UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO MULTIDISCIPLINAR
PROGRAMA DE PÓS-GRADUAÇÃO INTERDISCIPLINAR EM HUMANIDADES DIGITAIS

CIBERCRIMES E HUMANIDADES DIGITAIS – UMA INVESTIGAÇÃO TRANSDISCIPLINAR SOBRE O CASO DA SEGURANÇA PÚBLICA BRASILEIRA

EMERSON DE BARROS DUARTE

RIO DE JANEIRO
2023

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO MULTIDISCIPLINAR
PROGRAMA DE PÓS-GRADUAÇÃO INTERDISCIPLINAR EM HUMANIDADES DIGITAIS

CIBERCRIMES E HUMANIDADES DIGITAIS – UMA INVESTIGAÇÃO TRANSDISCIPLINAR SOBRE O CASO DA SEGURANÇA PÚBLICA BRASILEIRA

EMERSON DE BARROS DUARTE

Sob a orientação do Professor
Sergio Manuel Serra da Cruz, Dr.

Dissertação submetida como requisito para obtenção do grau de **Mestre em Ciências**, no Programa de Pós-graduação Interdisciplinar em Humanidades Digitais, Área de Concentração em Análise Qualitativa e Quantitativa de Dinâmicas Sociais.

Rio de Janeiro
2023

D53c

DUARTE, EMERSON, 1972-
CIBERCRIMES E HUMANIDADES DIGITAIS – UMA INVESTIGAÇÃO TRANSDISCIPLINAR SOBRE O CASO DA SEGURANÇA PÚBLICA BRASILEIRA / EMERSON DUARTE. - Rio de Janeiro, 2023.
99 f.

Orientador: Sergio Manuel Serra da Cruz.
Dissertação(Mestrado). -- Universidade Federal Rural do Rio de Janeiro, Programa de Pós-graduação Interdisciplinar em Humanidades Digitais, 2023.

1. Humanidades Digitais. 2. Segurança Pública. 3. Cibercrimes. 4. Estatística Descritiva. 5. Sistemas da Informação. I. Manuel Serra da Cruz, Sergio, 1965-, orient. II Universidade Federal Rural do Rio de Janeiro. Programa de Pós-graduação Interdisciplinar em Humanidades Digitais III. Título.

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO MULTIDISCIPLINAR
PROGRAMA DE PÓS-GRADUAÇÃO INTERDISCIPLINAR EM HUMANIDADES DIGITAIS

EMERSON DE BARROS DUARTE

Dissertação submetida como requisito parcial para obtenção do grau de **Mestre em Ciências,** no Programa de Pós-graduação Interdisciplinar em Humanidades Digitais, área de Concentração em Análise Qualitativa e Quantitativa de Dinâmicas Sociais.

DISSERTAÇÃO APROVADA EM 27/03/2023

Sergio Manuel Serra da Cruz, Dr., PPGIHD/UFRRJ (Orientador)

Ricardo Cordeiro Corrêa, Dr., PPGIHD/UFRRJ

Renato Cerceau, Dr., UFF

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS

FOLHA DE ASSINATURAS

Emitido em 27/03/2023

HOMOLOGAÇÃO DE DISSERTAÇÃO DE MESTRADO Nº 38/2023 - DCOMP (11.39.97)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 22/05/2023 13:58)
RICARDO CORDEIRO CORREA
PROFESSOR DO MAGISTERIO SUPERIOR
PPGIHD (11.39.00.16)
Matrícula: ###07#4

(Assinado digitalmente em 22/05/2023 09:31)
SERGIO MANUEL SERRA DA CRUZ
PROFESSOR DO MAGISTERIO SUPERIOR
DCOMP (11.39.97)
Matrícula: ###24#6

(Assinado digitalmente em 23/05/2023 09:18)
RENATO CERCEAU
ASSINANTE EXTERNO
CPF: ###.###.597-##

Visualize o documento original em https://sipac.ufrrj.br/documentos/ informando seu número: **38**, ano: **2023**, tipo: **HOMOLOGAÇÃO DE DISSERTAÇÃO DE MESTRADO**, data de emissão: **22/05/2023** e o código de verificação: **9ca5ab01fc**

DEDICATÓRIA

Dedico esta nova conquista à minha família (Alessandra minha amada esposa, Alexia e Nicolas, meus filhos lindos e meus dois cachorrinhos Jack e Tokyo). Amo cada um de vocês e agradeço a paciência e o carinho ininterrupto que me fizeram superar cada obstáculo ou dificuldade que encontrei.

AGRADECIMENTO

A Universidade Federal Rural do Rio de Janeiro, sobretudo aos professores do Programa de Pós-Graduação Interdisciplinar que, mesmo frente a todas as adversidades que um momento de pandemia trouxe nos últimos anos, ainda assim conseguiram proporcionar conhecimento e colaborar com minha evolução profissional.

Aos profissionais da área de segurança pública de todo o Brasil que dedicam suas vidas em defesa da sociedade.

Ao Prof. Dr. Ricardo Cordeiro e ao Dr. Renato Cerceau por terem disponibilizado tempo, críticas, sugestões, orientações e apoio para que essa dissertação fosse concluída.

Ao amigo, professor e orientador Dr. Sergio Manuel Serra da Cruz eu agradeço a amizade, a paciência, a condução e a dedicação incansável que foram vitais para que eu chegasse até aqui. Preciso registrar que foi através de seu incentivo e apoio que tomei a decisão de encarar esse desafio, e por tudo de positivo que isso me proporcionou em evolução pessoal e profissional lhe sou eternamente grato.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

RESUMO

DUARTE, Emerson de Barros. **Cibercrimes e Humanidades Digitais – Uma Investigação Transdisciplinar Sobre o Caso da Segurança Pública Brasileira**. 2023. 98p. Dissertação (Mestrado em Humanidades Digitais). Instituto Multidisciplinar, Universidade Federal Rural do Rio de Janeiro, Nova Iguaçu, RJ. 2023.

A internet trouxe entre outros avanços a agilidade e a facilidade no consumo de serviços, e com a produção massiva de dados transformou e continua transformando as relações entre pessoas, organizações e governos. No entanto, junto com todos esses benefícios as organizações criminosas também evoluíram e se adaptaram, passando a atuar intensivamente nesse novo território digital, inclusive se valendo do alcance global de suas ações, de instabilidades geopolíticas e das dificuldades dos Estados em proteger seus cidadãos dos cibercrimes. Essa dissertação tem caráter transdisciplinar e busca compreender a interseção das Humanidades Digitais e o processo de transformação digital tendo o foco no crescente fenômeno do cibercrime. Neste trabalho desenvolvemos um método para criar e analisar um *dataset* relacionado aos cibercrimes ocorridos entre os anos de 2006 e 2021 no Brasil, coletamos dados reais de mais de 30 instituições de segurança pública brasileiras que foram analisados qualitativa e quantitativamente com o intuito de compreender o cenário brasileiro do cibercrime. Adicionalmente, esta dissertação também apresenta e discute uma proposta conceitual de artefato computacional que pode ser considerado como uma contribuição inicial que poderá ser aprimorada pelo Estado brasileiro ou por suas instituições de segurança para aumentar a resiliência dos seus serviços ou mesmo apoiar os cidadãos no que tange a mitigação de problemas relacionados aos cibercrimes mais comuns.

Palavras-chave: Humanidades Digitais, Segurança Pública, Cibercrimes, Estatística Descritiva, Sistemas de Informação

ABSTRACT

DUARTE, Emerson de Barros. **Cybercrimes and Digital Humanities – A Transdisciplinary Investigation on the Case of Brazilian Public Security**. 2023. 98p. Dissertação (Mestrado em Humanidades Digitais). Instituto Multidisciplinar, Universidade Federal Rural do Rio de Janeiro, Nova Iguaçu, RJ. 2023.

The internet has brought, among other advances, agility, and ease of use of distributed services, the massive production of data has changed and continues to transform relationships between people, organizations, and governments. However, despite of these benefits, criminal organizations have also evolved and adapted, starting to operate intensively in this new digital territory, including taking advantage of the global reach of their actions, geopolitical instabilities, and the difficulties of national States in protecting their citizens against cybercrimes. This dissertation has a transdisciplinary approach, it seeks to investigate the intersection of the Digital Humanities and the process of digital transformation, focusing on the growing phenomenon of cybercrime. In this work we developed a method to create and analyse a dataset related to cybercrimes that occurred between the years 2006 and 2021, we collected real data from more than 30 Brazilian public security institutions. Data were analysed qualitatively and quantitatively to understand the Brazilian scenario of cybercrime. Additionally, this dissertation also presents and discusses a conceptual proposal of a computational artifact that can be considered as an initial contribution to increase cyber resilience of Brazilian State or augment cyber security of public institutions to support citizens regarding the mitigation of problems related to most serious cybercrimes.

Keywords: Digital Humanities, Public Security, Cybercrime, Descriptive Statistics, Information Systems

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A espécie humana, em constante busca de satisfação de suas necessidades, se apoia em processos inovadores, invenções, descobertas e avanços tecnológicos que são capazes de mudar, por vezes, o rumo da própria história e dos comportamentos humanos.

A transição da manufatura para as máquinas a vapor, a descoberta da eletricidade, a invenção do computador e da rede internet, da computação ubíqua e expansão dos serviços digitais, são exemplos de sucessivos ciclos de inovação ou da clássica "onda de destruição criadora" enunciada por Schumpeter (1942). Essas transformações e evoluções de base tecnológica são típicas do sistema capitalista, intimamente relacionadas com os meios de comunicação e sem dúvida nenhuma representaram verdadeiros marcos da nossa História apesar de suas contradições.

Esses marcos representam enormes mudanças de valores em todas as sociedades onde a difusão da informação digitalizada globalizou-se muito velozmente, afetando as economias e até as instituições sociais. Segundo Negroponte (1995), hoje a linha entre o virtual e o real se torna cada vez mais tênue. Em seu livro seminal *Being Digital*, ele aponta que "a mudança de átomos para bits é irrevogável e imparável". Segundo o autor, tudo o que pode ser digitalizado será digitalizado, e em decorrência disso, o conceito do que é digital acaba se relacionando e influenciando as sociedades, ele nos permite entender como as tecnologias estão remodelando a humanidade.

De acordo com Lupton (2015), vivemos em uma sociedade digital onde a tecnologia mudou radicalmente e continua mudando o mundo em que vivemos. Para Lupton, as tecnologias digitais são parte integrante da vida cotidiana das pessoas e a vida social está agora tomando forma através delas. Afirmar que a sociedade é digital é afirmar que os conceitos de sociedade e cultura não podem ser totalmente compreendidos hoje sem reconhecer que indivíduos, relacionamentos e instituições sociais são moldados em algum grau por dispositivos de software e hardware. Isto posto, compreendemos que há uma clara correlação entre os temas "ser digital" de Negroponte (1995), "vida digital" de Lupton (2015) e as inovações e transformações digitais que afetam a sociedade.

Adicionalmente, segundo Schwab (2018), vivemos a chamada Quarta Revolução Industrial, que engloba um amplo aporte de tecnologias digitais centradas em dados, como por exemplo a inteligência artificial, as redes de alta velocidades, a robótica, a

impressão 3D, a internet das coisas, a *big data*, a ciência de dados, gêmeos digitais, as nanotecnologias, e a computação em nuvem, entre outros exemplos.

A quarta revolução industrial não pode ser compreendida isoladamente por cada uma destas tecnologias, mas por sinergias e convergências e de modo geral, essas tecnologias digitais estão mudando não só as formas de produção, como também os comportamentos humanos (LUPTON, 2015), e até mesmo os modelos de negócios no Brasil e no mundo (SCHWAB, 2018). E justamente por isso pode-se conjecturar que a quarta revolução industrial trouxe implicações importantes para o que é conhecido ou chamado de Humanidades Digitais, que entre outros aspectos, surge como sendo um campo de estudos ou de práticas cuja especialidade são o uso e aplicação da tecnologia digital em pesquisas em ciências humanas sociais.

