



OS CRIMES CIBERNÉTICOS DURANTE A PANDEMIA DO COVID-19: registros do Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná

CYBERCRIMES DURING THE COVID-19 PANDEMIC: Records of the Paraná Civil Police's Cybercrime Combat Nucleus

Raphaela Schmidt Dybas¹

RESUMO

O cerne do presente trabalho parte da análise dos crimes praticados por meio do uso da internet, durante o distanciamento social causado pela pandemia do Coronavírus (COVID-19), que foram registrados em boletins de ocorrência sob a responsabilidade do Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná – NUCIBER, sendo utilizados como parâmetro o período compreendido nos anos de 2019 a 2021. Para tanto, sem delonga, é apresentada a origem da internet, além da sua difusão e meios de acesso no país, sendo de extrema importância a exposição dos principais diplomas legais pátrios e internacionais concernentes à garantia do direito à internet e aos crimes passíveis de serem perpetrados através deste meio, conceituando ainda os crimes cibernéticos. Na sequência, é abordada a repercussão do distanciamento social causado pela pandemia do Covid-19 no uso da internet no Brasil e, então, por fim analisado o ponto chave do trabalho: a apuração e análise dos crimes mais evidentes que ocorreram durante este período, com base nos registros do Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná. Derradeiramente, compreende-se que para combater a criminalidade cibernética mister se faz a implementação de medidas repressivas eficazes e, principalmente, a prevenção através da educação, que parece ser a melhor opção. Para prescrutar este fenômeno dentro de determinado tempo e espaço, foi realizada pesquisa bibliográfica associada à documental pautada na análise de documentos governamentais, extraídos da fonte de órgão público (relatórios e boletins de ocorrência), permitindo, assim, análises qualitativas e quantitativas de forma empírica.

Palavras-chave: crimes cibernéticos; NUCIBER; Covid-19.

ABSTRACT

This work is based on the analysis of crimes committed through the use of the internet, during the social distancing caused by the Coronavirus (COVID-19) pandemic, which were recorded in police reports under the responsibility of the Paraná Civil Police's Cybercrime Combat Nucleus – NUCIBER, using the period from 2019 to 2021 as a parameter. To this end, without delay, the origin of the internet is presented, in addition to its dissemination and means of access in the country, being extremely important to exposure of the main national and international legal diplomas concerning the guarantee of the right to the internet and the crimes that can be perpetrated through this medium, also conceptualizing cybercrimes. Next, the impact of social distancing caused by the Covid-19 pandemic on the use of the internet in Brazil is addressed and, then, finally, the key point of the work is analyzed: the investigation

¹ Pós-graduada em Análise Estratégica da Segurança Pública pela Escola Superior da Polícia Civil do Estado do Paraná. Agente de Polícia Judiciária da Polícia Civil do Estado do Paraná. E-mail: inv.raphaeladybas@pc.pr.gov.br.

- Artigo elaborado sob a orientação do Prof. Ms. Thiago Pereira Lima, Delegado da Polícia Civil do Estado do Paraná.



and analysis of the most evident crimes that occurred during this period, based on the records of the Paraná Civil Police's Cybercrime Combat Nucleus. Ultimately, it is understood that to combat cybercrime it is necessary to implement effective repressive measures and, above all, prevention through education, which seems to be the best option. In order to scrutinize this phenomenon within a certain time and space, a bibliographical research was carried out associated with the documental one based on the analysis of government documents, extracted from a public body source (police reports), thus allowing qualitative and also quantitative analyzes in a empirical way.

Keywords: cybercrimes; NUCIBER; Covid-19.

1. INTRODUÇÃO

O cerne do presente trabalho parte da análise dos crimes praticados por meio do uso da internet, durante o distanciamento social causado pela pandemia do Coronavírus (COVID-19), que foram registrados em boletins de ocorrência sob a responsabilidade do Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná – NUCIBER, sendo utilizado como parâmetro o período compreendido entre os anos de 2019 a 2021.

Inicialmente, parte-se do pressuposto de que com a disseminação mundial do Coronavírus (COVID-19), principalmente a partir de 2020, imperou-se o distanciamento social temporário de modo a conter a propagação da nova doença. Como consequência, o uso da internet foi largamente amplificado entre pessoas que buscavam se comunicar, bem como obter informações, entretenimento, realizar transações comerciais, etc. Além disso, muitas empresas e serviços públicos através de seus integrantes, e ainda estudantes, aderiram ao chamado *home office*, ao praticarem atividades remotas por meio da rede.

Assim, devido ao impacto causado pela pandemia do Coronavírus no comportamento geral da coletividade no Brasil, principalmente nos anos de 2020 a 2021, pessoas se afastaram fisicamente umas das outras, porém ao mesmo tempo, aproximaram-se mediante o uso da internet.

Todavia, o aumento do acesso à rede mundial de computadores não se deu apenas por usuários em busca de interação, distração, trabalho ou pesquisas, ou seja, a ocupação deste espaço não se deu apenas por atividades lícitas, mas também por práticas delituosas, uma vez que criminosos também se deleitam com a exposição difundida de variados usuários no ambiente virtual.

Com sustentação nas ideias de Cardoso (2020, p.1), pode-se afirmar que:



(...) em meio a uma das maiores ameaças da humanidade, o novo Corona-Vírus deixou às claras a vulnerabilidade decorrente enfrentada. Proporcionou aos cibercriminosos apenas mais uma oportunidade para práticas delituosas, aliada a uma população fragilizada e que estão mais tempo on-line em suas casas, buscando por informações relacionadas a pandemia, além de usarem a tecnologia para se comunicar com a família, na realização de trabalhos, compras, pagamentos e entretenimento.

Segundo a autora, os criminosos aproveitam momentos em que há crise e adversidades para praticar variados golpes. E neste ponto recai a importância do tema, pois qualquer indivíduo que adentra no espaço virtual precisa ter consciência sobre os riscos de estar exposto ao ambiente conectado à internet, precipuamente sobre a potencialidade de configurar como vítima de crimes cibernéticos, sendo imprescindível que tome as devidas cautelas através do conhecimento e informação sobre variadas formas de prevenção mediante auxílio das autoridades competentes no assunto.

