VANDERLEI SANT´ANNA LIMA

A DIALÉTICA MATERIAL DOS CRIMES CIBERNÉTICOS, FACE À PANDEMIA DE COVID-19

São Lourenço/MG

2021

VANDERLEI SANT´ANNA LIMA

A DIALÉTICA MATERIAL DOS CRIMES CIBERNÉTICOS, FACE À PANDEMIA DE COVID-19

Trabalho de Conclusão de Curso apresentado pelo aluno Vanderlei Sant´Anna Lima como requisito para obtenção do título de Bacharel, do Curso de Direito, da Faculdade de São Lourenço.

Orientador: Professor Me. Renato Augusto de Alcântara Philippini.

São Lourenço/MG

2021

A DIALÉTICA MATERIAL DOS CRIMES CIBERNÉTICOS, FACE À PANDEMIA DE COVID-19

Vanderlei Sant´Anna Lima[1]

Renato Augusto de Alcântara Philippini[2]

RESUMO

A globalização digital, mesmo durante a pandemia do coronavírus, oportunizou aos lugares mais remotos, o necessário acesso a internet e os seus benefícios. No entanto, o mesmo fenômeno fomentou grande incremento na prática de crimes cibernéticos, requerendo, pois avanços por parte da legislação penal e cibernética. Contudo um impacto inesperado ao ordenamento jurídico brasileiro surgiu da dialética entre a materialidade dos crimes cibernéticos, pandemia e a sociedade brasileira. Doutrinadores, reavaliaram possibilidades no Direito Penal Brasileiro para devida aplicação fática, frente às ocorrências desses crimes.Isto posto, este artigo científico busca discutir a problemática criminal cibernética em tempos pandêmicos..
Palavras-chave: Crimes cibernéticos. Pandemia. Internet..

ABSTRACT

Digital globalization, even during the coronavirus pandemic, provided the most remote places with the necessary access to the internet and its benefits. However, the same phenomenon fostered a great increase in the practice of cybercrime, thus requiring advances on the part of criminal and cyber legislation. However, an unexpected impact on the Brazilian legal system came from the dialectic between the materiality of cybercrime, pandemic and Brazilian society. Doctrinators, reassessed possibilities in Brazilian Criminal Law for due factual application, in view of the occurrences of these crimes. That said, this scientific article seeks to discuss the cyber criminal problem in pandemic times..
Keywords: Cyber crimes. Pandemic. Internet.

INTRODUÇÃO

A tecnologia digital revolucionou a forma do ser humano viver em sociedade. Estudar, comprar, trabalhar e até se relacionar pode ser feito por meio da internet. No entanto, a mesmo universo digital que facilita a realização das mais diversas condutas sociais, também permite uma gama enorme de novas práticas ilegais.

O presente trabalho traz a luz do direito, o auge dos crimes cibernéticos, tema controverso e motivador de questionamentos dos cidadãos pelo Brasil e no mundo;

[1] Bacharelando em Direito pela Faculdade São Lourenço/UNISEPE. E-mail: vanderlei-santanna@bol.com.br

[2] Mestre em Relações Internacionais e Ciência Política pela Universidade da Força Aérea. Docente e Coordenador do curso de Direito da Faculdade São Lourenço/UNISEPE. E-mail: rphi@uol.com.br

o que para muitos leitores do século XXI, em vigente globalização cultural e tecnológica, exigirá prévio conhecimento sobre as interações homem e máquina na rede mundial computadores-World Wide Web (WWW).

O tema apresentado versa sobre o mau uso dos meios cibernéticos, que contribuiu para o aumento da criminalidade em uma sociedade pandêmica. O objetivo geral desse artigo científico é investigar o porquê da alta ocorrência dos crimes cibernéticos no Brasil, durante a pandemia do coronavírus e elencar um caminho seguro para solução desse problema.

A pesquisa científica foi seccionada em quatro momentos, que nortearam novos rumos ao estudo do tema e resolução evidente do problema. O primeiro momento expõem a internet e o ciberespaço, suplementada pelas ideias de Émile Durkheim, sobre o “fato social”. No segundo tópico, a pesquisa trata os crimes cibernéticos, agentes criminosos e suas características. Na sequência foram expostas as dificuldades da materialidade penal durante a pandemia, quando foi afetado o Direito Penal Brasileiro e Mundial. Em última instância foi tratado o Crime Cibernético inserido na sociedade pandêmica

Foram citados, alguns autores familiares, o arcabouço jurídico brasileiro, e pontualmente dados sobre a temática criminal virtual, contextualizados no teor do artigo científico.

