

OS CRIMES CIBERNÉTICOS NO CONTEXTO DA PANDEMIA DO COVID-19

Beatriz Zuqui Nunes

Graduando em Direito
biazuqui14@hotmail.com

Rafael Martins Togneri

Professor Orientador Bacharel em Direito, Advogado, Pós-Graduado em Direito Penal e Direito Processual Penal
rafaeltog@hotmail.com

RESUMO

Os crimes cibernéticos são caracterizados por atos criminosos realizados através da internet, originados no ambiente virtual. E com o advento da Pandemia de Covid-19 e o consequente isolamento social, houve também um uso ainda mais intenso e prolongado da internet, o que, por sua vez, favoreceu a prática de crimes dessa natureza. Em contraponto, durante o mesmo período os crimes de roubo, de natureza não virtual, sofreram diminuição. Nesse contexto, o presente estudo tem como objetivo principal retratar o fenômeno dos crimes cibernéticos ocorridos durante a pandemia do Covid-19, suas consequências, bem como possíveis formas de prevenção e controle desses crimes.

Palavras-chave: Pandemia do Covid-19; crimes cibernéticos; leis; ambiente virtual.

1 INTRODUÇÃO

O crime cibernético pode ser conceituado como um crime econômico com amplitude global, de complexa identificação e rastreamento, cujos riscos e recompensas muitas vezes diferem do crime convencional (BENSON; MCALANEY; FRUMKIN, 2018). São caracterizados por atos criminosos realizados através da internet, que foram originados no ambiente virtual e que trazem a sensação de facilidade, unanimidade, velocidade de operação e uma enorme quantidade de alvos ao mesmo tempo (BURDEN; PALMER, 2003).

Todo o contexto relacionado aos crimes cibernéticos tem importante relação com o período da Guerra Fria. Esse momento foi contundentemente marcado pelo surgimento da grande rede de comunicação, conhecida hoje como internet. A disputa acirrada entre os Estados Unidos da América e a União Soviética, com a intenção de garantir vantagens, culminou no desenvolvimento de uma rede de comunicação avançada (CASTELLS, 2003). No Brasil, relata-se o início do uso da internet por volta da década de 80, quando as Universidades brasileiras começam a compartilhar algumas informações com os Estados Unidos. Porém, seu uso se concretizou após o primeiro investimento brasileiro, direto com a Microsoft de Bill Gates, quando as empresas se uniram em torno do objetivo comum de desenvolver novos serviços Web no Brasil (DIANA, 2019).

Paralelamente ao início da internet e ao desenvolvimento dos benefícios por ela oferecidos, surge a conduta criminosa, que se aperfeiçoa na mesma proporção da evolução da internet. Os primeiros crimes virtuais são relatados na década de 1960, onde os infratores manipulavam os dados contidos nos computadores, praticando atos de sabotagem, espionagem e abuso ilegal de

sistema de computadores (NASCIMENTO, 2006).

A prática dos crimes virtuais, denominados crimes cibernéticos, ganhou maiores proporções à medida que as redes de internet se tornaram mais acessíveis. Atualmente, o mundo vive um importante momento relacionado à saúde, que é a pandemia da Covid-19, ainda não totalmente controlada. Nesse contexto, Nagli (2020), defende a ideia de que a pandemia da Covid-19 criou condições para o surgimento de uma outra pandemia dentro da pandemia, neste caso criada pelos crescentes ataques cibernéticos, gerados pelo elevado número de usuários conectados às redes nesse período. Portanto, compreender a influência da pandemia da Covid-19 sobre os crimes cibernéticos pode fornecer subsídios para aprimorar o monitoramento e desenvolvimento de medidas que reprimam a prática de condutas ilícitas via internet, regulamentando leis eficazes ao combate a crimes cometidos sob a utilização da rede mundial de computadores.

Em razão disso, é fato que o aumento da acessibilidade às redes virtuais cada vez mais favorece a vida das pessoas, facilitando a interação social, o crescimento econômico, o desenvolvimento educacional e a qualidade de vida de forma geral. Porém, ao mesmo tempo que o favorecimento acontece, a internet também vem sendo utilizada para realização de crimes virtuais. De forma geral, em virtude do período de pandemia, o acesso à internet, que já era crescente, pode se expandir de forma mais intensa e pode ter trazido consigo o aumento da realização de crimes virtuais, chamados então de crimes cibernéticos.

2 REFERENCIAL TEÓRICO

Desde o avanço tecnológico decorrente da Terceira Revolução Industrial, foi possível perceber o seu efeito nas relações tecnológicas de informação e comunicação, destacando o desenvolvimento da internet, o que propiciou a conexão de dados, e causou o aumento das interações pessoais nesse meio virtual (SANTOS, 2021). Da mesma forma que ocorreu esse aumento tecnológico, o Direito Penal não permaneceu ileso, pois é possível constatar a possível cultura delinquente do perigo exposto nesse ambiente (SANTOS, 2021).

Sendo assim, é importante compreender que crime consiste numa violação à lei penal, que pode atingir uma ou diversas pessoas ao mesmo tempo. Com isso, os crimes cibernéticos, também chamados de virtuais, são atividades ilícitas que tem como alvo um aparelho conectado à rede atingindo inúmeras pessoas (COSTA, 2020).

À medida que os atos criminosos na internet foram ganhando maior proporção, o mundo percebe a necessidade de se mobilizar quanto a isso e discutir o assunto.

Em 1990, em Havana, a ONU – Organização das Nações Unidas, no 8º Congresso sobre Prevenção de Delito e Justiça Penal, elaborou uma relação de crimes relacionados aos meios informáticos. São eles: 1º - fraudes cometidas através de manipulação de computadores; 2º - falsificações informáticas; 3º - danos ou modificações de programas ou dados computadorizados (ONU, 1990).

No ano 2000, a ONU relacionou outros tipos de crimes cibernéticos, elaborados no 10º Congresso sobre Prevenção de Delito e Tratamento de Delinquente, realizado em Viena, os quais seguem a baixo:

1º - espionagem industrial para descoberta de segredos comerciais, técnicas e estratégias; sabotagem de sistemas; 2º - sabotagem e vandalismo de dados; 3º - lavagem de dinheiro; 4º - jogos de azar;

fraudes, principalmente contra consumidores; 5º - pornografia infantil; 6º - estratégias, com intuito de buscar sistemas restritos; 7º - averiguação de senhas secretas (ONU, 2000).