Sendo assim, devido a contemporaneidade do tema, a problemática deste trabalho consiste em analisar os crimes mais praticados por meio do uso da internet, sobretudo verificar os que mais incidiram durante o período de distanciamento social causado pela pandemia do Coronavírus - COVID-19, utilizando-se como referência os anos de 2019, 2020 e 2021, com base nos registros dos boletins de ocorrência de responsabilidade da Delegacia de Polícia do Paraná especializada no atendimento aos crimes cibernéticos com autoria desconhecida, mais conhecida como o Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná - NUCIBER, de modo a avaliar reflexos quantitativos e qualitativos de forma empírica.

Para tanto, primeiramente será apontado o surgimento da internet, além da sua difusão e uso no país, sendo de extrema importância conhecer, mesmo que brevemente, os diplomas legais pátrios quanto aos crimes que podem ser cometidos através da internet, conceituando os crimes cibernéticos. Na sequência, serão abordadas algumas repercussões do distanciamento social causado pela pandemia do Covid-19 no uso da internet e, então, por fim será analisado o ponto chave do trabalho que é a apuração dos crimes mais evidentes que ocorreram durante o período de pandemia do Covid-19, com base nos registros do Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná.



2. INTERNET: ORIGEM E O PANORAMA NO BRASIL

Primordialmente, conforme os ensinamentos de ABREU (2009), a origem da internet se remete ao período da Guerra Fria nos anos sessenta quando o governo norte-americano reagiu ao projeto denominado Sputnik da antiga União das Repúblicas Socialistas Soviéticas (URSS), chefiada pela Rússia.

De acordo com a mesma autora (2009, p. 2), o surgimento da internet ocorreu como consequência “do trabalho de peritos militares norte-americanos que desenvolveram a ARPANET, rede da Agência de Investigação de Projetos Avançados dos Estados Unidos, durante a disputa do poder mundial com a URSS”.

Tal ideia sobre os primórdios da rede mundial de computadores é corroborada pelo ensinamento de Monteiro (2001, p. 27 -28):

A internet atual surgiu de uma rede idealizada em meados dos anos 60, como uma ferramenta de comunicação militar alternativa, que resistisse a um conflito nuclear mundial. Um grupo de programadores e engenheiros eletrônicos, contratados pelo Departamento de Defesa dos Estados Unidos, desenvolveu o conceito de uma rede sem nenhum controle central, por onde as mensagens passariam divididas em pequenas partes, que foram chamadas de “pacotes”. Assim, as informações seriam transmitidas com rapidez, flexibilidade e tolerância a erros, em uma rede onde cada computador seria apenas um ponto (ou “nó”) que, se impossibilitado de operar, não interromperia o fluxo das informações. Baseado neste conceito, em outubro de 1969, com uma comunicação entre a Universidade da Califórnia e um centro de pesquisa em Stanford, entrou em operação a ARPAnet (Advanced Research Projects Agency Network), inicialmente ligando quatro computadores. Posteriormente, mais computadores se juntaram a estes, pertencentes a outras universidades, centros de pesquisa com fins militares e indústrias bélicas.

Baseado nas lições de Lins (2022, p. 13), é possível simplificar a compreensão sobre como funcionava a rede ARPAnet, onde consta que:

A ideia era bastante trivial: ao contrário de outras redes existentes, controladas de modo centralizado, seria criada uma rede em que cada equipamento seria relativamente autônomo e a comunicação se daria de modo distribuído. Com uma organização desse tipo, pedaços da rede que não fossem afetados por uma agressão poderiam manter-se em operação.



Com base nos estudos propostos pelo autor, nas décadas seguintes de 70 e 80, foram criados os protocolos TCP/IP onde poderiam ser compartilhados arquivos através do mesmo endereço de IP. E já em 1988, ocorreu a liberação das redes para fins comerciais mediante o uso da conexão dial-up, sendo assim o uso da rede foi ampliado para além do uso de algumas comunidades e do meio acadêmico.

Sem delonga, a partir da década de 1990 o uso da rede mundial de computadores cresceu exponencialmente, não sendo apenas útil, mas também necessário, em razão de que após ter sido colocada à disposição do público em geral, atualmente, a internet se tornou um ambiente de relacionamento social virtual usado continuamente.

Portanto, ao longo dos anos, desde que foi facilitada a oferta do serviço da rede à sociedade em geral, os usuários são favorecidos pelo seu acesso referente à diversas finalidades: busca por informação, comunicação, interação, lazer, jogos, distração, compras, trabalho, pesquisas, transações comerciais, etc. Nas palavras de Sydow (2021, p. 690): “A capacidade que a rede mundial de computadores tem no que se refere à quantidade de conteúdo de longe superou as pretensões da biblioteca de Alexandria”.

Tal conectividade se tornou ainda mais evidente no período da pandemia do Coronavírus (2019-2021), quando muitas empresas e serviços públicos através de seus integrantes, além de estudantes aderiram ao chamado *home office*, ao praticarem atividades remotas por meio da rede. Para se ter ideia à nível nacional, no ano de 2021 o número de total de domicílios no Brasil com acesso à internet alcançou a surpreendente quantia de 90 por cento, conforme Pesquisa Nacional por Amostra de Domicílios Contínua – PNADC do Instituto Brasileiro de Geografia e Estatística – IBGE.

Em que pese tais avanços, o território virtual pode ser considerado ambivalente, em razão de ser povoado também por pessoas voltadas às práticas delituosas. Derradeiramente, conforme os ensinamentos de Santos e Brumati, (2013, p. 4),

(...) o crescimento da internet, o uso dela pela população e os avanços que ela tem trazido consigo são cada dia maiores e até inesperados. A velocidade das mudanças é tão grande que já não se pode ter certeza total do que se espera dela.

Sendo assim, é fato que no contexto atual a inserção desta tecnologia constante na sociedade contemporânea, que se tornou essencial na vida das pessoas e contribui para muitas



facilidades, pode também acarretar num lado negativo da virtualidade, conforme será visto na sequência.

3. LEGISLAÇÃO BRASILEIRA QUANTO AOS CRIMES CIBERNÉTICOS

A pós-modernidade em que vivemos está estritamente vinculada à era digital, onde se abrem novos campos para a comunicação e informação com o crescimento de novas tecnologias, precipuamente, mediante o uso da internet.