Busca-se, ao final, chamar a atenção dos leitores ao acessarem a internet em dispositivos móveis ou privados, terão a cautela exigida ao uso dos meios virtuais, ainda que afetados pela carga emocional pandêmica.

2 A INTERNET E O CIBERESPAÇO

Em 1983, foi criada a definição da Internet, que nos primórdios possuía fins militares, sendo utilizada de forma alternativa aos meios convencionais de comunicação da década de 60. Conforme aponta Costa (2011, p. 23):

> A internet de fato passou a existir com a ligação dos backbones NSF com a ARPANET. Define-se backbone como a espinha dorsal de cabos de telecomunicação de dados entre computadores de grande porte e roteadores que controlam o tráfego na internet, possibilitando a visualização e a transferência de dados através de quilômetros de distância.

No fim dos anos 1980, surgiu à rede mundial de computadores, com abreviatura WWW(World Wide Web), que possibilitou a transmissão de hipertextos imagens e sons via internet, e disseminou através de provedores o acesso não popular a essa nova ferramenta de interação entre povos, primeiramente via computadores.

O World Wide Web é conforme leciona Correa (2002, p. 11):

> Um conjunto de padrões e tecnologias que possibilitam a utilização da Internet por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias pela utilização do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados.

As melhorias na interação entre os comunicadores na internet chegaram com a mundialização e amplitude do acesso informatizado; fator que diminuiu as fronteiras geográficas; aproximou culturas e acelerou a tentativa de controle estatal, necessários ao bom e mau uso dos meios virtuais.

O Brasil caminhava a passos lentos na utilização da internet, quando ocorreram ações governamentais para que desse início ao desenvolvimento das telecomunicações. No ano de 1995, foi criado o Comitê Gestor da Internet (CGI), que gerou a regulamentação necessária ao uso da rede e fomentou os serviços ligados à Internet.

Todavia, o mau uso da rede mundial de computadores, se ampliou pela falta prestação de serviço e resposta às demandas dos provedores e usuários, muitas vezes vítimas da inexperiência na interação homem e máquina e suas possibilidades, a exemplo o “e-commerce”.

Igualmente, foi à maximização dos usuários em interação eletrônica, agora coagidos por uma Pandemia de alta letalidade. Fatores que afetaram não só as rotinas on-line, mas o mundo de forma geral. Em suas interações rotineiras virtuais: via satélite, telefonia celular ou rádio.

Em prejuízo, ficaram as matérias do Direito e a materialidade na aplicação da Lei Penal, ante os transtornos evidenciados das interações entre os comunicadores no “ciberespaço” consoante Lévy (2003).

De acordo com Cessante (2014), em sua obra Crimes Virtuais, vítimas reais. A internet

> [...] é uma grande praça pública, o maior espaço coletivo do planeta. Estima-se que no final de 2013 cerca de 2,7 bilhões de pessoas em todo o mundo estarão conectadas. No Brasil a internet está atingindo um número crescente de usuários; somos 105 milhões de internautas que estão cada vez mais conectados e passando mais tempo on-line. A internet é um conjunto de redes de comunicações em escala mundial e dispõe de milhões de computadores interligados pelo protocolo de comunicação TCP/IP, que permite o acesso a informações e todo tipo de transferência de dados. A Internet carrega uma ampla variedade de recursos e serviços num espaço virtual também chamado de ciberespaço, daí que, como no mundo real, a segurança digital é um terreno de ferrenha disputa entre defensores e agressores.

Dessa maneira, existem diversas maneiras de invasão de um computador com conseqüências variadas, ao se tratar sobre os objetivos para infecção de um computador pessoal ou smartphones. Entretanto, a maioria dos ataques, não visa prejudicar a máquina e sim o usuário, na captura de informações com intuito de prover vantagem econômica.

Segundo o informativo da Federação Brasileira de Bancos (FEBRABAN) em 2011, a internet banking era utilizada por 46% das contas ativas do país e 24% das 66 bilhões de operações realizadas no citado ano, foram feitas pela internet (FEBRABAN, 2011).

Dessa maneira, a insurgente sinergia provocada pela troca de saberes nos meios virtuais, criou a necessária avaliação das matérias penais do direito, para legislar sobre a segurança e a aplicação da lei no seu espaço de interação nominado “ciberespaço”.