Nesse contexto da mobilização mundial contra os crimes cibernéticos, é importante destacar a Convenção Europeia sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, elaborada em 2001, pelo Conselho da Europa (Council of Europe), órgão intergovernamental que engloba 45 Estados membros, inclusive os membros da União Europeia. Essa convenção, marca o primeiro tratado internacional sobre crimes cometidos através de sistemas de computadores e objetiva uniformizar as normas de combate à prática destes crimes (NASCIMENTO, 2016).

O Brasil, por sua vez, já regulamentou algumas normas com a finalidade de regulamentar o uso da internet pelos seus usuários e criminalizar condutas ilícitas praticadas via internet. As principais são: Lei Carolina Dieckmann (Lei nº 12.737/2012), sancionada em dezembro de 2011, pela Presidente Dilma Rousseff, criada após a divulgação indevida de imagens íntimas da atriz Carolina Dieckmann, na internet, e considerando o avanço da tecnologia e o acesso facilitado às redes sociais, inclui ao Código Penal, o primeiro texto que tipificou os delitos virtuais, protegendo vítimas de compartilhamento de dados e imagens, tendo foco nas invasões a dispositivos sem a permissão do usuário. Outra Lei vigente no País é a Lei Marco Civil da Internet (Lei nº 12.965/2014), aprovada em abril de 2014, também pela Presidente Dilma Rousseff, a qual estabelece princípios, garantias e proteção uso de dados pessoais, regulamentando os direitos e deveres dos usuários da internet. A Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), incorporada ao ordenamento jurídico em maio de 2021, vetada pelo Presidente Michel Temer e posteriormente postergada a vigência devido ao surto mundial de coronavírus, é também importante para a proteção de pessoas físicas e jurídicas, principalmente consumidores, regulamentando direitos dos titulares de dados pessoais e a responsabilidade de seus operadores, aplicando sanções pelo uso indevido.

3 METODOLOGIA

Trata-se de uma revisão bibliográfica, do tipo narrativa. A coleta de dados foi realizada nas bases da Scielo, Portal de Periódicos CAPES, CONPEDI, site do Planalto e dissertações e teses publicadas. O estudo buscou principalmente responder as seguintes perguntas: Quais as causas do aumento de crimes cibernéticos durante a pandemia da Covid-19? Quais crimes cibernéticos sofreram aumento? Quais as consequências do aumento desse tipo de crime? O que já foi feito e o que ainda é possível fazer para reduzir a ocorrência de crimes dessa natureza? Para coleta, as seguintes palavras chaves foram utilizadas: crimes cibernéticos, Pandemia COVID-19, leis, também descritos em inglês: cyber crimes, pandemic covid-19, laws. Foram aplicados os descritores booleanos OR ou AND para realização da busca. Todos os artigos publicados entre os anos de 2019 a 2022, nos idiomas português e inglês foram selecionados para a leitura inicial, assim como todas as leis disponibilizadas no site do Planalto. Segundo Rother, 2007, a revisão narrativa não utiliza critérios explícitos e sistemáticos para a busca e análise crítica da literatura. A busca pelos estudos não precisa esgotar as fontes de informações. Não aplica estratégias de busca sofisticadas e exaustivas. A seleção dos estudos e a interpretação das informações podem estar sujeitas à subjetividade dos autores. Para este estudo, após a leitura dos títulos,

os artigos que responderam os objetivos foram selecionados para a leitura dos resumos e posteriormente a leitura na íntegra.

4 RESULTADOS

4.1. O aumento dos crimes cibernéticos durante a pandemia da Covid-19.

No final de 2019, com o início da Pandemia da Covid-19, a sociedade passou por um momento de isolamento social. O vírus da Covid-19 surgiu de forma repentina e, devido ao número alto de contágios, precauções tiveram que ser tomadas para controlar o contato físico e evitar a maior propagação (SOUZA; ALMEIDA, 2020).

Deste modo, as atividades que eram praticadas fora de casa, se adequaram ao novo cenário adotando aulas remotas, trabalhos em *home office*, cursos *online*, jogos, compras, entre outros, o que possibilitou o maior número de informações e dados compartilhados em bancos de cadastros, também por um tempo maior de acesso (COSTA; MENEGHETTI; MAIA, 2020).

Para Gabriel Chiovetto Carvalho (2019) “a internet nunca foi tão necessária como é agora, e a utilização de diversos dispositivos tecnológicos fizeram com que o acesso à rede se tornasse fundamental e constante”. Por isso desde março de 2020, período do primeiro *lockdown*, os crimes virtuais estão aumentando cada vez mais nas plataformas digitais (COSTA; MENEGHETTI; MAIA, 2020).

Antes da pandemia do Covid-19, os crimes cibernéticos já tinham grande incidência, porém desde o início do isolamento esses dados só aumentaram, trazendo grande preocupação para os países (COSTA; MENEGHETTI; MAIA, 2020).

Com base nas declarações da Secretaria de Estado de Segurança Pública do Distrito Federal – DF (2020), entre janeiro e junho do ano de 2020, os números de ocorrências relacionados aos crimes virtuais aumentaram, especificamente quanto ao crime de estelionato virtual, em 347%, se comparado ao ano de 2021, em consequência da pandemia da Covid-19. Segundo esses dados, os casos mais frequentes envolvem o aplicativo de mensagens WhatsApp (BRASIL, 2020).

Levantamentos feitos pela Federação Brasileira de Dados – FEBRABAN (2020), registraram aumento de 80% nas tentativas de ataques de *phishing* e aumento de 70% nos golpes do falso funcionário e falsas centrais telefônicas (BRASIL, 2020).

De acordo com o Governo do Estado do Mato Grosso do Sul (2022), em 2020, segundo dados da Central Nacional de Denúncias de Crimes Cibernéticos, o Brasil estimou cerca de 156.692 casos de denúncias relacionadas a crimes cibernéticos. O mais frequente foi o crime de estelionato, que em Mato Grosso do Sul, por exemplo, dobrou o número de casos (MATO GROSSO, 2022).

