UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ
INSTITUTO DE GEOCIÊNCIAS E ENGENHARIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS FORENSES

DISSERTAÇÃO

Crimes Cibernéticos: uma análise para o município de Belém, PA.

Nome do Autor: Luciana Corrêa e silva

Orientador: Prof. Dr. Diego de Azevedo Gomes

Marabá-PA, 2023

LUCIANA CORRÊA E SILVA

Crimes Cibernéticos: uma análise para o município de Belém, PA.

Dissertação apresentada ao Programa de Pós-graduação em Ciências Forenses da Universidade Federal do Sul e Sudeste do Pará (Unifesspa), como requisito para obtenção do grau de Mestre em Ciências Forenses.

Orientador: Prof. Dr. Diego de Azevedo Gomes

Marabá-PA, 2023

Dados Internacionais de Catalogação-na-Publicação (CIP)
Universidade Federal do Sul e Sudeste do Pará
Biblioteca Setorial II da UNIFESSPA

S586c Silva, Luciana Corrêa e
Crimes Cibernéticos: uma análise para o município de Belém, PA / Luciana Corrêa e Silva. — 2023.
38 f. : il.

Orientador(a): Diego de Azevedo Gomes.
Dissertação (mestrado) - Universidade Federal do Sul e Sudeste do Pará, Campus Universitário de Marabá, Instituto de Geociências e Engenharias, Programa de Pós-Graduação em Ciências Forenses, 2023.

1. Crime por computador – Legislação – Belém (PA). 2. Crime por computador – Investigação. 3. Crime por computador – Prevenção. 4. Assédio Virtual. 5. Prova digital. 6. Fraude na internet. 7. Internet – Aspectos sociais. I. Gomes, Diego de Azevedo, orient. II. Título.

CDD: 23. ed.: 345.810268098115

Elaborada por Hully Thacyana da Costa Coelho – CRB2/1593

LUCIANA CORRÊA E SILVA

Crimes Cibernéticos: uma análise para o município de Belém, PA.

Dissertação apresentada ao Programa de Pós-graduação em Ciências Forenses da Universidade Federal do Sul e Sudeste do Pará (Unifesspa), como requisito para obtenção do grau de Mestre em Ciências Forenses.

Orientador: Prof. Dr. Diego de Azevedo Gomes

Marabá(PA), 02 de março de 2023.

Banca Examinadora:

DIEGO DE AZEVEDO GOMES:83983023215

Assinado de forma digital por DIEGO DE AZEVEDO GOMES:83983023215
Dados: 2023.03.30 16:33:44 -03'00'

Prof. Dr. Diego Gomes de Azevedo
Orientador

FERNANDA CARLA LIMA FERREIRA:73051004391

Assinado de forma digital por FERNANDA CARLA LIMA FERREIRA:73051004391
Dados: 2023.03.30 16:29:38 -03'00'

Profª. Dra. Fernanda Carla Limeira Ferreira
Examinador Interno

gov.br
Documento assinado digitalmente
PEDRO BAPTISTA FERNANDES
Data: 30/03/2023 16:12:55-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Pedro Baptista Fernandes
Examinador Externo

RESUMO

Este estudo objetivou investigar a dinâmica de crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2022 fazendo o levantamento dos crimes cibernéticos mais prevalentes, classificando-os, além de identificar o perfil das vítimas deste tipo de crime. Para alcançar tal objetivo, usou-se neste estudo, procedimentos oriundos da pesquisa bibliográfica, documental e abordagem quantitativa, quanto ao objetivo caracteriza-se como pesquisa descritiva. Para a pesquisa foi realizada coleta de dados estatísticos, referentes aos crimes cibernéticos, produzido pela Secretaria de Segurança Pública do Estado do Pará. A metodologia empregada para o desenvolvimento dos gráficos se baseou na utilização do Software Excel para processamento e análise de grande quantidade de dados e para melhor visualização da dinâmica de ocorrência de crimes cibernéticos na cidade de Belém. Assim sendo, o estudo se debruça em abordagem quantitativa, análise estatística e interpretação dos dados. Os dados possibilitaram identificar que o crime de maior destaque foi o crime de Invasão de dispositivo Informático, seguido dos crimes de Estelionato e dos crimes contra honra (calúnia, injúria e difamação). Notou-se ao perfil das vítimas que, quanto ao sexo, a prevalência maior foi do sexo feminino; ao quesito profissão, foi identificado vítimas nos mais variados e independentes seguimentos profissionais; em relação a faixa etária, a maior prevalência está entre os adultos de 34 a 64 anos de idade; A região de Belém com maior ocorrência de crimes cibernéticos está no distrito central do município, onde se concentra os bairros de classe média alta da capital do Estado do Pará.

Palavras-chave: Virtual Crimes . Internet. Legislação.

ABSTRACT

This study aimed to investigate the dynamics of cyber crimes that occurred in the city of Belém/PA from 2018 to 2022 by surveying the most prevalent cyber crimes, classifying them, in addition to identifying the profile of victims of this type of crime. In order to achieve this objective, procedures from bibliographic and documentary research and a quantitative approach were used in this study. As for the objective, it is characterized as descriptive research. For the field research, statistical data were collected, referring to cyber crimes, produced by the Secretariat of Public Security of the State of Pará. The methodology used for the development of the graphics is based on the use of Excel Software for processing and analyzing a large amount of data and for better visualization of the dynamics of the occurrence of cyber crimes in the city of Belém. Therefore, the study focuses on a quantitative approach, statistical analysis and data interpretation. The data made it possible to identify that the most prominent crime was the crime of Invasion of a Computer Device, followed by the crimes of Embezzlement and crimes against honor (slander, injury and defamation). It was noted from the profile of the victims that, regarding gender, the highest prevalence was female; regarding profession, victims were identified in the most varied and independent professional segments; regarding age group, the highest prevalence is among adults aged 34 to 64 years old; The region of Belém with the highest occurrence of cyber crimes is in the central district of the municipality, where the upper middle class neighborhoods of the capital of the State of Pará are concentrated.

Key words: Cyber Crimes. Internet. Legislation.

LISTA DE FIGURAS

SUMÁRIO

.

1. INTRODUÇÃO

Nos dias atuais, é comum a notícia de um crime ocorrido em espaço cibernético, ou seja, através da internet, por meio do uso de um computador ou aparelho eletrônico similar e, a vítima muitas vezes não percebe de forma imediata, apenas depois de algum tempo. O presente estudo tem como tema “Crimes Cibernéticos: uma análise para o município de Belém, PA” e visou analisar a ocorrência de crimes cibernéticos ocorridos no período de 2018 a 2022, no município de Belém, a partir da tipificação criminal e identificação dos crimes mais recorrentes, além de investigar o perfil das vítimas destes crimes.

Mediante a análise dos resultados obtidos, observou-se um destaque considerável para os crimes de invasão de dispositivo informático e estelionato. Diante deste contexto, será realizada uma análise mais específica para estes tipos de crime, a partir das características consideradas relevantes para o estudo.

A disponibilidade dos resultados obtidos neste estudo poderá motivar a geração de políticas públicas de mitigação da problemática em diversos setores: sociais, economicos, acadêmicos e científicos contribuindo para a visualização da tematica de forma mais abrangente na capital paraense, pois traçará um quadro atual sobre a dinâmica de ocorrências de crimes cibernéticos na área amostrada.

Diante deste cenário, entende-se que este estudo tem extrema relevância em todos os aspectos e setores sociais e serve como aprofundamento do conhecimento social acerca deste novo espaço de interação entre pessoas que num primeiro momento foi salutar devido o estreitamento de barreiras impostas pelos limites territoriais, porém, acabou por se tornar espaço também de perigo, propício ao mundo do crime.

1.1. OBJETIVOS

- **Objetivo Geral:**

Analisar os principais crimes cibernéticos ocorridos no município de Belém/PA, no período de 2018 a 2022.

- **Objetivos Específicos:**

✓ Identificar a tipificação criminal de crimes cibernéticos ocorridos no município de Belém/PA, no período de 2018 a 2022.

✓ Identificar os crimes cibernéticos mais recorrentes.

✓ Investigar o perfil das vítimas de crimes cibernéticos.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. ASPECTOS GERAIS DOS CRIMES CIBERNÉTICOS

A evolução tecnológica, o fácil acesso à internet e a redução nos preços dos computadores e dispositivos móveis fez com que a utilização da internet aumentasse consideravelmente nos últimos anos (WENDT; JORGE, 2013). Tal evolução trouxe a ampla dependência da segurança e eficiência da Tecnologia da Informação nas relações sociais, na administração pública e sociedade em geral (CRESPO, 2011). Entretanto, também ocorreu o beneficiamento para as ações e práticas criminosas, as quais evoluíram e adaptaram-se surgindo os chamados cibercrimes (DEMEAU, et al. 2019).

Toda atividade em que um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecida por cibercrimes (CASSANTI, 2014). Corroborando com tal definição, Correia e Jesus (2016) conceituam crime informático como o cometimento de ações ilícitas em que se usa a informática para executá-lo, os autores enfatizam ainda, que este tipo de ilícito é de difícil detecção e prova. Desse modo, Souza (2017) destaca que as fronteiras que antes eram definidas entre o legal e o ilegal estão se tornando menos eficientes, pois as legislações e as jurisdições se entrelaçam sem que os limites geográficos sejam as referência definitiva.

Para Garcia et al. (2018), o impulso para o crime cibernético advém de demandas pessoais, que se ativam na direção da prática ilegal e imoral. Azzam (2019) alerta para os perigos dessas atividades criminosas, uma vez que envolvem ataques aos sistemas de dados de centros de informação podendo assentar até graves ameaças aos governos e às suas informações confidenciais através do acesso aos seus sistemas e dados de segurança.

Barreto, Kufa e Silva (2021) destacam as dificuldades em determinar uma nomenclatura que abarque os crimes e delitos cometidos por meios digitais, de modo que muitos termos são utilizados para determinarem os gêneros de delitos ou até mesmo misturar as espécies. Os autores citam como exemplo dessas pluralidades os diversos nomes das delegacias especializadas de Polícia Civil em diferentes estados brasileiros, tais como: Departamento de Combate aos Crimes Tecnológicos (DCCT) – MA, Delegacia de Repressão aos Crimes Cibernéticos (DR-CCIBER) – AP, Delegacia de Repressão a Crimes Eletrônicos (DRCE) – ES, Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia (DERCAT) – PI, Delegacia de Repressão aos Crimes de Informática (DRCI) – RJ, entre outras.

No Estado do Pará foi instituída a Diretoria Estadual de Combate a Crimes Cibernéticos, no âmbito da Polícia Civil no Estado do Pará, através do Decreto nº 690, de 16 de abril de 2020. A referida diretoria possui atribuições para prevenção e repressão aos crimes cibernéticos e possui as seguintes subunidades, conforme descreve o artigo quarto deste decreto:

> I - Secretaria;
> II - Divisão de Combate a Crimes contra Direitos Individuais Praticados por Meios Cibernéticos;
> III - Divisão de Combate a Crimes Econômicos e Patrimoniais Praticados por Meios Cibernéticos
> IV - Divisão de Combate a Crimes contra Vulneráveis Praticados por Meios Cibernéticos. (PARÁ, 2020).

