

FACULDADE SANTO AGOSTINHO
UNIDADE SETE LAGOAS
CURSO DE DIREITO

EROS TEODORO RIBEIRO SILVA

**A SEGURANÇA JURÍDICA NO ÂMBITO CIBERNÉTICO E A
QUESTÃO DA EFETIVIDADE DA LEI PENAL EM RELAÇÃO A
TIPIFICAÇÃO DOS CRIMES DIGITAIS DECORRENTES DAS NOVAS
“TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO”.**

Discente: EROS TEODORO RIBEIRO SILVA
Direito: 09º período

**A SEGURANÇA JURÍDICA NO ÂMBITO CIBERNÉTICO E A
QUESTÃO DA EFETIVIDADE DA LEI PENAL EM RELAÇÃO A
TIPIFICAÇÃO DOS CRIMES DIGITAIS DECORRENTES DAS
NOVAS “TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO”.**

Artigo Científico apresentado à
Faculdade Santo Agostinho de Sete
Lagoas (FASASETE), como requisito
parcial para obtenção do título de Bacharel
em Direito.

Orientador: Prof^a Tereza Cristina Sader
Vilar.

Sete Lagoas/MG

2022

SUMÁRIO

1. INTRODUÇÃO	4
2. SOCIEDADE DA INFORMAÇÃO	7
2.1 Modernidade Líquida	9
2.2 “Sociedade de Risco”	9
3. CRIMES CIBERNÉTICOS	10
3.1 Situação no mundo	10
3.2 Crimes Cibernéticos no Brasil e o Direito Penal	12
4. ORDENAMENTO JURÍDICO BRASILEIRO EM RELAÇÃO À TIPIFICAÇÃO DOS PRINCIPAIS CRIMES DIGITAIS	14
4.1 Cooperação entre os órgãos	20
4.2 Convenção de Budapeste	22
5. CONCLUSÃO	23
REFERÊNCIAS	24

A SEGURANÇA JURÍDICA NO ÂMBITO CIBERNÉTICO E A QUESTÃO DA EFETIVIDADE DA LEI PENAL EM RELAÇÃO A TIPIFICAÇÃO DOS CRIMES DIGITAIS DECORRENTES DAS NOVAS “TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO”.

RESUMO: O presente trabalho visa abordar a temática dos crimes cibernéticos e conjuntamente com a análise da legislação pertinente, em que houve o aprimoramento dos preceitos normativos sobre direito cibernético, porém é necessário se atentar a seguinte problemática: Diante do surgimento recorrente das novas “**TIC’s**”, qual caminho seria viável para o legislador brasileiro adotar, tendo em vista o aumento exponencial desses delitos, principalmente de situações advindas depois da pandemia? O tema do seguinte trabalho foi escolhido por ter bastante pertinência na atualidade e tem por objetivo propor uma discussão a respeito de utilizar um “novo olhar” jurídico-social perante à essas inovações. Por fim, foi constatado que se tem segurança jurídica penal efetiva em relação à tipificação dos crimes digitais, onde urge de outras medidas de lidar com a situação proposta.

Palavras-chave: contexto histórico; internet; Direito Penal; crime digital; legislação adotada.

1 INTRODUÇÃO

O presente trabalho tem por tema a segurança jurídica no âmbito cibernético e a questão da efetividade da lei penal em relação à tipificação dos crimes digitais decorrentes das novas “Tecnologias de Informação e Comunicação.” Foi desenvolvido a partir do seguinte questionamento: diante do surgimento recorrente das novas “**TIC’s**” (Tecnologias de Comunicação e Informação), qual caminho seria viável para

o legislador brasileiro adotar, tendo em vista o aumento exponencial desses delitos, principalmente de situações advindas da pandemia?

Sobre a temática proposta, pode-se esclarecer, inicialmente que com o advento da informática em meados da década de 90, segundo o filósofo, sociólogo francês Pierre Lévy, os seus efeitos ainda não foram devidamente dimensionados até hoje. O primórdio da internet se iniciou em 1969 com o projeto ARPANET, e depois do “sucesso” desse experimento de compartilhamento de rede, que se iniciou com a percepção da transmissão de dados, acarretou uma série de efeitos aos longos dos anos, expandindo tanto no âmbito comercial como na revolução da comunicação, no impacto e controle da informação, nas relações de trabalho e a quebra das fronteiras tradicionais do Estado Nacional pelos famosos algoritmos.

A chamada “Modernidade Líquida” por Zigmunt Bauman (1999), ou a “Sociedade de Risco” por Ulrich Beck (1986), trazem uma profunda ligação com a cibercriminalidade fundada ao longo dos anos.

Assim, além do espaço real, o ciberespaço surgiu, e necessita-se de um acompanhamento cada vez mais minucioso nesse processo de modernização assegurando dessa forma, a plena segurança jurídica para o avanço do Estado Democrático de Direito.

A inovação tecnológica, fez muitos países se preocuparem cada vez mais com a criação de prerrogativas para assegurar os bens jurídicos tutelados e aplicarem diante de uma previsibilidade legal, sanções punitivas devidas para a prática de crimes virtuais, sendo estas por meio de uma legislação comum, legislação penal especial ou um modelo híbrido. A cooperação jurídica internacional se tornou cada vez mais presente entre os órgãos de persecução penal. O objetivo principal da pesquisa foi propor uma discussão a respeito de utilizar um “novo olhar” jurídico-social perante à essas inovações. Quanto aos objetivos específicos, esses foram: Verificar o contexto histórico do cyber digital; Demonstrar a inovação dos novos bens jurídicos; Reconhecer o incremento da segurança jurídica no âmbito digital e contextualizar a situação do Brasil sobre a Convenção de Budapeste.

O motivo principal da elaboração do trabalho é justamente tratar da questão problematização a respeito dos crimes digitais. Norteando o tema, cumpre destacar a relevância dos princípios da Legalidade e Territorialidade no âmbito criminal, onde resulta uma fragmentação dos regimes nacionais. É válido ressaltar também ao longo da pesquisa, o avanço da lei penal brasileira no que diz respeito ao âmbito cibernético e seus pontos positivos.

