GOVERNO DE SERGIPE
SECRETARIA DE ESTADO DA EDUCAÇÃO
COMISSÃO PERMANENTE DE INQUÉRITO

EDITAL Nº 001/2013

A COMISSÃO PERMANENTE DE INQUÉRITO ADMINISTRATIVO DA SECRETARIA DE ESTADO DA EDUCAÇÃO **CITA**, através do presente, e em conformidade com o Art. 291 da Lei 2.148/77, o Professor **ALAN FIGUEIREDO DE OLIVEIRA FREIRE**, R.G.130.825-9/SSP-SE, CPF 882.830.385-91, a fim de comparecer à sala 47- bloco B, na Rua Gutemberg Chagas, nº 169 – Bairro Distrito Industrial de Aracaju(SEED), no prazo de 15(quinze) dias, a contar da data da publicação deste, com a finalidade de ser interrogado e se defender em Inquérito Administrativo, onde figura como Denunciado.

Aracaju(SE), 22 de fevereiro de 2013

JOÃO PACHECO VITAL
PRESIDENTE DA COMISSÃO