Neste sentido pode-se observar ainda as diversas nomenclaturas utilizadas para denominar essa categoria de crimes, que de acordo com Terron, Correa e Correia (2020) são "Conhecido popularmente por crimes digitais, crimes on-line, crimes eletrônicos, crimes virtuais, crimes cibernéticos, entre demais denominações, o termo cibercrime surgiu no final dos anos 90". Do ponto de vista sociológico, ressalta Gouveia (2018) "quanto mais sujeitos são incluídos na categoria "criminoso", ou mais condutas são incluídas na categoria "crime", mais se alimentam essas próprias estruturas que geram mais crimes, mais criminosos e – consequentemente – m ais vítimas".

Considerando o surgimento e crescimento de práticas de crimes em meio virtual, foram criadas as Leis n° 12.7 35 e nº 12.737, ambas de 30 de novembro de 2012, as quais são tidas como marco jurídico para frear os avanços de crimes em ambientes virtuais no Brasil, uma vez que, as referidas leis alteraram artigos do Código Penal e do Código Penal Militar para tipificar as condutas praticadas em âmbito eletrônico, digital e similares. É relevante destacar

a redação do art. 4º da Lei nº 12.735/2012 onde determina que “os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado” (Brasil, 2012).

Ao código penal foram inseridos os Arts. 154-A e 154-B, em virtude da lei nº 12.737/2012, a qual trata dos chamados crimes informáticos.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (Brasil, 2012).
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (Brasil, 2012).

Outra alteração pertinente se deu ao art. 266 do Código Penal, Decreto-Lei nº 2.848/1940 “Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento” (Brasil, 1940) com acréscimo de dois parágrafos: §1º “Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento” e § 2º “Aplicam-se as penas em dobro se o crime for cometido por ocasião de calamidade pública” incluído pela Lei 12. 737/2012.

O crime de falsificação de cartão também foi inserido ao Código Penal, com o advento da Lei nº 12.737/2012, que acrescentou o parágrafo único ao art. 298: “Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito” (Brasil, 2012). Ademais, na legislação brasileira, foi também sancionada a lei nº 12.965/2014, a qual em seu Art.1º “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria” (Brasil, 2014). A referida lei em seu Art. 7º dispõem que:

> Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. (Brasil, 2014).

É importante salientar que a inviolabilidade da intimidade e da vida privada já são direitos garantidos por nossa Constituição Federal de 1988, conforme versa o Inc. X, do Art. 5º da CF/1988: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (Brasil, 1988). Embora a época da promulgação de nossa Carta Magna não se vislumbrava que a revolução tecnológica alcançaria os patamares dos dias atuais, pode-se dizer que o legislador teve a consciência racional no que tange a privacidade e a intimidade, independente da época, em que se vive, são bens jurídicos tutelados intrínsecos dos homens.

Portanto, “o direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros” (Mendes et al. 2008). Entende-se com tal afirmação que, em virtude da rápida divulgação através dos meios eletrônicos de quaisquer matérias, seja da vida pública e/ou da vida particular tal direito encontra-se cada vez mais infringido ao ponto de ser necessária a criação de novas leis para se frenar danos irreparáveis provocados pelo descumprimento, moral e ético dos usuários da internet, a ponto de migrarem para o campo criminal.

Sendo assim, Zuboff (2020, p.14), afirma que:

> “A realidade digital está tomando conta e redefinindo tudo que é familiar, antes mesmo de termos tido a chance de ponderar e decidir sobre a situação. Nós celebramos o mundo conectado por causa das muitas maneiras pelas quais ele enriquece nossas capacidades e perspectivas, mas ele gerou novos grandes territórios de ansiedade, perigo e violência conforme o senso de um futuro previsível se esvai por entre nossos dedos” (Zuboff, 2020).

Ante ao exposto, embora as legislações sejam de extrema importância, inclusive simbólica, não é uma condição definitiva para a erradicação dos crimes (Menezes; Cavalcanti, 2017). Dessa forma, é relevante levar em consideração as interações sociais entre indivíduos e máquinas e suas atitudes de segurança cibernética e comportamento (Benson et al. 2018) (tradução nossa). De modo que, “há uma grande necessidade de refletir o impacto da informação na sociedade digital e suas implicações diretas e indiretas no estabelecimento de novos padrões de moralidade e ética” (Azevedo et al, 2015) (tradução nossa).

Desse modo, Viana e Meneghett (2020, p.9) alertam para “falta de percepção dos usuários sobre as reais consequências dessa conectividade” (tradução nossa). A ideia de liberdade sem limites, deixa-nos vulneráveis, não vigilantes ao perigo iminente que pode surgir. A internet, para os usuários, não é apenas espaço de lazer, é espaço de trabalho, de estudos e infelizmente de muitos perigos.

2.2. INVASÃO DE DISPOSITIVO INFORMÁTICO

Como já mencionado anteriormente o crime de invasão de dispositivo informático foi criado através da Lei nº 12.737/2012 e inserido ao Código Penal, Art.154-A do CP (BRASIL, 2012; BRASIL, 1940). No ano de 2021, houve nova modificação através da Lei nº 14.155/2021 (BRASIL, 2021), a qual alterou o texto do mencionado artigo e aumentou a pena do crime, passando a vigorar atualmente com a seguinte redação:

> Art. 154-A: Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940).

O crime de invasão de dispositivo informático, atualmente bastante recorrente, por exemplo, no município de Belém/PA, vem retratando aspectos abrangentes desta nova sociedade que se mescla ao mundo virtual cada vez mais, e desconhece os perigos existente nesta nova sociedade virtual, possibilitando aos mal intencionados a conseguir vítimas fáceis neste meio. Junqueira e Botelho-Francisco (2021) enfatiza que as vulnerabilidades digitais podem ser entendidas como sendo marcas sensíveis individuais, grupais e/ou globais de riscos, inseguranças, superexposição, exclusões e ameaças, em que o sujeito contemporâneo as conhece em sua rotina digital cotidiana.

Diante disso, torna-se necessário uma compreensão mais abrangente sobre as formas de invasão de dispositivos informáticos, quem os pratica para se criar consciência para uma conduta de segurança eficiente.

2.2.1 Tipos de invasão (ou ataque) a dispositivo informático

Conforme Honorato(2017) dados extraídos do relatório de riscos do Fórum Econômico Mundial, “O Brasil sofre, aproximadamente, três vezes a média mundial de ataques”. Ainda de acordo com o referido relatório, os ataques cibernéticos mais comuns são: Modificação de Navegador, Trojan, Worms, Pacote de Software, Pacote de Software, Downloaders e Droppers; Ofuscadores e Injetores, Adware, Explorações, Vírus, Backdoor, Randsonware, Ladrão de Senha e Ferramentas de Monitoramento. Segue abaixo a definição de cada um.

a) Modificação de Navegador

De acordo com a RS DATA SECURITY, as principais vulnerabilidades utilizadas contra navegadores são:Explorações de Execução de Código no Navegador, Explorações de Execução de Código em Plug-ins, Ameaças Persistentes Avançadas (APTs), Ataques Man-In-The-Middle e Envenenamento de DNS.

- Explorações de Execução de Código no Navegador: é mais observado e também o mais raro, ocorre em virtude de vulnerabilidade existentes no navegador, a qual provoca a execução de código binário arbitrário em visitas do usuário a sites já comprometidos.
- Explorações de Execução de Código em Plug-ins: Plug-ins são vetores conhecidos para downloads drive-by,os quais baixam e executam de forma silenciosa códigos nativos no sistema.
- Ameaças Persistentes Avançadas (APTs): Ataque que instala de forma silente código malicioso em um endpoint, rouba dados, alterando, até mesmo o que o usuário no navegador, podendo ficar por anos sem ser detectado.
- Ataques Man-In-The-Middle: Forma de invasão onde o invasor se “hospeda” em qualquer ponto da conexão, entre o usuário e sites confidenciais (“homem no meio”) , possibilitando ao invasor observar e adulterar o tráfego de dados entre o navegador e os servidores da Web.
- Envenenamento de DNS: Forma de ataque, onde um arquivo especial na máquina pode ser mudado com objetivo de trocar os servidores DNS, comprometendo-os e forçando-os a servir endereços IP inválidos para sites confiáveis. Neste caso, o navegador entrará em contato com o servidor do invasor.

b) Trojan

"Projetado para executar funções para as quais foi feito, sendo essas funções maliciosas. Ele se passa por um "presente" para os usuários nas mais diversas formas como por exemplo: cartão virtual; álbum de fotos, protetor de tela (RIBEIRO,2020).

c) Worms

"Os Worms (vermes) é um programa capaz de se multiplicar pela rede, pois envia cópias de si mesmo entre os computadores, se propagam pela execução direta de suas cópias ou através da exploração automática de vulnerabilidades existentes em programas" (SILVA,2023).

d) Downloaders e Droppers

"São malwares utilizados para baixar e instalar outros tipos de malware em sistemas infectados. Os downloaders são responsáveis por baixar e armazenar arquivos maliciosos, enquanto os droppers são responsáveis por instalar e executar esses arquivos" (Wu & Lee, 2010)

e) Ofuscadores e Injetores

São técnicas utilizadas para modificar ou ocultar o código malicioso. Os ofuscadores modificam o código, escondendo sua natureza ou intenções. Os injetores inserem códigos maliciosos em processos legítimos, tornando-o mais difícil de ser detectado. (VINCIGUERRA, 2016)

f) Adware

"Se trata de uma publicidade maliciosa, apresenta várias publicidades indesejadas de forma simultânea, usando de meios nocivos. É feito com a intenção de criar publicidade, sendo recorrente sua aparição quando instalado programas"(RIBEIRO,2020).

g) Vírus

"É um programa de computador ou parte dele, normalmente malicioso, que se propaga inserindo cópias dele. O vírus depende da execução do programa ou arquivo hospedeiro, para se tornar ativo e continuar o processo de Infecção(SILVA,2023). Ribeiro (2020) discorre que "um grande propagador de vírus são os e-mails de origem desconhecida,

por isso a orientação é de que não sejam abertos e, principalmente, que jamais sejam baixados arquivos anexos a eles".

h) Backdoor ou portas dos fundos (controlador)

"É um vírus de computador que permite ataques ou invasão ao computador. Prepara o computador hospedeiro, permitindo que criminosos, de forma remota, possam controlá-lo e monitorá-lo, de forma parcial ou total" (KOLBE JUNIOR,2020).

i) Ransomware

"É um ataque perpetrado através de um malware que trava um computador ou impede que sejam acessados os dados usando criptografia privada até que seja pago um resgate"(PINHEIRO, 2022).