Assim, considerando que o avançado grau tecnológico influencia a vida das pessoas de maneira global, é notório que a navegação na internet passa a ser um meio através do qual é possível exercer e, lamentavelmente, também violar uma gama de direitos.

Portanto, atualmente é perceptível que a internet é imprescindível para diversas atividades quotidianas que migraram para o contexto online, porém uma das consequências do seu uso é a constatação da ocorrência de variadas infrações penais, tendo em vista que existe a possibilidade de se criar uma aparente cortina virtual que dificulta a identificação do criminoso.

No entanto, diferentemente do que se pode pensar, corrobora o ensinamento de Sydow (2021, p. 691) de que:

(...) a tecnologia da informação, por mais que se defenda que goze da concepção de anonimidade, não foi construída para a impunidade. Não é verdadeira a afirmação de que a virtualidade é sempre uma forma segura e impune de se cometer atos delinquentes.

Nesta seara da pós-modernidade e dos “perigos” da internet, pode-se citar Bauman (1998, p. 25) em sua obra “O mal-estar da pós-modernidade”, que assim exprime:

(...) você ganha uma coisa e, em troca, perde outra coisa: a antiga norma mantém-se hoje tão verdadeira quando o era então. Só que os ganhos e as perdas mudaram de lugar: os homens e as mulheres pós-modernos trocaram um quinhão de suas possibilidades de segurança por um quinhão de felicidade. Os mal estares da modernidade provinham de uma espécie de segurança que tolerava uma liberdade pequena demais na busca da felicidade individual. Os mal-estares da pós-modernidade provém de uma espécie de liberdade de procura do prazer que tolera uma segurança individual pequena demais.



Desta maneira, pode-se depreender que um dos mal-estares vividos atualmente é o dos crimes cometidos através do meio internet, uma conectividade tão útil quanto imprescindível para a sociedade moderna. Tais crimes são conhecidos como crimes cibernéticos, conforme se depreende do conceito de cibercrime nas lições de Simas (2014, p. 12):

A prática de crimes na internet assume várias denominações, entre elas - crime digital, crime informático, crime informático-digital, «high technology crimes», «computer related crime». Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes, contudo, atendendo aos diversos instrumentos legislativos, consideramos ser de especial interesse utilizar a denominação de cibercrime.

Diante do exposto, torna-se importante apresentar brevemente os diplomas legais pátrios e internacionais concernentes à garantia do direito à internet e citar alguns dos crimes/contravenções passíveis de serem perpetrados através deste meio, conceituando ainda os crimes cibernéticos.

Inicialmente, cabe salientar que este trabalho não tem por escopo distinguir os crimes das contravenções penais, portanto quando for referido o termo “crimes” cometidos pela internet que sejam entendidos por crimes virtuais no sentido genérico (amplo) de infração penal.

Importante frisar que, a internet se tornou um instrumento facilitador para a prática de atos ilícitos, no geral denominados como crimes tradicionais dispostos no Código Penal e outros em legislações especiais. Uma vez que os crimes já existem tipificados na legislação pátria, o que mudam são suas modalidades de cometimento perpetradas através da internet. Neste âmbito, quanto à existência de normas legais, Lima (2011, p. 02) afirma que:

Com a difusão da tecnologia informática, tornando-se uma presença constante na maioria das relações sociais, o direito deve cuidar de reconhecer valores penalmente relevantes, criando normas protetoras a fim de estabelecer a segurança dessas relações. Também é dever do direito penal a proteção de bens jurídicos tradicionalmente reconhecidos e lesionados com o uso da tecnologia informática, bem como a proteção de outros valores jurídicos recentes havidos com o advento e a proliferação dos computadores.

Deste modo, no intuito de proteger os usuários dentro do espaço cibernético, os operadores do direito recorrem aos diplomas internacionais e a legislação brasileira vigente



que concernem à garantia do direito à internet, além de definirem os crimes passíveis de serem perpetrados através deste meio.

Por conseguinte, impõe-se citar em primeiro lugar a norma fundamental do país: a Constituição Federal de 1988, que teve uma importante alteração em 2022 pela Emenda Constitucional, onde foi acrescentado o inciso LXXIX ao artigo 5º, com os seguintes termos: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Ainda, referente à dificuldade na comprovação da real identidade do ofensor através da rede, o art. 5º, inciso IV, da Carta Magna deixa bem claro que o anonimato é vedado, com exceção do sigilo profissional, conforme inciso XIV.

No que diz respeito aos crimes cibernéticos, também existe a Convenção sobre o Cibercrime realizada em Budapeste no ano de 2001, sendo um dos mais importantes documentos que surgiram como resposta aos crimes cometidos pela tecnologia informática, onde constam as principais práticas abusivas cometidas através da rede de computadores, internet. Dez anos mais tarde, o Brasil ratificou o acordo internacional e aprovou a Convenção por meio do Decreto Legislativo nº 37 de 16/12/2021, considerando que os crimes cibernéticos não respeitam fronteiras.

Além disso, desde o dia 16 de maio de 2011, a Organização das Nações Unidas – ONU garantiu dentre outros direitos, o acesso à internet, considerado como um direito humano básico e fundamental, conforme Relatório da Assembleia Geral da ONU, A/HCR/17/27.

Quanto às leis infraconstitucionais para aplicação nos casos concretos, no Brasil existe uma legislação extravagante conhecida como Marco Civil da Internet, na qual dispõe em seu art. 7º que “o acesso à internet é essencial ao exercício da cidadania”. No art. 2º, inc. II, desta lei, são adotados alguns fundamentos como os da liberdade de expressão e o reconhecimento da escala mundial de rede, com o desenvolvimento da personalidade e o exercício da cidadania em meios digitais.

Este Marco Civil da Internet objetiva à promoção do direito de acesso à internet para todos as pessoas, quanto à informação, conhecimento e participação na vida cultural e nos assuntos públicos, além de fomentar a ampliação ao acesso de novas tecnologias. Além disso, o art. 3ª desta Lei 12.965/2014 garante os seguintes princípios:



- I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
- II - proteção da privacidade;
- III - proteção dos dados pessoais, na forma da lei;
- IV - preservação e garantia da neutralidade de rede;
- V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
- VII - preservação da natureza participativa da rede;
- VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

No que tange aos delitos que podem ser consumados mediante o uso da internet, no Código Penal vigente, Lei 2.848/1940, existe a tipificação de diversas infrações, a título de exemplo: auxílio ou instigação ao suicídio, calúnia, injúria, ameaça, difamação, divulgação de segredo, furto, extorsão, estelionato, violação de direitos autorais, favorecimento da prostituição, ato obsceno, escárnio por motivo de religião, incitação ao crime, a apologia de crime ou criminoso, falsa identidade, formação de quadrilha ou bando, falsa comunicação de crime por meio do registro em boletim de ocorrência eletrônico, entre outros.