Os crimes virtuais cometidos são de ampla dimensão. Os casos mais recorrentes e que se destacaram na pandemia foram: O racismo (art. 140, §3º, CP) que consiste na ofensa a honra subjetiva de uma pessoa em razão da cor, raça, religião, etnia e origem nos meios virtuais. A pornografia infantil (art. 241-E do ECA) que ocorre com crianças e adolescentes em atividades sexuais de forma real ou simulada e o estupro virtual (art. 213, CP) com o constrangimento, mediante violência ou grave ameaça, a praticar com ele ato libidinoso. Além deles, os crimes contra o patrimônio (art. 158, CP) foram constantes, pois são através dos dados e das informações pessoais que os criminosos têm acesso a eles. E

por fim, os crimes contra a honra: calúnia (art. 138 do CP), difamação (art. 139 do CP) e injúria (art. 140 do CP) que ainda são muito frequentes no ambiente virtual (VIEIRA; REZENDE, 2020).

Outrossim, segundo dados da Gazeta do Povo (2020), outro golpe também frequente na pandemia foi a clonagem de conta de WhatsApp, onde o criminoso se passa por alguma empresa enviando códigos para a vítima colhendo dados pessoais até mesmo pedindo dinheiro, afinal de contas, pessoas em isolamento social e constantemente conectadas à internet são alvos fáceis para o cybercrime (VIEIRA; REZENDE, 2020).

Anteriormente à Pandemia da Covid-19, o Brasil, segundo relatório global publicado pela Symantec, era o terceiro país que mais sofria ataques cibernéticos ficando atrás apenas da China e dos Estados Unidos. Porém, com o implemento do sistema *Home Office* para trabalhar, estudar ou até mesmo distrair, a Anatel-Agência Nacional de Telecomunicações, informou um aumento de 40% a 50%, principalmente nos crimes de estelionato, extorsão e criação de páginas falsas (CRUZ, 2022).

Já relacionado a América Latina, o Brasil ocupou o segundo lugar com aumento de mais de 950% de ataques cibernéticos, chegando a registrar 289 bilhões de ataques no total (SILVA; MARINHO, 2022).

Em relação a esses ataques, alguns crimes foram mais frequentes, como o *Phishing* ou estelionato virtual, que é a prática criminosa de enganar pessoas para conseguir informações confidenciais delas, como dados e senhas. Na prática os criminosos enviam uma fonte confiável, fazendo as pessoas acreditarem ser verdadeiras, permitindo assim que tenham acesso ao sistema roubando a identidade virtual (NEVES; PEREIRA, 2021).

Dentre os ataques de *phishing*, os mais destacados foram: *Spear-phishing*, *Vishing* e *Smishing* (NEVES; PEREIRA, 2021).

- O *Spear-phishing* tem um alvo de ataques específico, assim os criminosos juntam as informações sobre a vítima e fazem elas acreditarem que o golpe é verdadeiro (NEVES; PEREIRA, 2021);
- O *Vishing* é a junção do *phishing* com a voz, ou seja, é um ataque aplicado através de ligações, aplicando a persuasão com o contato direto com a vítima (NEVES; PEREIRA, 2021);
- E o *Smishing* que é o ataque feito por meio de *Short Message Service* (SMS), fazendo a vítima acessar *links* ou *download* captando assim os dados pessoais dela (NEVES; PEREIRA, 2021);

O crime de *Stalking* também teve alto percentual de incidência durante a pandemia. É também conhecido como “crime de perseguição” e consiste em uma forma repetida de invasão à vida privada da vítima nas redes sociais, causando danos temporários ou permanentes à integridade emocional e psicológica a ela (SILVA; MARINHO, 2022).

O *Malware* ou sequestro de dados, também se tornou comum na pandemia devido aos sites maliciosos, que sequestram dados ou controlam o sistema por meio de um “vírus resgate”, infectando o dispositivo das vítimas, controlando suas ações e obtendo informações privadas (SILVA; MARINHO, 2022).

Diante disso, o progresso da tecnologia virtual de um lado facilita as comunicações, o trabalho, o estudo e a pesquisa, trazendo benefícios aos usuários conectados no mundo todo, mas, por outro lado, esses mecanismos eletrônicos criam oportunidades para os criminosos, causando danos a população. Antes da pandemia da Covid-19, os índices de crimes cibernéticos já tinham

grandes proporções, porém desde o início do isolamento os casos só se agravaram, pelo fato da dependência tecnológica que foi gerada para diversas pessoas (VIEIRA; REZENDE, 2020).

4.2. A influência da pandemia da Covid-19 no aumento dos crimes cibernéticos.

Tendo em vista a mudança social provocada pela pandemia da Covid-19, as atividades passaram a ser desenvolvidas no meio virtual. Com base nisso, Mendes et al. (2021) destaca a Teoria das Atividades Rotineiras, e ainda diz que: “o aumento da taxa de crimes não se fundamenta exclusivamente nas características dos criminosos, mas sim nas circunstâncias do meio em que estes se encontram”.

Desse modo, considerando todas as mudanças provocadas pelo isolamento social, o aumento e o surgimento de crimes virtuais se deram em razão das novas oportunidades surgidas por meio desse novo cenário (MENDES; FERREIRA; SANTOS, 2021).

No momento atual, compreende-se que os crimes cibernéticos são atividades que tem como meio o uso de computadores, celulares e outros aparelhos que podem ser conectados à rede de internet. Com isso, outros crimes como roubos e furtos passaram a ser menos frequentes e os crimes virtuais mais frequentes, levando os criminosos a se adaptarem a nova realidade (ALBRECHT; PEREIRA; PITON, 2021).

Um estudo recente, realizado por Dultra et. al (2021), evidencia a redução dos crimes de roubo e o aumento dos crimes de estelionato devido a permanência da população em casa durante o isolamento social:

De acordo com os autores, os resultados foram distintos para os crimes, sendo que, enquanto o roubo e o patrimônio apresentaram quedas no ano de 2020 em relação ao ano de 2019, o estelionato apresentou um aumento 47% no mesmo período. No mesmo estudo, foi salientado que o aumento dos crimes de estelionato pode ser explicado pelo fato de que grande parte da população permanece em casa, tornando-se suscetível aos crimes virtuais. (DULTRA et. al, 2021, p. 3)

De acordo com os estudos citados anteriormente, identifica-se que o desfecho da pandemia da Covid-19 foi caracterizado pelo aumento dos crimes cibernéticos, ao mesmo tempo em que crimes de roubo diminuíram devido à permanência da população em casa durante o isolamento social. Esse dado se faz importante pois colabora com o direcionamento da elaboração de leis e medidas de segurança mais específicas.