Leva (2001, p. 71) relata que:

> [...] O ciberespaço (que também chamarei de ‘rede’) é o novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ele abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo ‘cibercultura’, especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço.

Consoante Durkeim, em sua obra “Les régles de la méthode sociologique, o crime, em qualquer sociedade, seja de qualquer tipo e de qualquer época, estará presente, por não ser algo patológico. Logo, seria o crime parte da vida coletiva,

enquanto elemento funcional da fisiologia, e não da patologia da vida social. Entretanto, o crescimento excessivo somado a pandemia de Covid-19, evidenciou a inesperada patologia criminal cibernética.

3. O CIBERCRIME, SEUS AGENTES E CARACTERÍSTICAS

A terminologia *Cybercrime* teve origem na cidade de Lyon, na França, durante uma reunião de um subgrupo das nações do G8 (composto pelos sete países mais ricos e industrializados do mundo, mais a Rússia),que debateu, crimes promovidos por dispositivos eletrônicos conectados à internet, no final dos anos 90.

Segundo Ferreira (2005, p.261), cibercrime é classificado como sendo:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Entretanto, para Cassanti (2016, p. 51): “Crimes virtuais são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão.”

Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.

Por conseguinte, a difícil materialidade dos crimes cibernéticos, começa pela dificuldade em diferenciar os agentes *hackers* dos *crackers*.

Em linhas gerais, ambos são experts em computadores, e dedicam boa parte do tempo para estudar sistemas e programações e contam com habilidades avançadas. A principal diferença está na forma como cada um utiliza este conhecimento.

Os *hackers* são programadores com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos, e assim classificados: *white hat* é, em geral, um hacker especialista em cibersegurança, que conhece as técnicas do cibercrime e as usa em favor do desenvolvimento de sistemas mais seguros.

Por outro lado, o hacker *black hat* outrora denominado *cracker* trata-se de um indivíduo de alto conhecimento em segurança, mas com técnicas usuais para fins criminosos.=, geralmente voltadas ao roubo de informações e dinheiro. Os *black hat*

tem outras habilidades não muito conhecidas, cada qual com um forma de se designar.

Nesse sentido, *carder* é o termo utilizado para designar a pessoa que atua para conseguir dados e informações de cartões de crédito, cartões de conta corrente ou poupança, ou contas em sites de movimentações bancárias para realizar fraudes online. *Defacer*, por sua vez, é o individuo que utiliza a tecnica *Deface* para pichar sites, eles exploram vulnerabilidades através de técnicas para conseguir acesso administrativo a um site para alterar a página inicial do mesmo, por uma que ele (invasor) criou. Já o *spammer* é alguém que envia anúncios por e-mail a pessoas que não desejam recebê-los e vírus que podem danificar e roubar informações dos usuários, como senhas bancárias. O *phisher*, por sua vez, é especializado em aplicar golpes diversos. Eles são profundos conhecedores das falhas de um sistema. Por fim o *phreaker* é o especialista que utiliza técnicas para burlar os sistemas de segurança das companhias telefônicas, normalmente para fazer ligações de graça ou conseguir créditos.

3. CRIMES CIBERNÉTICOS PUROS, MISTOS E COMUNS

Crimes cibernéticos puros são aqueles relacionados a comportamentos ilícitos que visam o ataque aos sistemas informáticos e seus componentes, integrando os dados e demais sistemas particulares. Nessa modalidade, a investida do agente tem por objetivo atingir o equipamento físico, o sistema informático e as informações dos bancos de dados. Nessa modalidade, exemplificativamente, temos a invasão de servidores e sites. Define-se crime cibernético misto, um evento criminoso condicionado ao uso do ciberespaço com efetivação, não obstante o autor visar bens jurídicos distintos dos meios virtuais (LEVI, 2003). O agente perfaz a conduta em rede de computadores ou aos seus componentes, no intuito de consumar o crime. À exemplo, cita-se o uso de software maliciosos (malware e ransoware) para retirar valores monetários de contas bancárias aleatórias, em homebanking.

Em suma, os crimes puros, mistos e comuns, fazem da rede mundial de computadores o instrumento, necessário a eficaz consumação de crimes tipificados no Código Penal Brasileiro, similares em descrição a lei de combate aos crimes cibernéticos.