Além dos crimes previstos implicitamente do Código Penal Brasileiro, existem outras legislações extravagantes que também compõem o conjunto de normas relevantes que podem ser aplicadas aos cibercrimes como a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional (Lei 7.716/89), pedofilia e pornografia infantil regulamentada pelo Estatuto da Criança e Adolescente (Lei 8.069/1990), interceptação não autorizada de comunicação telefônica, informática ou telemática (Lei 9.296/96); pirataria de software (Lei 9.609/98), tráfico de drogas (Lei 11.343/06), além de outros crimes cibernéticos dispostos na Lei 12.737/2012 (conhecida como Lei Carolina Dieckmann).

4. REFLEXOS DA PANDEMIA DO COVID-19 NOS CRIMES CIBERNÉTICOS

Antes de tudo, apresenta-se a origem do COVID-19, mais conhecido por Coronavírus, o qual atingiu escalas alarmantes de contágio ao redor mundo e acabou por influenciar e fomentar as interações *online*, repercutindo também no campo dos crimes cibernéticos, conforme segue diante das lições de Pinto (2021, p.03):



O novo coronavírus, chamado de Síndrome Respiratória Aguda Grave – Coronavírus - 2 (SARS-CoV-2), foi identificado na China, em dezembro de 2019, associado a grupos de pacientes com pneumonia que foram epidemiologicamente ligados a um mercado de frutos do mar e animais vivos na cidade de Wuhan, Província de Hubei (apud Zhu et al., 2020). Devido ao seu elevado potencial de contágio resultou num aumento exponencial de casos de infetados. A sua transmissão generalizada foi reconhecida pela Organização Mundial da Saúde como uma Pandemia, a 11 de março de 2020 (WHO, 2020). Como esperado, o alcance geográfico do vírus, o número de infetados e a taxa de mortalidade, causaram na população sentimentos de medo e de insegurança, impuseram medidas de contenção raramente observadas na história da humanidade e, em consequência, diminuíram a mobilidade e a interação direta, aumentaram o afastamento e o isolamento social e afetaram, globalmente, a saúde mental das populações (apud Ornell et al., 2020).

A Organização Internacional de Polícia Criminal - INTERPOL, em análise do período pandêmico inicial, constatou aumento preocupante referente às taxas de crimes cibernéticos no mencionado recorte espaço-temporal, exprimindo que:

Com organizações e negócios rapidamente migrando para sistemas remotos, e, consequentemente, com pessoas trabalhando em *home-office*, criminosos também tomaram vantagem do aumento de vulnerabilidades para subtrair dados, auferir lucro e causar problemas. (...). Projeções: Um aumento nas taxas de cibercrimes é altamente provável no futuro próximo. Vulnerabilidades relacionados às atividades online em casa e o potencial de lucro galopante aos cibercriminosos, os fará aumentar as atividades delitivas com *modus operandi* mais avançado e diversificado. (Tradução livre da autora).

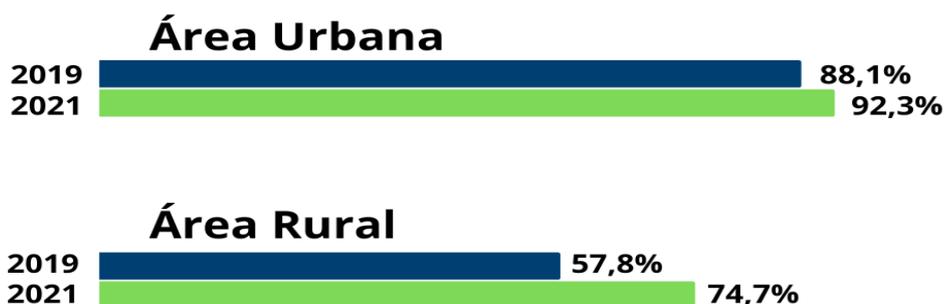
No que diz respeito à mudança no comportamento social causada pelo efeito da pandemia no Brasil, durante o período de 2020 a 2022, pode-se extrair dos estudos de Bezerra (2021, p. 05) que:

No Brasil, o uso da internet ganhou ainda mais força durante o período da pandemia do Sars-Cov-2, conhecido popularmente como Corona Vírus. Desde o início desse período, os brasileiros enfrentam o desafio de adaptar sua rotina agitada aos cômodos da própria casa, reorganizando e improvisando ambientes para que possam ser o seu novo local de trabalho e estudo. Ademais, com o fechamento de shoppings center, bares e restaurantes, cinemas e outros locais de lazer, a população precisou encontrar, também dentro de casa, alternativas que satisfizessem os momentos de entretenimento do dia a dia, o que deu espaço às redes sociais e outras plataformas de interação social que funcionam através da internet.