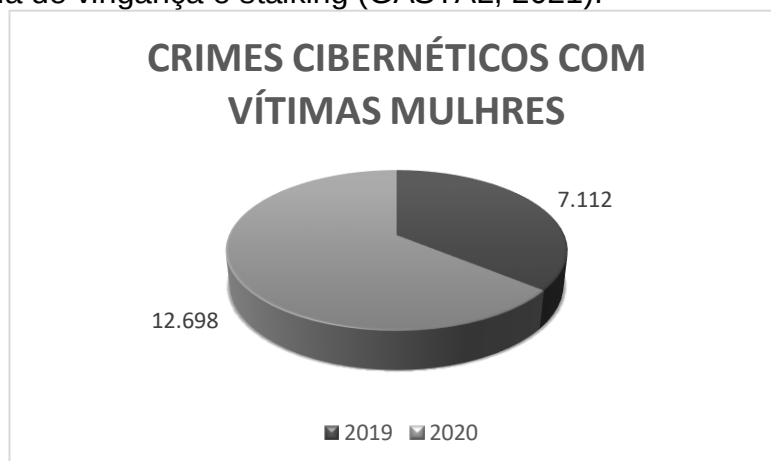
De acordo com Gastal (2021), no artigo publicado em *Women in Law Mentoring Brasil*, de janeiro a setembro de 2020 o Brasil já havia sofrido mais de 3,4 bilhões de tentativas de ataques na internet. Além disso, apresentou dados da Federação Brasileira de Bancos:

A Federação Brasileira de Bancos apontou ter havido um aumento de 80% nas tentativas de ataques de *phishing*, de 70% de golpes do falso funcionário e de falsas centrais telefônicas e de 60% em tentativas de fraudes contra idosos.

Especificamente em relação a crimes contra mulheres, da mesma forma como houve um crescimento vertiginoso de delitos no contexto doméstico e familiar [8], também ocorreu no universo digital (GASTAL, 2021).

Do ano de 2019 para 2020 os ataques de crimes cibernéticos com vítimas mulheres tiveram um aumento de quase 80%, com aumento de 5.586 registros, conforme dados abaixo, sendo os mais recorrentes os crimes de ameaça, contra

honra, pornografia de vingança e stalking (GASTAL, 2021).



Fonte: elaborado pelo autor, 2022.

Foram registradas também, segundo dados da Central Nacional de Denúncias de Crimes Cibernéticos com o Ministério Público Federal e a ONG Safernet, o aumento de 98.244 denúncias nos crimes relacionados a pornografia infantil e 156.692 denúncias nos outros crimes, dobrando o valor registrado no ano anterior que era de 75.671 (CARDOSO, 2022).

Desse modo, em março de 2020, período em que o Brasil estava passando por *lockdown* e as pessoas começaram a adotar o sistema *home office*, o país, nesse período, se tornou o mais atingido pelos crimes cibernéticos da América Latina, com 60% de ataques virtuais (CARDOSO, 2022).

Considerando isso, de imediato, não havia tempo hábil para que medidas de segurança fossem adotadas, mas com o decorrer da pandemia, foi e é de extrema importância se prevenir quanto aos sites falsos, evitando assim a consumação dos crimes cibernéticos. Por isso, é essencial pesquisar em sites confiáveis, inclusive em casos que envolvam crianças e adolescentes, procurando sempre fiscalizar as redes sociais e adaptar a faixa etária. Nesse caso, contra softwares sem boas intenções, é importante manter o dispositivo sempre atualizado com o pack de segurança e atualizar o antivírus. Dessa forma, a vigilância é uma forma de prevenção aos ataques de crimes virtuais (CARDOSO, 2022).

Deste modo, em razão da quarentena imposta pela pandemia da Covid-19, a segurança de dados e informações se tornou suscetível a violações. As pessoas tiveram que se adaptar à nova realidade e lidar com os equipamentos eletrônicos. Além disso, a aplicação de dados pessoais em plataformas, aplicativos e redes sociais também se tornaram frequentes. E assim, surgiram os ataques cibernéticos na pandemia da Covid-19 (BARBOSA et. al, 2021).

4.3. Leis relacionadas aos crimes cibernéticos, que colaboram com a segurança da população.

Antes da Pandemia da Covid-19, nos anos de 2012 e 2014, surgiram as primeiras leis de proteção contra os crimes virtuais no Brasil: A Lei Carolina Dieckmann (Lei 12.737/2012) e Lei do Marco Civil da Internet (Lei 12.965/2014), leis estas que deram início a prevenção aos crimes cibernéticos e que colaboraram com a segurança da população durante o período de isolamento social. Em 2018, foi aprovada e sancionada a Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018), que entrou em vigor em 2020 e é referência na

regulamentação de dados pessoais, tanto por pessoa física, quanto jurídica, nos meios virtuais, e protege a privacidade e a liberdade de cada uma delas (ALMEIDA et. al, 2020).

Dentre essas leis, a Lei Geral de Proteção de Dados (LGPD) foi imprescindível à defesa dos direitos fundamentais diante da utilização desenfreada de dados pessoais agravada pela pandemia da Covid-19 (GARCEL et. al, 2020).

Embora existam Leis em vigor, a necessidade de adotar políticas criminais atribuídas à prevenção e controle a esses crimes foi indispensável. Diante disso, em janeiro de 2021, o Brasil apoiou a Convenção de Budapeste, também conhecida como Convenção sobre Crimes Cibernéticos, proporcionando ao país acessos mais rápidos, além do apoio jurídico internacional, o que vem somar à Lei 12.965/2014 (AARÃO, 2021).

Em 2020, segundo dados da Polícia Civil (2020), o Pará foi o primeiro estado no Brasil a instituir a Diretoria de Combate a Crimes Cibernéticos (DECCC). O principal objetivo do órgão é a prevenção e a repressão dos delitos cometidos por redes digitais e outros meios tecnológicos que sofrem ações de ataques, subtrações e danificações ao patrimônio das pessoas (BRASIL, 2020).