Dentre as inúmeras formas, são exemplos de crimes cibernéticos: a fraude por e-mail e pela Internet; a fraude de identidades, quando informações pessoais são roubadas e usadas; o roubo de dados financeiros ou relacionados a pagamento de cartões; o roubo e venda de dados corporativos; a extorsão cibernética, que exige dinheiro para impedir o ataque ameaçado; os ataques de *ransomware*, um tipo de extorsão cibernética; o *cryptojacking*, que é o ato de explorar criptomoedas usando recursos que não se têm; e a espionagem cibernética, que ocorre quando hackers acessam dados do governo ou de uma empresa.

4 CRIMES CIBERNÉTICOS PRÓPRIOS E IMPRÓPRIOS

Os crimes próprios são aqueles que em que o sistema informático do sujeito passivo é o objeto e o meio do crime. Caracterizam-se pela sua autonomia e distinção das infrações positivadas no Código Penal. Algumas ações, não possuem tipificação legal devida a constante evolução desses crimes, uma vez que, pauta-se pela estrita legalidade, não punindo infrações não previstas em lei. São crimes praticados em sua maioria em violação de informações automatizadas.

São crimes cibernéticos impróprios, aqueles que fazem mero uso dos sistemas de informação como meio de execução, contra um bem jurídico comum, e a conduta se amolda ao tipo penal do Código Penal Brasileiro.

Dentre as modalidades criminais cibernéticas, se destacaram na vigência da pandemia do Covid-19, três frentes criminosas cibernéticas:

a) fraudes bancárias e furtos mediante fraude utilizando diversos métodos tais como Phishing, engenharia social, clonagem de cartões de crédito e key loggers;

b) invasão de dispositivos informáticos alheios, mediante violação indevida de sistemas de segurança e monitoramento, em tempo real, de comunicações telemáticas (dados) sem autorização judicial; e

c) lavagem de dinheiro.

Ressalta-se, que a principal prática criminal cibernética durante a pandemia, foi cometida no acesso dos atacantes, a interface dos servidores particulares das vítimas, quando em" trabalho remoto" ou simples uso rotineiro; via malwares ou ransowares, que violam o texto constitucional em seu artigo 5º e incisos, e ainda normas supralegais humanitárias.

Ademais, o objetivo dos ofensores supracitados, é obter das vítimas mediante "abuso de confiança", uma qualificadora do crime de furto, descrito no Código Penal Brasileiro, em seu artigo 155, §4.º, inciso II; o acesso irrestrito aos dados pessoais e financeiros, que são informações de grande valia para a criminalidade cibernética.

As circunstâncias pandêmicas, aceleram a fidelidade entre autores e vítimas, que restritos a pouca liberdade de locomoção por força de lei, ligados aos ciberespaço de Leviano, deixaram evidentes a falta de eduação digital dos usuários, agora vítimas dos crimes cibernéticos.

Outra facilidade é a mudança das rotinas laborais, com ampla necessidade dos meios virtuais, uma vez que trabalhar em casa gerou a desproteção de empresas e instituições, e fomentou a alta incidência criminal cibernética, através da particularidade dos identificadores virtuais vulneráveis (Ip) utilizados e possívelmente rastreados por black hats e engenheiros sociais ,focados objetivamente no acesso inrrestrito de dados pessoais, empresariais e institucionais, via computadores, notebooks e smartphones, envoltos no ambiente insociável, disseminado a população mundial, por força das normas pandêmicas.

5. A MATERIALIDADE CRIMINAL CIBERNÉTICA NA PANDEMIA COVID-19

A criminalidade cibernética viola, quando consumada, alguns princípios norteadores ao bom uso dos meios virtuais, são eles: confidencialidade, integridade e disponibilidade.

O princípio da confidencialidade: define que somente pessoas autorizadas poderão acessar determinada informação, caso ocorra o contrário, estará violando o princípio descrito. Um exemplo de quebra de confidencialidade seria a invasão de um sistema computacional, com senha de proteção ou não.

Em segundo momento, o princípio da integridade, indica que a informação que íntegra, confiável e inalterável, pode ser adulterada, intencionalmente ou não, e, com isto, a informação perde a confiabilidade.

Por último, o princípio da disponibilidade, que define a disponibilidade das informações a quem esteja autorizado sempre que for necessário. Um exemplo de quebra de disponibilidade é o ataque de negação de serviço contra um servidor, que faz o equipamento parar o funcionamento, e dessa maneira, deixa a informação indisponível.

No auge da pandemia de Coronavírus, os crimes cibernéticos se apresentaram em elevados números, a causa relevante a esse processo, é falta de conhecimento a respeito da segurança nos meios virtuais pelo mundo.