2.2.2 Outras formas de invasão/ataque

a) Spyware

De acordo com Diorio (2018) et al. *Apuld* Pinheiro (2022) o spyware é um programa "projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros".

b) Botnets

"São computadores infectados por arquivos maliciosos que possibilitam ao criminoso, de forma remota, realizar qualquer atividade com o computador da vítima. Eles exploram vulnerabilidades na configuração do sistema operacional ou softwares"(WENDT E JORGE, 2021).

c) Keylogger

"É um programa capaz de gravar tudo o que está sendo digitado no teclado, incluindo, nessas capturas, as senhas de acesso a sites bancários e redes sociais" (KOLBE JUNIOR,2020).

d) Hijacker

"É um programa que objetiva controlar os navegadores de internet. Abrem páginas diferentes daquelas que foram digitadas. Abrem também de forma automática pop-ups, armadilhas para o usuário, direcionando para sites falsos, com fins ilícitos"(KOLBE JUNIOR,2020).

e) Rootkit

"São programas que permanecem ocultos no computador e podem ser instalados de forma local ou remota, ou seja, a pessoa que tiver acesso físico a ele pode promover sua instalação ou por intermédio de outro computador , à distância" (WENDT E JORGE, 2021).

f) Phishing Scan

"É um tipo de golpe por meio do qual por meio do qual um criminoso tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social" (SILVA, 2023).

2.3. ESTELIONATO EM MEIO ELETRÔNICO

No Brasil, o crime de estelionato é definido no Art. 171, caput, da Lei Penal: "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", culminando em pena de reclusão de um a cinco anos (BRASIL, 1940). Ainda de acordo com o código penal, o referido ilícito encontra-se no rol dos crimes contra o patrimônio, ou seja, a intenção do autor é lesar o patrimônio de terceiros e causar dano ou prejuízo para obter alguma vantagem ilícita e, sem que a vítima perceba, comete fraudes, engana e mantém a vítima em erro.

Neste contexto, e observando ainda o constante no Código Penal brasileiro, percebe-se que fraude e/ou meio fraudulento são partes integrantes do crime de estelionato, conforme definição também das modalidades deste crime, contidas especificamente no § 2º do Art.171: disposição de coisa alheia como própria; alienação ou oneração fraudulenta de coisa própria; defraudação de penhor; fraude na entrega de coisa; fraude para recebimento de indenização ou valor de seguro; fraude no pagamento por meio de cheque; fraude eletrônica e estelionato contra idoso ou vulnerável (BRASIL,1940).

É relevante pontuar a possibilidade do cometimento do crime de estelionato de forma eletrônica ou pela internet, considerando que no Brasil já houve a tipificação criminal para os

chamados crimes cibernéticos com o advento da Lei nº 12.737/2012, a qual incluiu ao Código Penal o crime de Invasão de dispositivo informático. Ainda neste cenário, e no que tange ao crime de estelionato praticado em meio eletrônico ou pela internet, a Lei nº 14.155/2021 tornou tal conduta mais grave, tendo em vista que incrementou ao código penal a modalidade de fraude eletrônica, bem como tornou a penalidade mais dura, conforme previsão no § 2º-A do art. 171 do CP:

> § 2º- A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo (BRASIL,1940).

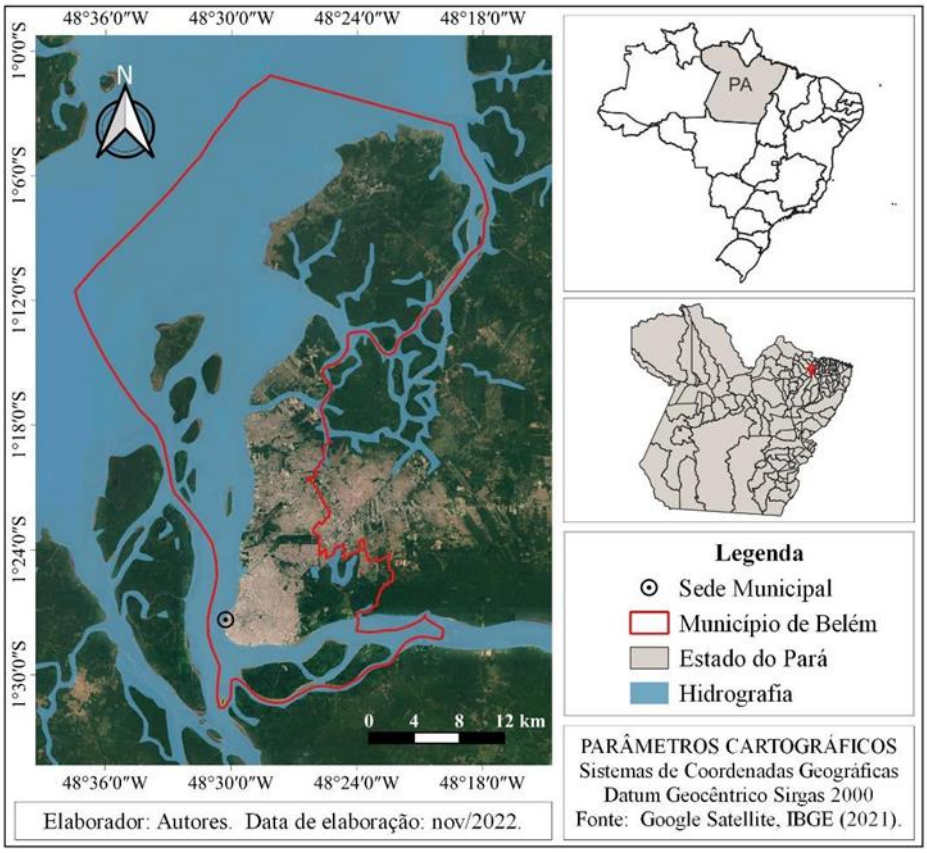
É notório o esforço do Estado brasileiro em frear os avanços destes tipos de crime, conforme argumenta Kunrath (2017): “o chamado cibercrime constitui a exteriorização de condutas ilícitas dos usuários das tecnologias da informação e internautas, cada vez mais recorrentes no ciberespaço, e vem exigindo do Estado brasileiro reação célere e eficaz no seu combate”. Somado a isto Moraes, Silva e Santiago (2020) afirmam que mediante as mudanças sociais, e tendo em vista que a criminalidade pós-moderna acompanha a evolução dos avanços tecnológicos, é primordial que o Direito atue dinamicamente, especialmente o Direito Penal, o qual reflete a ética social.

3. METODOLOGIA

3.1. ÁREA DE ESTUDO

O município de Belém, capital do estado do Pará, de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE, 2021) possui uma população estimada de 1.506.420 habitantes, área territorial é de 1.059,466 km².

Figura 1: Mapa de localização de Belém/PA



Fonte: Autora (2023).

É importante destacar que o município de Belém, de acordo com a Lei nº 7. 806-30/07/1996, possui 72 bairros está dividido em 08 (oito) Distritos Administrativos (IBGE, 2021). Assim discriminados com seus respectivos bairros:

● Distrito Administrativo de Belém (DABEL) - Bairros: Batista Campos, Nazaré, Campina, Cidade Velha, Reduto, São Brás, Umarizal e Marco.

● Distrito Administrativo do Guamá (DAGUA) - Bairros: Canudos, Condor, Cremação, Guamá, Jurunas, Montese (Terra Firme).

● Distrito Administrativo da Sacramenta (DASAC) - Bairros: Barreiro, Fátima, Marancangalha, Miramar, Pedreira, Sacramenta e Telégrafo.

● Distrito Administrativo do Benguí (DABEN) - Bairros: Benguí, Cabanagem, Coqueiro, Parque Verde, Pratinha, São Clemente, Tapanã e Una.

● Distrito Administrativo do Entroncamento (DAENT) - Bairros: Águas Lindas, Castanheira, Aurá, Curió-Utinga, Guanabara, Mangueirão, Souza, Val-de-Cans e Universitário.

● Distrito Administrativo de Icoaraci (DAICO) - Bairros: Águas Negras, Agulha,

Campina de Icoaraci, Cruzeiro, Maracacuera, Paracuri, Parque Guajará, Ponta Grossa, Tenoné e Antônio Lemos.

● Distrito Administrativo de Mosqueiro (DAMOS) - Bairros: Aeroporto, Ariramba, Baia do Sol, Bonfim, Carananduba, Caruará, Chapéu Virado, Farol, Mangueiras, Maracajá, Marahú, Murubira, Natal do Murubira, Paraíso, Porto Arthur, Praia Grande, São Francisco, Sucurijuquara e Vila.

● Distrito Administrativo de Outeiro (DAOUT) - Bairros: Água Boa, Brasília, Itaiteua e São João do Outeiro.

3.2. TIPO DE PESQUISA

Os procedimentos deste estudo são oriundos de pesquisa bibliográfica, pois utiliza-se como embasamento teórico as fontes bibliográficas que discorrem sobre o tema proposto, conforme Marconi e Lakatos (2003) ao afirmarem que este tipo de pesquisa busca expor o pesquisador a todo conteúdo publicado, incluindo artigos, livros, teses, entre outros. Além disso, também foi desenvolvida a pesquisa documental, a qual está restrita a documentos escritos ou não (MARCONI; LAKATOS, 2003), pois foram utilizadas as legislações existentes no país que buscam coibir as ações criminosas em ambientes virtuais. Possui abordagem quantitativa que, de acordo com Gerhardt e Silveira (2009) se fundamenta na quantificação de dados, com ênfase no raciocínio dedutivo e regras lógicas. Quanto ao objetivo, caracteriza-se como pesquisa descritiva, pois, de acordo com Gil (2008), esta busca a caracterização de determinada população ou fenômeno, bem como avaliar a relação entre as variáveis estudadas.

3.3 COLETA DE DADOS

A coleta de dados se deu junto a Secretaria de Segurança Pública do Estado do Pará - SEGUP, a fim de se verificar a evolução temporal da ocorrência de crimes cibernéticos na região de estudo, a pesquisa abrangerá dados de uma série histórica de 2018 a 2022, sendo que os dados do ano de 2022 compreendem até o mês de julho.

3.4. ANÁLISE E INTERPRETAÇÃO DE DADOS

Para a análise e a interpretação dos dados obtidos no estudo foi utilizada a estatística descritiva para a elaboração de médias e frequências, bem como a elaboração de gráficos no Software Excel para melhor visualização da dinâmica de ocorrência de crimes cibernéticos na cidade de Belém.

A estatística descritiva é fundamental para a análise dos conjuntos de dados em virtude de transformá-los em informações, para compará-los com outros resultados, ou ainda para julgar sua adequação a alguma teoria (MORETTIN, 2017). Por isso, é amplamente utilizada, já que as informações estatísticas quase sempre são obtidas de amostras, sendo que, as observações são feitas em parte de um conjunto grande de dados, e isso significa que sua análise exige generalizações que vão além dos dados (GUPTA, 2017).