O Governo Federal do Brasil (2022) anunciou que o Ministério da Justiça e Segurança Pública iniciou o primeiro Plano Tático de Combate a Crimes cibernéticos, visando medidas preventivas e educativas, com vistas a tornar o espaço cibernético mais seguro e penalizar as organizações criminosas que atual nesse tipo de crime (BRASIL, 2022).

Todas essas medidas foram necessárias, pois diversos tipos de crimes cibernéticos sofreram aumento e aperfeiçoamento durante o período da pandemia.

Além das medidas de prevenções adotadas, até o ano de 2012 não havia leis específicas para punir os crimes cibernéticos próprios, só existiam as que punem crimes cibernéticos impróprios, como já mencionado. Por isso, leis e atualizações legislativas foram necessárias para que houvesse a redução dos ataques virtuais (CARDOSO, 2022).

4.4. Leis de regulamentação e prevenção criadas durante a Pandemia da Covid-19.

Os crimes cibernéticos fazem menções a todos os crimes que se materializam no meio virtual. Podem ser classificados como: puros, quando possuírem finalidade de alcançar um sistema virtual, e mistos, quando o foco vai além do sistema e atinge a posse da vítima. Além disso, podem ser próprios, quando acontecem exclusivamente através de computadores, por exemplo, e impróprios quando atingirem também o bem comum da vítima. Considerando isso, a Legislação Brasileira não acompanha integralmente a diversidade de crimes cibernéticos existentes, mas pode aplicar analogia para não deixar o infrator impune, como a exemplo o crime de Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal) e Injúria (art. 140 do Código Penal). Além deles, o crime de Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Pedofilia (art. 240 e 241 da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96 e de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software ou vulgarmente

conhecido como “Pirataria” (art. 12 da Lei nº 9.609/98) e crime de Dano (art. 163 do Código Penal) (SANTANA, 2021).

Em 2021, o Presidente Jair Bolsonaro sancionou a Lei 14.132 de 2021 que tipifica o crime de perseguição ou crime de *stalking*, alterando o Código Penal e dando mais segurança às vítimas em decorrência de um crime que começa virtual e migra para perseguição física e psíquica da pessoa (AGÊNCIA SENADO, 2021).

Antes, a prática era apenas uma contravenção penal, que previa o crime como perturbação da tranquilidade alheia. Com a nova Lei, o crime passou a ter pena de 6 meses a 2 anos de reclusão e multa, com aumento de 50% quando contra crianças, adolescentes, idosos ou mulheres em razão do gênero. Também recebe essa punição em casos de uso de armas com participação de duas ou mais pessoas (AGÊNCIA SENADO, 2021).

O crime de perseguição (*stalking*) deve ser combatido antes que se torne algo mais grave, por isso foi necessária a criminalização com a validação dessa nova lei (SILVA; MARINHO, 2022). Segue a tipificação legal:

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. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. § 1º A pena é aumentada de metade se o crime é cometido: I – contra criança, adolescente ou idoso; II – contra mulher por razões da condição de sexo feminino, nos termos do §2º-A do art. 121 deste Código; III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. § 3º Somente se procede mediante representação (SILVA; MARINHO, 2022).

Segundo Pinheiro (2022), Greco analisa a liberdade pessoal e a natureza física e psíquica da vítima como os bens juridicamente protegidos no crime de *stalking*. As mulheres são as vítimas mais comuns, sendo o crime tratado como uma forma de violência contra mulheres em outros países. Nesse ponto, é importante relacionar o crime de perseguição com a Lei 11.340, de 2006, ou seja, Lei Maria da Penha, que apresenta diversas condutas em relação à violência psicológica e ameaças contra as mulheres.

Os crimes cibernéticos como fraude, furto e estelionato passaram a ser punidos com penas mais duras, através da Lei 14.155, de 2021, sancionada também pelo Presidente Jair Bolsonaro. O texto alterou o Código Penal agravando as penas de invasão de dispositivo, furto qualificado e estelionato ocorridos em meio digital (AGÊNCIA SENADO, 2021).

O crime de invasão de dispositivo informático passou a ser punido com reclusão, de um a quatro anos, e multa, e um terço a dois terços de aumento se resultar prejuízo econômico. Já se provocar obtenção de conteúdos sigilosos, a pena será de reclusão de dois a cinco anos, e multa (AGÊNCIA SENADO, 2021).

No caso do furto, a pena será de reclusão de quatro a oito anos, e multa, por acrescentar uma qualificadora por meio eletrônico ao Código Penal. A pena também poderá ser aumentada de um terço ao dobro, se for praticado contra idoso ou vulnerável e um terço a dois terços se for praticado com uso de servidor de informática de fora do país. O estelionato passou a ter pena de reclusão de quatro a oito anos, e multa, quando a vítima for enganada e fornecer informações por meio de redes sociais e tem o mesmo aumento de pena similar ao crime de furto (AGÊNCIA SENADO, 2021).

Portanto, na Pandemia causada pela Covid-19, devido ao aumento de utilização da internet e seus dispositivos, por conta do isolamento social, ocorreu a

modificação nos tipos penais, o que necessitou o aperfeiçoamento do Código Penal e do Código Processual Penal, alterando e incluindo tipos penais a essas leis, a fim de proteger os usuários dos crimes cibernéticos (PINHEIRO, 2022).