Os brasileiros, aumentaram o acesso ao recursos tecnológicos e digitais, mas sem o devido acompanhamento informativo, foram vitimados em instituições escolares; espaços públicos e de lazer; postos de trabalho e até por pequenos anúncios virtuais(spams).Simplesmente, ao terem o acesso cibernético sem a prevenção devida, transformara o mau uso e perigos ali existentes, na materialidade criminal nunca antes vista em sociedade ciberespacial.

No entanto este não é um fenômeno novo. Já em 2012, várias fotos da atriz Carolina Dieckmann, foram extraviadas de seu computador, via acesso indevido de um hacker, que invadiu o email da atriz e pegou suas fotos pessoais, para serem disseminadas na Internet.

Dessa maneira, confirmado tamanho prejuízo a intimidade da citada atriz, somada a grande comoção popular, gerou a oportuna discussão sobre crimes cibernéticos no Brasil.

Destarte, foi promulgada a Lei nº 12.737/12, popularmente conhecida como Lei Carolina Dieckmann, sancionada em 30 de novembro de 2012 Os delitos previstos em tal norma são:

O art. 154-A, do CP, que cuida dai Invasão de 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. Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

O art. 266, do CP, que cuida da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - Pena - detenção, de um a três anos, e multa.

O art. 298 do CP, que trata da falsificação de documento particular/cartão , cominando pena de reclusão, de um a cinco anos e multa.

Em 23 de Abril de 2014, foi criado o Marco Civil da Internet, com a lei nº 12.965/14, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Em seu artigo 3º e incisos, disciplinaram o uso até então da internet:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte, à exemplo: [...] (BRASIL, 2014).

Porquanto, ainda que regulamentado o uso da internet, os cibercriminosos organizados, usaram técnicas avançadas e lacunas de sistemas informáticos e telefônicos, para invadirem dispositivos móveis(smartphones) de inúmeras autoridades políticas brasileiras.Ocasião, que as condutas foram adequadas ao descrito, no artigo 154-A do Código do Penal Brasileiro, em que o bem jurídico protegido pelo novo tipo penal é a “intimidade”, a “vida privada”, a “honra” e a “imagem das pessoas”, por ser um tipo de “invasão de dispositivo informático”.

Ainda no primeiro semestre de 2019, antecedente a pandemia do Coronavírus no Brasil, foi desencadeada uma operação da Policial Federal Brasileira, batizada “Spoofing”, expressão relativa a um tipo de falsificação tecnológica, que procura enganar uma rede ou uma pessoa fazendo-a acreditar que a fonte de uma informação é confiável quando, na realidade, não é.

O Ministro da Justiça e Segurança Pública, à Sérgio Moro, informou em denúncia que hackers tinham tentado invadir o seu telefone celular. Ainda em suas palavras, essa tentativa foi percebida no dia 4 de junho do mesmo ano, quando recebeu uma ligação do seu próprio número. Os trechos da conversa entre o

ministro e procuradores da força-tarefa da Lava Jato, do Ministério Público Federal (MPF), vazaram e foram divulgados por veículos de imprensa.

Não distante, já no auge pandêmico, no mês de janeiro de 2021 houve um vazamento de 223 milhões de dados de indivíduos no Brasil, além de um grupo de pessoas falecidas, que compunham dados desse vazamento e muitas informações importantes, são elas: nome, cadastro de pessoas físicas, fotos, score das relações de consumo, adimplentes, inadimplentes, endereços e várias questões pessoais.

O projeto de lei do senador Izalci Lucas, fez os crimes cibernéticos considerados crimes menores e muitas das vezes substituídos por penas alternativas"; serem reforçados quanto a punição.No período pandêmico tais crimes, somados a outros menores de complementação normativa no Código Penal Brasileiro, proporcionaram o caos social dessa época.

A solução a essa materialidade criminal, não está nas leis, porque apenas 11% das pessoas afirmam conhecer "muito bem" as leis de proteção de dados e 45% acham que conhecem "mais ou menos". Outros 31% conhecem "pouco" e 11% não conhecem "nada". Sobre a Lei Geral de Proteção de Dados (LGPD), 9% dizem conhecer muito bem e 28% conhecem mais ou menos; a maioria (60%) conhece só de ouvir falar (33%) ou não conhece (27%). Quanto à Lei 14.155 que prevê punições mais severas para fraudes e golpes cometidos em meios eletrônicos: 6% conhecem muito bem e 30% conhecem mais ou menos; 61% conhecem só de ouvir falar (35%) ou não conhecem (26%).