Como elemento comum aos autores supracitados, se percebe a centralidade e a importância das humanidades nesta era de rápida transformação tecnológica, levando inclusive ao entrelaçamento de alguns pontos com a área de Humanidades Digitais, onde se consideramos o "ser digital" de Negroponte (1995), a "cibercultura" de Lévy (1997), "vida digital" de Lupton (2015) e o avanço da quarta revolução industrial discutido por Schwab (2018) e que também é conhecido sob a nomenclatura de Indústria 4.0, eles não estariam desconectados do processo da globalização e suas consequências como discutido por Bauman (2000).

Os autores, através de perspectivas complementares, destacam conceitos que indicam as profundas implicações da tecnologia nas atividades humanas e indiretamente nas Humanidades Digitais, como as mudanças referentes a instantaneidade dos transporte e acesso às informações, a crescente escala de produção derivada da automação dos processos da cadeia produtiva, e as formas de trocas de dados entre empresas, governos e sociedade, além da possibilidade do surgimento de novas culturas e modelos de negócios digitais que passam então a ser cada vez mais mediados por dados, sistemas e computadores.

O conceito Industria 4.0 foi incialmente utilizado pela primeira vez na Feira de Hannover em 2011 e foi anunciado pelo Governo Federal Alemão como uma das iniciativas-chaves na estratégia de um conjunto de tecnologias disruptivas para tornar a indústria nacional em ativos altamente tecnológicos, com a implantação de "indústrias inteligentes" ou "manufatura inteligente" (HERMANN; PENTEK; OTTO, 2016 e

SCHWAB, 2018). A contemporaneidade destes conceitos apresenta um tremendo desafio: a confusão do real com o ficcional traz implicações profundas nas transformações sociais e digitais que vivenciamos e ocasiona impactos profundos em como as organizações (lícitas ou ilícitas) percebem os valores dos seus processos, dados e repositórios.

Ou seja, a Industria 4.0 além de propiciar a integração em cadeias globais de valor, tem impacto significativo na produtividade das organizações, governos e principalmente como a sociedade se relaciona com os novos negócios e serviços digitais. Observando-se o conceito para além do aumento do desenvolvimento de produtos de uso em larga escala, um efeito colateral passa a ser a dependência tecnológica que, entre outros potenciais problemas, traz uma crescente preocupação pela segurança digital sobre as transações e os dados propriamente ditos.

Isto posto, há a necessidade de novos olhares com relação aos desafios e oportunidades que estas tecnologias digitais geram para as nações, organizações, serviços e pessoas, principalmente com relação aos impactos causados nos aspectos relacionados à segurança digital sob o ponto de vista do debate filosófico, político-sociológico, histórico e educacional envolvido na multidisciplinariedade da área de Humanidades Digitais.

Esta dissertação pretende compreender e estudar o conceito de cibercrime sob o ponto de vista das Humanidades Digitais tendo como escopo o cenário brasileiro de segurança pública, onde através de um estudo de caso inicial baseado em dados reais coletados em diversos estados da federação através dos serviços de ouvidoria e transparência pública governamental, apoiados pela Lei de Acesso à Informação (Lei nº 12.527, sancionada em 18 de novembro de 2011), se buscará um maior entendimento do que é e como o Estado brasileiro, em específico as unidades de segurança pública da Federação, lidam com esse desafio.

A linha de pesquisa proposta buscará explorar a interseção das Humanidades Digitais e o impacto derivado do processo de transformação digital e a adoção das tecnologias pela sociedade como um todo, tendo o foco o cibercrime como fenômeno social.

1.1 MOTIVAÇÃO

Amplos segmentos da nossa sociedade vêm se digitalizando velozmente. Segundo Bauman (2000), nos últimos anos, o processo de transformação digital das sociedades é decorrência do irreversível processo da globalização que se acelerou e amplificou as polarizações da condição humana graças às rápidas difusão e massificação das conexões de baixo custo entre computadores através de redes digitais distribuídas (também conhecida como rede Internet ou apenas internet).

Bauman (2000), destaca que a instantaneidade de transporte da informação junto ao baixo custo das comunicações inunda e sufoca a memória, em vez de alimentá-la e estabilizá-la. O autor sustenta que a globalização atinge a todos de modo diferenciado, com as elites e corporações se aproveitando desse rompimento de barreiras temporais, materiais e de localização como uma forma de se colocar acima da sociedade. Mantendo-se conectada utilizando os meios virtuais, mas não se aproximam das comunidades em que estão inseridas e em que geram sua desestruturação. Ele também destaca que virtualização afeta a todos de modo inevitável, incluindo o próprio Estado que não está imune a essas transformações quando cita por exemplo a difusão da internet.

A internet surgiu nos Estados Unidos na década de 1960, como consequência de pesquisas na área de tecnologia militar e de algumas universidades, e essa iniciativa tinha como objetivo estabelecer uma rede de telecomunicação [1]o menos vulnerável possível a um ataque nuclear soviético, na época da guerra fria entre americanos e russos (LEINER et al, 1997). Esse modo de agir eminentemente imaterial, impessoal e estratificado, aliado a dissolução do conceito de fronteiras físicas e geográficas através do intensivo uso de tecnologias digitais ultrapassou os círculos militares e alcançou a sociedade civil, trazendo consequências diretas e grandes mudanças em uma parte da humanidade, onde também se incluem as organizações criminosas.

Para Bauman (2000), essas mudanças velozes exacerbam as assimetrias (previamente existentes) e trazem em seu bojo algumas desvantagens como por exemplo, acentuar o distanciamento entre as ações do ser humano físico e o seus reflexos em ações digitais e, paradoxalmente, até mesmo o afastamento entre os próprios indivíduos físicos de seus grupos sociais. A globalização e esses distanciamentos, sob determinada ótica, poderiam vir a facilitar incursões maliciosas que explorariam limitações cognitivas e

[1]https://www.internetsociety.org/internet/history-internet/brief-history-internet/

comportamentais humanas, somadas as limitações tecnológicas presentes desde as primeiros versões de serviços na rede internet e seus protocolos.

É possível pressupor que o somatório dos fatores citados anteriormente permitiria que criminosos e as organizações criminosas viessem a perceber que suas ações delituosas poderiam ser aprimoradas através de novas oportunidades trazidas pela tecnologia. Giddens (2001) indica que essas ações criminosas podem surgir com o uso da tecnologia ou mesmo através dela, e o indicador de que isso foi efetivamente notado pode ser através das crescentes ondas de delitos cibernéticos cujos prejuízos passam a ser reportados por cidadãos, empresas e até mesmo Estados.

Um outro bom exemplo disso é introduzido por Lévy (1997) e discutido por Castells (1999), onde os autores discorrem sobre os aspectos sociais de como o uso da rede internet e a revolução do acesso às informações trouxe agilidade em processos antes basicamente materiais e que agora eram efetivamente digitais e realizados em tempo real, pontuando que esses avanços tecnológicos também (re)modelaram comportamentos e foram rapidamente percebidos e aproveitados por atividades criminosas e organizações ao estilo da máfia de todo o mundo, indicando que a transformação digital da sociedade impactou não só os negócios lícitos, mas também a forma de condução dos ilícitos.

Ainda nesse contexto, é possível assegurar que a prática de crimes, ou aquilo que é socialmente indicado como tal, é um fenômeno quase tão antigo quanto a própria humanidade, entretanto os delitos cibernéticos de amplitude global, com a formação de redes entre poderosas organizações criminosas e associados, é algo relativamente novo e que afeta profundamente a economia no âmbito internacional e nacional, a política e a segurança pública. Em última análise, essa conjunção afeta toda a sociedade em geral (CASTELLS,1999).

Diversos autores clássicos da área da sociologia tais como Castells (1999), Bauman (2000) e Giddens (2001), afirmam que a noção de "ação desviante" não é fácil de ser definida e que as organizações criminosas são flexíveis, elas vêm se expandindo e estabelecendo redes de parcerias com operações que ocorrem de uma forma distribuída e transnacional, aproveitando-se da globalização e das novas tecnologias de comunicações para transformar o "rosto do crime". Ou seja, ocorrem evoluções ou adaptações de delitos e crimes que antes ocorriam materialmente no *mundo analógico* e que agora aparecem nesse espaço digital que é popularmente chamado de "ciberespaço".

Sobre ciberespaço, Nye (2010) o define como um "regime híbrido único com propriedades físicas e virtuais". De forma semelhante, Melzer (2011) define o ciberespaço como uma rede global interconectada de informação digital e infraestrutura de comunicações, incluindo a internet, redes de telecomunicações, sistemas de computadores e toda a informação ali contida. Isto posto, apesar de toda a evolução e importância do ciberespaço, é necessário apontar que não houve a devida atenção à proteção e segurança dos usuários, sistemas e dados, criando oportunidades que são exploradas intensivamente por organizações criminosas ou indivíduos mal-intencionados.

Os avanços tecnológicos característicos do século XXI se apresentam em velocidades cada vez maiores, deixando evidente a frágil mobilidade dos sistemas jurídicos de diversos países. Com a digitalização da sociedade, os crimes também se digitalizaram. Ao considerar esse contexto de crimes pela internet, é possível se constatar que ocorreram migrações de eventos criminosos para esse novo espaço, onde existe relativa facilidade e consequentemente massificação de delitos cibernéticos. E esse fenômeno, que já era crescente mesmo antes da pandemia de COVID-19, acelera-se ainda mais nos dias de hoje onde segundo relatório[2] do FBI[3], as denúncias de vítimas de crimes cibernéticos aumentaram 69% em 2020 se comparados aos números de 2019 e foram 7% maiores em 2021 se comparados aos números de 2020.

No Brasil, segundo os dados da Coordenadoria de Estatística e Análise Criminal (CEACrim) divulgados pela Secretaria de Segurança Pública de Sergipe, o ano de 2020 apresentou um crescimento de 265% nos crimes praticados no ambiente virtual registrados no estado[4]. O amplo alcance da internet e seus serviços, e a relativa facilidade de atrair novos usuários inexperientes tornaram-se por si só um poderoso atrativo para o desenvolvimento de atividades ilícitas, e esses eventos de crimes cometidos no ciberespaço passam então a serem identificados como cibercrimes entre outras definições.

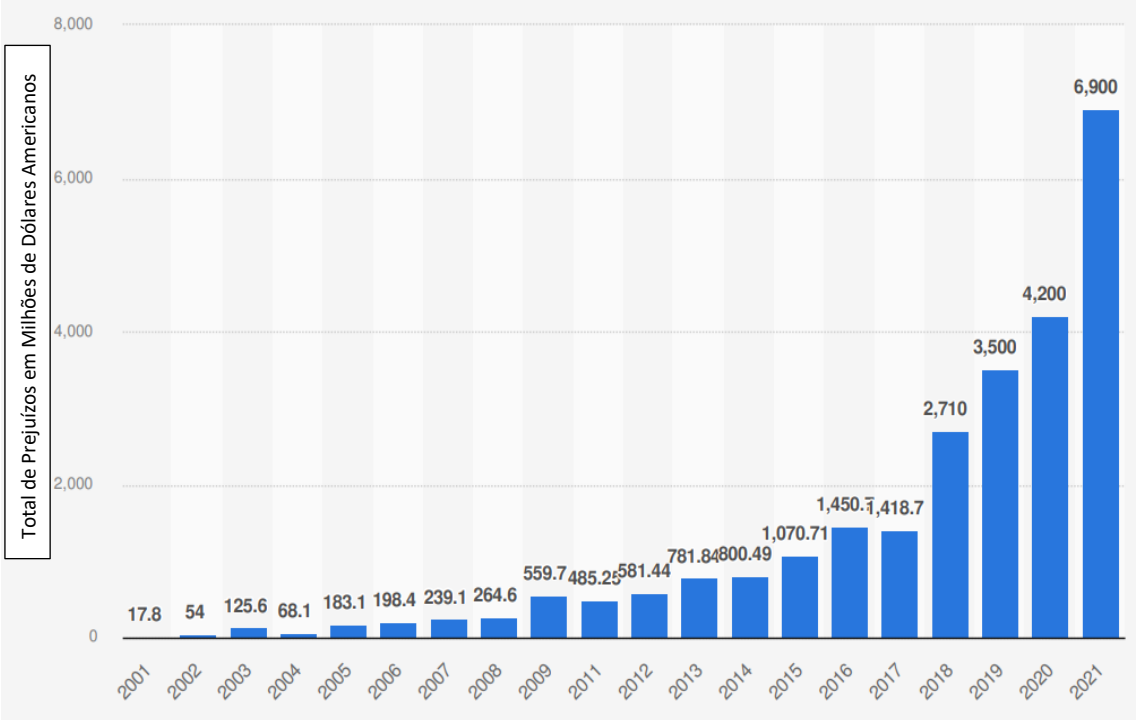
Neste ponto merecem destaque a subdenunciação, ou seja, há falta de conscientização sobre como, o que e onde denunciar e até inexistência uma tipificação amplamente aceita para denominar os crimes que são cometidos no ciberespaço. Existem várias definições que aparecem como sinônimos, tanto em trabalhos acadêmicos, como

[2] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[3] Federal Bureau of Investigation – "FBI, Polícia Federal dos Estados Unidos."
[4] https://www.ssp.se.gov.br/Noticias/Detalhes?idNoticia=17634

em artigos publicados na mídia, todos com ausência de concordância terminológica. Neste trabalho, doravante adota-se como designação padrão para o crime cometido no ciberespaço o termo “cibercrime”.