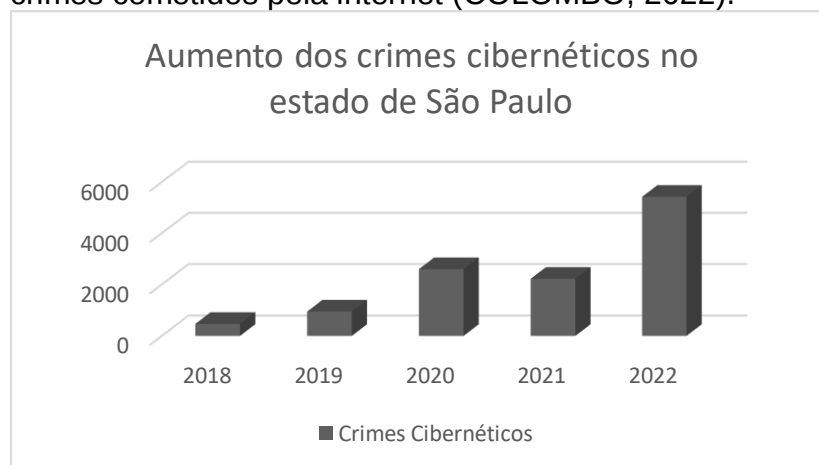
Diante disso, os avanços tecnológicos elaborados a partir da evolução da internet, os seres humanos também ampliaram as formas de comunicação e interação com a sociedade. Assim, a necessidade da evolução legislativa, se faz necessária, pois a internet se tornou imprescindível para as necessidades básicas do dia a dia, principalmente no momento de isolamento social. Por isso, é importante colocar em prática as inovações legislativas, bem como aprimorá-las no decorrer do tempo (PINHEIRO, 2022).

Finalmente, além das leis mencionadas, a modernização das polícias especializadas e do Poder Judiciário também foi necessária para que houvesse uma maior segurança jurídica virtual, pois, o número de casos, segundo a central Nacional de Denúncias de Crimes Cibernéticos, registrou do ano de 2019 até o ano de 2020, mais de 80 mil denúncias (PINHEIRO, 2022).

Por isso, as leis foram necessárias e, da mesma maneira, é importante que haja mais estudos, principalmente de outras áreas do direito, para que os crimes cibernéticos ocorram com menos frequência e quando ocorrerem, que o criminoso seja punido. Assim, é possível o aprimoramento das ferramentas legislativas e operacionais para combater ao crime, tanto real, quanto virtual (PINHEIRO, 2022).

Enfim, apesar de todas essas medidas, ainda é possível perceber um aumento dos crimes cibernéticos nos dias atuais. Segundo COLOMBO (2022), dados da Secretaria de Segurança Pública apontam que no estado de São Paulo os crimes cibernéticos aumentaram em 144% em relação ao ano de 2021 e ainda fez uma comparação desde antes da pandemia da covid-19 e o isolamento social até o ano de 2022.

Em 2018 foram registrados 468 casos; em 2019 foram registrados 945 casos; em 2020 aumentou mais que o dobro chegando a registrar 2.596 casos; em 2021 teve uma pequena queda para 2.219 casos e; em 2022 aumentou para 5.424 casos de crimes cometidos pela internet (COLOMBO, 2022).



Fonte: elaborado pelo autor, 2022

Diante disso, a aplicação da legislação e das medidas de prevenção devem continuar sendo aplicadas de forma mais severa, porém novas medidas poderão ser estudadas para beneficiar ainda mais a população sujeita a sofrer os crimes cibernéticos.

4.5. Demais medidas realizadas para regulamentação e prevenção dos ataques cibernéticos.

No dia 28 de junho de 2022, proposta pelo Ministério da Justiça e Segurança Pública (2022), apoiada pela Federação Brasileira de Bancos (Febraban), a Polícia Federal inaugurou a UEICC – Unidade Especial de Investigação de Crimes Cibernéticos, em parceria público/privada, para intensificar a repressão aos ataques cibernéticos e promover a busca de soluções e prevenções mais rápidas contra eles.

O Ministério da Justiça e Segurança Pública (2022) anunciou que além dos crimes cibernéticos relacionados a instituições bancárias, a UEICC também irá incentivar a repressão a pornografia infantil, os crimes contra instituições públicas, crimes contra operadores de telefonia, entre outros sofridos no ambiente virtual.

Em relação as fraudes bancárias, alvo dos criminosos cibernéticos, a Febraban criou um laboratório para simular ataques cibernéticos para conter fraudes, capacitando assim mais de quatro mil colaboradores. Esses dados serão compartilhados com a Polícia Federal, por meio de Acordo de Cooperação Técnica, intensificando assim o combate aos crimes virtuais (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2022).

Além disso, o Sindicato das Empresas de Seguro e Resseguros (2020) listou uma série de medidas de combate aos crimes cibernéticos durante o *home office*, dentre elas é importante destacar a manutenção de softwares, a atualização de navegadores web, a ativação de proteção contra vírus e firewalls, a alteração regular de senhas, dentre outros.

Para Meireles (2020), existe uma grande dificuldade em investigar e punir esses crimes, devido ao fato dos criminosos agirem de forma anônima e silenciosa, por isso a maior dificuldade está relacionada na identificação da origem do delito, na autoria e na materialidade, bem como na falta de conhecimento técnico das vítimas.

Outro motivo que dificulta a punição dos crimes virtuais é a ausência de capacitação dos profissionais para combater esses crimes. Além disso, as medidas legislativas isoladas por si só não são capazes de solucionar e prevenir os ataques cibernéticos (MEIRELES, 2020).

Por isso, diante das atualizações legislativas e demais medidas realizadas durante o início da pandemia até os dias atuais, os crimes cibernéticos ainda continuam aumentando. Mas considerando os esforços governamentais, a atuação da Polícia Federal e a criação das Unidades de Prevenção é possível ver resultados positivos para o futuro, diminuindo, dessa forma, os crimes cibernéticos.

5 CONCLUSÃO

A pandemia da Covid-19 foi caracterizada pelo aumento dos crimes cibernéticos, ao mesmo tempo em que crimes de roubo diminuíram devido à permanência da população em casa durante o período de isolamento social. Embora já existissem leis vigentes anteriores ao período pandêmico, a necessidade de se adotarem novas políticas criminais dedicadas à prevenção e controle a crimes dessa natureza se tornou indispensável nos últimos anos. Aliás, mesmo as inovações legislativas ocorridas no período analisado não foram suficientes para reduzir a prática criminosa em questão. No entanto, as investigações de novos crimes, assim como denúncias e novas pesquisas são ferramentas importantes para a atualização desses dados relacionados à

execução de crimes em ambientes virtuais. Com isso, novas medidas de segurança poderão ser estudadas, elaboradas e implantadas em benefício da população.