Entretanto, os crimes digitais são transnacionais por natureza, ou seja, quebram as respectivas “barreiras” e por isso, há uma necessidade de existir ou se adequar a um preceito normativo acima do Estado soberano, pelo menos em algumas questões de matéria penal substantiva. Tem-se por hipótese a problematização feita anteriormente, que é a percepção de que se ao longo das últimas mudanças na legislação penal brasileira, o texto normativo garante a segurança jurídica e efetividade da lei penal em relação as condutas ilícitas decorrentes do âmbito cibernético. Tal hipótese foi confirmada ao final da pesquisa, consoante com os argumentos que serão abordados ao longo de todo o trabalho.

O tipo de pesquisa irá se desenvolver através de um estudo bibliográfico de livros(manuais), artigos já publicados, legislações, posicionamento jurisprudencial e caso seja percebido, dados ou casos de levantamento pertinentes que podem ser de uso quantitativo para exemplificação de algumas modalidades de crimes cibernéticos. Em se tratando do método de abordagem, será empregado o hipotético-dedutivo.

Para a interligação das principais ideias, foram utilizados como referência no trabalho obras de autores que vão contribuir muito para o avanço da discussão sobre a problemática, fazendo-se a comunicação dos avanços da tecnologia da informação, com a Sociologia, tendo em especial, ideais de Zygmunt Bauman e Ulrich Beck. Sobre os crimes digitais, Damásio de Jesus e José Antônio Milagre ilustram bem como se dá essa temática no Direito e servem de fundamentação para determinadas terminologias.

O presente trabalho para seguir de acordo com os objetivos propostos, este trabalho foi estruturado em três capítulos, cada um deles divididos em dois subtópicos.

O primeiro capítulo tratou da Sociedade da Informação e sobre o viés sociológico por trás do tema.

O segundo capítulo abordou a origem dos crimes cibernéticos, e como a situação se deu no mundo e no Brasil.

O terceiro capítulo, por fim, trouxe a análise do ordenamento jurídico brasileiro em relação a tipificação de determinadas modalidades de delitos, com suas mudanças, disposições e posicionamentos jurisprudenciais e doutrinários. Na seara do Direito Internacional, foi abordado sobre a Convenção de Budapeste e a cooperação dos órgãos internos.

Ante o exposto, passa-se ao desenvolvimento da pesquisa a partir da estruturação mencionada.

2 SOCIEDADE DA INFORMAÇÃO.

No seguinte capítulo, tem por objetivo tratar da Sociedade da Informação e sua conceituação por Pierre Lévy, e sobre o viés sociológico por trás do tema que será dividido em duas partes. Antes de adentrar aos subcapítulos, vai ser abordado o contexto histórico da internet pelos autores americanos Richard Alan Clarke, e Robert K. Knake. Já nos subcapítulos, Zygmunt Bauman vai contribuir para o início da discussão e o segundo tópico vai trazer os ideais do sociólogo alemão Ulrich Beck, mais precisamente sua obra Sociedade de risco.

Adentrando sobre o tema, é válido ressaltar o papel fundamental de Alan Turing, considerado o pai da computação (1912-1954). Ele foi um cientista, matemático e criptógrafo inglês, que foi o precursor para criação dos computadores modernos e também teve papel fundamental na Segunda Guerra Mundial, com a criação de um sistema utilizando força eletromagnética para possibilitar a tradução de comunicações alemãs codificadas na época.

Entretanto, sua honraria veio apenas com a invenção da “Máquina de Turing”, criada em 1936, e sua ideia era basicamente de que o mecanismo tinha que manipular símbolos em uma fila de acordo com uma série de regras predeterminadas, para o armazenamento de informações, ideia essa que decorre a maior parte dos nossos dispositivos eletrônicos que são programáveis. Além disso, Turing também desenvolveu os primeiros testes capazes de realizar a distinção entre a inteligência artificial da inteligência humana.

A partir do entendimento de CLARKE e KNAKE, percebe-se que o primórdio da internet se iniciou em 1969 com o projeto ARPANET (Rede de Projetos e Pesquisas Avançadas), financiada pela DARPA (Agência de Projetos e Pesquisas Norte-Americanas Avançadas) e depois do “sucesso” desse experimento de compartilhamento de rede, que se iniciou com a percepção da transmissão de dados, e por fim a conexão entre os polos universitários de *Utah*, *Stanford*, *UCSB*(Universidade da Califórnia em Santa Bárbara) e a *UCLA*(Universidade da Califórnia em Los Angeles), acarretou uma série de efeitos aos longos dos anos, expandindo tanto no âmbito comercial como na revolução da comunicação, o impacto e controle da informação, as relações de trabalho e a distância. (CLARKE; KNAKE, 2015).

Pelo advento da informática em meados da década de 90, segundo o filósofo francês e pesquisador científico digital LÉVY, os seus efeitos ainda não se têm uma determinada dimensão até hoje. (LÉVY, 1999)

Nesse contexto, surgiu o que Gibson definiu de ciberespaço em sua obra científica chamada Neuromante. Nela, a compreensão do termo deve se partir do universo das redes digitais e da nova roupagem que expandiu o meio social, as multinacionais, os conflitos mundiais e principalmente a economia e a cultura. (GIBSON, 1984, *apud* LÉVY, 1999)

A sociedade tem passado por grandes transformações nas últimas décadas. Inúmeros fatores têm contribuído para tanto. Mas, sem dúvida nenhuma, o que mais tem influenciado no comportamento humano são as Tecnologias de Informação e Comunicação (TICs). Faz se necessário a conceituação deste termo, que pode ser entendido dos ideais de Damásio e José Antônio (2016), e é caracterizado por um conjunto de ferramentas relacionadas à transmissão, processamento e armazenamento digitalizado de informações.

Com a expansão das novas TICs, houve uma grande alteração na forma em que nos comunicamos, agimos em sociedade, no meio profissional, principalmente em relação aos novos meios de redes sociais e uso do *E-commerce*. Diante disso, inevitavelmente surgiram novos crimes e novas formas de cometimento de crimes. Consoante com as ideias de Émile Durkheim em sua obra: Regras do Método Sociológico: “em primeiro lugar, o crime é normal porque uma sociedade que estivesse isenta seiria inteiramente impossível.” (DURKHEIM, 2014, p.68)

“O crime é, portanto, necessário; ele está ligado às condições fundamentais de toda a vida social e, por isso mesmo, é útil; pois as condições de que ele é solidário são elas mesmas indispensáveis à evolução normal da moral e do direito. (DURKHEIM, 2014, p.71)

Diante o exposto, o que se pode compreender de Durkheim, é que onde há sociedade, há crime. O delito faz parte da vida coletiva, e é algo muito mais próximo da sociedade em si, do que uma doença ou um mal excepcional. Entretanto, em sua obra, Durkheim não adentra a respeito do que poderia ser configurado um perceptível excesso da criminalidade em sociedades diversas.