Com foco no cibercrime, usando os dados do relatório publicado pelo Polícia Federal Americana (FBI) (Gráfico 1) para se avaliar o quanto ele potencialmente afeta a população, é possível identificar que o prejuízo contabilizado em perdas para o cibercrime em 2021 foi o maior desde o início da monitoração estatística em 2000, chegando a perdas estimadas em US$ 6.9 bilhões.

Gráfico 1 – Prejuízos por ano



Fonte: Site statista[5]

Ou seja, como motivação para a realização dessa pesquisa, uma vez contextualizados os problemas trazidos pelo crescente fenômeno dos cibercrimes e suas implicações na sociedade digital, parece ser evidente a característica interdisciplinar que acaba por ser um dos indicadores de relevância e potencial para um estudo da área das Humanidades Digitais.

[5] Disponível em = https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/. Acesso em 18/09/2022

Esta dissertação apresentará um estudo desse problema sob a ótica das Humanidades Digitais e que merece destaque e aprofundamento da reflexão crítica envolvendo uma visão sobre os riscos e desafios decorrentes do exponencial uso das tecnologias e suas consequências, trazendo foco na análise de como o Brasil está se posicionando frente ao chamado cibercrime e como seria possível contribuir no grande desafio que envolve o tópico em questão.

1.2 OBJETIVOS GERAIS

O objetivo geral dessa proposta de dissertação é apresentar um estudo de caso interdisciplinar, sob a égide das Humanidades Digitais, baseado em dados reais sobre cibercrimes obtidos diretamente de órgãos de Segurança Pública pertencentes ao Estado. Neste estudo consideraremos o cenário brasileiro sobre cibercrimes, e visamos inicialmente compreender o que é esse tipo de crime, como o Estado brasileiro, em específico a área de segurança pública, está tratando do assunto, além de realizar considerações dentro do preconizado nas humanidades digitais e propor um artefato computacional que poderá vir a contribuir com a mitigação dos problemas relacionados do tema.

1.3 OBJETIVOS ESPECÍFICOS

Os objetivos específicos dessa pesquisa são:

- Caracterizar e analisar o cibercrime como fenômeno, utilizando os conceitos das Humanidades Digitais e Revisão Sistemática da Literatura como referenciais teóricos;
- Desenvolver estratégia e método para coletar dados públicos das estruturas de segurança pública brasileira relacionados a cibercrimes e criar uma corpora com os dados obtidos;
- Compreender e analisar esses dados e efetuar análise qualitativas e quantitativas e apresentar esses resultados;
- Apresentar uma proposta de um arcabouço conceitual de apoio à segurança pública, no que diz respeito a mitigação dos principais tipos de cibercrimes.
- Produzir artigo científico para apresentar os resultados desta pesquisa em eventos ou revistas da área.

- Registrar um produto de inovação e disponibilizar em um repositório público do tipo GitHUB todos os dados abertos desta pesquisa permitindo que ele seja reprodutível por outros interessados.

1.4 METODOLOGIA

Esta pesquisa é um estudo de caso que envolve aspectos teórico-práticos. Segundo Eisenhardt (1989), estudo de caso é uma estratégia de pesquisa que se concentra na compreensão das dinâmicas presentes dentro de cenários específicos. Os estudos de casos podem envolver casos únicos ou múltiplos e numerosos níveis de análise (YIN, 2010) e métodos de coleta de dados, tais como análise documental, entrevistas, questionários, observações e artefatos físicos (EISENHARDT, 1989; YIN, 2010). As evidências podem ser qualitativas, quantitativas ou ambas e ainda, os estudos de caso podem ser usados para fornecer descrições, testar ou gerar teorias (EISENHARDT, 1989).

Yin (2010) define o estudo de caso como uma pesquisa empírica, que investiga fenômenos contemporâneos dentro de um contexto de vida real, utilizado especialmente quando os limites entre o fenômeno e contexto são pouco evidentes. Atribui-lhe o objetivo de explorar, descrever e explicar o evento ou fornecer uma compreensão profunda do fenômeno.

1.4.1 ABORDAGEM E ESTRATÉGIAS ADOTADAS

Para atender os objetivos propostos desse estudo, foi necessário definir qual seria a abordagem mais adequada para o contexto (qualitativa, quantitativa ou uma combinação delas) e nesse sentido, Selltiz, Jahoda e Destsch (1974) descrevem uma classificação das pesquisas sociais em três grupos distintos: estudos exploratórios, estudos descritivos e estudos que verificam hipóteses causais.

Os estudos exploratórios são descritos como “todos aqueles que buscam descobrir ideias e soluções, na tentativa de adquirir maior familiaridade com fenômeno de estudo”. O estudo descritivo “expõe características de determinada população ou de determinado fenômeno. Podendo também estabelecer correlações entre variáveis e definir sua natureza. Não tem compromisso em explicar os fenômenos que descreve, embora sirva de base para tal explicação” (VERGARA, 2004, p. 47), e o estudo explicativo (ou causal) busca identificar os fatores que contribuem para a ocorrência de determinado fenômeno, deste modo, visa a explicar a razão dos acontecimentos (GIL, 2007; VERGARA, 2004).

Godoy (1995, p. 63) argumenta que quando estamos lidando com problemas pouco conhecidos e a pesquisa é de cunho exploratório, este tipo de investigação parece ser o mais adequado. Se o estudo é de caráter descritivo, e o que se busca é o entendimento do fenômeno como um todo, é possível que a análise qualitativa seja a mais indicada e que se a preocupação for a compreensão da teia de relações sociais e culturais que se estabelecem no interior das organizações, o trabalho qualitativo pode oferecer interessantes e relevantes dados e nesse sentido, a opção pela metodologia qualitativa se faz após a definição do problema e do estabelecimento dos objetivos da pesquisa que se quer realizar.

A abordagem qualitativa possui uma interação dinâmica "entre o mundo real e o sujeito, isto é um vínculo indissociável do mundo objetivo e a subjetividade do sujeito que não pode ser traduzida em números" (SILVA; MENEZES, 2005, p. 20). Em outros termos, o foco não é quantificar uma ocorrência ou quantas vezes uma variável aparece, mas sim na qualidade em que elas se apresentam (MINAYO,1994), ou seja, como as coisas acontecem.

Como esta proposta de pesquisa pretende analisar como são tratados os aspectos relacionados as interações sociais quando no uso e acesso à tecnologia dentro do escopo da segurança pública e os cibercrimes, a escolha pela metodologia de estudo de casos com foco qualitativo e quantitativo se justifica, pois, segundo Yin (2001), é a abordagem mais adequada quando faz-se questões do tipo "como" ou "porque" sobre um conjunto contemporâneo de acontecimentos sobre o qual o pesquisador tem pouco ou nenhum controle.

1.5 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está organizada da seguinte forma, além deste capítulo introdutório temos, o capítulo 2 que trata do referencial teórico, o capítulo 3 apresenta a revisão sistemática da literatura, o capítulo 4 a coleta e análise dos dados, no capítulo 5 é apresentada a proposta conceitual de ambiente digital de registro de ocorrências de cibercrimes, sendo o capítulo 6 o último capítulo onde apresento as conclusões, limitações e os possíveis desdobramentos em trabalhos futuros.

2 REFERENCIAIS TEÓRICOS

Este capítulo tem como objetivo apresentar os principais conceitos relacionados ao cibercrime e suas correlações, tendo ao final a apresentação de um conjunto de trabalhos relacionados.

2.1 A SOCIEDADE DA INFORMAÇÃO E A QUARTA REVOLUÇÃO INDUSTRIAL

Grandes porções da sociedade atual encontram-se visceralmente interligadas devido as tecnologias de informação e comunicação (TIC). Castells (1999), ainda no século XX, já conjecturava que a sociedade estaria umbilicalmente ligada a uma densa revolução que se apoiaria na dependência de dados digitais que seria a base da reestruturação do sistema capitalista que visaria estabelecer um novo paradigma.

Castells destacou as características fundamentais desse novo paradigma:

(a) a informação como matéria-prima;

(b) os efeitos de hiper conectividade e ubiquidade;

(c) o predomínio da lógica das redes;

(d) a flexibilidade dos sistemas e dispositivos móveis;

(e) a hiper convergência de tecnologias digitais.

Baseado nesse conjunto de características, o autor cunhou o termo “Sociedade da Informação” onde a informação (na verdade os dados em forma digital) e sua disponibilização se constituem como “o principal ingrediente de nossa organização social, e os fluxos de mensagens e imagens entre as redes constituem o encadeamento básico de nossa estrutura social.” (CASTELLS, 1999, p. 573). O autor também destacou que a hiper conectividade seria ao mesmo tempo uma forma de viver dependente das redes digitais e um método que poderia gerar marginalização de determinadas regiões ou grupos sociais.

Ao considerarmos uma perspectiva histórica mais ampla, se percebe um fio condutor entre a primeira revolução industrial e o início do século XXI, tendo um vasto

conjunto de transformações estruturais na economia global. Atualmente, as demandas por inovações tecnológicas são reflexos dessas transformações, gerando inovações com fluxos incessantes que atuam como um diferencial competitivo entre organizações e países. As inovações podem levar a rupturas de modelos de negócio tradicionais e ao surgimento de novos paradigmas, que acontecem de modo cada vez mais célere impactando profundamente as sociedades e a forma como os humanos, empresas e o até mesmo os crimes se relacionam.

O mundo contemporâneo vive um processo de aceleradas mudanças baseadas em diversas tecnologias, sobretudo as de ligação com a computação e dados. Esse processo é descrito por inúmeros autores que teorizam e buscam compreender e explicar esse momento. Por exemplo, Rifkin (2011) o nomeia de "terceira revolução industrial". Já Brynjolfsson e McAfee (2014) o intitula "segunda era das máquinas". Por fim, Schwab (2018) o define como "quarta revolução industrial". Nesta pesquisa adotaremos a perspectiva de Schwab.

Schwab (2018) apregoa:

> "Atualmente, enfrentamos uma grande diversidade de desafios fascinantes; entre eles, o mais intenso e importante é o entendimento e a modelagem da nova revolução tecnológica, a qual implica nada menos que a transformação de toda a humanidade. Estamos no início de uma revolução que alterará profundamente a maneira como vivemos, trabalhamos e nos relacionamos".