Portanto, no enfrentamento deste mal, para que se alcancem resultados efetivos, é necessário um esforço conjunto de diversas medidas, dentre elas o investimento em tecnologias de segurança virtual e monitoramento, educação dos usuários de dispositivos eletrônicos – por meio de campanhas publicitárias, por exemplo -, aumento do contingente policial e investigativo especializado e aperfeiçoamento legislativo.

REFERÊNCIAS

BENSON, V., McAlaney, J., & Frumkin, L.A. (2018). **Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape**. In Psychological and Behavioral Examinations in Cyber Security (pp. 266-271). IGI Global. Londres, 1 mar. 2018.

BURDEN, K., & Palmer, C. (2003). **Internet crime**. Computer Law & Security Review, 19(3), 222-227. Semantic Scholar, 1 may 2003.

ROTHER, Edna Terezinha. **Revisão sistemática X revisão narrativa**. Acta Paulista de Enfermagem [online]. 2007, v. 20, n. 2 [acessado 15 abril 2022], pp. v-vi. Disponível em: <<https://doi.org/10.1590/S0103-21002007000200001>>. Epub 17 Jul 2007. ISSN 1982-0194. <https://doi.org/10.1590/S0103-21002007000200001>.

CASTELLS, Manuel. **A galáxia da Internet, reflexões sobre a Internet, os negócios e a sociedade**. 1ª ed. Editora Zahar, 2003.

NAGLI, Luiz Sergio Dutra. **Pandemia Na Pandemia: A Escalada de Ataques Cibernéticos Pós Covid-19**. Congresso Transformação Digital, 2018.

DIANA, Daniela. **História da Internet**. Set. 2019. Seção Artigos. Disponível em <<https://www.todamateria.com.br/história-da-internet/>>. Acesso em: 22 abril. 2022.

DO NASCIMENTO, Natália Lucas. **Crimes cibernéticos**. Projeto de pesquisa apresentado ao Curso de Processamento de Dados do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão. 2006, 2016.

CANO, Gabriela Tedeschi. **Os desafios do desenvolvimento humano da ONU, a partir do Relatório do Desenvolvimento Humano d 1990**. Programa San Tiago Dantas (UNESP, Unicamp e PUC-SP), 2006. Disponível em <<https://www.funag.gov.br/ipri/btd/index.php/10dissertacoes/562-os-desafios-do-desenvolvimento-humano-da-onu-a-partir-do-relatorio-do-desenvolvimento-humano-d-1990>>.

DOS SANTOS, Rosangela. **Criminalidade digital em tempos de pandemia: principais ocorrências em sergipe no ano de 2020**. Universidade Federal de Sergipe Departamento de direito-ddi, 2021. Disponível em:

<https://ri.ufs.br/bitstream/riufs/14606/2/rosangela_santos.pdf>.

DA COSTA, Taís Barros Trajano Ribeiro. **O Aumento do Crime Cibernético Durante a Pandemia do Covid-19**. Jus.com.br, 2020. Disponível em: <<https://jus.com.br/artigos/84536/o-aumento-do-crime-cibernetico-durante-a-pandemia-do-covid-19>>.

DA COSTA, Fabrício V. et, al. **Direito, Autonomia Privada e Tecnologia**. Congresso Internacional de direito do vetor norte, 2020. Disponível em: <<http://site.conpedi.org.br/publicacoes/cw352q6w/qg0y7i81/29u40ae5c1twndxe.pdf>>.

DE MIRANDA, Wesley F. et, al. **A Proteção de Dados e Segurança da Informação na Pandemia Covid-19: Contexto Nacional**. Research, Society and Development, v. 10, n. 2, 2021. Disponível em: <<file:///c:/users/karol/downloads/12557-article-167309-1-10-20210220.pdf>>.

BRASIL. Secretaria de Estado de Segurança Pública. **Não Caia no Golpe! Crimes Cibernéticos Aumentaram 347%**. Agência Brasília, 2020. Disponível em: <<http://www.ssp.df.gov.br/nao-caia-no-golpe-crimes-ciberneticos-aumentaram-347/>>.

BRASIL. **Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los**. FEBRABAN – federação brasileira de bancos, 2020. Disponível em: <<https://portal.febraban.org.br/noticia/3522/pt-br/>>.

MENDES, Ana Beatriz S.M. et, al. **A Influência da Pandemia do COVID-19 no Aumento dos Crimes Cibernéticos**. JusBrasil. Disponível em: <<https://ribeirobeatriz.jusbrasil.com.br/artigos/1308143695/a-influencia-da-pandemia-do-covid-19-no-aumento-dos-crimes-ciberneticos>>.

ALBRECHT, Evandro Carlos et, al. **Anuário pesquisa e extensão UNOESC são Miguel do Oeste – 2021 qual a influência da pandemia do Covid-19 aos crimes cibernéticos?** UNOESC. Disponível em: <https://portalperiodicos.unoesc.edu.br>.

DE ARAÚJO, Bethânia et, al. **Preservação Da Privacidade no Enfrentamento da Covid-19: Dados Pessoais e a Pandemia Global**. Scielo, Saúde coletiva. 05 jun 2020. Disponível em: <<https://www.scielo.org/article/csc/2020.v25suppl1/2487-2492/#>>.

GARCEL, Adriane et, al. **Lei Geral De Proteção De Dados: Diretrizes E Implicações Para Uma Sociedade Pandêmica**. Clássica Editora. Disponível em: <https://www.tjpr.jus.br/documents/18319/47149551/42.+Artigo+Lei+Geral+de+Prot+e%C3%A7%C3%A3o+de+Dados.pdf/f4e4281e-2318-9799-39a8-f394a68230b3>.

AARÃO, Melhyna Pires. **O Assustador Aumento de Cibercrimes na Pandemia Covid-19**. The Frightening Increase In Cybercrime In The World Pandemic, Covid-19. Disponível em: <<https://conpedi.org.br/wp-content/uploads/2021/07/Livro-10-Direito-Penal-e-Cibercrimes.pdf>>.

BRASIL. **Polícia Civil**. Estado do Pará. 17 abr 2020. Disponível em:

<<https://www.policiacivil.pa.gov.br/par%C3%A1-%C3%A9-o-primeiro-estado-no-pa%C3%ADs-instituir-diretoria-de-combate-crimes-cibern%C3%A9ticos>>.