O teor de texto científico desencadeou uma dialética Hegueliana, entre: a materialidade dos crimes cibernéticos(tese); os índices criminais cibernéticos (antítese); e a insegurança cibernética na sociedade pandêmica(síntese).

6. INDICES CRIMINAIS CIBERNÉTICOS e INSEGURANÇA DIGITAL NA PANDEMIA

Segundo a pesquisa Febraban, 91% dos entrevistados avalia que os crimes aumentaram muito (46%) ou aumentaram (45%) no período da pandemia; e somente 5% acham que diminuíram (4%) ou diminuíram muito (1%). Nos últimos 12 meses, os próprios entrevistados ou familiares foram vítimas, sendo as situações

mais comuns aquelas envolvendo recebimento de mensagens ou ligação telefônica com solicita.

Uma solução a materialidade desses crimes não está apenas em lei, porque apenas 11% das pessoas afirmam conhecer “muito bem” as leis de proteção de dados e 45% acham que conhecem “mais ou menos”.

Outros 31% conhecem “pouco” e 11% não conhecem “nada”. Sobre a Lei Geral de Proteção de Dados (LGPD), 9% dizem conhecer muito bem e 28% conhecem mais ou menos; a maioria (60%) conhece só de ouvir falar (33%) ou não conhece (27%). Quanto à Lei 14.155 que prevê punições mais severas para fraudes e golpes cometidos em meios eletrônicos: 6% conhecem muito bem e 30% conhecem mais ou menos; 61% conhecem só de ouvir falar (35%) ou não conhecem (26%).

O reforço dialético, veio com o advento da Lei nº 14.155, de 27 de Maio de 2021, que alterou 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.

As atividades ou situações apontadas como mais suscetíveis para que empresas ou instituições acessem seus dados são: compras online (35% das citações), sites em geral (33%), pesquisas on-line sobre termos e uso de sites de busca (23%) e serviços bancários online ou telefônicos (21%). Abaixo do patamar de 20% estão: postagens e atividades nas redes sociais (17%).

Destarte, se faz necessária a criação de um novo pensamento moral e científico, concatenado para a materialidade desses crimes, favorecidos por novas rotinas restrita aos lares, trabalho remoto, home-office e o fadado controle de circulação por forças de segurança pública.Itens que conexos, abarcaram novos questionamentos sobre cibersegurança e o combate aos evolutivos fatos sociais, agora crimes propriamente materializados na legislação penal.

Segundo Durkeim (1895), o fato social como objeto de estudo exerce sobre o indivíduo uma coerção. Logo, fatos sociais à época, influenciaram o modo de agir, de pensar e de sentir da população.

Atualmente, as rotinas suprimidas a pequenos espaços e deslocamentos em via pública, fizeram a população mundial e brasileira, ser tornarem reféns do acesso

inseguro aos meios virtuais, sem prévia a “educação digital”, que alavancou em escala evolutiva, os crimes cibernéticos materializados e consumados.

Contributivas foram as alterações legislativas brasileiras, penais e suas jurisprudências, as insurgentes trocas de saberes, via meios virtuais cibernéticos,o que fez a reavaliação das matérias penais do direito, quando da aplicação da lei no espaço de interação nominado “ciberespaço”.

Por ser fator mutante a qualquer sociedade, constata Émille Durkeim (1895), em sua obra “Les régles de la méthode sociologique”. O crime, em qualquer sociedade, seja de qualquer tipo e de qualquer época, estará presente, por não ser algo patológico. Logo, seria o crime parte da vida coletiva, enquanto elemento funcional da fisiologia, e não da patologia da vida social.Entretanto,os números excessivos atrelados as ocorrências em pandemia do Covid-19, evidenciaram a inesperada patologia criminal, motivada pela amplitude de um vírus fatal”(C)ORONA (V)IRUS (D)ISEASE”-doença do coronavírus, o popularmente conhecido COVID-19 em suas variações mundiais.

Então, tipificar ou materializar crimes cibernéticos, entre os fenômenos sociais normais, é afirmar que o crime também é fator de saúde pública, ou seja parte integrante de qualquer sociedade ainda sã.

Enfim, Durkheim sustenta que o crime tem função na estrutura social, uma vez que provoca e estimula a reação social, estabiliza e mantém vivo o sentimento coletivo que sustenta a conformidade às normas. Igualmente o crime tem um papel direto no desenvolvimento moral de uma sociedade.