Em decorrência da transformação em vários fatores da vida coletiva, os crimes também acompanharam essa mudança e é nesse contexto que surgem o conceito de cibercriminalidade, ou, de forma ampla, crimes cometidos através das tecnologias de informação e comunicação, sendo as tecnologias meio ou objeto do crime.

Os crimes cibernéticos são frutos da sociedade de informação, e esta propiciou a criação de novos bens jurídicos, quais sejam, os próprios dados, ambientes e espaços virtuais a serem atacados. Vale uma breve definição do conceito de “Sociedade da informação” da obra Cibercultura, de LÉVY (1999), que pode ser entendida basicamente como uma expressão cunhada por cientistas sociais para referir-se às transformações técnicas, organizacionais e administrativas.

Tendo em vista essa conceituação, os capítulos seguintes irão abordar uma essencial ligação sociológica.

2.1 Modernidade Líquida

A matéria-prima da época da sociedade industrial, perdeu seu espaço para a disseminação da informação, na era da tecnologia. Em relação a essa intangibilidade, Zigmunt Bauman classificou como “MODERNIDADE LÍQUIDA” e “SOCIEDADE LÍQUIDA.” (BAUMAN, 2001).

Fazendo uma ligação de ideias entre os autores, a liquidez e a volatilidade que BAUMAN tratou, serviu para alterar como o mundo se portava diante de situações rotineiras, e como onde há sociedade, há também crime, ideal trazido por DURKHEIM, em decorrência disso, naturalmente vão surgir diante dessa nova sociedade fluida, novos crimes, os chamados crimes digitais. Feito tal explanação, o próximo subtópico irá adentrar na ideia da sociedade de risco.

2.2 Sociedade de Risco

A sociedade tem se usufruído de uma evolução tecnológica expansiva diante das TIC's vinculadas à informática, internet e recentemente à robótica e as novas alterações do mercado econômico mundial. Entretanto, esse avanço cobra um preço: a elevação dos fatores de risco na nossa sociedade. Ideal esse trazido pelo sociólogo alemão Ulrich Beck, que em sua obra mais famosa, Sociedade de Risco, diz que: “este conjunto de riscos geraria “uma nova forma de capitalismo, uma nova forma de economia, uma nova forma de ordem global, uma nova forma de sociedade e uma nova forma de vida pessoal.” (BECK, 1999, p. 2-7)

Não há um parâmetro de mensurar quantitativamente esse impacto, mas ele atinge toda a sociedade estrutural em si. Nessa quebra de dimensões, criado pela sociedade de risco as pessoas se tornaram “transparentes”, e convivem com a

ameaça de vários direitos adquiridos ao longo desse Estado Democrático de Direito formado.

3 CRIMES CIBERNÉTICOS

É de relevância reconhecer a mudança das relações sociais, e de que novas práticas surgiram nesse meio do ciberespaço, tanto no mundo como no Brasil. Nesse cenário, foram surgindo gradualmente os crimes cibernéticos.

3.1 Situação no Mundo

Em se tratando de evolução histórica, a doutrina não consegue ser unânime em apontar um posicionamento claro em relação a quando e onde ocorreu o 1º crime cibernético, entretanto o surgimento passou pela criação dos computadores modernos na década de 1960.

Segundo JESUS e MILAGRE (2016), parte de alguns doutrinadores apontam que o primeiro delito informático teria ocorrido dentro do Massachusetts Institute of Technology (MIT), no ano de 1964, quando um universitário teria cometido um ato considerado cibercrime. Já em relação a Europa, o primeiro estudo sobre o assunto foi desenvolvido por Ulrich Sieber, na década de 70.

Na década de 1980, o hacker e programador norte-americano John Draper, ficou conhecido como “Capitain Crunch”, na qual adaptou um apito que vinha embalado em caixas de cereal, para produzir o tom de 2.600 Hz. Como se tratava da mesma frequência que as filas da AT&T (Companhia Americana de Telecomunicações) emitiam para indicar que uma linha estava disponível para dar prosseguimento a uma nova chamada, ele conseguiu o feito de realizar várias ligações gratuitas. Antes de adentrar no próximo caso, é de relevância fazer a definição das terminologias: “malware”, vírus e “worms.”

LATTO (2020) ressalta muito bem que os malwares, se tratam de todos os códigos e aplicativos desenvolvidos com a finalidade de dano em dispositivos ou a usuários que utilizam serviços. Vírus e worms, fazem parte dos malwares e sua diferenciação é que, no primeiro eles se espalham automaticamente com a ajuda do usuário executando alguma ação necessária para ativação. Quanto ao segundo, a multiplicação automática se dá de forma independente.

As consequências dos malwares, podem ser inúmeras, tanto na questão de mensagens ou anúncios excessivos, perda da capacidade de desempenho do dispositivo, perda de dados, recursos financeiros, informações pessoais ou até mesmo

em ataques mais vastos como a nível governamental a determinadas instituições. Tendo em vista essa explanação, podemos adentrar na próxima situação.

Em 1988, tivemos o maior caso emblemático de um ataque a computadores utilizando um worm. Robert Tapan Morris, estudante de engenharia da informática pela faculdade de Cornell/Eua, criou um esse tipo de worm para infectar a internet com o objetivo de demonstrar as próprias vulnerabilidades da segurança da informática, prejudicando seis mil computadores e o percentual de 10% da internet da localidade em um único dia.

Com base em um artigo publicado pela Tacet Global - Agência de Inteligência, Investigação e Segurança sediada no Reino Unido (2020), o feito de Morris foi ilícito pela lei federal: Computer Fraud and Abuse Act (1986), que proíbe o acesso não autorizado a sistemas protegidos. Os promotores colocaram Morris em julgamento em 1989 e no ano seguinte, ele foi considerado culpado por um júri, tornando Morris a primeira pessoa a ser condenada sob a lei de 1986. No entanto, ele foi poupado do tempo de prisão de 3 anos, e recebeu uma pena de multa e quatrocentas horas de serviço comunitário. Após o cumprimento, ele dedicou ao papel acadêmico na mesma instituição que disseminou o seu próprio worm.