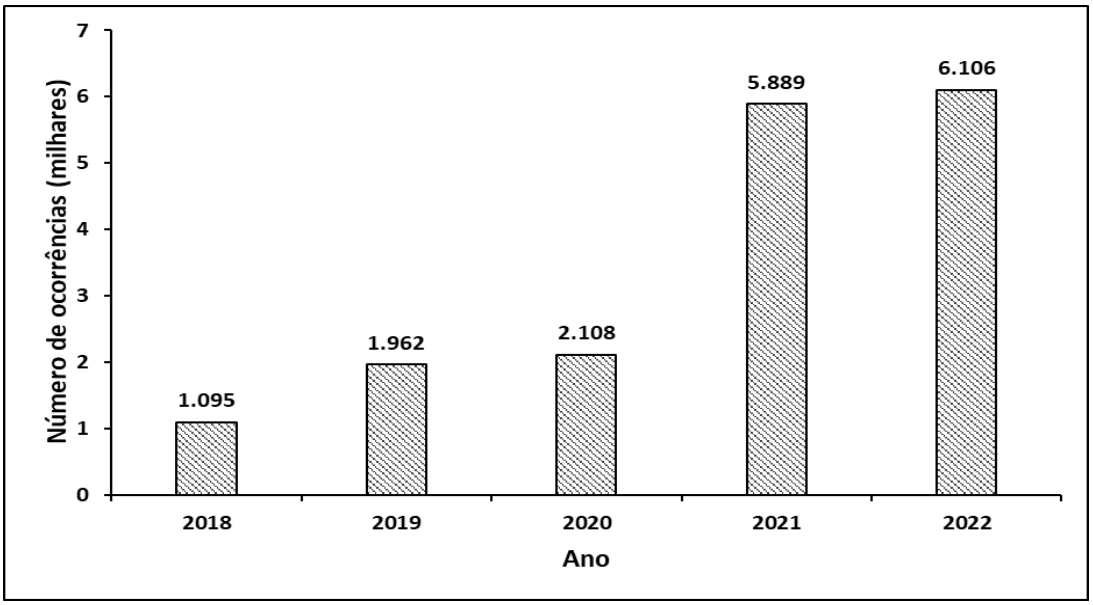
Já a representação gráfica tem por finalidade expressar de forma imediata as conclusões sobre a evolução do fenômeno ou sobre como se relacionam os valores da série, podendo ser representada de diversas maneiras, tais como, gráficos de barra, gráfico em pizza, gráfico polar, cartograma, entre outros (PEREIRA, 1990).

Para análise estatística de dados, foi aplicado ainda o teste paramétrico t de Student (teste t), com o objetivo de verificar diferença estatística entre dados. Para tanto, inicialmente verificou-se a normalidade por meio do teste de Shapiro-Wilk seguido da verificação da homocedasticidade para análise da homogeneidade de variâncias. Para os dados considerados normais e de variâncias iguais foi aplicado o teste t, considerando que a hipótese nula estabelece que não há diferença estatística ($p\text{-valor}>0,05$) enquanto que a hipótese alternativa estabelece a existência de diferença significativa ($p\text{-valor}<0,05$).

4. RESULTADOS E DISCUSSÃO

A Figura 2 mostra o quantitativo de ocorrências de crimes cibernéticos, na qual pode-se notar o crescimento no número de tais ocorrências ao longo da série histórica analisada. O maior resultado obtido se refere ao ano de 2022, embora os valores correspondem apenas ao período entre os meses de janeiro a julho deste ano. O aumento do número de ocorrências de crimes cibernéticos pode estar relacionado ao processo de universalização do acesso à internet em todos os setores sociais, conforme argumenta Marra (2019, p.163): “A Internet ultrapassou os limites impostos pelas fronteiras tornando-se, na atualidade, o principal veículo de divulgação da informação, comunicação, comercialização e, inclusive, de práticas delituosas”. Observou-se também ao longo do período pandêmico um crescimento acelerado de crimes cometidos em ambiente virtual. Isso se deve, conforme argumenta Borges (2022) que o acesso ao uso da Internet se manteve em nível elevado em relação aos notados antes da pandemia COVID-19, o que revelou a ampliação da busca por conectividade em virtude do direcionamento de várias atividades para o ambiente digital. No período analisado também observamos um crescimento abrupto do ano de 2020 para 2021, para o qual ainda não temos informações que permitam explicar tal comportamento.

Figura 2: Evolução na ocorrência de crimes cibernéticos por ano



Fonte: Autora (2023)

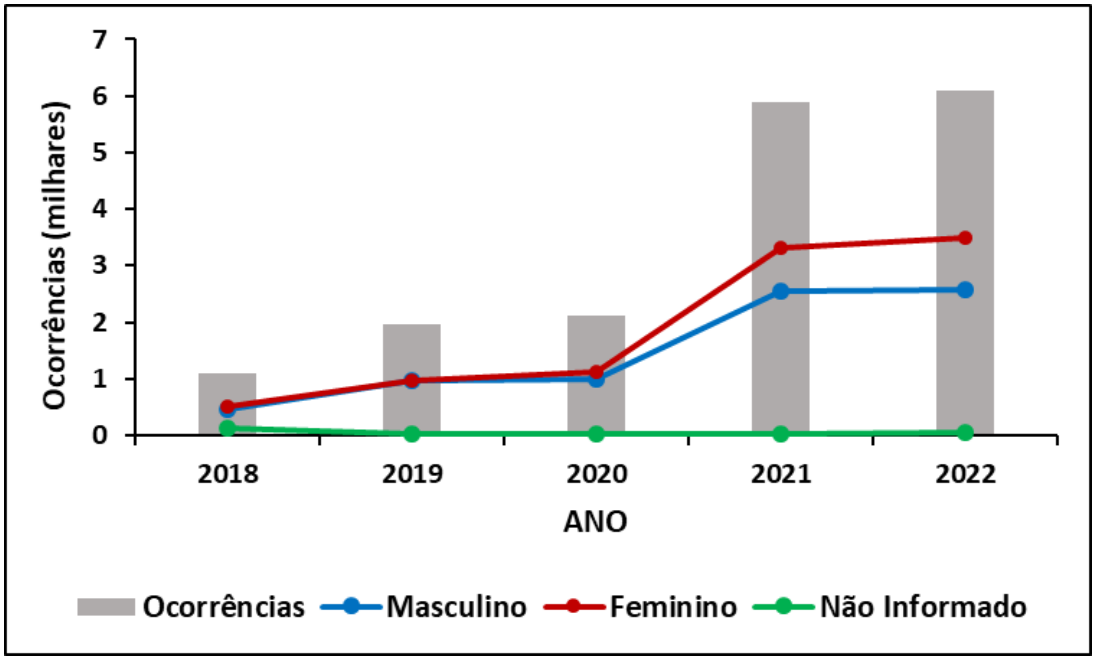
Para o período analisado, foi observado maiores valores para o sexo feminino, como mostrado na Fig. 3 , principalmente entre os anos de 2021 e 2022, que corresponderam a 3.308 e 3.489 ocorrências, respectivamente. Dos Anjos (2006) discorre que "o combate à violência contra a mulher depende, fundamentalmente, de amplas medidas sociais e profundas mudanças estruturais na sociedade (sobretudo extrapenais)".

Paralelo a isto, Martinez (2019) comenta que:

> Dados de uma pesquisa feita em 2013 revelam que mulheres seriam "mais propensas" ao uso de redes sociais do que os homens; entre elas, o Facebook, o Instagram e o Pinterest seriam os mais utilizados, perfazendo uma diferença de 8% a mais no uso do que os homens. Em relação à América Latina, uma recente pesquisa revela que as mídias sociais são a categoria que mais consome horas on line por mês, sendo que o maior percentual de usuários se concentra no Brasil (42%), onde as mulheres constituem a maior quantidade de acesso às redes sociais (58,2%).

Apesar de observarmos que as mulheres são mais vítimas destes crimes, a diferença não foi significativa em relação ao recorte do banco de dados cedidos para este estudo.

Figura 3- Ocorrências de crimes cibernéticos conforme sexo da vítima



Fonte: Autora (2023)

A Figura 4 mostra os tipos de crimes ocorridos no período avaliado. Ao longo do período de estudo, notou-se que o crime com menor ocorrência foi o de importunação sexual, com 82 registros. Enquanto que os crimes de invasão de dispositivo informático e estelionato apresentaram os maiores valores, sendo 6.496 e 4.990 registros, respectivamente. De acordo com Brasil et al. (2017), "independente de qualquer classificação, os riscos na rede vão desde a identificação de vulnerabilidades em sistemas informatizados à prática de crimes, simples ou complexos, de menor ou grande potencial ofensivo".

Para melhor compreensão das informações extraídas do recorte do banco de dados fornecidos pela SEGUP/PA, faz-se necessário detalhar a tipificação dos crimes inseridos em cada grupo:

- Invasão de dispositivo informático - Este crime ao qual, teve a maior prevalência ao longo do período de 2018 a 2022, sendo que foi inserido ao código penal, em virtude da edição da lei que trata da tipificação dos delitos informáticos, Lei nº 12.737/2012.
- Estelionato por meio de dispositivo eletrônico ou pela internet. Neste estudo, os dados revelaram que o crime de Estelionato teve a segunda maior prevalência.
- Dos Crimes contra a Honra - Observou-se a recorrência dos Crimes de Calúnia, Injúria e Difamação, com maior prevalência, o crime de difamação.
- Dos crimes contra a liberdade pessoal - Nos dados obtidos, somente foram identificados os crimes de ameaça e de constrangimento ilegal, entretanto a maior prevalência foi do crime de

ameaça.

● Dos crimes contra a fé pública - Para esse tipo de crime, somente foram identificados os crimes de falsa identidade, falsidade ideológica e falsificação de documento particular, sendo que, a maior prevalência foi do crime de falsa identidade.