Faz-se, pois, mister, a busca por uma inteligência coletiva. Nesse sentido, destaca, Lévy (2003) que [...] “inteligência coletiva seria àquela distribuída por toda parte, incessantemente valorizada, coordenada em tempo real, que resulta em uma mobilização efetiva das competências”.

Competências oriundas de uma desterritoriliazação dos saberes, geradora da real inteligência coletiva, por vezes benéfica, que em outros momentos, é prejudicial às rotinas humanas diárias.

Também diz Levy (2003) que seria interessante, tratar a questão da virtualização sem a separação do meio real e o virtual, pois os acontecimentos nesses meios alteram a realidade do indivíduo de forma complementar.

Em desfecho, os intervencionismos educacionais digitais sobre o tema e a aplicação da lei no combate ao crime, são pragmáticos e exigem da sociedade

brasileira e mundial, a adequação de suas rotinas pessoais, as possibilidades evolutivas criminais cibernéticas.Tanto que, historicamente a origem dos sistemas informativos globalizados pode pontuar itens que somados dialeticamente, positivam o nascimento do tema apresentado.

As interações no ciberespaço endurecerão as normas penais em branco, de necessária complementação, à exemplo o artigo 268 do Código Penal Brasileiro.Afim de que, a norma penal em branco seja justa ao estado de necessidade e anseios sociais, as mudanças em razão do tempo e lugar, são submissas à lenta apreciação do poder legislativo.

Por mais que, a finalidade dessa norma, é entre outras, oferecer proteção ao bem jurídico por ela tutelado, não gerou a segurança jurídica necessária quando aplicadas na pandemia.

Segundo Liberati (2000, p. 160):

> [...] o bem jurídico escolhido pela sociedade representa a base existencial do sistema de penas de qualquer Estado, transformando-se num instrumento limitador da intervenção estatal [..] com a identificação de objetos concretos de tutela penal, tornando-se ele a ratio e o próprio conteúdo da tutela penal.

Para tanto, admite-se o exercício do poder-dever estatal de punir justificado na tutela criminal dos valores, consagrados como bens jurídicos essenciais à convivência social pacífica.

Quanto mais, nota-se o “Direito Penal de Risco” somado a normas penais em branco, ainda que paliativas a sociedade, não comprovadamente eficazes aos brasileiros, em notória “Sociedade de Risco” perante as altas taxas criminais cibernéticas e Pandemia Covid-19.

O sociólogo alemão Beck (2010), em sua obra Risikogesellschaft: Auf dem Weg in eine andere Moderne, lançado em 1986 e 24 anos depois no Brasil, no ano de 2010 como o nome- Sociedade de Risco: rumo a outra modernidade, defendeu no teor de sua obra literária sociológica, uma sociedade que passa por uma reconfiguração, através de uma ruptura histórica.

Reconfiguração esta que traz a globalização democrática dos riscos, de forma equalizada. Onde pobres e ricos, não são totalmente imunes às ameaças produzidas e agravadas pelo progresso, outrora industrial e a presente inteligência artificial cibernética.

Segundo Beck (2010) é a mudança no potencial dos perigos atuais relacionados aos de épocas anteriores, já que os de agora são artificiais e não meramente causados por infortúnios naturais, pois são produzidos pela atividade do homem e vinculados à decisão deste.

Beck (2010) não concebe mais as ameaças como situações de classe, a exemplo do que acontecia na sociedade industrial clássica. Segundo ele, os riscos são produtos, ao mesmo tempo, reais e irreais, por aliarem danos e perigos já ocorridos àqueles calculados.

Por isso mesmo, os escritos de Beck não perderam vitalidade em face de contemporaneidade pandêmica, em que o risco penal e vital, representam uma realidade objetiva e mensurável, passível de cálculo, somada aos indicadores de risco para medir a morbidade (taxa de portadores de determinada doença em relação à população total estudada, em determinado local e momento).Neste sentido, as análises de Beck nos ajudam a entender um pouco mais a respeito não só da necessidade humana de querer controlar o mundo frente às inseguranças com as quais a sociedade diariamente se defronta, mas também da própria impossibilidade desse controle total.

A resposta brasileira, está na “Educação”, não somente para a instrução material e científica , mas a educação digital necessária ao uso dos meio virtuais em constantes atualização.