BARBOSA, Juliana S. et, al. **A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional.** Research, Society and Development, v. 10, n. 2, 2021. Disponível em: <<http://repositorio.asces.edu.br>>.

GOVERNO DO BRASIL. **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos.** 23 mar 2022. Disponível em: <<https://www.gov.br/ptbr/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos>>.

DUTRA, Gilson José et, al. **Ocorrência de crimes durante a Pandemia de Covid 19: Investigações iniciais para o Estado do Rio Grande do Sul.** Universidade Federal de Santa Catarina, 11 jan 2021. Disponível em: <https://www.ufsm.br/app/uploads/sites/820/2021/01/Textos-para-Discussao-23-A-ocorrencia-de-crimes-durante-a-Pandemia-de-Covid-19.pdf>.

SOUZA, Marina N. e col. **Incidência de sintomas de ansiedade em profissionais da área da Saúde atuantes no combate à pandemia da covid-19.** 2020. Disponível em: < <https://repositorio.animaeducacao.com.br>>.

MATO GROSSO DO SUL. Governo de Estado. **Crimes virtuais: MS registrou mais de 3,5 mil ocorrências em 2021; neste ano já são 1.126 casos.** Mato Grosso do Sul, 2022. Disponível em: <http://www.ms.gov.br/crimes-virtuais-policia-de-ms-registrou-mais-de-35-mil-ocorrencias-em-2021-neste-ano-ja-sao-1-126-casos/>.

VIREIRA, Isadora C. e col. **Os crimes virtuais a partir da pandemia da covid-19.** Congresso internacional de direito do vetor norte, 2020. Disponível em: < <http://site.conpedi.org.br/publicacoes/cw352q6w/qg0y7i81/29u40aE5c1twnDXE.pdf> >.

CRUZ, Lara Melana Galice, **Aumento de crimes cibernéticos durante a pandemia do covid-19 no Brasil.** Conteúdo Jurídico. 25 mai 2022. Disponível em:<<https://conteudojuridico.com.br/consulta/artigo/58466/aumento-de-crimes-cibernticos-durante-a-pandemia-do-covid-19-no-brasil#:~:text=Segundo%20relat%C3%B3rio%20global%20divulgado%20pela,parte%20dos%20brasileiros%20tem%20permanecido>>

ALVES, João Pedro e col. **O aumento dos crimes virtuais na pandemia e os limites da liberdade de expressão.** Universidade Potiguar. 2022. Disponível em: <<https://repositorio.animaeducacao.com.br/bitstream/ANIMA/25232/1/O%20AUMENTO%20DOS%20CRIMES%20VIRTUAIS%20NA%20PANDEMIA%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESS%C3%83O.pdf>>

NEVES, Lucas Miranda e col. **Congresso de Segurança da Informação das Fatec11 FatecSeg -Congresso de Segurança da Informação.** Ransomware e phishing durante a pandemia covid-19 (coronavírus). Disponível em:

<https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/39/6>

AGÊNCIA SENADO. Lei que criminaliza stalking é sancionada. Da Redação 05 mai 2021. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2021/04/05/lei-que-criminaliza-stalking-e-sancionada>>

ALVES, João Pedro e col. **O aumento dos crimes virtuais na pandemia e os limites da liberdade de expressão**. Universidade Potiguar. 2022. Disponível em: <<https://repositorio.animaeducacao.com.br/bitstream/ANIMA/25232/1/O%20AUMENTO%20DOS%20CRIMES%20VIRTUAIS%20NA%20PANDEMIA%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESS%C3%83O.pdf>>

DA SILVA, Ricardo Leopoldo. **Segurança cibernética: o cenário dos crimes virtuais no Brasil**. Ciência da computação. 20 abr 2021. Disponível em <<https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais>>

AGÊNCIA SENADO. **Lei com penas mais duras contra crimes cibernéticos é sancionada Rodrigo Baptista**. 28 mai 2021. 28/05/2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada#:~:text=Foi%20publicada%20no%20Di%C3%A1rio%20Oficial,Senado%20no%20in%C3%ADcio%20do%20m%C3%AAs>.

PINHEIRO, Bruno Victor de Arruda. **As novas disposições sobre os crimes cibernéticos: uma análise acerca das Leis 14.132 e 14.155/2022**. Jus.com.br. 22 mai 2022. Disponível em: <https://jus.com.br/artigos/98006/as-novas-disposicoes-sobre-os-crimes-ciberneticos>

SANTANA, Roque Felipe da Silva. **Crimes cibernéticos: análise evolutiva da legislação penal brasileira e seus desafios universidade católica do Salvador**. Curso de Direito. 2021. Disponível em: <http://ri.ucsal.br:8080/jspui/bitstream/prefix/4456/1/tccroquesantana.pdf>

GASTAL, Mariana. **Crimes Cibernéticos e a Pandemia de Covid-19**. Women in law mentoring Brazil. Disponível em: <https://www.wlm.org.br/crimes-ciberneticos-e-a-pandemia-de-covid-19/>.

CARDOSO, Wdson Rogério. **O aumento de crimes virtuais durante a pandemia da covid-19**. Conteúdo Jurídico, 2022. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/58543/o-aumento-de-crimes-virtuais-durante-a-pandemia-da-covid-19>.

COLOMBO, Anderson. **Crimes cibernéticos aumentam 144% no estado de São Paulo este ano, apontam dados da SSP**. G1. 4 ago 2022. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2022/08/04/crimes-ciberneticos-aumentam-144percent-no-estado-de-sao-paulo-este-ano-apontam-dados-da-ssp.ghtml>.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Polícia Federal cria Unidade Especial para intensificar a repressão a crimes cibernéticos.** gov.br. 28 jun 2022. Disponível em: <<https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos>>.

SINDICATOS DE EMPRESAS DE SEGURO E RESSEGUROS. **10 medidas para combater crimes cibernéticos durante home office.** Sindsefsp. 25 mai 2020. Disponível em: < <https://www.sindsefsp.org.br/site/noticia-texto.aspx?id=32726>>.

MEIRELES, Júlia. **Crimes Virtuais e as Dificuldades de Combatê-los.** JusBrasil. Disponível em: < <https://juapmeireles.jusbrasil.com.br/artigos/876548834/crimes-virtuais-e-as-dificuldades-de-combate-los>>.