A quarta revolução industrial, ainda que em muito se baseie na hiper conectividade das TIC caracterizada por Castells (1999) e promova significativos, profundos e irreversíveis reflexos no sistema capitalista, atrai também olhares das organizações criminosas. Bezerra et al. (2021) e Filho (2021) pontuam que o cibercrime é um dos maiores riscos para a prosperidade na quarta revolução industrial, pois à medida que cresce o uso da internet surgem novos problemas cada vez mais complexos, com relevante destaque para as atitudes nocivas à segurança digital de pessoas e organizações.

É possível perceber que há uma correlação entre a "Sociedade da Informação" de Castells e a quarta revolução industrial de Schwab. Nossa percepção é que esses conceitos podem ser conectados através do paradigma da transformação digital.

2.2 A TRANSFORMAÇÃO DIGITAL

A transformação digital é um paradigma exclusivo do nosso tempo, é um processo em que as mudanças podem alterar fundamentalmente serviços, expectativas e comportamentos dos consumidores, pressionando organizações tradicionais e até interromper vários mercados; é um processo dinâmico e que *a priori*, não pode ser prevista no horizonte do tempo (VENKATRAMAN, 2017).

Verhoef et al., (2021) relata que a transformação digital é multidisciplinar por natureza, pois envolve mudanças de estratégia, organização, tecnologia da informação, cadeias de suprimentos e marketing. Adicionalmente, os autores informam que apesar da onipresença e do impacto visível da transformação digital nos novos modelos de negócios, a literatura acadêmica, até o momento, tem surpreendentemente prestado pouca atenção a esses desenvolvimentos, apenas recentemente começando a abordar os tópicos de digitalização e transformação digital.

De fato verificamos que no momento existe um amplo leque de definições na internet, desde as mais simplórias, como por exemplo, Sauvage (2018) que define transformação digital como: "O uso de todas as tecnologias digitais disponíveis, para melhorar o desempenho dos negócios e contribuir para um aumento geral no padrão de vida" e Dabi-Schwebel (2018) que a define como "o conjunto de processos de integração total das tecnologias digitais de uma organização em todas as suas atividades", ou até mesmo as sofisticadas revisões sistemáticas apresentadas por Venkatraman, (2017), Zaoui e Souissi (2020) e Verhoef et al., (2021).

Nesta dissertação, a transformação digital é considerada como um fenômeno paradigmático presente em todas as organizações (lícitas ou ilícitas) com amplas implicações no *modus operandi* do empreendimento em que principalmente, o modelo de negócio da organização está sujeito a mudanças por meio do uso de tecnologia da informação e comunicação. Em busca da transformação digital, as organizações lícitas buscam e implementam inovações e novos modelos de negócios enquanto as

organizações ilícitas buscam aprimorar seus métodos para refinar os ilícitos ou cibercrimes contra pessoas, empresas e contra o próprio Estado.

Ou seja, é necessário compreender um aparente paradoxo onde à medida que as organizações lícitas aceleram seus processos de transformação digital e envolvem mais dados digitais, serviços e consumidores, a segurança cibernética se torna uma das principais prioridades no gerenciamento de riscos corporativos contra a crescente escalada de ataques, ameaças e cibercrimes perpetrados por organizações ilícitos e que também se apropriam do paradigma da mesma transformação digital para evoluírem.

Um desdobramento desse paradoxo também pode ser compreendido ao se considerar as novas formas de comunicação e representação de dados, podendo-se afirmar seguramente que manter dados com segurança é tão importante quanto usá-los ou compartilhá-los e que qualquer possibilidade de falha, por mais simples que seja, irá eventualmente se transformar em vulnerabilidade.

2.3 HUMANIDADES DIGITAIS

As Humanidades Digitais podem ser consideradas uma área recente, mas já consagrada e institucionalizada na academia, tendo seu início nos anos 1950. McCarty (2015) destaca que elas surgiram nos primórdios da expansão da computação digital. O primeiro trabalho de Humanidades com métodos computacionais que se tem notícia foi liderado pelo jesuíta e teólogo Roberto Busa quando procurou Thomas J. Watson, fundador da IBM, requisitando ajuda para indexar os trabalhos de Tomás de Aquino.

Segundo McCarty (2015), as Humanidades Digitais não devem ser compreendidas meramente como atividades tecnológicas impulsionadas pela sua própria progressão evolucionária no tempo, nem mesmo um surgimento repentino de uma atividade singular, mas a capacidade de inventar e ser reinventado pela tecnologia digital. O autor defende que tal atividade ainda pode ser encarada como uma *nova heurística* para os acadêmicos oriundos das Humanidades, permitindo observar relações que demandariam muito esforço ou até mesmo seriam improváveis de serem apontadas apenas pela dedicação da capacidade pessoal sem o apoio de métodos computacionais.

McCarty (2015) apregoa que as Humanidade Digitais podem ser divididas em três fases baseadas na compreensão do início da Web como sendo um dilúvio de dados que se alastra, perpetua e se expande até os dias hoje:

1) *Fase Antediluviana* (1949-1991) - iniciada por Busa, cujo trabalho pode ser considerado um dos, senão o pioneiro da utilização dos métodos computacionais para as pesquisas nas Humanidades, ainda na década de 50, até a criação da Web, com um domínio no campo linguístico e literário;

2) *Fase Diluviana* (1990-2005) - centrado no surgimento da Web, com a difusão de repositórios e dados na Web, inserção de objetos digitais em forma virtual e a explosão das plataformas digitais para diversos tipos de usuários;

3) *Pós-Diluviana* (2005-atualidade) - baseadas nas questões que dizem respeito a análise, visualização, geolocalização de dados redes sociais e a problematização disciplinar dos usos de dados se tornam centrais nos estudos de Humanidades

Outros autores também tentam conceituá-la para descrever o que seriam as Humanidades Digitais. Por exemplo, Kirschenbaum (2010, p. 56) afirma tratar-se de um campo de estudo, pesquisa, ensino e invenção relacionado à interseção da computação e as disciplinas das ciências humanas, sendo metodológico por natureza e interdisciplinar em escopo, envolvendo a investigação, análise, síntese e a apresentação das informações em formato eletrônico e como essas mídias afetam as disciplinas em que são usadas.

Ao se buscar o que seria a área de atuação das Humanidades Digitais, em março de 2010 foi elaborado o "Manifesto das Humanidades Digitais" durante o THATCamp (The Humanities and Technology Camp) em Paris, que foi um encontro onde humanistas e tecnólogos de todos os níveis de habilidade buscaram aprender e construírem juntos o que seria essa nova área de estudo, e o que foi apresentado é que as Humanidades Digitais englobariam o conjunto de pesquisas e experiências com uso dos recursos digitais de forma fácil, intuitiva e acessível, com foco nas comunidades de pesquisa e nos atores que integram os processos de criação, edição, valorização e conservação dos conhecimentos. Os signatários afirmam que as Humanidades Digitais são mais do que uma "transdisciplina, portadora dos métodos, dos dispositivos e das perspectivas heurísticas ligadas ao digital no domínio das Ciências humanas e sociais", as Humanidades Digitais referem-se "ao conjunto das Ciências humanas e sociais, às Artes e às Letras. Não

negando o passado, apoiando-se no conjunto dos paradigmas, *savoir-faire* e conhecimentos próprios dessas disciplinas, mobilizando simultaneamente os instrumentos e as perspectivas singulares do mundo digital." (THATCAMP, 2010).

Outros autores, tais como Krapp (2020), consideram que as Humanidades Digitais não necessariamente precisam implementar ferramentas tradicionais da área de Ciências de Dados para explorar as dimensões quantitativas dos seus objetos de interesse. O autor anuncia que é possível utilizar uma abordagem interpretativa e manter a conversação entre as Humanidades Digitais com as Humanidades propriamente ditas. O autor acredita que é possível que as Humanidades Digitais possam construir formas de aplicar os métodos das Ciências Humanas à cultura digital, e não apenas utilizar as ferramentas digitais para exibir e representar temáticas tradicionais das Humanidades.

Conforme artigo de Moura (2019), as Humanidades Digitais constituíram uma série de valores e métodos à medida de sua ampliação como comunidade de prática de proporções globais. Ainda sobre as Humanidades Digitais, ao citar Honn (2014) são indicados valores como o caráter crítico e teórico da atuação humanista na análise das ferramentas, tecnologias e plataformas, com foco na produção de forma colaborativa entre diferentes atores, múltiplos modos de expressão do conhecimento e com orientação da produção científica de forma ampla e irrestrita buscando a circulação do conhecimento produzido e a colaboração entre os pares.

Por último, Berry (2011), contextualiza as Humanidades Digitais como um modo de se pensar as mudanças nas estruturas sociais e na área de pesquisa, e que são condicionadas pela tecnologia, sua disponibilidade e acesso. Desta forma e partindo destes conceitos e abordagens, é possível afirmar que nessa dissertação consideramos que as Humanidades Digitais podem ser definidas como sendo a interseção do conhecimento dos estudos nas ciências humanas que, quando expostos ao uso de ferramental tecnológico, sofrem transformações metodológicas e estruturais em suas visões e resultados.

Se consideramos a tríade da contemporaneidade das Humanidade Digitais, as crescentes demandas da sociedade em termos de segurança digital e o "Manifesto das Humanidades Digitais" de 2010, verificamos que existem poucos estudos e investigações que explicitem suas inter-relações em termos de Brasil. No entanto, é importante salientar

que "transdisciplinaridade" do Manifesto não só permite como também nos estimula a buscar associação de novos métodos, dispositivos e perspectivas heurísticas das ciências humanas e sociais com perspectivas singulares abertas pelas tecnologias digitais. Essa faceta vai de encontro do tema dessa dissertação que busca compreender e desvendar as inter-relações das Humanidades digitais com os cibercrimes.

2.4 CIBERCRIMES

A sociedade digital vem se transformando significativamente nas últimas décadas o que também se reflete nas mudanças das atividades no mundo do crime organizado (DI NICOLA, 2022). Os crimes e seus perpetradores estão em constante mutação por conta da evolução tecnológica, como por exemplo, em termos de tipologias e *modo operandi,* usando a tecnologia como meio ou objetivo de cometimento de ilícitos, e atuando de forma onde fica cada vez mais difícil identificar as barreiras entre o crime cometido no mundo real e no mundo digital. O cibercrime é um fenômeno mundial e desde a criação da internet vem crescendo exponencialmente na mesma proporção da ampliação da Web (KUNRATH, 2017).

O Brasil, conforme notoriamente noticiado pela imprensa nacional e estrangeira, é um paraíso da pirataria virtual e alvo de organizações criminosas, e isso pode ser visto em levantamento realizado pela empresa Serasa Experian[6] que em seu *Indicador de Tentativas de Fraude,* mostra que o primeiro semestre de 2021 teve uma movimentação possivelmente fraudulenta a cada 8 segundos com 1,9 milhão de ataques ao longo dos seis primeiros meses do ano, o que significa um aumento de 15,6% com relação ao mesmo período de 2020 e é o maior volume já registrado no semestre desde o início do índice, em 2011. Outra indicação do cibercrime atuante no Brasil é apresentada pelo site Olhar Digital[7], que reproduz uma matéria sobre um vírus desenvolvido por "cibercriminosos" brasileiros e que tem como alvos instituições bancárias na Europa e América Latina.

Atualmente existem várias nomenclaturas e terminologias na literatura sendo utilizadas para designar um crime praticado através de um computador conectado à rede Internet, dentre elas podemos citar: *crimes virtuais, crimes digitais, crimes informáticos,*

[6] https://www.serasaexperian.com.br/sala-de-imprensa/analise-de-dados/brasileiros-sofrem-uma-tentativa-de-fraude-a-cada-8-segundos-revela-levantamento-da-serasa-experian/
[7] https://olhardigital.com.br/2021/09/13/seguranca/virus-brasileiro-bradesco/

crimes cibernéticos, crimes de computador, fraude informática, cibercrimes, crimes perpetrados pela internet, e-crime, entre outras.