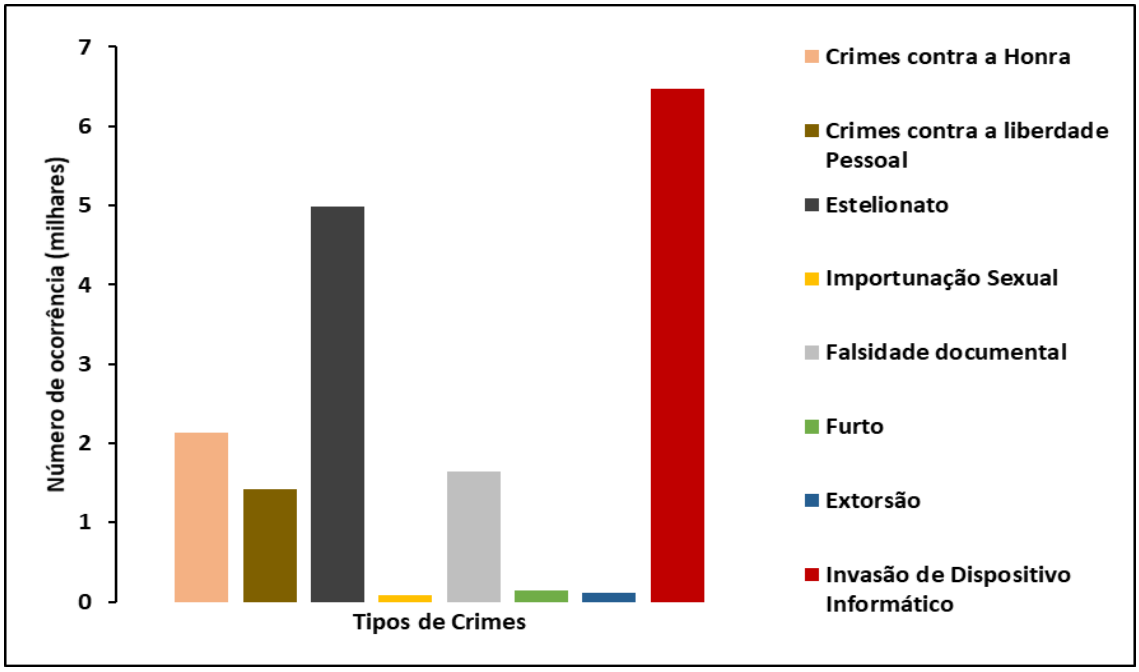
● Furto qualificado - Crime de recorrência relevante, ao qual foi definido pela Lei nº 14.155/2021.

● Extorsão - Crime de recorrência relevante entre os dados obtidos. Pode ser praticado através das redes sociais. Os dados não esclarecem quais as modalidades deste crime foram mais recorrentes.

● Importunação sexual - Tipo penal criado pela Lei nº 13.718/2018, a qual altera o Código Penal teve recorrência relevante entre os dados deste estudo.

● Crimes sexuais contra crianças e adolescentes - Embora esse tipo de crime tenha ocupado a penúltima colocação nesta pesquisa, o mesmo, deve ser considerado de grande relevância, dada a sua gravidade e seu caráter perverso. É importante destacar que tais crimes estão previstos na Lei nº 11.829/2008.

Figura 4: Análise por tipo de crime.



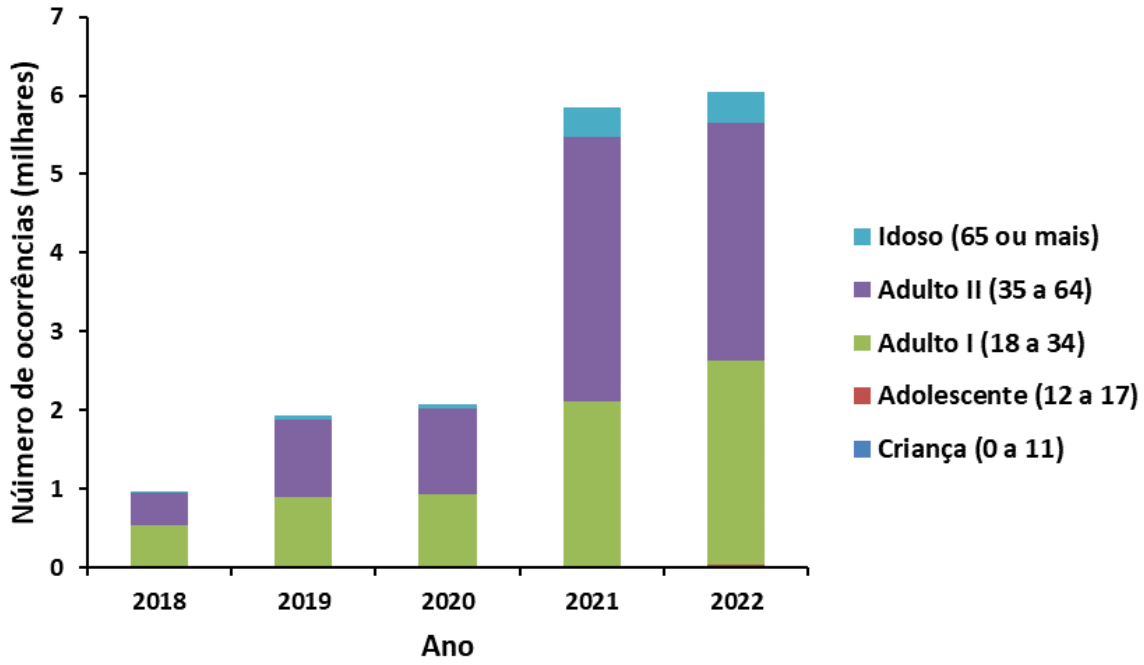
Fonte: Autora (2023)

Em relação à faixa etária das vítimas de crimes cibernéticos, observa-se que a ocorrência mais prevalente é na fase adulta, como observado na Figura 5. A baixa ocorrência de registro de crimes cibernéticos tanto na fase de crianças quanto de adolescentes pode ser

justificada em função de que essas faixas etárias costumam ser monitoradas no uso dessas tecnologias, entretanto Borges (2022) revela que houve um incremento na proporção de crianças e adolescente de 9 a 17 anos que fazem uso de internet no país, o que era de 89% em 2019 , e em 2021 chegou a 93%.

Em relação à faixa etária dos idosos, embora o número de ocorrência se apresente relativamente baixo, indica que essa categoria também é alvo dos criminosos cibernéticos, uma vez que, essa geração, mesmo com algumas dificuldades em operacionalizar determinadas tecnologias, vem ganhando cada vez mais acesso às ferramentas tecnológicas, como avaliam Almeida et al (2019) ao concluírem que os idosos também foram abarcados na ascendência das tecnologias porque estas podem lhes proporcionar maior autonomia, bem-estar e integração social.

Figura 5. Ocorrência de crimes cibernéticos conforme faixa etária

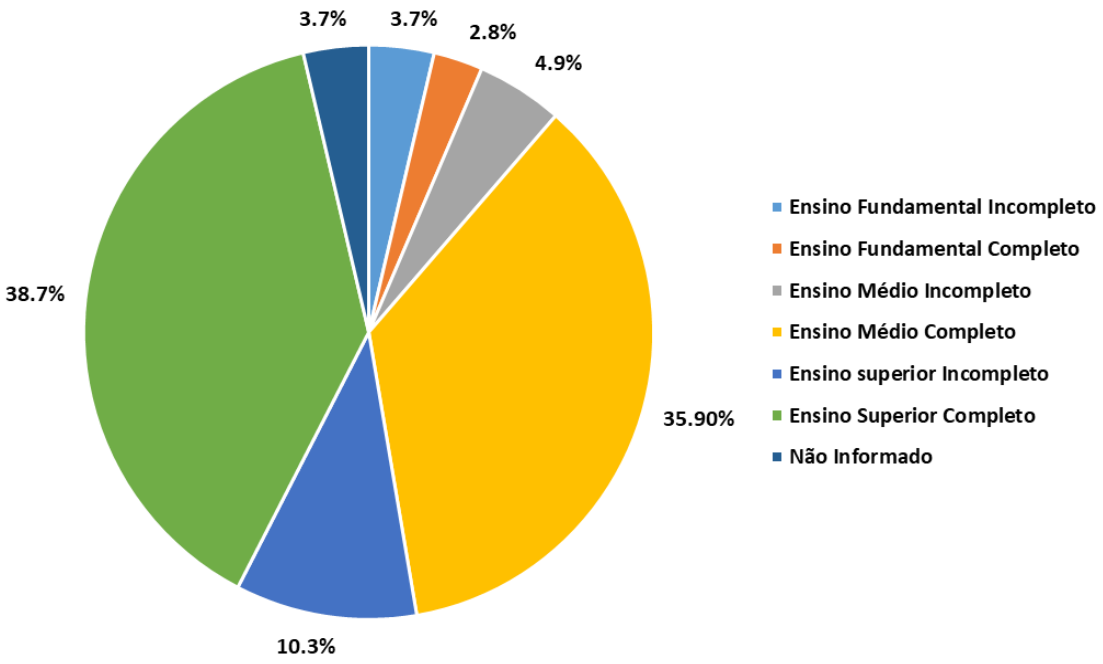


Fonte: Autora (2023)

Quanto à escolaridade, embora a ocorrência de crimes cibernéticos seja observada em todos os níveis de escolaridade, percebeu-se que quanto mais alto é o nível intelectual de uma pessoa mais propensa está de se tornar vítima de crimes cibernéticos, conforme observado na Figura 6, em que as vítimas mais prevalentes possuem ensino superior completo (38.7%) e ensino médio completo (35.9%), transparecendo que escolaridade e inclusão digital estão diretamente interligadas. Deste modo, o público mais escolarizado tem mais acesso às

Tecnologias da Informação e Comunicação(TIC), por isso, são mais propensos a se tornarem vítimas de crimes cibernéticos. Junqueira e Botelho-Francisco (2021) enfatizam que o acesso diferencial às TIC no Brasil não constitui apenas uma questão de exclusão digital, mas, de fato, um vetor da vulnerabilidade digital.

Figura 6: Ocorrência de crimes cibernéticos conforme escolaridade



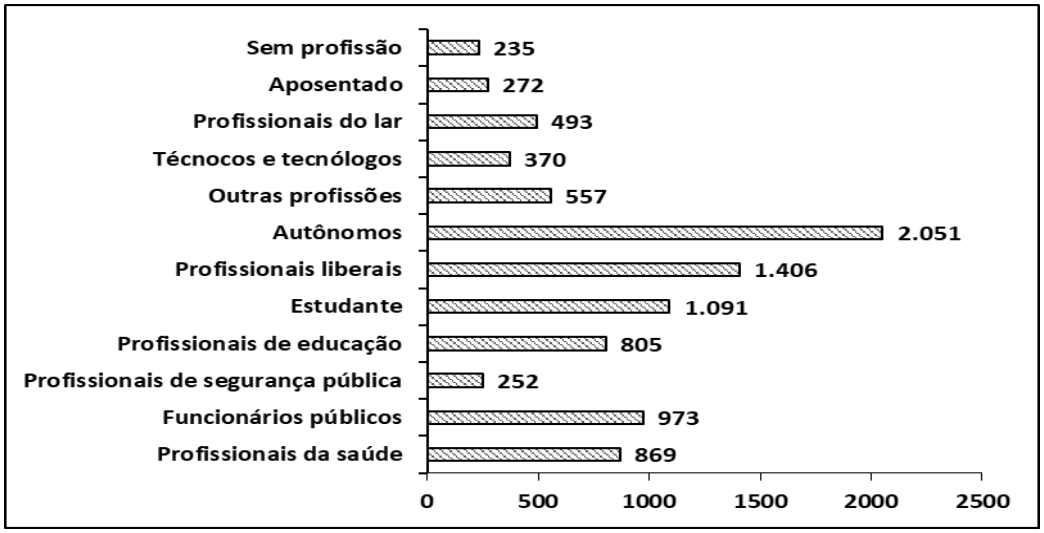
Fonte: Autora (2023)

Ao analisar os dados sobre as profissões das vítimas de crimes cibernéticos, foram identificadas ocorrências em diversos setores profissionais, com destaque dentre elas aos profissionais autônomos, que atingiram a maior prevalência ao longo da série histórica analisada. Destaca-se também a categoria de profissionais liberais e de estudantes, ocupando a segunda e terceira colocação, respectivamente, como as categorias mais atingidas para este estudo.