Em 1990, já com as primeiras condenações, Kevin Mitnick invadiu a rede de computadores das operadoras de telefonia e provedores de internet dos EUA, sendo condenado a 5 anos de prisão. Ficou famoso nos Estados Unidos como “The Career Hacker;” ou o Hacker Profissional.

Também em 1990, Kevin Poulsen interceptou as ligações a uma emissora de rádio na Califórnia para participar de um concurso para ser o 102º ouvinte e com isso conseguiu ganhar um Porsche. Condenado a 4 anos de prisão, hoje em dia é diretor do site Security Focus e editor da revista Wired.

Na Itália, as discussões envolvendo crimes informáticos se deram entre 1992 e 1993, com a edição do Decreto Legislativo n. 518, de 29 de dezembro de 1992, e Lei n. 547, de 23 de dezembro de 1993, onde tipos penais tiveram redação alterada para incluir os crimes informáticos.

A situação na Alemanha começou a ser tipificada em 1986, com a previsão já de condutas como falsificação de dados, espionagem, sabotagem, fraude informática e alteração de dados.

Já na China, a proteção deu-se com a lei Computer Information Network and Internet Security, Protection and Management Regulations (2011).

Na Inglaterra, em 1984 já havia disposições sobre a proteção de dados com a chamada Data Protection Act.

Na Espanha, em 1995 conforme o Código Penal de 1995, houve alterações prevendo inúmeros tipos penais relativos aos crimes digitais.

3.2 Crimes Cibernéticos no Brasil e o Direito Penal

No Brasil temos o ano de 1997 como o ano inaugural. Uma jornalista, passou a receber centenas de e-mails de cunho erótico- sexual, juntamente com mensagens de ameaça a sua integridade física. O crime foi investigado e conseguiu-se chegar ao autor das mensagens, um analista de sistemas que foi condenado a prestar serviços junto a ACADEPOL, ministrando aulas sobre esse tipo de modalidade.

Segundo JESUS e MILAGRE (2016), também em 1997, em MG, um site com sexo explícito entre crianças foi retirado do ar pela Justiça, onde o responsável possuía apenas 15 anos.

Em 1998, chega o primeiro caso ao Supremo Tribunal Federal (STF), julgando o habeas corpus (HC 76.689/PB), que enfrentou o primeiro crime cibernético a chegar na Suprema Corte Brasileira. Tratou-se de pornografia infantil na internet.

É válido ressaltar que o ministro Sepúlveda Pertence já demonstrou naquela época que nem todos os crimes cibernéticos precisavam de nova tipificação, já que às vezes o bem jurídico já era tutelado pelo Direito Penal, apenas o meio utilizado, informático, que era novo, no caso tratando de crimes cibernéticos impróprios.

A necessidade do afastamento social causado pela pandemia da Covid-19 fez com que o uso da internet aumentasse em mais de 40% no Brasil, segundo dados da Agência Nacional de Telecomunicações. Desde necessidades formais, como tele aulas, home office e reuniões de negócios por videoconferência, como o uso por puro lazer, com horas gastas em sites de buscas, proporcionou um efeito em contrapartida muito indesejado: o aumento dos ataques cibernéticos.

Durante a pandemia causada pelo novo coronavírus, os golpes financeiros cometidos através da internet cresceram exponencialmente. Segundo informações da Federação Brasileira de Bancos (Febraban), em 2020 o número de *phisings* aumentou 80% no pós-covid. A modalidade de crime trata-se no caso de criminosos que tentam convencer as vítimas, e se passam por pessoas idôneas, mas na verdade, aproveitam-se de uma situação de vulnerabilidade e uso de técnicas da Engenharia Social, enviando mensagens com informações que chamam a atenção do usuário, que clica em um link e, a partir daí, permitem a captura dos dados pessoais, bancários e senhas.

De acordo com dados do FortiGuard Labs, laboratório de inteligência de ameaças da empresa, apenas no Brasil foram mais de 16,2 bilhões tentativas de

ataques cibernéticos entre janeiro e junho 2021. E segundo último levantamento (08/02/2022), o Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021, um aumento de mais de 950% com relação a 2020 (com 8,5 bi), segundo a [Fortinet](#).

Crimes virtuais, crimes cibernéticos, cibercrimes, delito informático, delitos 2.0, delito virtual, infocrimes, são várias as nomenclaturas utilizadas pela doutrina para se referir ao mesmo fenômeno. Essas nomenclaturas, enquanto definiam novos tipos de crime, passaram a sofrer críticas da doutrina. A principal crítica era a inexistência de um denominador comum, visto que os bens jurídicos tutelados diferem em cada caso específico.

Segundo Jesus e Milagre:

“crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. (JESUS; MILAGRE, 2016, p. 49-50)

Já ROSSINI (2004), define:

“o conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.”

Exemplificando, os crimes digitais, tratam-se de duas modalidades. Incluem tantos os delitos específicos da internet, como um ataque de denegação de serviço ou os delitos tradicionais, mas cometidos através de meios eletrônicos, como por exemplo estelionato.

Ao adentrar nos crimes cibernéticos próprios e impróprios, faz valer o entendimento dos chamados bens jurídicos. Segundo Bitencourt: “A fragmentariedade do Direito Penal tem como consequência uma construção tipológica individualizadora de condutas que considera gravemente lesivas de determinados bens jurídicos que devem ser tutelados”. (BITENCOURT, 2020, p. 768).

Pode-se compreender que o bem jurídico é um valor ou um conjunto de valores que por serem dotados de uma importância ao ser humano e para a sociedade, ele passa a ser tutelado pelo Direito. O bem jurídico vai variar se estamos tratando de crime cibernético próprio ou crime cibernético impróprio.

Em se tratando caso a tecnologia da informação for o objeto do crime em si, estaremos diante de um crime cibernético próprio ou propriamente dito. Por exemplo, um ataque de denegação de serviço, uma invasão de computadores, envio de vírus, trojans.

Já no caso dos crimes cibernéticos impróprios, dizem a respeito quando a tecnologia da informação for o meio utilizado para a agressão de outros bens jurídicos já protegidos pela legislação penal, estaremos diante de um crime cibernético impróprio.

Em outras palavras, crimes cibernéticos impróprios são aqueles que, apesar de serem cometidos por meio de sistemas informatizados, poderiam ser cometidos independentemente do sistema informatizado, violando bens jurídicos já protegidos no Código Penal. Como por exemplo, difamação, crimes para atingir o patrimônio(estelionato).