Existem variedades desafiadoras de definições conceituais correlacionadas com o tema cibercrime. As definições variam conforme área de *expertise* do autor, mas em geral tem a TI como elemento central para a realização dos atos. Por exemplo, para o Escritório das Nações Unidas que cuida de Drogas e Crime (UNODC) (UNODC, 2013) "cibercrime" se compreende como uma ampla variedade de ofensas, incluindo aquelas contra dados e sistemas de computador ("hackers"), falsificação e fraude relacionadas a computadores ("phishing"), ofensas de conteúdo (disseminação de pornografia infantil) e ofensas de direitos autorais (divulgação de conteúdo pirateado).

Segundo Neto e Guimaraes (2003) o cibercrime significa: "qualquer conduta ilegal, não ética ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados". Já para Silva (2018) os crimes informáticos são gênero do qual os crimes cibernéticos são espécie. O autor pontua que a diferença é sutil. Ele informa que, apesar de ambos serem cometidos com a utilização de um computador, os crimes cibernéticos são perpetrados no âmbito ou por meio da internet.

Com o consumo exponencial pela população de tecnologias digitais e consequentemente possuindo uma maior presença em aspectos cotidianos, os pontos positivos que derivariam desse fenômeno e que levaram ao aprimoramento da sociedade como um todo se potencializaram. Infelizmente também os aspectos negativos dessa adoção foram beneficiados e, usando a internet como maior expoente ou representante desse contexto, a criminalidade também encontrou espaço para sua atuação frente à facilidade de cometimento do ilícito e acesso a ferramental que poderia ser usado indiscriminadamente contra quaisquer usuários que são vistos nesse prisma como potenciais alvos.

Com o advento de organização da sociedade como dependente diretamente da tecnologia, os crimes nesse ambiente tomam proporções alarmantes e passam a se tornar grandes desafios para aqueles responsáveis pela segurança pública. Um bom exemplo dessa afirmação é a dificuldade em se realizar as devidas identificações dos criminosos e a condução da persecução penal, já que as demarcações de um território em função dos

seus recursos físicos e do raio de abrangência de determinada cultura foram rompidas, conforme definido por Pinheiro (2010).

Nesse ponto, é necessário apresentar que a definição de crime não existe, sendo eminentemente doutrinária e tendo como conceito amplo a definição de que "*crime é um fato típico, ilícito e culpável*", ou seja, se não houver a base legal ou a tipificação de um crime, a ninguém pode ser imputada qualquer penalidade, independentemente de eventuais apontamentos éticos ou morais. Assim, de acordo com Greco (2014), vários doutrinadores consideram que "para que se possa falar em crime é preciso que o agente tenha praticado uma ação típica, ilícita e culpável". E trazendo o foco para o objeto desse estudo, esse tipo de abordagem leva a situações em que por exemplo, determinadas ações realizadas através da internet que poderiam ser considerados como crimes em uma jurisdição, não o são em outra justamente pela ausência de legislação específica.

De forma resumida, os chamados cibercrimes seriam basicamente os crimes previstos em legislação específica e que são cometidos através do uso de meios tecnológicos, de forma predominante para ferir, constranger ou lesar.

O crime sofreu evoluções ao migrar para modalidades que são realizadas ou facilitadas pela tecnologia, e o Brasil também tem demonstrado algum nível de evolução em seu arcabouço jurídico nesse escopo, podendo ser citadas a promulgação das leis n.º 12.735/2012 e n.º 12.737/2012, que são as chamadas leis de crimes informáticos, a atualização do Código Penal e que ao serem utilizadas em conjunto com a lei do Marco Civil da Internet de n.º 12.965/2014 integram o conjunto de instrumentos legais mais usados atualmente pelas estruturas de segurança pública para suportar o enfrentamento aos cibercrimes.

2.4.1 CLASSIFICAÇÃO DO CIBERCRIME

A dinâmica dos cibercrimes tem como consequência a necessidade de se ajustar as classificações jurídicas frente as constantes mudanças que ocorrem com esse tipo de delito no meio virtual. Usando como exemplo dessa argumentação a classificação sugerida por Ferreira (2005, p. 261) traz a seguinte redação:

"Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o

patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial."

Outras duas classificações que também são muito citadas fazem a classificação dos crimes cibernéticos em puros, mistos e comum, enquanto a segunda divide os crimes de informática em próprios e impróprios.

Segundo Costa (1997, p. 03), os crimes cibernéticos puros seriam "toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas."

No crime cibernético puro o agente visa a atingir especificamente o sistema de informática ou os dados armazenados no referido sistema, sendo um exemplo disso uma invasão com intenção de causar danos de um sistema feita por um hacker.

Já os crimes cibernéticos mistos, como apontado por Pinheiro (2000), "são aqueles em que o uso da internet ou sistema informático é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático." Ou seja, o criminoso não tem como resultado do seu ato o acesso ao sistema informatizado ou seus dados, mas se utiliza dessa tecnologia para a execução de sua conduta ilícita, tais como as transferências ilegais por meio da invasão de um sistema de conta corrente pela internet.

Por fim, os chamados crimes cibernéticos comuns seriam aqueles em que o objetivo é se utilizar da internet ou sistema de informática para realizar o crime. Ou seja, a informática é mero instrumento.

Os cibercrimes próprios ou puros, são aqueles crimes em que o computador como sistema tecnológico é usado como objeto e meio para execução, ou seja, são aqueles crimes em que a utilização do sistema de informática é o meio e o objetivo. Um exemplo dessa modalidade seriam os crimes de invasão de sistemas com o objetivo de danificá-los ou alterá-los, bem como a prática de inserir ou adulterar dados.

Os cibercrimes denominados impróprios são aqueles realizados com a utilização do computador, onde este é utilizado como instrumento para realização de condutas ilícitas. praticados contra um sistema de informática em todas as suas apresentações. Em resumo, as classificações propostas se baseiam basicamente na distinção entre os crimes

executados ou facilitados pela utilização da informática, e as ações de abuso do recurso tecnológico.

Conceitualmente, os cibercrimes envolvem três elementos centrais:

i) infratores (indivíduos e redes) – são aqueles que perpetram o cibercrime; compreender as características dos infratores, suas carreiras criminais e os processos psicológicos que desempenham no desenvolvimento do cibercrime são importantes para compreender seus modos de operação. Além disso, compreender a qual a relação com as redes criminosas, estruturas de oportunidades, modelos adotados também é importante.

ii) vítimas – são aqueles que são sofrem as ações do cibercrime, por exemplo, obter novos *insights* sobre como os usuários podem se tornar mais resilientes contra-ataques cibernéticos, características das vítimas e seu comportamento on-line e off-line são pontos centrais para a realização do cibercrime

iii) combate ao cibercrime – São as estruturas ou ações desempenhadas pelas autoridades competentes no combate aos diferentes tipos de cibercrime. As autoridades competentes podem desempenhar ações previstas em lei sobre pessoas, organizações, sistemas de informação, plataformas de mídias sociais entre outros.

2.5 SEGURANÇA PÚBLICA NO BRASIL

Segundo Cavalcante (2015), os órgãos públicos brasileiros estão cada vez mais preocupados e buscando novos meios e soluções para combater os cibercrimes, apoiando e demandando desenvolvimento de novos dispositivos e até mesmo avançando na cooperação policial e jurídica internacional. Desse modo, os governos procuram evoluir e penalizar aqueles que cometem crimes em ambiente virtual.

Além de atualizar a legislação para suportar o combate ao cibercrime e entendendo que a dinâmica evolutiva desse delito demanda entre outras ações cooperação internacional, recentemente, o Brasil aderiu a Convenção do Conselho da Europa (também conhecida como "Convenção de Budapeste”) contra o cibercrime com a

publicação do Decreto Legislativo 37/2021[8]. A convenção recomenda que as partes signatárias adotem medidas legislativas para tipificar crimes cibernéticos, tais como infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com conteúdo e infrações relacionadas com a violação do direito de autor e direitos conexos.

Essa Convenção reforça, ou ao menos clareia os caminhos que devemos seguir e se alinha com o que já está determinado na Constituição da República de 1988, no artigo 5º, caput, que institui a segurança pública como status de direito fundamental assegurando aos brasileiros e estrangeiros o direto à vida, liberdade, igualdade, propriedade e segurança (BRASIL, 1988).

Segundo Silva (2005), segurança pública consiste em "uma situação de preservação ou restabelecimento dessa convivência social que permite que todos gozem de seus direitos e exerçam suas atividades sem perturbação de outrem, salvo nos limites de gozo e reivindicação de seus próprios direitos e defesa de seus legítimos interesses". Citando o artigo 144 da Constituição Federal de 1988, "A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio".

2.5.1 LEGISLAÇÃO NACIONAL

A maioria dos países tem leis que tratam de cibercrimes ou de algumas de suas facetas (UNODC,2013). Nesse tópico são destacadas as principais legislações especializadas e relacionadas ao cibercrime no Brasil.

A Lei 7.170/1983 (Lei de Segurança Nacional) tipifica os crimes contra a segurança nacional. Nos seus artigos 13 e 15, podem ser enquadrados vários crimes cibernéticos, respectivamente, quanto à divulgação de documentos sigilosos e à sabotagem de sistemas militares, de comunicações, de transporte e de energia.

A Lei 12.737/2012 (Lei Carolina Dieckmann) tipifica os delitos informáticos, tornando crimes, entre outros, a invasão de dispositivos e a interrupção ou perturbação do funcionamento.

[8] https://www.in.gov.br/en/web/dou/-/decreto-legislativo-368859089

A Lei 12.965 (Marco Civil) que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

A Lei Nº 12.735/2012. que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares.

Merece destaque que na Lei nº 12.735 de 30 de Novembro de 2012, usada para tipificar as condutas criminosas realizadas mediante uso de sistema eletrônico, digital ou similares, em seu artigo 4º determinou 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.", ou seja, o Estado compreendeu a necessidade de repressão ao cibercrime ao incluir em um dispositivo legal de tipificação criminal a obrigação de criação de unidades policiais judiciárias especializadas nesse tipo de crime e, em um levantamento inicial realizado pela internet[9], é possível identificar que quase todos os estados do país indicam possuir unidades especializadas em cibercrimes, com disponibilização de sites e alguns serviços de apoio a população, sendo o mais comum o de registro de ocorrências.

Isto posto, e em considerando as definições e contextos apresentados nesse tópico como um todo, identifica-se que o objetivo desse trabalho, que é a análise do fenômeno de adoção de tecnologias digitais e suas consequências, especificamente sobre o comportamento do Estado frente ao cibercrime para a proteção da população, se situa dentro do escopo preconizado do estudo das Humanidades Digitais.

2.6 REFERENCIAIS TEÓRICOS CORRELACIONADOS AOS TEMAS DA PESQUISA

Muitos pesquisadores têm publicado artigos e ensaios sobre crimes digitais, sobretudo os facilitados pelo uso das tecnologias digitais e sobre as implicações da evolução tecnológica e da transformação digital sobre as ciências sociais e humanidades.

No que diz respeito a internet e as tecnologias que interagem com ela, os estudos indicam que os criminosos migraram e se adaptaram a esse novo tipo de ambiente, cujo alcance passa a ser global e que se vale de uma parcial anonimidade com uma falsa sensação de impunidade (NOGUEIRA, 2009). Já sobre as humanidades a avaliação é que ao executar a necessária transformação digital faltou aos envolvidos no processo o

[9] https://new.safernet.org.br/content/delegacias-cibercrimes

conhecimento e a preocupação em entender e proteger o conteúdo que agora estava sendo disponibilizado em um novo meio e formato.

Esta seção apresenta um sumário de trabalhos relevantes pré-existentes na literatura que tratam da avaliação e realce destas características, especialmente nos temas cibercrimes e Humanidades Digitais.

Conforme Mello (2021) aborda em seu artigo "Cibersegurança em gestão de museus no século 21 nas Humanidades Digitais", a falta de formação e informação à respeito de cibersegurança de muitos gestores de instituições culturais tem como consequência direta uma fragilização do trabalho de proteção aos espaços digitais e físicos, sobretudo as relações e especificidades das Humanidades (Museologia, a História, a Sociologia, a Antropologias, as Artes, etc.) que alimentam museus, galerias, centros culturais, bibliotecas, arquivos, dentre outros.