CONSIDERAÇÕES FINAIS

A discussão elencada no presente artigo, busca creditar a atenção da sociedade brasileira, a urgente implementação da “educação digital” no país.Outrossim foi a inexperiência dos usuários do ciberespaço, que facilitraram o provado aumento da criminalidade cibernética no Brasil. Os aliados a elevação desses índices criminais,são: o mau uso dos meios virtuais e o acesso irrestrito a internet na pandêmia; onde os ofensores cibernéticos endossaram uma gama de possibilidades criminais, devido a fidelização homem- máquina durante a pandemia, em “Estado de Necessidade” provocado por normas em branco de necessária complentação.

Uma questão de suma importância, é prevenção dos crimes cibernéticos, em detrimento das inúmeras ocorrência, provenietes da interação do homem

ciberespaço.Logo,se faz necessário positivar a inteligência coletiva,que é superior a inteligência individual .

Tais ações combativas, somadas a evolução educacional brasileira, terão resultados menos alarmantes, perante os prejuízos ocasionados pelos ofensores contextualizados em sociedade. Essas ações farão jus ao art.144 da Constituição Brasileira, onde o termo “segurança pública”, engloba a participação de todos, em contexto social, e agora no ciberespaço, palpável e comprovado durante a ociosa pandemia de Coronavírus, onde se perdeu a normalidade em sociedade por ausência de uma e-democracia ou ciberdemocracia.

REFERÊNCIAS BIBIOGRÁFICAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasi**l.Brasília-DF.Centro Gráfico,1988.

BRASIL.**Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez.

Marco Civil da Internet: **Lei 12.965/2014**. São Paulo: Editora Revista dos Tribunais, 2014.

Lei Carolina Dieckmann**: Lei nº 12.737 de 30 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**.Brasília-DF.Centro Gráfico,(2012).

BECK, Ulrish, 1944.**Sociedade de Risco:rumo a outra modernidade**, tradução NASCIMENTO, Sebastião. São Paulo, (2010).

CASSANTI, Moisés de Oliveira.**Crimes Virtuais,vítimas reais**. Rio de Janeiro: Brasfort,(2014).

HEIDEGGER, Martin. **A questão da técnica. Scientiae studia**, São Paulo, v. 5, n. 3, p. 375-98, 2007.

FERREIRA, Ivette Senise.Direito **& Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: Quartier Latin, 2005.

LÉVY, Pierre.**Cibercultura**. São Paulo: Ed. 34, 2003.

DURKHEIM, David Émile,(1895).**Le régles de la Méthode Sociologique” - As regras do método sociológico”.** tradução NOGUEIRA, Eduardo Lúcio.Portugal.Lisboa(2004).Ed. Presença.

CÔRREA, Gustavo Testa,(2000).**Aspectos Jurídicos da Internet**.São Paulo.Ed. Saraiva.

KASPERSKY:**Dicas sobre como se proteger contra o crime cibernético**.Disponível em <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime >. Acesso em 04 nov. 2021.

CONAMP: Reflexões **sobre o crime de infração de medida sanitária preventiva – "coronavírus"–do art. 268 do CP**. Disponível em <https://www. https://www.conamp.org.br/publicacoes/artigos-juridicos/6987-reflexões-sobre-o-crime-de-infração-de-medida-sanitária-preventiva-coronavírus-do-art-268-do-cp-6987.html >. Acesso em 04 nov. 2021.

YOUTUBE:**Cibercrime multiplicou durante a pandemia**.Disponível em https://pt.euronews.com/2020/10/22/cibercrime-multiplicou-durante-a-pandemia. Acesso em 12out.2021

JUSBRASIL:**CrimesCibernéticos**.Disponívelem:gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos.Acesso em 12out 2021.

SCHULTZ, Elisa Stroberg: **A pandemia da COVID-19, as condutas criminosas e os novos criminosos**. Canal ciências criminais, ISSN 2446-8150, Abril de 2020.Disponível em: https://canalcienciascriminais.com.br/a-pandemia-da-covid-19-as-condutas-criminosas-e-os-novos-criminosos/. Acesso em 04 nov2021.

RODRIGUES,Alex. **A PF detém quatro suspeitos telefone de Sérgio Moro**. Disponívelem:<https://agenciabrasil.ebc.com.br/geral/noticia/2019-07/pf-detem-quatro-suspeitos-de-invadir-telefone-de-sergio-moro>. Acesso em 04nov21.
FEBRABAN,EquipeNoomis. Brasileiros temem fraudes e veem alta nas violações de dados,indica estudo.Disponível em<https://noomis.febraban.org.br/videos/brasileiros-temem-fraudes-e-veem-alta-nas-violacoes-de-dados-indica-estudo>.Acesso em 12 out 2021.