O bem jurídico nos crimes cibernéticos impróprios não se refere às tecnologias da informação, mais sim a propriedade, liberdade, honra, dignidade sexual entre outros bens que são protegidos pelo Direito Penal.

4. ORDENAMENTO JURÍDICO BRASILEIRO EM RELAÇÃO A TIPIFICAÇÃO DOS PRINCIPAIS CRIMES DIGITAIS

No último capítulo a seguir, a temática irá tratar do avanço da legislação brasileira em relação a tipificação dos principais crimes cibernéticos. Tendo em vista a amplitude das modalidades, foi feito um recorte das mais recorrentes para título de exemplificação. Fim da abordagem de tais preceitos, o encerramento vai conter dois subcapítulos finais e posteriormente a conclusão sobre a problematização do tema.

Quanto a proteção cibernética no Brasil, se tem inicialmente a tipificação dos crimes relacionados a liberdade sexual, que tratam da pedofilia e a pornografia infantil, trazidos no ECA.

Crimes de Pedofilia – Venda ou exposição à venda de material pornográfico infantojuvenil. Regulamentado pelo ECA, **no art. 241-ECA (Crime Cibernético Impróprio)**

Lei 11.829 de 2008 incluiu o art 241-A no ECA (Divulgação de Pornografia Infantojuvenil e Asseguramento de meios ou serviços para a divulgação).

Lei nº 11.829 de 2008 incluiu o art 241 -B no ECA, que trata da criminalização de aquisição, posse ou armazenamento de material pornográfico infantojuvenil.

Lei nº 11.829 de 2008 incluiu o art 241 -C no ECA que trata da simulação de pornografia infantojuvenil

Lei nº 11.829 de 2008 incluiu o art 241 -D no ECA que tipificou o aliciamento, assédio, instigação ou constrangimento para a prática de ato libidinoso com a criança, por qualquer meio de comunicação.

No ano de 2012, teve-se a promulgação da Lei Nº 12.735/12 – “Lei Azeredo”), que tratou da criação de uma estruturação dos órgãos da polícia judiciária para o enfrentamento dos crimes digitais e a prerrogativa de cessamento de transmissões por meio digital.

Outra novidade no mesmo ano foi a conhecida lei: Nº 12.737 de novembro de 2012 – “Lei Carolina Dieckman” para tratar em seu artigo 154-A do CP, da tipificação dos delitos informáticos (conduta de invasão de dispositivo informático) e com o objetivo assegurar os bens jurídicos tais como a intimidade, a privacidade e o sigilo informático.

Em 2012 também foi incluído pela Lei Carolina Dieckman, a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública. Inclusão do § 1º, e 2º no art. 266 do CP quando o crime é praticado em situação de calamidade pública, na qual a aplicação da pena é em dobro, e no artigo 298º do Código Penal o crime de falsificação de documento particular, que foi equiparado ao cartão de crédito ou débito.

Já em um âmbito civilista, em 2014 tivemos a Lei do Marco Civil Regulatório da Internet: 12.965/2014. Os casos de crimes contra a honra começaram a se sofisticar, e o objetivo da lei veio para regulamentar sobre o uso da internet no Brasil, sobretudo, em razão entre usuário e provedor de internet e empresas.

Atendendo o inciso XLIII do artigo 5º da CF/88, o legislador em 2016 tipificou o crime de terrorismo e cyber terrorismo no art.2º da Lei 13.260-2016):

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XLIII - a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática da tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem; (Regulamento)

art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

Analisando os dispositivos seguintes, é perceptível que o legislador poderia ter atuado com mais taxatividade, visto a complexidade da temática. O uso de expressões vagas como: “guardar, portar ou trazer consigo” (...), prejudica de certo modo o instituto da legalidade.

Antes de adentrar na explanação sobre esse crime, é necessário antes conceituar os termos “*hacker*” e “*cracker*.” Deve ser compreendido de Crespo, que a origem da palavra *hacker* surgiu nas grandes universidades dos EUA, nos propriamente ditos como institutos de tecnologia, são pessoas que detêm com propriedade o manejo do conhecimento tecnológico e conseguem realizar invasões, acessar elementos sigilosos, embora essa não seja a ideia, pois eles geralmente trabalham com a área da informática, engenharia, e implementam programas, sistemas operacionais, etc. Já os *crackers*, são especialistas em usar o conhecimento para conseguir benefício próprio, como por exemplo proveito financeiro, invasão de dados e destruição de informações, ataques a instituições, serviços públicos e privados, etc. (CRESPO, 2011)

No art 2º, o ciberterrorismo pode ser explicado como ações de “terror” dos crackers que põe em risco a incolumidade pública, ao coletivo e ao patrimônio.

Em se tratando da defesa do consumidor, em 2018, com a problemática do grande número de vazamento de dados pessoais, eis que chega a Lei Geral de Proteção de Dados Pessoais. Os dados pessoais careciam de uma proteção e a finalidade foi justamente de regulamentar o tratamento desses dados pessoais, tanto os presenciais, quanto os coletados no âmbito virtual, zelando pelos dados relacionados às pessoas naturais e jurídicas de direito público e privado.

A lei Geral de Proteção de Dados (LGPD), aprovada em 2018, mas que foi entrar em vigor a partir de 18 de setembro de 2020, prevê a imposição de processos regulatórios e até mesmo sanções administrativas e penalidades em caso de descumprimento de suas normas.

Também em 2018, veio a tipificação trazida na Lei nº 13.718/2018 – “Lei de Importunação Sexual”, que tratou do chamado “PORN REVENGE”: Divulgação de cena de estupro ou de cena de sexo ou de pornografia sem autorização da vítima (art. 218-C do CP):

Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro

ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Aumento de pena

§ 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.

Em 2019, pelo advento da Lei 13.964/2019 (“Pacote Anticrime”) e em 19/04/2021, pela derrubada do veto presidencial pelo Senado, entrou em vigência a pena triplicada quando o crime contra honra (Calúnia, Injúria e Difamação), é no meio digital, o § 2º do artigo 141 do Código Penal:

§ 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena. [\(Incluído pela Lei nº 13.964, de 2019\)](#) [\(Vigência\)](#)

O caso acima é a exemplificação do crime de Cyberbullying, tido como um dos crimes contra honra. Pode-se compreender das ideias de Segundo Bitencourt (2020), que o Direito Penal protege o bem jurídico da honra objetiva, por meio da caracterização do crime de calúnia, que diz respeito a conduta da pessoa que imputa, falsamente, fato tipificado e penalizado como crime a outrem.