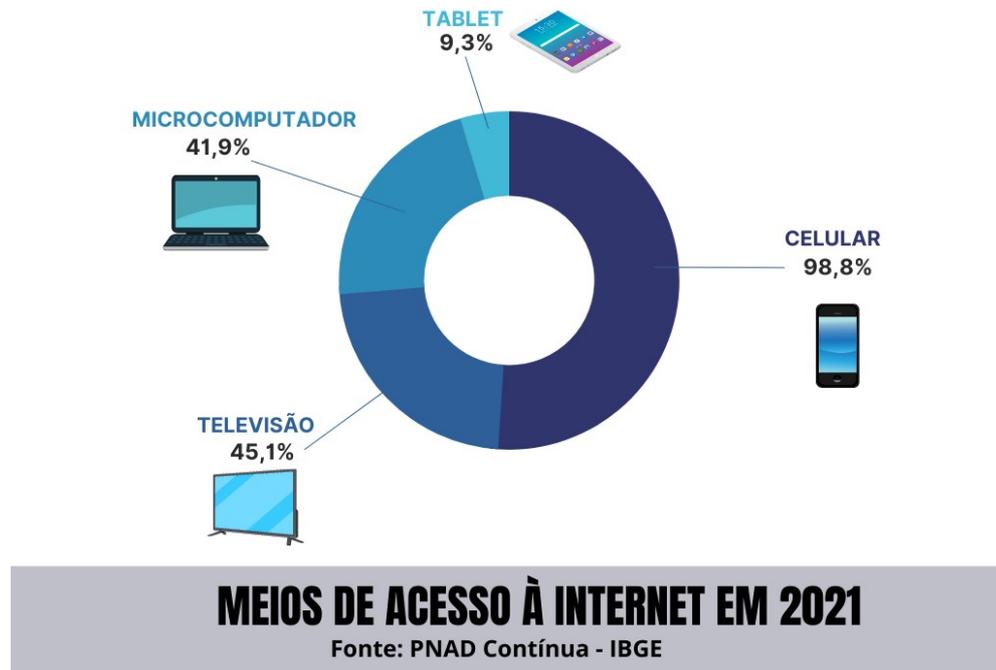
Conforme já afirmado anteriormente, no ano de 2021 o número total de domicílios no Brasil com acesso à internet alcançou a surpreendente quantia de 90%, sendo que a conectividade cresceu de 88,1 para 92,3 por cento na área urbana, e aumentou consideravelmente, quase 17%, na área rural, onde o sobreveio o aumento de 57,8 para a marca de 74,7 por cento em relação ao ano de 2019, conforme Pesquisa Nacional por Amostra de Domicílios Contínua – PNADC do Instituto Brasileiro de Geografia e Estatística – IBGE publicada em 2022.

DOMICÍLIOS NO BRASIL COM ACESSO À INTERNET



Fonte: PNAD Contínua - IBGE

Em paralelo, pela mesma pesquisa foi constatado que o equipamento mais importante de acesso à rede seguiu sendo o aparelho celular (*smartphone*), sendo que relativo ao ano de 2021, o aparelho foi utilizado em 99,5% nos domicílios do país com acesso à Internet.



Note-se ainda que, com base no mesmo estudo da pesquisa do PNAD Contínua/IBGE de 2022, há uma estatística muito importante com relação à faixa etária das pessoas que utilizaram a internet nos anos de 2019 e 2021, onde se constatou que os jovens adultos com idade entre 20 aos 39 anos foram os que mais acessaram a rede nesses dois anos.

No entanto, apesar do crescimento em todos os grupos etários, a constatação mais importante relacionada à referida investigação do PNAD Contínua/IBGE concerne ao aumento considerável no acesso à internet pelos infantojuvenis de 10 a 13 anos, passando de 77,5% em 2019 para 82,2% em 2021.

E ainda, mais surpreendentemente, foi a observação da expansão acelerada relativa às idades mais avançadas, onde o uso da internet acentuou entre os anos de 2019 e 2021 pelos grupos etários de 50 a 59 anos (aumento de 8,9%) e, mais ainda, pelas pessoas de 60 ou mais anos de idade (maior crescimento de 12,7%).

Diante dos valores analisados, constata-se que a partir de 2019, ano do surgimento do Coronavírus, cresceu acentuadamente o número de acessos à internet por pessoas de terra idade e aquelas com tempo de vida avançado, ou seja, crianças com menos de 12 anos e idosos a partir de 60 anos, geralmente considerados vulneráveis frente à maior fragilidade que



apresentam perante outros grupos sociais. Sendo assim, cautelas devem ser tomadas pelos próprios usuários da rede ou de seus responsáveis, para a prevenção de possíveis crimes perpetrados por pessoas más intencionadas no ambiente virtual. Nas palavras de Sydow (2021, p. 691):

É, pois, a vítima, um sujeito de foco adequado, um alvo que se mostra preferencial seja por quem é, como se porta, pelo que possui ou por onde está. A virtualidade é ambiente propício para a execução de delitos, especialmente porque sua estrutura propicia a oportunidade, no sentido de que a contemporaneidade por si só traz a vítima para o ambiente e a vulneraliza.

Nesse diapasão, dentro da esfera de abrangência da Polícia Civil do Paraná, se faz necessário investigar quais os crimes que mais incidiram neste período em que imperou o distanciamento social como forma de contenção à propagação da pandemia do COVID-19, de modo a apurar se realmente houve aumento nas ocorrências dos crimes cibernéticos, conforme os registros do Núcleo de Combate aos Cibercrimes da mesma instituição.

5. ANÁLISE DOS REGISTROS DO NÚCLEO DE COMBATE AOS CIBERCRIMES DA POLÍCIA CIVIL DO PARANÁ

Preliminarmente, cabe salientar que a unidade policial especializada no combate aos crimes cometidos através da internet foi criada dentro da Polícia Civil do Paraná em data de 18 de novembro de 2005, através da Resolução nº 293/05 da Secretária da Segurança Pública do Paraná, sendo nomeada por Núcleo de Combate aos Cibercrimes – NUCIBER.

De acordo com o art. 39 do Decreto nº 4.884 de 24 de abril de 1978, que regulamenta e estrutura a Polícia Civil do Estado do Paraná, no que tange às competências comuns às Delegacias Especializadas:

competem em geral, adotar as medidas necessárias para a investigação, prevenção, repressão e processamento, no Município de Curitiba, os crimes previstos no Código Penal Brasileiro, Lei das Contravenções Penais e em outras legislações de caráter penal, segundo a atribuição específica; proporcionar apoio investigatório às unidades policiais do interior quando formalmente requisitados ou quando determinado por autoridade policial competente em função de dificuldades do aparelhamento policial local, ou extrema repercussão do fato criminoso ou ainda quando o iter criminoso se projetar a diversas comarcas e as ações forem perpetradas por duas ou mais pessoas; [...]