A transdisciplinaridade apregoada pelas Humanidades Digitais, que sugere vincular métodos, dispositivos e perspectivas heurísticas das ciências humanas e sociais ao mesmo tempo em que mobiliza as ferramentas e perspectivas singulares abertas pela tecnologia digital, aponta que a incorporação dos saberes tradicionais às tecnologias computacionais requer também a incursão dos saberes tradicionais no terreno do conhecimento tecnológico, ou seja, historiadores, museólogos, geógrafos, antropólogos e demais pesquisadores deveriam aprender tanto o funcionamento como os formatos de criação das tecnologias digitais, entretanto, o que se identifica na realidade é que essas discussões permanecem no ambiente acadêmico sem alcançar efetividade em aplicações práticas dos profissionais das Humanidades.

Como exemplos das consequências desse distanciamento, Mello (2021) destaca incidentes que ocorreram em grandes mostras de obras de artes em museus e galerias onde a invasão ocorreu como forma de protesto e até mesmo para sequestro dos dados com prejuízos aos museus e aos visitantes frente a insegurança que foi gerada.

A autora conclui indicando que cada vez mais, diante de um mundo altamente digitalizado, cujo processo de transformação digital foi inclusive acelerado por conta da pandemia da COVID-19, e onde várias instituições ampliaram o acesso virtual às suas exposições durante o isolamento social, é premissa fundamental o estudo e desenvolvimento de projetos de cibersegurança para uma gestão cultural segura e confiável a expansão das Humanidades Digitais.

No artigo de Vellozo (2015) “Crimes informáticos e criminalidade contemporânea” a visão sobre a importância da internet no cotidiano das pessoas e o crime facilitado pelo uso da tecnologia é abordado com a proposta de se analisar o conceito dos cibercrimes e a sua ingerência no âmbito do Direito Penal, identificando possíveis classificações conforme sua amplitude e objetivo, além de apresentar exemplos e propostas de legislações ainda em debate pelos governantes no Brasil.

Ao afirmar que a informação passa a ser uma riqueza, o autor cita o óbvio interesse que atrai a criminalidade frente a uma ausência de regulamentação e o falso anonimato proporcionado pela internet.

Ao se identificar que inúmeros delitos surgem e se propagam pela internet, a necessidade de uma regulamentação e controle das atividades se torna urgente, pois dentre os cenários possíveis no prisma da atividade criminosa, a internet pode ser considerada tanto como instrumento, como o alvo dos agentes criminosos. Alguns crimes já conhecidos tais como o furto, a fraude e o estelionato são cometidos diariamente na internet e de maneira bem explícita, mas existem outras atividades não tipificadas, e igualmente prejudiciais que ocorrem nesse ambiente e por causa disso, é indispensável um regramento para este gigantesco e, muitas vezes, descontrolado universo.

Em conclusão, o autor propõe a criação de normas flexíveis, adequáveis a essa diversidade de possibilidades encontradas pelos criminosos no ciberespaço, destacando que a legislação brasileira vem evoluindo com alterações recentes no Código Penal, bem como o Marco Civil da internet que tem por objetivo o de estabelecer princípios, garantias e deveres para o uso da internet no Brasil.

Em seu artigo, Lorenzo e Scaravelli (2021) destacam que os crimes virtuais ou cibercrimes surgem como um mal moderno e cada vez mais presente na sociedade atual, que é altamente dependente das tecnologias e sobretudo das redes sociais e que tem como consequência o surgimento de novas espécies delitivas, com novas formas de se praticar crimes já existentes e novas condutas criminosas.

A necessidade de combinar legislações, alternando entre os ramos do direito, vem como medida de ampliação da proteção e da reação do Estado ao problema do cibercrime. Um destaque é o fato da grande instabilidade dos crimes virtuais, já que as provas de ocorrência dos delitos podem ser alteradas, levando a ausência de provas contra o autor do crime e dificuldade quanto a sua identificação, ocasionando obstáculos na atuação

policial perante tais casos. Os crimes cibernéticos são peculiares desde sua autoria e materialidade como na tipificação de seus institutos.

Em suas considerações finais, as autoras afirmam que o Direito vem se moldando e se adequando ao novo cenário dos cibercrimes, e que é notório que a inovação criminológica por hora está bem à frente da legislação o que levaria a insegurança para o usuário. Ainda nessa linha, elas indicam que o Direito precisa acompanhar a evolução da sociedade que está em uma era informatizada, e que os avanços tecnológicos tendem a crescer cada vez mais trazendo também o aumento da criminalidade virtual.

2.6.1 AMBIENTES COMPUTACIONAIS CORRELACIONADOS AOS TEMAS DA PESQUISA

Um ponto que merece atenção nesse contexto é o mecanismo em que ocorrem as denúncias do cibercrime pelas vítimas.

De forma geral, para uma investigação ou combate ao cibercrime começar tem de existir uma denúncia às autoridades competentes, e segundo estudos realizados pela UNODC (2013) há uma grande subdenunciação de cibercrimes em todo o mundo.

A implementação de iniciativas destinadas a melhorar a comunicação de crimes através da simplificação do registro de ocorrências de ilícitos é uma das recomendações feitas pela agência e a ausência de uma plataforma de recebimento de denúncias e registro de ocorrências para as vítimas, junto as estruturas de segurança pública gera também um trabalho adicional aos profissionais de segurança pois o obriga a receber uma vítima de um cibercrime longe do dispositivo onde ocorreu o fato e com poucos dados ou informações sobre o contexto do delito e que inegavelmente apoiariam sobremaneira uma investigação.

Observando as forças policiais do mundo, a polícia federal americana (FBI) e a polícia europeia (EUROPOL), é possível identificar que esse problema de acesso das vítimas é conhecido e vem sendo tratado de formas similares e que serão detalhadas mais à frente. Por exemplo, O FBI no site[10] da unidade especializada em cibercrimes, disponibiliza um sistema Web assemelhado ao um formulário em que vítimas podem declarar suas ocorrências e fazer denúncias de cibercrimes.

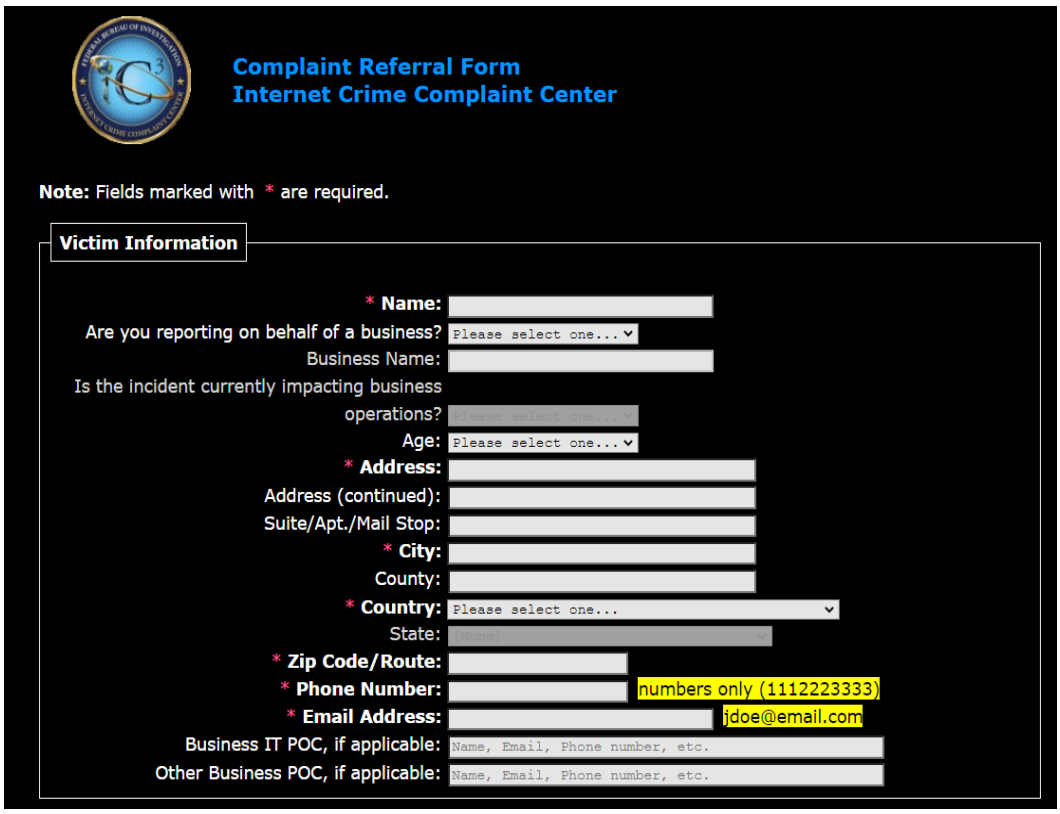
[10] https://www.ic3.gov

O fluxo adotado no formulário é de inicialmente explicar o que é possível fazer nesse formulário, as implicações legais das denúncias e quais os dados que são importantes nesse tipo de procedimento, explicando detalhadamente quais seriam, como inserir e identificar a relevância do que está sendo informado.

Na sequência, o declarante é apresentado ao possível fluxo do processo investigatório e como deverá ser conduzido, neste caso sendo informado inclusive que a declaração realizada será tratada por um grupo de analistas treinados que irá direcionar as informações para outras unidades policiais em todo o país.

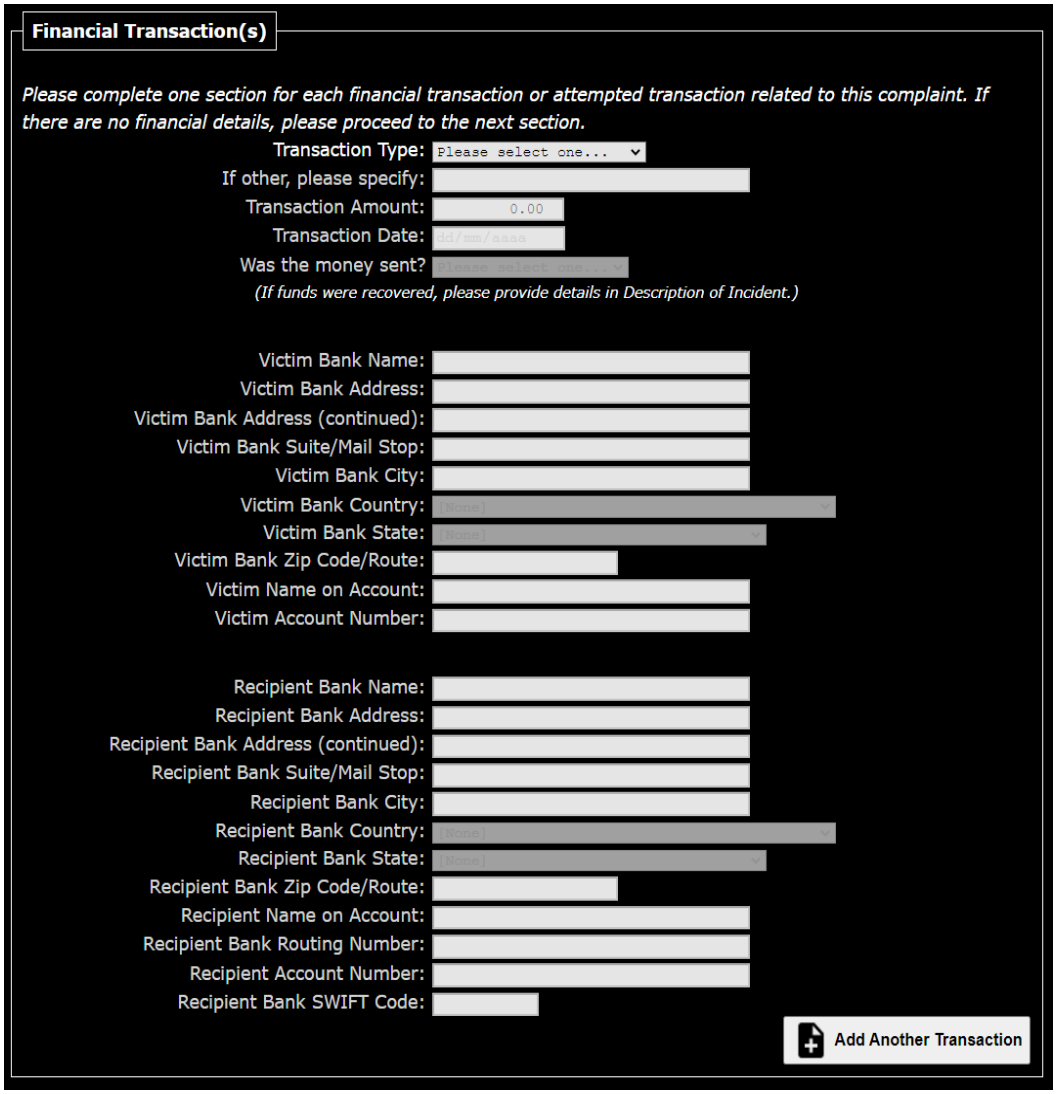
Apenas para visualização das informações apresentadas, segue a captura do site em destaque com suas subdivisões e áreas para inserção das informações (Figuras 1 até 6):