Da mesma forma há previsão legal para conduta da pessoa que denegrir a imagem ou reputação de outra pessoa, divulgando algum fato ofensivo, assim estaremos diante do delito de difamação. Já quem ofende o decoro de outrem, incitando atributos ou qualidades negativas, defeitos, poderá responder pelo crime de injúria.

No ano de 2020 o CNJ editou a Recomendação 73/2020, de suma importância, que “orientou os órgãos do Poder Judiciário a adotarem medidas para a adequação dos tribunais às disposições da legislação de proteção de dados.”

Em 2021, o legislador buscou trazer mais inovações, acompanhando o cenário da COVID-19. Foi promulgada a lei da Perseguição no meio digital ou chamada de “CYBERSTALKING” - LEI Nº 14.132, DE 31 DE MARÇO DE 2021), que foi inserida no artigo 147-A do Código Penal, com as devidas majorantes.

Art. 147-A. 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. (Incluído pela Lei nº 14.132, de 2021)
Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
(Incluído pela Lei nº 14.132, de 2021)

§ 1º A pena é aumentada de metade se o crime é cometido: (Incluído pela Lei nº 14.132, de 2021)

I – contra criança, adolescente ou idoso; (Incluído pela Lei nº 14.132, de 2021)

II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código; (Incluído pela Lei nº 14.132, de 2021)

III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. (Incluído pela Lei nº 14.132, de 2021)

§ 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. (Incluído pela Lei nº 14.132, de 2021)

§ 3º Somente se procede mediante representação. (Incluído pela Lei nº 14.132, de 2021)

Violência psicológica contra a mulher (Incluído pela Lei nº 14.188, de 2021)

Outro ponto positivo desse dispositivo é a devida proteção ao bem jurídico da liberdade, tanto pessoal, quanto integridade física da vítima.

Justamente com aumento expressivo das fraudes virtuais, que se deram com a pandemia, foi promulgado a Lei Nº 14.155, DE 27 DE MAIO DE 2021. Houve a alteração de 3 tipos penais.

A invasão de dispositivo informático 154-A da Lei 12.737 (crime informático próprio) que definiu a pena de 1-4 anos, melhorou a redação que antes era dúbia e também majorou as penas do §2 e §3. Quanto ao parágrafo 2º, trata da invasão que causa prejuízo econômico, aumentou de $\frac{1}{6}$ a $\frac{1}{3}$ para $\frac{1}{3}$ a $\frac{2}{3}$. Fato esse que pode possibilitar uma prisão preventiva, o que não é possível se o delito for cometido apenas nos termos do caput. O parágrafo 3º, traz uma modalidade qualificada desse delito:

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: [\(Incluído pela Lei nº 12.737, de 2012\)](#)
[Vigência](#)

A modificação pelo legislador foi bem efetiva e recrudescer a pena anterior que era de 6 meses a 2 anos, para 2 a 5 anos.

É válido destacar a alteração feita na redação do art 154-A, dada pela Lei 14.155, de 27 de maio de 2021:

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: [\(Incluído pela Lei nº 12.737, de 2012\)](#)

~~Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa~~

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: [\(Redação dada pela Lei nº 14.155, de 2021\)](#)
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)

A lei também incluiu uma nova modalidade de furto qualificado mediante emprego de meio eletrônico, adicionando o parágrafo § 4º-B no art. 155º do Código Penal, que vai de 4-8 anos e multa e as suas devidas majorantes no -§ 4º-C, que dizem respeito a utilização de servidor mantido fora do território nacional ou se o crime é praticado contra idoso ou a vulnerável.

§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado 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. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

A inovação acima é de extrema importância, pois enquanto o art.154-A, requer para sua tipicidade a violação de um mecanismo de segurança, uma senha por exemplo, o Furto Qualificado mediante fraude na internet, não necessita dessa violação ou se quer qualquer programa malicioso.

Em se tratando dos famosos golpes digitais, como por exemplo o “GOLPE DO PIX” foi incluída uma nova modalidade qualificada de estelionato (Fraude Eletrônica), que pode ser chamado também de “Estelionato Digital”, com isso acrescentando dois novos parágrafos no artigo 171 do CP, o § 2º-A e § 2º-B e aumentou a causa de aumento do §4º, que trata do Estelionato contra o idoso ou a vulnerável.

Estelionato

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

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. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

§ 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. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

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. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

Por fim, uma recente e essencial alteração feita em 10 de fevereiro de 2022, o Congresso Nacional promulgou a Emenda à Constituição 115, que incluiu a proteção de dados pessoais como direito fundamental. Essa emenda foi resultado da Proposta de Emenda à Constituição 17/2019, que houve aprovação em ambas as Casas Legislativas. Em decorrência disso, no artº 5 da Constituição Federal (1988), que traz o rol dos direitos individuais e coletivos, Direitos e Garantias Fundamentais, ele passa a prever no inciso LXXIX – “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

Além disso, no art.22 da Constituição Federal que trata da competência privativa da União legislar, foi incluído o inciso XXX que diz sobre a proteção e tratamento de dados pessoais.

Discorrendo mais sobre essas inclusões, antes da EC 155, a Lei Geral de Proteção de Dados (2018), estava sujeita a alterações legislativas, inclusive para revogar a proteção trazida em seu texto. No presente momento, insta salientar que Direitos e Garantias Individuais são cláusulas pétreas, ou seja, não pode posterior lei ou (PEC) suprimir esses direitos já previstos, apenas podem ser alterados com a finalidade de aprimorá-los. Quanto ao inciso XXX, é permitido uma lei complementar posterior, autorizando os Estados e ao DF, legislar sobre questões mais específicas sobre essa matéria. Nota-se que o Estado está se adequando aos fundamentos instituídos pela Lei Geral de Proteção de Dados Pessoais nº 13.709/2018, com o caráter de direito fundamental.

É de relevância reconhecer a mudança das relações sociais, e de que novas práticas estão surgindo nesse tempo, tanto no Brasil como no mundo. Diante de toda gradual evolução ao longo dos anos, o Direito Penal e o ordenamento jurídico Brasileiro, acompanha atento a essa evolução e trata dessas novas formas de criminalidade tanto num aspecto doutrinário quanto de forma legal.