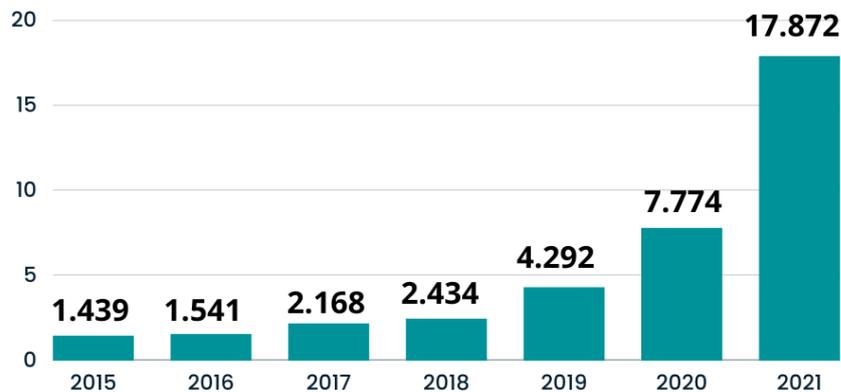
Em consonância ao acima exposto, o disposto no artigo 2º, III, da referida Resolução de criação do NUCIBER, também prevê como sua atribuição “auxiliar os demais órgãos da Polícia Civil nas investigações e inquéritos policiais ou administrativos, quando haja necessidade de pesquisa na rede mundial de computadores”.

Desta forma, torna-se evidente que as ocorrências cometidas fora da circunscrição de Curitiba, deverão ser registradas e investigadas pela Delegacia de Polícia local, embora possam contar com auxílio e suporte especializado do NUCIBER quando houver investigações que envolvam crimes cibernéticos, principalmente naqueles em que a autoria é incerta ou desconhecida, de acordo com o art. 42 do Decreto Estadual nº 4.884/78.

A partir deste momento, no intuito de analisar a possível relação entre o aumento da inserção das pessoas no ambiente virtual em consequência do distanciamento social causado pela pandemia do Coronavírus e os crimes cometidos mediante o uso da rede dentro de determinado tempo e espaço, serão apresentados neste trabalho os números dos registros de boletins de ocorrência registrados e sob responsabilidade do Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná referente aos anos de 2015 a 2021. Para tanto, foi realizado um levantamento prévio de dados com base na pesquisa documental pautada na análise de documentos governamentais (boletins de ocorrência) permitindo, assim, análises qualitativas e quantitativas, de modo empírico e dedutivo.



CRESCIMENTO NO REGISTRO TOTAL DE BOLETINS DE OCORRÊNCIA DO NUCIBER PCPR



Fonte: NUCIBER PCPR, unpublished observations.

Conforme o gráfico anterior, percebe-se que ao longo dos anos houve um crescimento constante, ano a ano, no registro total de boletins de ocorrência do NUCIBER, porém é nítido que ocorreu aumento significativo a partir do ano de 2019, sendo constatada uma alta exponencial nos crimes registrados no ano de 2021, em comparação com os anos anteriores.

Em razão disso, no intuito de compreender parte deste espantoso fenômeno, demonstrou-se necessário também coletar e analisar a natureza dos crimes que tiveram representatividade neste súbito aumento das ocorrências criminais registradas e sob responsabilidade do NUCIBER, no período compreendido dos anos 2019, 2020 e 2021, quais sejam, os anos antes, durante e pós o auge da pandemia do COVID-19.

Cabe salientar que os dados foram coletados, tabulados e em seguida analisados com atenção, chegando-se ao principal resultado: o crime que mais incidiu durante e logo após o período de isolamento social causado pela pandemia do Coronavírus - COVID-19, foi o delito de estelionato, representando só em 2021 o número de 16.538 das 17.872 ocorrências totais registradas e sob responsabilidade do Núcleo de Combate aos Cibercrimes.



REGISTROS DE BOLETINS DE OCORRÊNCIA DO NUCIBER PCPR

NATUREZA DO DELITO	2019	2020	2021
ADQUIRIR, POSSUIR OU ARMAZENAR MATERIAL PORNOGRAFICO C CRIANCA OU ADOLESCENT	42	30	41
ALICIAR CRIANCA PARA A PRATICA DE ATO LIBIDINOSO	6	12	24
AMEAÇA	236	141	169
CALUNIA	103	55	69
DIFAMAÇÃO	265	91	97
ESTELIONATO	1715	6007	16538
EXTORSÃO	96	113	75
FALSA IDENTIDADE	921	330	122
FURTO	338	721	486
INJURIA	178	98	83
INVADIR DISPOSITIVO INFORMÁTICO	879	430	186
PERTURBACAO DA TRANQUILIDADE	150	51	25

Fonte: NUCIBER PCPR, *unpublished observations*.

Com base na análise dos dados levantados, ainda foi possível constatar uma outra avaliação importante: durante o período de 2019 a 2021, ocorreu o aumento em progressão geométrica de dois tipos penais: ocupando o primeiro lugar, o delito de estelionato (art. 171, Código Penal) e, em segundo lugar, o crime de aliciamento de criança, com o fim de com ela praticar ato libidinoso (art. 241-D, da Lei nº 11.829/2008, que dispõe sobre o Estatuto da Criança e do Adolescente – ECA).

De acordo com o ECA, a lei prevê proteção integral à criança e ao adolescente, sendo as primeiras consideradas como as pessoas menores de 12 anos de idade. Nesta seara, conforme já abordado anteriormente, pode-se inferir que há probabilidade de existir uma relação entre pessoas dos 10 aos 13 anos e acima de 50 anos, que estão se lançando no ambiente da internet, possivelmente configurando como as vítimas mais vulneráveis dos dois tipos penais mais incidentes e que duplicaram a cada ano (2019-2021), conforme os registros do NUCIBER/PCPR acima. No entanto, serão necessários novos estudos para dar continuidade ao presente trabalho e confirmar quais são os grupos etários mais vitimados pelos cibercrimes com autoria desconhecida no Estado do Paraná.



Sendo assim, a pretensão deste trabalho não é afirmar taxativamente quais os motivos pelos quais houve o aumento da criminalidade pela internet na pandemia, mas indicar que há, sim, uma forte evidência de que o período do distanciamento social vivenciado em consequência da pandemia do COVID-19, colaborou com o engajamento de pessoas de variadas faixas etárias dentro do universo virtual no país.