Essa diversidade, no que tange aos setores profissionais pode estar ligada a migração em massa de serviços e atividades em geral para o campo virtual conforme afirma Getschk (2022) que ao longo da pandemia houve um acentuado estímulo ao processo de digitalização em todas as esferas da vida humana. Com isso mudamos nossas formas de trabalhar, estudar, comprar e pagar, assim como modificamos também a forma de fazer consultas médicas e de nos comunicarmos com amigos e familiares.

Destaca Mans (2022) que houve modificação, durante a pandemia, no perfil de pessoas que realizavam trabalho remoto, sendo que em 2019 era composto por profissionais autônomos ou informais, e em 2020 abrangeu também os professores, gerentes, administradores e funcionários de escritório. No decorrer da pandemia, passaram a desempenhar suas atividades laborais de forma remota 65% dos profissionais com ensino superior e 59% dos profissionais das classes A e B.

Figura 7: Ocorrência conforme a profissão das vítimas

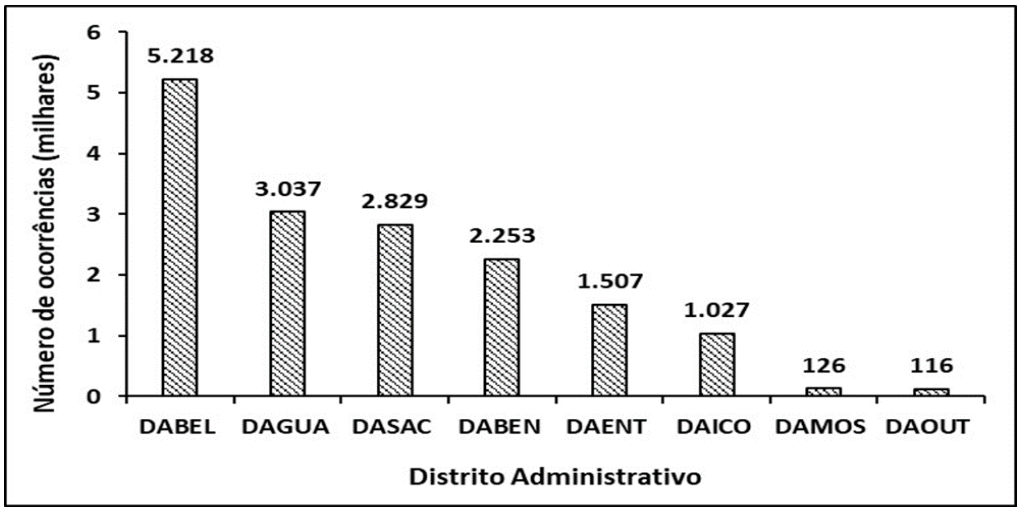


Fonte: Autora (2023)

Em relação ao local onde residem as vítimas foi possível identificar que a maior ocorrência de vítimas de crimes cibernéticos reside no Distrito Administrativo de Belém - DABEL, sendo este, o Distrito mais centralizado e que engloba os bairros mais nobres da capital do Estado, conforme apresenta a figura 8. A pesquisa TIC domicílios 2021, desenvolvida pelo Comitê Gestor da Internet no Brasil (CGI.br), constatou que a utilização da internet ainda é absoluta entre os usuários com maior renda. Em contrapartida, mesmo que o acesso tenha crescido entre os usuários que possuam menor renda, estes ainda têm acesso limitado à rede, com acesso através de um único dispositivo (telefone celular) com um único tipo de conexão (rede móvel ou Wi-Fi).

Alerta Lehfeld et al (2021) que a informatização em rede de forma global gera várias melhorias e facilidades na vida de todos, porém isto tem correspondido ao relaxamento da postura do usuário e atraído aqueles que têm intenções ilícitas relacionadas aos crimes cibernéticos.

Figura 8: Análise de vítimas por Distrito Administrativo do município de Belém/PA

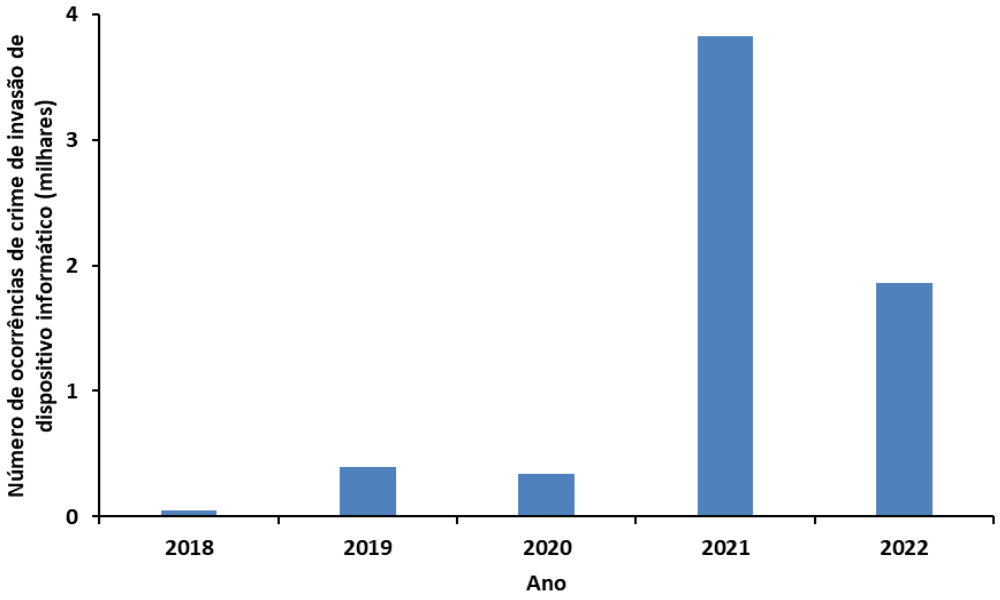


Fonte: Autora (2023)

4.1. ANÁLISE DO CRIME DE INVASÃO DE DISPOSITIVO INFORMÁTICO

A figura 9 abaixo, mostra que o crime de invasão de dispositivo informático teve destaque, principalmente para o ano de 2021. Isto tem relação com o momento pandêmico ocorrido no período, onde houve a otimização das atividades on-line(“home office”) e com isso o incremento considerável das demandas de crimes cibernéticos, não só na capital paraense, mas em todo país conforme argumenta Gastal (2021) ao afirmar que “foi durante a pandemia de COVID-19 que os crimes cibernéticos alcançaram os maiores índices vistos até então, de janeiro a setembro de 2020, o país sofreu mais de 3,4 bilhões de tentativas de ataques na internet”. Em relação a gravidade deste crime comentam Bomfati e Kolbe Junior (2020) que em uma invasão os invasores passam a ter acesso a informações particulares, isto é, a fotos, senhas bancárias, documentos, vídeos. Também causam danos às máquinas e equipamentos e roubam as informações encontradas. Com a vida inteira conectada, à medida que mais aparelhos

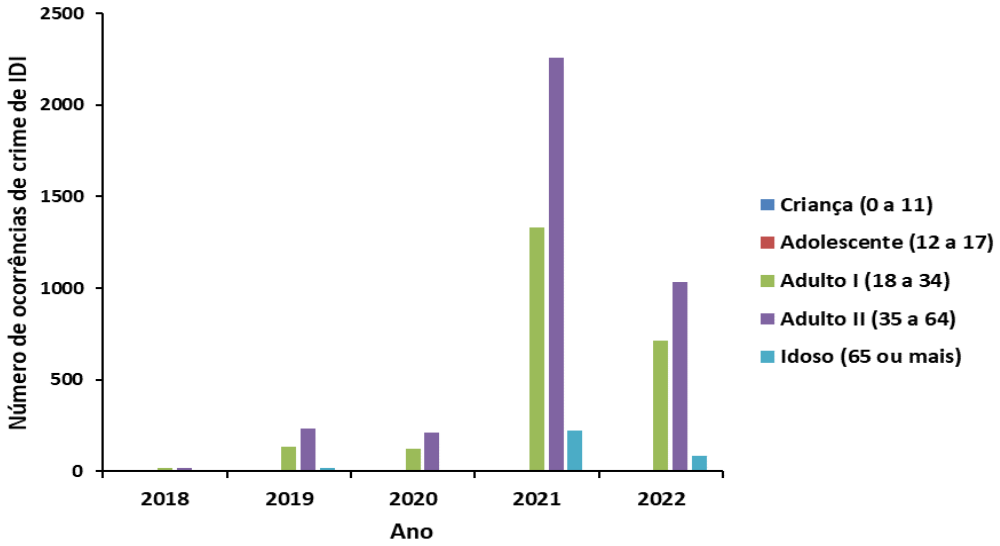
Figura 9 : Ocorrência de crime de invasão de dispositivo informático ao longo do período



Fonte: Autora (2023)

Em relação à faixa etária, conforme visualizado na figura 10, e de acordo com os dados para o município de Belém, percebe-se que as vítimas mais frequentes para este tipo penal são adultos entre 35 a 64 anos de idade. Ressalta-se que os maiores índices se deram para o ano de 2021, bem como se vê que esta faixa etária sempre aparece como a mais atingida ao longo de toda série histórica.