4.1 Cooperação entre os órgãos

Os avanços constantes e surpreendentes da Tecnologia da Informação e Comunicação causaram uma verdadeira revolução na interação de pessoas, questões econômicas, políticas e jurídico-sociais. Porém, em contrapartida, podem ser utilizados de forma criminosa, gerando um efeito erga omnes em determinados casos como por exemplo em invasões a órgãos ou instituições públicas.

Nesse cenário, a Polícia Federal por meio do Serviço de Repressão a Crimes Cibernéticos (SRCC) e com a Diretoria de Investigação e Combate ao Crime Organizado (DICOR), coordena e articula todos os esforços, em nível nacional e internacional, para prevenir e reprimir tais crimes. Segundo matéria publicada em 25/02/2022 pelo Ministério da Justiça e Segurança Pública, a Polícia Federal realizou uma reunião inédita com cerca de 20 instituições incluindo entre elas o Banco do Brasil, Caixa Econômica, Santander, Federação Brasileira de Bancos (Febraban), XP, Mercado Livre, Zetta e ainda associações financeiras, de crédito e do varejo. A finalidade foi de divulgar um projeto de cooperação para o enfrentamento das ameaças cibernéticas com a futura criação de uma Força-Tarefa tanto do setor público e privado, com o intuito de gerar maior proteção de dados pessoais e financeiros dos cidadãos.

Quanto ao papel do MP dos Estados, Os Centros de Apoio Operacional das Promotorias de Justiça (CAOs), juntamente com as ações investigativas dos Órgãos de Segurança Pública e de seus setores de inteligência, fomentam a efetividade e repressão desses delitos. O MPF tem atuação assegurando o equilíbrio da proteção e privacidade no tratamento dos dados pessoais juntamente com a efetividade da persecução penal, inclusive em nível internacional.

Por fim, em relação a jurisprudência apresentada pelo Supremo Tribunal de Justiça (STJ), vale citar a tese de que é ilícita a prova obtida diretamente dos dados armazenados no celular do acusado, sem prévia autorização judicial. Conforme (RHC 89.981), foi anulado pelo STJ, provas que foram obtidas por agentes policiais que acessaram as mensagens no telefone de um suspeito que indicavam o repasse de informações sobre imóveis onde uma organização criminosa pretendia cometer furtos. Quanto ao crime de furto mediante transferência em meio eletrônico, a Terceira Seção do STJ pacificou o entendimento de que a competência é definida pelo local onde o bem foi subtraído da vítima, de acordo com o Conflito de Competência 145.576.

Nos crimes de Cyberstalking, ameaças feitas por meio digital em redes sociais, o STJ tem decidido que o juízo competente para julgamento de pedido de medidas

protetivas será aquele de onde a vítima tomou conhecimento das intimidações, por ser este o local de consumação do crime previsto no artigo 147 do Código Penal. (CC 156.284). É válido ressaltar que, o art.70º do CPP está em conformidade com essa decisão.

Outra decisão que foi pacificada pelo STJ, foi a diferenciação do furto mediante fraude no meio virtual e fraude eletrônica (“Estelionato Digital), na qual para configurar o estelionato, a vítima tem que ser induzida ao erro, e no caso do furto qualificado mediante emprego de meio eletrônico, a fraude é utilizada para burlar a vigilância da vítima.

4.2 Convenção de Budapeste

Em tempo de sociedade da informação, observamos o surgimento de nova classe de bens jurídicos, relacionados à segurança de dados, como previsto na Convenção de Budapeste, a “confidencialidade, a integridade e a disponibilidade de sistemas de computador, redes e dados de computador.”

No mundo, a maior implementação em se tratando da proteção e combate ao cibercrime é o Convênio de Budapeste. O Convênio foi criado pelo Conselho da Europa, em Budapeste em 23 de novembro de 2001 e foi o primeiro tratado internacional sobre os chamados cibercrimes. É composto por 66 países signatários, e por mais 158 como modelo para as suas legislações nacionais. Tem por seu objetivo fazer com que os países signatários implementem normas de direito material e de cooperação internacional, na qual os órgãos governamentais passam a contar com uma série de ferramentas, que tornarão mais eficaz o combate aos crimes cibernéticos no Brasil.

Foi promulgado pelo presidente do Senado e do Congresso Nacional, Rodrigo Pacheco em dezembro de 2021, o Decreto Legislativo (DL 37/2021), que teve sua origem no PDL 255/2021, com o senador Nelsinho Trad (PSD-MS) como relator, e o projeto foi aprovado pela Câmara e pelo Senado. O processo de andamento do tratado está em fase que precisa da assinatura do chefe do Poder Executivo para a ratificação, por meio de um Decreto-Lei e posteriormente a publicação no Diário Oficial da União.

5. CONCLUSÃO

A lei penal brasileira, durante muito tempo foi escassa no sentido de não garantir uma efetiva proteção em relação aos crimes decorrentes das novas TIC's. Situação essa que se alterou, tendo em vista o avanço pontual do ordenamento jurídico em relação a proteção contra o cometimento dos crimes cibernéticos.

Porém foi constatado que, o simples fato da tipificação ou previsão excessiva de parte do legislador para repressão desses delitos, não contribuiu para a diminuição do número exponencial dessas modalidades ao longo dos anos. Isso dá com a comprovação aos recorrentes casos que surgem no decorrer do tempo, exemplificando, os ataques reiterados a diversos órgãos públicos, como o TSE, STJ, STF, Ministério da Saúde, a empresas privadas e no âmbito social aos próprios usuários de serviços diversos.

A realidade trazida pela pandemia da Covid-19, pôs em amostra a necessidade pela busca tanto pelo avanço da proteção dos dados pessoais, quanto aos dados informáticos.

O autor Marcelo Xavier de Freitas Crespo, assume papel fundamental ao contribuir com a tese firmada ao longo do artigo de que há segurança jurídica no âmbito cibernético e a lei penal já é efetiva, mas para o enfrentamento dessa realidade pelo legislador e pela sociedade tem que dizer a respeito de utilizar um “novo olhar” jurídico-social perante à essas inovações.

O Brasil age com um grande papel visando a repressão do delito digital, mas falha fundamentalmente em aplicar medidas de prevenção à longo prazo. Tendo em vista a explanação, urge medidas com um enfoque mais de conscientização da educação digital de todos os usuários, para contornar a problemática vigente. Com as relações pessoais tão fluidas, o que ocorre é que, se tem um grande número de usuários conectados diariamente, por longas horas as redes de conexão, porém, não buscam por uma cultura de prevenção desses delitos. A própria coletividade tem que ter um papel mais ativo, desestimulando a atividade criminosa com o uso de canais de denúncia fornecidos tanto pela Polícia Civil, Polícia Militar, Coordenadorias Estaduais de Combate aos Crimes Cibernéticos e a SaferNET.