Diante do todo o exposto, há fortes indícios sobre a relação entre o indicador referente ao crescimento alarmante na incidência dos crimes registrados e sob responsabilidade do NUCIBER/PCPR, principalmente no que tange ao crime patrimonial do estelionato, e a postura do próprio usuário da rede, que pode ser um fator primordial de fragilidade. Assim, há de se constar conforme Cruz (2006, p.15) que há uma ligação no ciberespaço entre o criminoso e a vítima:

Com respeito aos fatores que incrementam a vulnerabilidade dos sistemas informáticos, é importante dizer que as próprias vítimas contribuem indiretamente para o aumento da criminalidade informática. Esse fenômeno criminoso afeta vários tipos de vítima, tanto pessoas jurídicas como físicas.

Fácil é observar o número de pessoas que possuem dispositivos com acesso à internet e que raramente sabem explorar as funcionalidades de seus aparelhos, talvez por falta de leitura do manual de instruções, bem como por terem o mínimo de conhecimento sobre funcionalidades da rede (e às vezes nem isso). Assim, lançam-se no ambiente virtual, sem os devidos cuidados, tornando-se potenciais vítimas de abusos via internet, fato corroborado pelas lições de Sydow (2021, p.49):

Destarte, a grande maioria dos internautas vaga por endereços virtuais sem ser capaz de ponderar o quão seguro está e o quanto é prudente permanecer se embrenhando em tais sítios. Também, quando abordado por e-mail, mensagem de rede social ou até mesmo por SMS, vê-se no interlocutor mal intencionado a aparência neutra, quiçá a mesma de seus contatos, conhecidos, amigos, entre outros.

6. CONSIDERAÇÕES FINAIS

Considerando os dados revelados até ao momento, embora traduzam somente uma pequena parcela do fenômeno constatado, por si só já são preocupantes e exigem uma



resposta rápida de intervenção em tais resultados, baseada na repressão e principalmente na prevenção.

Em síntese, a prevenção baseada na educação digital pode ser considerada uma excelente aliada no enfrentamento aos cibercrimes, uma vez que muitos dos crimes virtuais ocorrem em consequência da atuação das próprias vítimas, as quais acessam links de origem duvidosa, enviam documentos pessoais para pessoas desconhecidas, cadastram seus dados em sites desconhecidos, expõem-se através de fotos/imagens/vídeos na internet, além de negligenciarem a instalação de aplicativos/programas/*softwares* de proteção aos diversos tipos de vírus virtuais, entre diversas outras condutas dos usuários no ambiente virtual sem as devidas cautelas.

Destarte, a divulgação por órgãos públicos a respeito de informações pertinentes a navegação segura na internet direcionada ao público internauta, auxilia na disseminação do conhecimento para que pessoas não incorram como vítimas em golpes ou abusos pelo ambiente virtual. Embora já existam diversas cartilhas de boas práticas na internet, talvez seja necessário difundi-las ainda mais, mesmo que seja por plataformas digitais.

Noutra vertente, em que pese existir uma legislação extensa que visa coibir crimes que podem ser praticados pelo meio virtual, tais ilícitos acontecem, necessitando serem solucionados e reprimidos.

Derradeiramente, no que tange à repressão, com base no trabalho produzido e no intuito de reduzir os elevados índices e solucionar as ocorrências criminais virtuais, torna-se imprescindível um estudo mais apurado sobre a metodologia que os cibercriminosos utilizam nas suas práticas delitivas, principalmente em relação àquelas voltadas aos crimes de aliciamento de criança para a prática de ato libidinoso e, sobretudo, ao de estelionato, os quais foram registrados no NUCIBER no período da pandemia do COVID-19, resultando numa progressão geométrica, sendo que o segundo delito cresceu exponencialmente no ano de 2021.

Ainda no intuito de reprimir os crimes cibernéticos, é importante lembrar que na Polícia Civil do Estado do Paraná – PCPR, já existe uma unidade especializada no registro e investigação dos crimes virtuais que presta atendimento aos cidadãos que sofreram abuso via internet, o Núcleo de Combate aos Cibercrimes – NUCIBER, bem como auxilia às demais unidades policiais do Estado quando a situação requerer.



Além disso, a referida instituição prevê diretrizes básicas envolvendo a temática, denominada Procedimento Operacional Padrão – POP, um importante documento que funciona como um manual prático e padrão aos policiais da corporação.

Por fim, em razão de a cada dia surgirem novas modalidades delitivas envolvendo os cibercrimes, que surpreendem até os policiais mais bem treinados, a Polícia Judiciária deve enfrentar o problema de forma eficaz, aparelhando-se constantemente com a aquisição e implementação de novas tecnologias, além de contar com um número adequado de recursos humanos, sendo preciso investir na capacitação continuada dos servidores, os quais deverão ser designados para locais chave, visando a ramificação do seu núcleo especializado, NUCIBER, para outras áreas do Estado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Karen Cristina Kraemer. História e usos da Internet. **BOCC–Biblioteca Online de Ciências da Comunicação**, p. 1-9, 2009. Disponível em: <<http://www.bocc.ubi.pt/~boccmirror/pag/abreu-karen-historia-e-usos-da-internet.pdf>>. Acesso em 27 maio 2022.

BAUMAN, Zygmund. **O mal-estar da pós-modernidade**. Rio de Janeiro: Jorge Zahar, 1998. Disponível em: <https://drive.google.com/file/d/0B3GQrRvm4KXOOFh0SE1CSDVfBGM/view?resourcekey=0-Uvm_qzwJUPMiJ6nU1IVCmQ>. Acesso em 01 abr 2023.

BEZERRA, Maria Paula Rodrigues Ribeiro. Crimes contra a honra na internet: Os limites da liberdade de expressão no campo virtual e o reflexo na sociedade brasileira durante a pandemia. **Pontifícia Universidade Católica de Goiás**, 2021. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/handle/123456789/2989>>. Acesso em 27 maio 2022.

BRASIL. **Constituição Federal de 1988**. Brasília, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 25 jun 2022.

BRASIL. Decreto-Lei 2.848/1940. **Código Penal Brasileiro**. Rio de Janeiro 7 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 25 jun 2022.

BRASIL. Decreto-Lei nº 37/2021. **Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001**. Brasília, 16 dez 2021. Disponível em: <<https://www2.camara.leg.br/legin/fed/decleg/2021/decretolegislativo-37-16-dezembro-2021-792105-republicacao-164154-pl.html>>. Acesso em: 09 mar 2023.