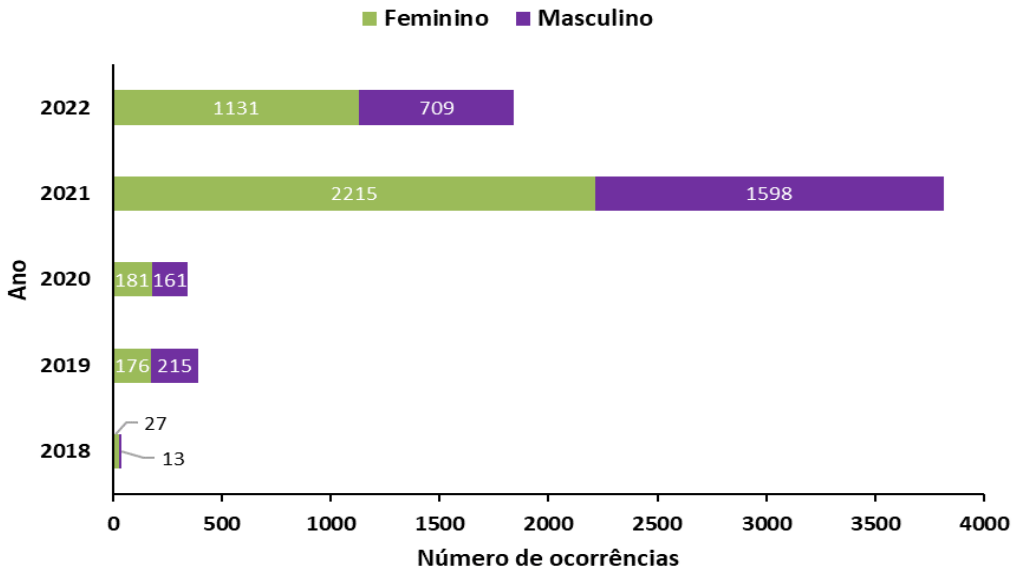
Figura 10 : Ocorrência de crime de invasão de dispositivo informático por faixa etária



Fonte: Autora (2023)

O crime de invasão de dispositivo informatico, teve como vitimas mais recorrentes pessoas do sexo feminino as quais continuam ocupando lugar de destaque no ranque de vitimas. Enfatiza Gastal (2021) que no período de “2019 para 2020, os registros de crimes cibernéticos com vítimas mulheres saltou de 7.112 para 12.698, um aumento de quase 80%. Dentre os delitos mais recorrentes, destacaram-se ameaças, crimes contra a honra, pornografia de vingança e stalking”. Observou-se um aumento extremo para o ano de 2021 e 2022 para capital paraense considerando que tal aumento está relacionado também com o período de pandemia, onde só cresceram os índices de crimes cibernéticos em razão da utilização em massa das tecnologias da informação e comunicações durante o isolamento social.

Figura 11 : Ocorrência de crime de invasão de dispositivo informático por sexo



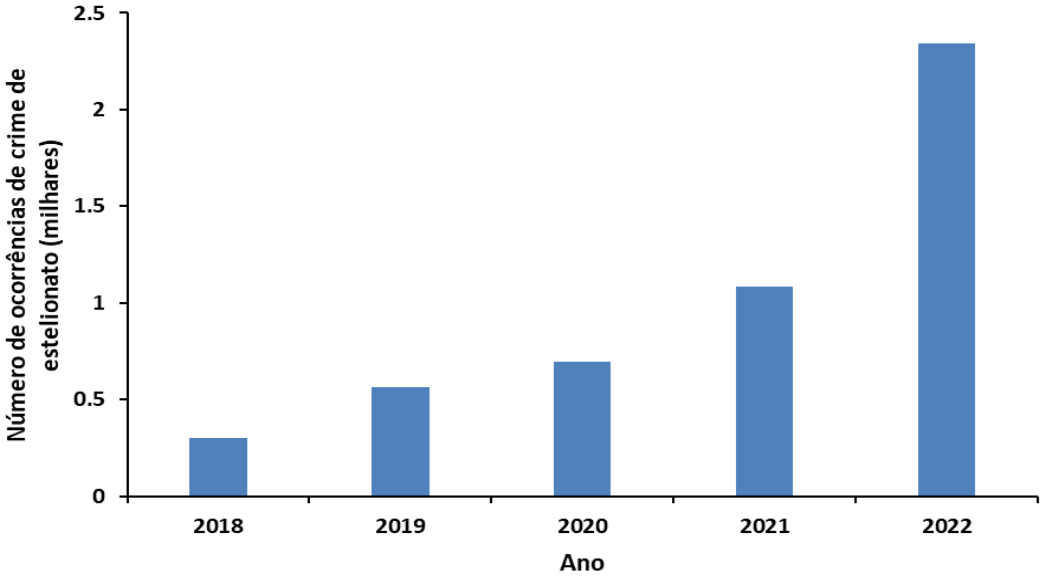
Fonte: Autora (2023)

4.2. ANÁLISE DO CRIME DE ESTELIONATO

Pontua-se que este crime teve, aumento do número de ocorrência com o passar do tempo, ao longo de todo o período analisado. Vale lembrar que o período analisado para o ano de 2022, corresponde apenas aos 06 seis primeiros meses(de janeiro a julho). Assim , pode-se dizer que este tipo penal, atualmente e principalmente tem ocorrido com muita frequência pelo simples fato da facilidade de enganar alguém através dos meio virtual, induzir e manter alguém em erro ao erro e a demora da pessoa enganada perceber o fato. Machado e Grott (2022) afirmam que o estelionato foi conduzido para ambientes virtuais em virtude dos avanços tecnológicos os quais facilitaram o cotidiano da sociedade. O crime com sua

característica de ligeireza encaixou-se na nova realidade virtual, dos meios eletrônicos, e assim expandiu-se.

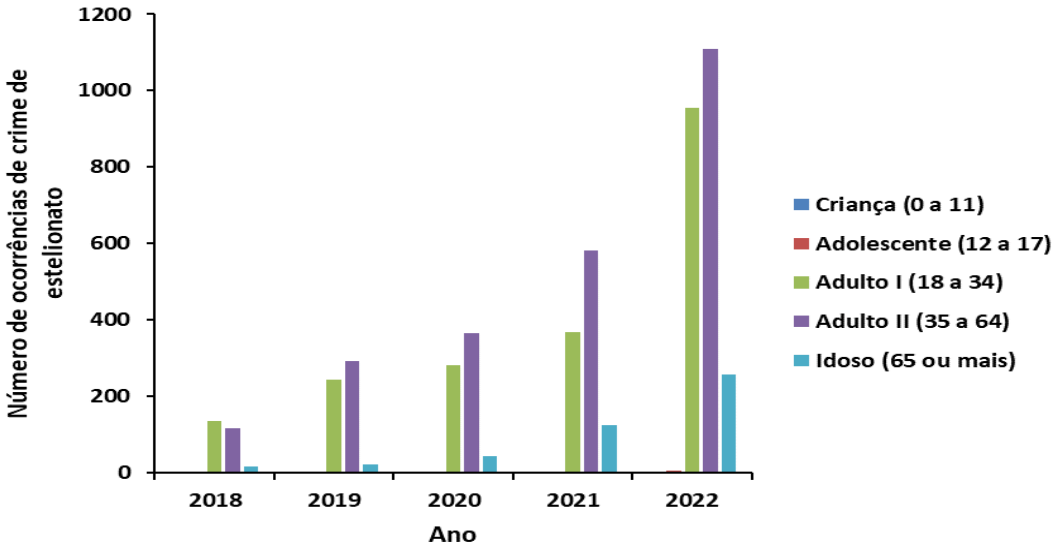
Figura 12 : Ocorrência de crime de estelionato ao longo do período



Fonte: Autora (2023)

Em relação à faixa etária das vítimas do crime de estelionato, figura 12, percebe-se que as vítimas mais frequentes para este tipo penal são também adultos entre 35 a 64 anos de idade. Entretanto, é relevante comentar que para a faixa etária de adultos com idades entre 18 a 34 e idosos (65 anos ou mais), observou-se também um aumento contínuo e expressivo. Para estas faixas comentadas constata-se que houve um aumento contínuo para todas ao longo do recorte temporal, bem como os dados mostram que os maiores índices se deram para o ano de 2022, considerando-se apenas os meses de janeiro a julho do ano de 2022.

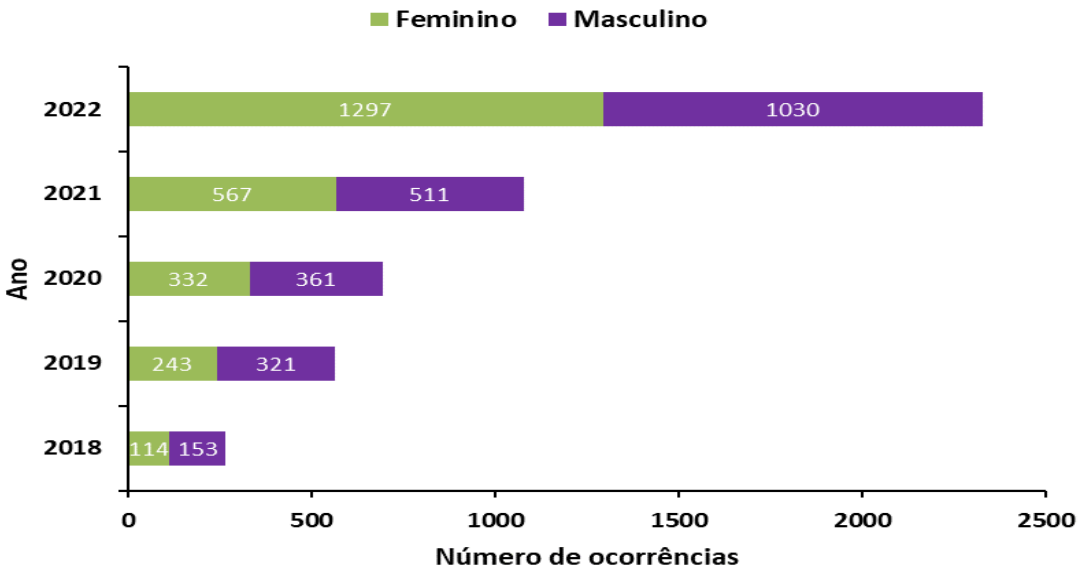
Figura 13 : Ocorrência de crime de estelionato por faixa etária



Fonte: Autora (2023)

No que que tange ao sexo das vítimas para o crime de estelionato é também recorrente o número de vítimas do sexo feminino, o que marca a ideia que mulheres são mais vulneráveis em meio virtual. Ressalta-se o amento para este sexo ao logo de todo o período analisado

Figura 14 : Ocorrência de crime de estelionato por sexo



Fonte: Autora (2023)

5. CONCLUSÃO

Através deste estudo e de acordo com constante no banco de dados da Secretaria de Segurança Pública do Estado do Pará, foi possível fazer uma análise acerca dos principais crimes Cibernéticos ocorridos no município de Belém/PA, bem como foi possível classificá-los e identificar o perfil das vítimas desses crimes no período de 2018 a 2022.

Assim, foi observado que o crime de maior destaque foi o crime de Invasão de dispositivo informático, seguido do crime de estelionato e em seguida os crimes contra honra (calúnia, injúria e difamação). Tais crimes observados para a realidade do municipio de Belém estão de acordo com os principais crimes cibernéticos ocorridos no país, o que revela uma tendência nacional nesta modalidade criminológica.

Notou-se ainda quanto ao perfil das vítimas quanto ao sexo, que há uma prevalência maior no sexo feminino, quanto ao quesito profissão, foi identificado vítimas nos mais variados seguimentos profissionais e em relação a faixa etária, a maior prevalência está entre os adultos de 35 a 64 anos de idade. Quanto à região de Belém com maior ocorrência de crimes cibernéticos foi no distrito central do município, onde se concentram os bairros de classe média alta da capital do Estado do Pará.