Figura 1 – FBI IC3 - Informação da Vítima



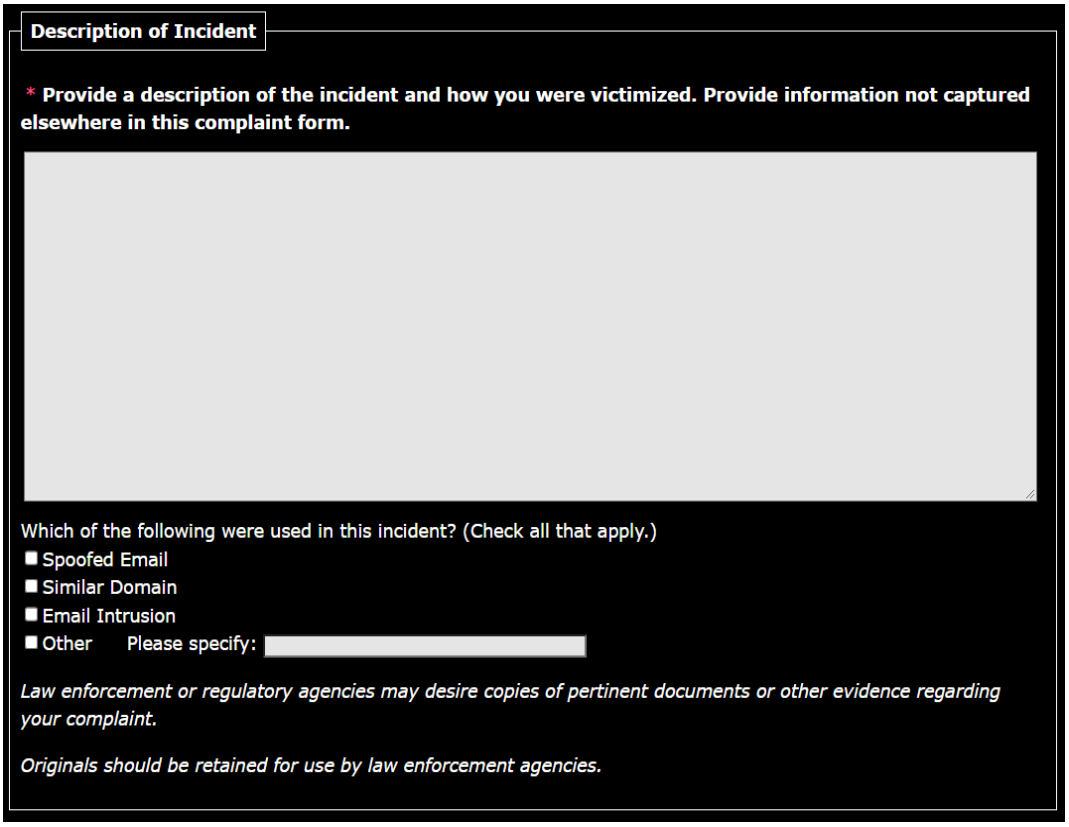
Nessa parte o processo começa com as informações cadastrais da pessoa ou, em caso de estar fazendo a denúncia em nome de uma empresa, os dados referentes a ela.

Figura 2 – FBI IC3 - Informações Financeiras



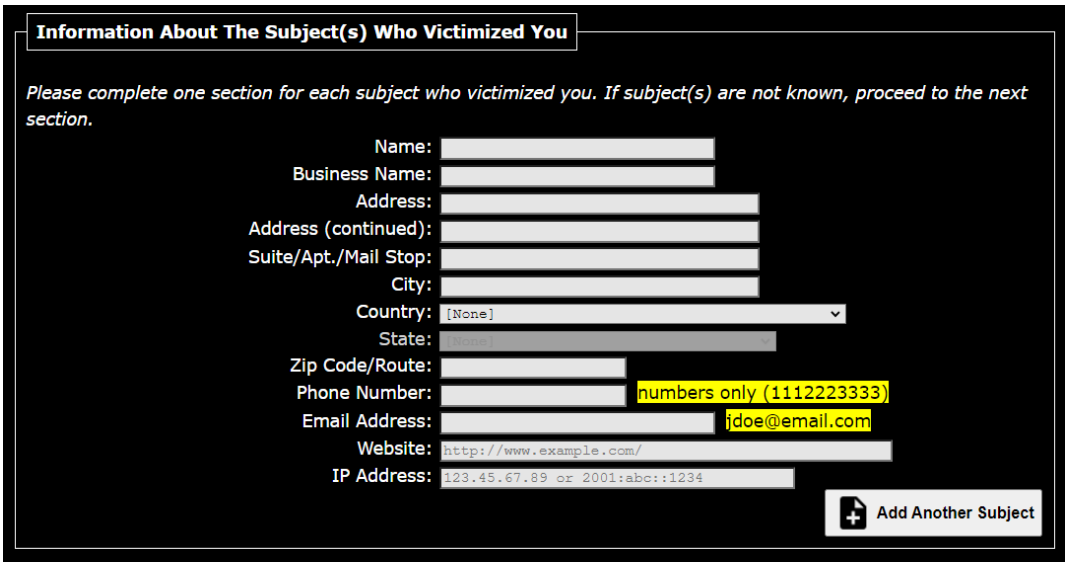
Nessa parte são solicitadas informações especificamente da parte financeira caso tenha relação com a denúncia, indicando instituições financeiras envolvidas, valores e outras informações relevantes a esse escopo.

Figura 3 – FBI IC3 - Descrição do Incidente



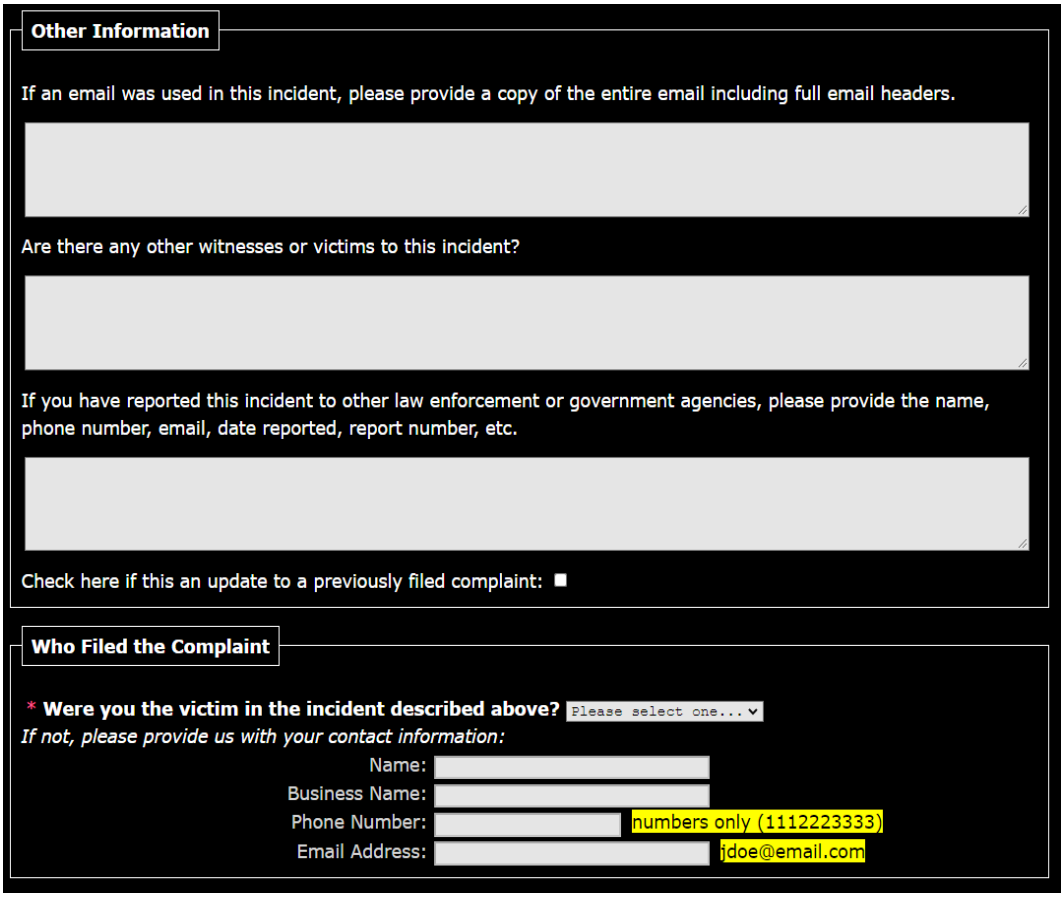
Nesse ponto o denunciante é solicitado a descrever o que houve, os impactos e inclusive por onde imagina ou acredita ter se iniciado o incidente reportado.