A sociedade tem que estar mais preparada para situações envolvendo a Engenharia Social. Em se tratando dessas práticas relacionadas aos crimes digitais, é o nome que se dá a um conjunto de subterfúgios pelos quais os possíveis criminosos conseguem inúmeros dados pessoais de determinada vítima. A pessoa passa a ter confiança no discurso de modo que ela não percebe que está sendo submetida a um

erro, uma enganação. Tais situações poderiam ser evitadas com uma simples mudança comportamental da sociedade, seja com o disposto no parágrafo acima, ou como não fornecer informações pessoais a desconhecidos, fazer o uso de senhas fortes e autenticadores de dupla-verificação, manter os sistemas operacionais atualizados, estar atento a URL's enviadas por email, SMS ou Whats App, realizar backup's de conversas mensalmente, entre outras medidas de proteção.

O tema vai continuar sendo passível de mudanças, mas o Estado deve continuar buscando convênios entre órgãos, parcerias público-privada, incentivos em relação a melhoria do quadro de aparelhamento policial e o aperfeiçoamento de técnicas com a possibilidade de cooperação entre os agentes a nível estadual, federal e internacional, para assim lidar de frente com essa problemática abordada ao longo do presente artigo.

REFERÊNCIAS

BAUMAN, Zygmunt. **Modernidade Líquida**. 1ª.ed. Rio de Janeiro: Zahar, 2001

BECK, Ulrich. **Sociedade de Risco**. 2ª.ed. São Paulo: Editora 34 Ltda, 2011.

BITENCOURT, Cezar Roberto. **Parte geral** – Coleção Tratado de direito penal volume 1 - 26. ed. São Paulo: Saraiva Educação, 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado,1988.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 abr. 2022.

BRASIL. Lei nº 11.829, de 25 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, 26 nov. 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm . Acesso em: 22 abr. 2022.

BRASIL. Lei 12.735, de 30 de novembro de 2012. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, 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, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 23 abril. 2022.

BRASIL. Lei 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.** Diário Oficial da União, Brasília, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20112014/2012/lei/l12737.htm>. Acesso em: 23 abril. 2022.

BRASIL. Lei 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Diário Oficial da União, Brasília, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm>. Acesso em: 23 abril. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acesso em: 22 abr. 2022.

BRASIL. Lei nº 13.718 de 24 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, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, 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).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm> Acesso em: 22 abr. 2022.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. **Aperfeiçoa a legislação penal e processual penal.** Brasília, DF: Presidência da República, 2019b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm>. Acesso em: 22 abr. 2022.

BRASIL Lei n. 14.155, de 27 de maio de 2021. Alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (**Código Penal**). Diário Oficial da União, Brasília, 28 maio 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993>. Acesso em: 22 abr. 2022.

BRASIL sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. **Fortinet**, São Paulo, 08/02/2022, Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/brasilsofre-mais-16-2-bilhoes-tentativas-ataques-ciberneticos-na-primeira-metade-2021> . Acesso em: 23 abr. 2022.

CLARKE, Richard A; KNAKE, Robert K. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito.** 1ª. ed. Brasport, 2015.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

CONVENÇÃO SOBRE O CIBERCRIME. Conselho da Europa. Budapeste, 23 nov.

2001. Council of Europe. Disponível em: <<http://conventions.coe.int/treaty/EN/Treaties/PDF/185-POR.pdf>>. Acesso em: 10 abr. 2022.

CRIMES PELA INTERNET, NOVOS DESAFIOS PARA A JURISPRUDÊNCIA. Supremo Tribunal de Justiça, Brasília, 17 jun. 2018. Disponível em: <http://www.stj.jus.br/sites/porta/p/Paginas/Comunicacao/Noticias/antigas/2018/201806-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx> Acesso em: 23 abril. 2022.

DURKHEIM, Émile. **As Regras do Método Sociológico**. 9ª. ed. Barcarena: Editorial Presença, 2004.

Estelionato digital: MPMG intensifica atuação para combater golpes pelo WhatsApp em MG. **MPMG**, 2021. Disponível em: <<https://www.mpmg.mp.br/portal/menu/comunicacao/noticias/estelionato-digitalmpmg-intensifica-atuacao-para-combater-golpes-pelowhatsappem-mg8A9480687CEBDB46017CF0ECEB305789-00.shtml>> . Acesso em: 23 abr. 2022.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Editora Saraiva, 1ª. ed. 2016.

JONH Draper. **Stringfixer**, Disponível em: < https://stringfixer.com/pt/John_Draper> . Acesso em: 23 abr. 2022.

JUNIOR, Lhonidas Senna. **Alan Turing**. Unicentro, [S.l.] 23 abr. 2022. Disponível em: <https://www3.unicentro.br/petfisica/2019/03/29/alan-mathison-turing-1912-1954/#top>. Acesso em: 23 abr. 2022.

LATTO, Nica. Worm X Vírus: descubra as diferenças e os perigos dessas ameaças. **Avast**, [S.l], Disponível em : < <https://www.avast.com/pt-br/c-worm-vs-virus>>. Acesso em: 23 abr. 2022.

LÉVY, Pierre. **Cibercultura**. 1ª. ed. São Paulo: Editora 34 Ltda, 1999.

MATEMÁTICO que decifrou código nazista estampa nota de £ 50. **DW News**, [s.i], Disponível em: <<https://www.dw.com/pt-br/matem%C3%A1tico-que-decifrou-c%C3%B3digo-nazista-vai-estampar-nota-de-50-libras/a-49605884>>. Acesso em 23 abr. 2022.

O que fazemos? **SAFERNET**, [s.i]. Disponível em: < <https://new.safernet.org.br/content/o-que-fazemos>> . Acesso em: 23 abr. 2022.

ROBERT Tappan Morris Worm. **Tacet Global**, [s.i], 14 jan. 2021. Disponível em: < <https://tacetglobal.com/robert-tappan-morris-worm/>> . Acesso em 23 abr. 2022.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

UM marco na regulamentação sobre dados pessoais no Brasil. **STJ**, [s.i], Disponível em: < <https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-dedados-pessoais-lgpd>>. Acesso em 23 abr. 2022.