Deste modo, a pesquisa possibilitou ampliar os conhecimentos sobre a dinâmica dos crimes cibernéticos, para poder traçar um perfil das vítimas destes ilícitos. Sendo assim, espera-se que o conhecimento produzido seja de grande valia para o desenvolvimento de importantes trabalhos e até mesmo servir de inspiração para implementação de políticas públicas de segurança que trarão benefícios tanto para sociedade acadêmica quanto para a sociedade em geral.

6. REFERÊNCIAS

ALMEIDA, C.; COSTA, C.; MONTEIRO, M. J.; RAINHO, C.; BARROSO, I.; CASTRO, J.; RAIMUNDO, F.; RODRIGUES, V. Utilização de Novas tecnologias por Idosos Institucionalizados. **Revista Motricidade**. V15, Nº 4. pp. 31-35. 2019.

AZEVEDO, J. C., et al. The Controversies of Self - From(info) Ethics to Cyber Terror. **Journal of Information Systems and Technology Management**. Vol. 12, Nº. 3. pp. 577-594. 2015.

AZZAM, F. A. F. A adequação dos meios de cooperação internacional para combater o cibercrime e formas de modernizá-los. **JANUS.NET, e-journal of International Relations**. Vol. 10, Nº. 1, pp. 68-86. 2019.

BARRETO, A. G.; KUFA, K.; SILVA, M. M. Cibercrimes e seus reflexos no direito brasileiro.2ª Edição. **Editora Jus Podivm**. p.48. 2021.

BENSON, V.; MCALANEY, J.; FRUMKIN, L. A. 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. 2018.

BOMFATI, C. A; KOLBE JUNIOR, A. Crimes cibernéticos. Curitiba. **Editora Intersaberes**. 2020.

BORGES, L. E. Python para desenvolvedores: aborda Python 3.3. **Novatec Editora**. 2014.
Brasil (2021). Instituto Brasileiro de Geografia e Estatística – IBGE. Cidades e Estados. Disponível em: https://www.ibge.gov.br/cidades-e-estados/pa/belem.html. Acesso em: 26 out 2021.

Brasil. (1940). Decreto-Lei nº 2.848, de 07 de dezembro de 1940. Código Penal Brasileiro. Disponível em: www2.senado.leg.br/bdsf/bitstream/handle/id/529748/código_penal_1ed.pdf. Acesso em: 13 mai 2021.

Brasil. (1988). Constituição da República Federativa do Brasil de 1988. Disponível em: planalto.gov.br/ccivil_03/constituicao/ constituicao.htm. Acesso em 13 mai 2021.

Brasil. (2012). Lei n° 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http//www.planalto.gov.br/ccivil_03_ato2011-2014/2012/lei/l12735.htm. Acesso em: 13 mai 2021.

Brasil. (2012). Lei n° 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http//www.planalto.gov.br/ccivil_03_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 mai 2021.

Brasil. (2014). Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em: http//www.planalto.gov.br/ccivil_03_ato2011-2014/2012/lei/l12965.htm. Acesso em: 13 mai 2021.

BRASIL, B.S; RAMOS, E. M. L.S; ALMEIDA, S. DOS S.; BRASIL, M .M. A violência na prática de crimes no ciberespaço.Novos Cadernos NAEA. V.20, nº 2, p. 127-148,2017.

CASSANTI, M. O. Crimes Virtuais Vítimas Reais. **Editora Brasport livros e multimídia LTDA**. 2014.

CORREIA, P. M. A. R.; JESUS, I. O. A. Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas. **Revista Direito GV**. v. 12 n. 2. 542-563. 2016.

CRESPO, M. X. F. Crimes Digitais. **Editora Saraiva**. 2011.

DE FREITAS, E. S.; DA SILVA, M. G. Pesquisa-ação sobre a implementação do trabalho padronizado em uma célula de manufatura de uma fábrica de tratores. **Revista Espacios**, v. 38, n. 46, p. 21, 2017.

DEMEAU, E.; MONROY, M. E. V.; JEFFREY, K. Wildlife trafficking on the internet: a virtual market similar to drug trafficking? **Revista Criminalidad**, 61(2): 101-112. 2019.

DOS SANTOS, F. V. **Direito Penal simbólico e a Lei de combate a violência doméstica e familiar contra a mulher.** Boletim IBCCRIM. Ano 14, nº 167, 2006.

GARCIA, P. S.; MACADAR, M.; LUCIANO, E. M. A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. **Journal of Information Systems and Technology Management – Jistem USP**. Vol. 15. 2018.

GERHARDT, T. E.; SILVEIRA, D. T. Métodos de pesquisa. **Editora da UFRGS**. 1ª ed. 2009.

GETSCHK, D. **Um país mais conectado**. Revista br. Ed.19. Ano 13. 2022.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**, 6. ed. São Paulo: Atlas, 2008.

GOUVEIA, H. C. Sociologia do Crime. Salvador: UFBA, Faculdade de Direito; Superintendência de Educação a Distância, 64 p. il. 2018.

JUNQUEIRA, A.H.; BOTELHO-FRANCISCO, R. **Raça: dimensão interseccional das vulnerabilidades digitais.** Contemporanea, Revista de Comunicação e Cultura. V.19, Nº 03, p. 63-78. 2021.

KOLBE JUNIOR, A. **Investigação de crimes digitais**. Curitiba. Contentus. 2020.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

GASTAL, M. **Crimes Cibernéticos e a Pandemia de Covid-19**. Disponível em: https://www.wlm.org.br/crimes-ciberneticos-e-a-pandemia-de-covid-19/. Acesso em 18 fev 2023.

MARRA, F. B. Desafios do direito na era da internet: Uma breve análise sobre crimes cibernéticos. **Revista campo jurídico**, V.7, Nº 2. p.145-167. 2019.

MACHADO, D. R. G; GROTT, S. **Estelionato virtual: uma análise da pratica e repressão desse crime na cidade de Macapá-AP, entre os anos de 2018 a 2021**. Revista científica multidisciplinar do CEAP. 2022.

MANS, M. **O Teletrabalho persiste, mas não para todos**. Revista br. Ed.19. Ano 13. 2022.

MARTINEZ, F. **Feminismo em movimento no ciberespaço**. caderno pagu (56). 2019.

MENDES, G. F.; COELHO, I. M.; BRANCO, P. G. G. Curso de Direito Constitucional. **Editora Saraiva**. 4ª edição. 2008.

MENEZES, M. R. C.; CAVALCANTI, V. R. S. Mulher Jovem e Cibercultura: Liberdade, Subordinação e Reminiscências Patriarcais no meio Virtual. **Revista Ex aequo** (35), 33-47. 2017.

MORETTIN, P. A.; BUSSAB, W. O. Estatística básica. **Saraiva Educação SA**. 2017.
Pará. (1996). Lei nº 7. 806, de 30 de julho de 1996. Delimita as áreas que compõem os bairros de Belém, revoga a lei nº 7.245/84, e dá outras providências. Disponível em: https://cm-belem.jusbrasil.com.br/legislacao/581764/lei-7806-96. Acesso em: 26 out 2021.

PARÁ. Decreto Nº 690, de 16 de Abril de 2020. Institui a diretoria estadual de combate a crimes cibernéticos no âmbito da Polícia Civil do Estado do Pará, e dá outras providências. Diário Oficial do Estado do Pará. Ano CXXIX da IOE 130º da República Nº 34.187, em 17/04/2022

PEREIRA, W.; TANAKA, O. Estatística. 1990.

PINHEIRO, P. P. **Segurança da informação e meios de pagamento eletrônicos**. Curitiba. InterSaberes. 2022.

SILVA, M. B. F. DA. **Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet**. Rio de Janeiro. Freitas Bastos. 2023.

SOUZA, J.L.C. Crime, Polícia e Tecnologias da Informação. **Mediações**, Londrina, V. 22 N. 1, P. 301-324. 2017.

RIBEIRO, P. B. **Guerra cibernética: cenário mundial de defesa e segurança**. Curitiba. Contentus. 2020.

TERRON, L. L. S.; CORRÊA, R. A.; CORREIA, T. M. Cibercrimes: aspectos panorâmicos dos crimes informáticos mais praticados e as condutas de prevenção. e-Civitas - **Revista Científica do Curso de Direito do UNIBH - Belo Horizonte**. Volume XIII, número 1, jullho de 2020.

Viana FRM, Meneghetti FK. Is It Crowdsourcing or Crowdsensing? an Analysis of Human Participation in DigitaL Platforms in the Age of Surveillance Capitalism. REAd. Vol.26, N.º 1. p. 176-209. 2020

VICENTAINER, D.; MATTEDI, M.; MELLO, B. Aplicação das Bibliotecas Python para tratamento de dados em tempo real: A análize dos dados de isolamento social em Santa Catarina. **Metodologias e Aprendizado**. V.3.2020.

VINCIGUERRA, L., & al. **"An Overview of Code Obfuscation Techniques"**. Proceedings of the 2016 ACM Workshop on Information Hiding and Multimedia Security. 2016.

WENDT, E. JORGE, H. V. N. **Crimes Cibernéticos Ameaças e Procedimentos de Investigação**. Editora Brasport livros e multimídia LTDA. 2ª edição. 2013.

WENDT, E. JORGE, H. V. N. **Crimes Cibernéticos Ameaças e Procedimentos de Investigação**. Editora Brasport livros e multimídia LTDA. 3ª edição. 2021.

Wu, X., & Lee, W. **"Automatic Detection and Classification of Downloader Trojans"**. Proceedings of the 19th ACM Conference on Computer and Communications Security. 2010.

ZUBOFF, S. **A era do capitalismo de vigilância: a luta por um ser humano futuro na nova fronteira do poder**. Tradução de George Schlesinger. 1ª edição. **Intrínseca**. 2020.

BARBOSA ,A. F. Et Al. **Resumo Executivo TIC Domicilios 2021 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cetic.br/media/docs/publicacoes/2/20221121125804/resumo_executivo_tic_domicilios_2021.pdf. acessado em 04/02/2023.**

.

7. LISTA DE PUBLICAÇÕES (artigo, patente etc) DO AUTOR COM O OIRENTADOR EM ANDAMENTO E PUBLICADO.

- Artigo 1: Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020

Research, Society and Development, v. 11, n. 1, e43411125214, 2022
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v11i1.25214

Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020

Balance of the main cyber crimes that occurred in the municipality of Belém/PA in the period 2018 to 2020

Balance de los principales delitos cibernéticos ocurridos en el municipio de Belém/PA en el período 2018 a 2020

Recebido: 28/12/2021 | Revisado: 03/01/2022 | Aceito: 07/01/2022 | Publicado: 11/01/2022

Luciana Corrêa e Silva
ORCID: https://orcid.org/0000-0002-8665-7155
Universidade Federal do Sul e Sudeste do Pará, Brasil
E-mail: lucianacsilva@unifesspa.edu.br
Diego de Azevedo Gomes
ORCID: https://orcid.org/0000-0002-4005-8579
Universidade Federal do Sul e Sudeste do Pará, Brasil
E-mail: diagomes@unifesspa.edu.br

Publicado em 11 de janeiro de 2022