BRASIL. **Emenda Constitucional nº 115/2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** Brasília, 10 fev 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE%2010%20DE%20FEVEREIRO,legislar%20sobre%20prote%C3%A7%C3%A3o%20e%20tratamento%20de%20dados%20pessoais>. Acesso em: 18 mar 2023.

BRASIL. Lei 7.7716/1989. **Define os crimes resultantes de preconceito de raça ou de cor.** Brasília, 05 jan. 1989. Disponível. em: <http://www.planalto.gov.br/ccivil_03/leis/17716.htm>. Acesso em: 25 jun 2022.

BRASIL. Lei 8.069/1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.** Brasília, 13 jul. 1990. Disponível. em: <http://www.planalto.gov.br/ccivil_03/leis/18069.htm>. Acesso em: 25 jun 2022.

BRASIL. Lei 9.296/1996. **Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal e trata da interceptação telefônica, de qualquer natureza.** Brasília, 19 fev. 1998. Disponível. em: <http://www.planalto.gov.br/ccivil_03/leis/19296.htm>. Acesso em: 06 mar 2023.

BRASIL. Lei 9.609/1998. **Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.** Brasília, 19 fev. 1998. Disponível. em: <http://www.planalto.gov.br/ccivil_03/leis/19609.htm>. Acesso em: 25 jun 2022.

BRASIL. Lei 11.343/2006. **Institui o Sistema Nacional de Políticas Públicas sobre Drogas.** Brasília, 23 ago. 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111343.htm>. Acesso em: 25 jun 2022.

BRASIL. Lei [12.737/2012](#). **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.** Brasília, 30 nov. 2012. Disponível. em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 25 jun 2022.

BRASIL. Lei [12.965/2014](#). **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.** Brasília, 23 abr. 2014. Disponível. em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 25 jun 2022.

CARDOSO, Nágila Magalhães. A Pandemia do Cibercrime. **Revista Eletrônica Direito & TI**, v. 1, n. 12, p. 8-8, 2020. Disponível em: <<https://direitoeti.emnuvens.com.br/direitoeti/article/view/88/86>>. Acesso em: 13 maio 2022.

CRUZ, Danielle da Rocha. **Criminalidade Informática: tipificação penal das condutas ilícitas realizadas com cartão de crédito.** Rio de Janeiro: Forense, 2006, p. 15.



FRANCE. **INTERPOL report shows alarming rate of cyberattacks during COVID-19.** Lyon, 4 ago 2020. Disponível em: <<https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>>. Acesso em: 04 mar 2023.

HUNGRIA. **Convenção do Conselho da Europa Contra a Criminalidade Cibernética.** Budapeste, 23 nov 2001. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1963474>. Acesso em 12 mar 2023.

IBGE. **Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2021.** Instituto Brasileiro de Geografia e Estatísticas, Coordenação de Pesquisas por Amostra de Domicílios. Rio de Janeiro: Editor IBGE, 2022. Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101963_informativo.pdf>. Acesso em: 15 de março de 2023.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional.** 2. ed. São Paulo: Atlas, 2011.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, v. 48, p. 11-45, 2013. Disponível em: <http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf>. Acesso em 24 maio 2022.

MONTEIRO, Luís. A internet como meio de comunicação: possibilidades e limitações. In: **Congresso Brasileiro de Comunicação.** 2001. Disponível em: <https://d1wqtxts1xzle7.cloudfront.net/57799090/Internet_como_meio_comunicacao-with-cover-page-v2.pdf?Expires=1654469230&Signature=bbJMTaIusim8Q62qJpZdqHl-FTNcoMZ0-qMlzZ6EvkH~rkTJHQQGOVMWVMEe1hVDR7h8JFvllIUuFcWq2jS3ke9SzkM2~xG-eq~hExTIQzKjbsfy64wNllwFa8gERs-XqcEV7oUzrecpJEiZmsdli6knSbImzyj~UWLBq5GlJr6pX2pLRXk-I7rH1T6OuShwhGNLR4Lllxe5J7riCW1hxpI54Y85kusCWvDMduSFBasY8B75MGrmgdNhVfFpeb2Oh8CJ7irUC~3L76dABTJN9tjHg5daZzi2CyDnMIGdd9NEQ22DRHgoGJHU-yntlk1Aie4u0ctSWHPcI6j-pe9xsg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>. Acesso em: 28 maio 2022.

ONU. **Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.** Human Rights Council Resolution. A/HRC/17/27, 2011. Disponível em: <https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>. Acesso em: 15 de março de 2023.

PARANÁ. Decreto Estadual nº 4.884/1978. **Regulamenta e Estrutura da Polícia Civil do Estado do Paraná.** Curitiba, 24 abr 1978. Disponível em:



<celepar7cta.pr.gov.br/PRPrevidencia/SitePRPrev.nsf/3b1ce059ee8f9514832569fa0049eab1/cf55cd9651e14be583256fb6004c5b3c?OpenDocument=>. Acesso em 16 mar 2023.

PARANÁ. Resolução Secretarial da Secretaria de Segurança Pública nº 293/2005. **Cria o Núcleo de Combate aos Cibercrimes da Polícia Civil do Estado do Paraná.** Curitiba, 18 nov 2005. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1452406&filename=DOCCPI%207/2016%20CPICIBER%20=%3E%20RCP%2010/2015>. Acesso em: 02 mar 2023.

PINTO, Liliana Patrícia Peralta. **Impacto da Pandemia de Covid-19 no uso da Internet e nos comportamentos de interação sexual online.** Faculdade de Psicologia e de Ciências da Educação da Universidade do Porto, 2021. Disponível em: <<https://hdl.handle.net/10216/134930.1.pdf>>. Acesso em: 27 maio 2022

SANTOS, Milena Grasiela Silva; BRUMATTI, Vitor Pachioni. A influência da internet na comunicação e seus reflexos na sociedade1. In: **Congresso de Ciências de Comunicação da Região Sudeste XVIII.** 2013. Disponível em: <<https://portalintercom.org.br/anais/sudeste2013/resumos/R38-1497-1>>.pdf. Acesso em: 27 maio 2022

SIMAS, Diana Viveiros de; **O Cibercrime.** Universidade Lusófona de Humanidades e Tecnologias de Porto, p. 12, 2014. Disponível em: <<http://hdl.handle.net/10437/5815>>. Acesso em: 27 fev 2023.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático.** Salvador: Editora Juspodvm, 2021.