Figura 4 – FBI IC3 - Potenciais Autores



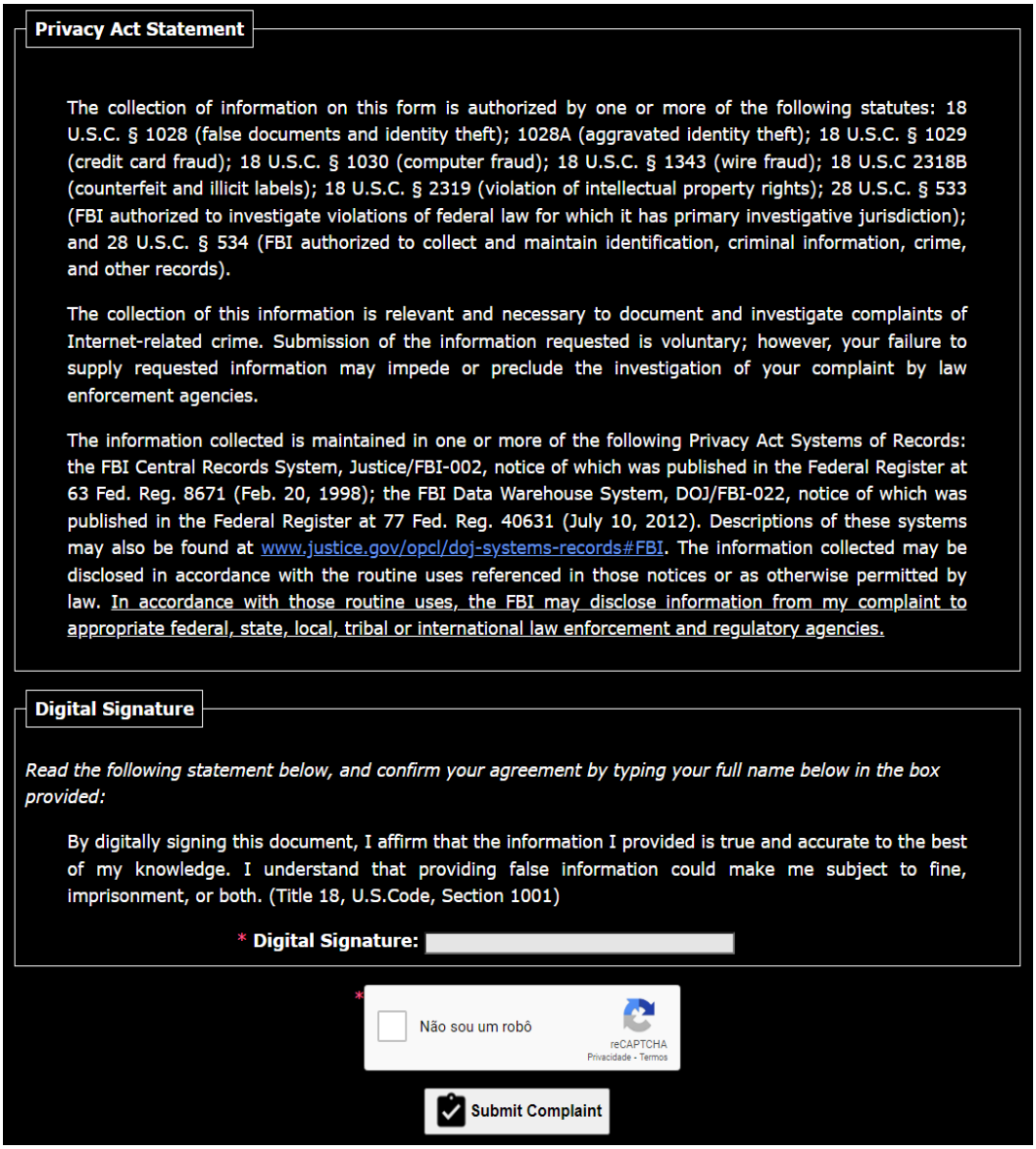
Se houver algum tipo de indício ou suspeita de quem perpetuou o incidente, é nessa tela que devem ser indicados e referenciados.

Figura 5 – FBI IC3 - Outras Informações



Aqui são solicitadas informações finais, potenciais evidências no formato de e-mail e informações finais sobre eventual contato com outros ramos policiais.

Figura 6 – FBI IC3 - Declaração de Privacidade e Assinatura Final



Aqui a denúncia é finalizada e são apresentadas as ressalvas legais relacionadas a privacidade das informações obtidas, solicitando o aceite e finalmente enviando a denúncia ao FBI.

Um outro exemplo é o do bloco europeu. Em função do acordo que criou a União Europeia, existe a colaboração das forças de segurança dos Estados-Membros através de uma unidade de segurança chamada de EUROPOL, cuja missão declarada em seu site[11] é de "apoiar na prevenção e luta contra todas as formas graves de criminalidade internacional e organizada, cibercriminalidade e terrorismo".

[11] https://www.europol.europa.eu/about-europol

O combate ao cibercrime é uma das prioridades declaradas pela EUROPOL e nesse sentido, eles criaram em 2013 um centro europeu especializado no cibercrime (European Cybercrime Centre - EC3) que se especializou em crimes envolvendo o uso de tecnologia, exploração sexual infantil e fraudes em sistemas de pagamento entre outros.

Essa unidade fornece apoio operacional, analítico e forense aos Estados-Membros da União Europeia e conduz interações técnicas e ações conjuntas de forças policiais e de inteligência com foco no combate ao cibercrime.

Cada país membro tem seu canal de acesso para o cidadão realizar sua denúncia ou registrar uma ocorrência de cibercrime e apesar de variarem no formato, quase todos usam formulários simples para que sejam inseridas informações sobre o crime e como buscar apoio das unidades especializadas de segurança pública, ou usam apenas um e-mail institucional onde a vítima declara e contextualiza o que houve.

3 REVISÃO SISTEMÁTICA DA LITERATURA

A revisão da literatura é um termo genérico, que compreende todos os trabalhos publicados que oferecem um exame da literatura abrangendo assuntos específicos. A revisão sistemática de literatura (RSL) vai muito além disso. Trata-se de uma modalidade de pesquisa que utiliza uma metodologia e protocolos bem definidos para identificar, analisar e interpretar todas as evidências disponíveis a respeito de uma questão de pesquisa particular de maneira imparcial e repetível. (KEELE e KITCHENHAM, 2007). Em última análise, a revisão sistemática de literatura busca entender e trazer logicidade a um grande corpus documental, especialmente, verificando o que funciona e o que não funciona num dado contexto.

Neste capítulo faremos uma revisão sistemática cujo propósito é tornar os resultados da pesquisa mais formais e com maior potencial de alinhamento com pesquisas subjacentes. Logo, é apresentado uma RSL seguindo um protocolo alinhado com as recomendações metodológicas propostas por Kitchenham & Charters (2007).

3.1 ETAPAS DA REVISÃO SISTEMÁTICA

3.1.1 OBJETIVOS E PERGUNTAS DA PESQUISA

O objetivo desta revisão sistemática foi buscar referências e conhecimentos sobre o cibercrime, o que é esse tipo de crime e como o estado brasileiro, com foco específico na área de segurança pública, estaria atuando, utilizando como referencial analítico os princípios e conceitos das Humanidades Digitais (HD's).

Foram definidas oito questões de pesquisa para a seleção dos estudos e a extração dos dados:

1. O que são os cibercrimes?
2. Como o Estado Brasileiro está combatendo o cibercrime?
3. Como são tratadas as informações de segurança pública?
4. Qual o suporte legal para o combate ao cibercrime?
5. Como o Estado Brasileiro organiza sua segurança pública?
6. Quais as estatísticas relacionadas a segurança pública?
7. Qual a correlação entre Humanidades Digitais e estudos sobre cibercrimes?
8. O que são Cibercrimes no contexto brasileiro?

3.1.2 SELEÇÃO DAS BASES DE DADOS

O critério de seleção das bases de dados baseou-se na viabilidade de acesso através do Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), através da Comunidade Acadêmica Federada (CAFe) em 19/6/2022 e 02/7/2022, e nas bases de pesquisa com acesso direto e gratuito conforme listagem abaixo.

- ACM (https://dl.acm.org/)
- Google Scholar (http://scholar.google.com/)
- Science@Direct (http://www.sciencedirect.com)
- Scopus (http://www.scopus.com)
- Web Of Science (www.webofscience.com)

3.1.3 DEFINIÇÃO DAS *STRINGS* DE BUSCAS

A definição das *strings* de busca foi realizada nos idiomas português e inglês, além de serem ajustadas através de simulações iniciais e experimentações como indicado por Kitchenham e Charters (2007). Ao final das simulações, a *string* de busca foi:

("Cibercrimes" OR "Crimes Digitais" OR "Crimes Virtuais" OR "Crimes de Internet" OR "Cybercrimes" OR "Digital Crimes" OR "Virtual Crimes") AND ("Digital Humanities" OR "Humanidades Digitais")

3.1.4 CRITÉRIOS DE EXCLUSÃO E INCLUSÃO

Uma vez definida a *string* de busca, foi necessário delimitar os critérios usados para inclusão e exclusão dos estudos retornados das bases de dados e para isso os parâmetros foram:

Os critérios de exclusão de itens da RSL foram os seguintes:

- Estudos duplicados,
- Estudos fora do escopo,
- Textos em línguas diferentes de português e inglês,
- Textos incompletos,
- Textos pagos.

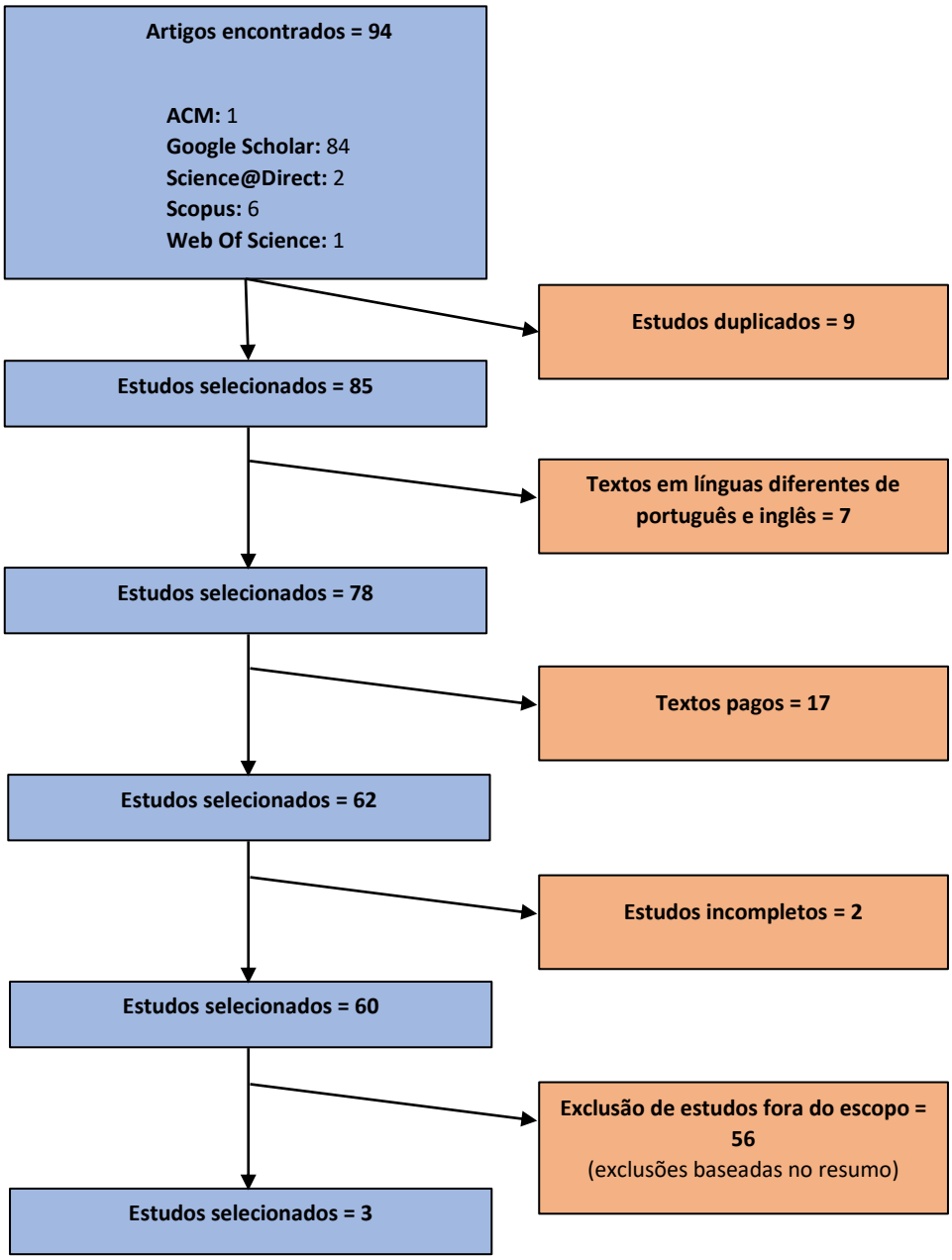
Os critérios de inclusão de itens da RSL foram os seguintes:

- Estudos de segurança pública,
- Estudos em Humanidades Digitais e Crimes,
- Estudos sobre cibercrimes,
- Estudos sobre crimes.

3.1.5 RESULTADOS ENCONTRADOS:

Os resultados obtidos são apresentados em um formato de fluxograma conforme figura 7.

Figura 7 - Fluxograma do Processo de Seleção de Estudos



3.1.6 CRITÉRIOS DE QUALIDADE

Para que fossem selecionados os estudos com maior relevância para pesquisa, foram criados critérios de qualidade, com vínculos à estruturação, resultados e ao grau de atendimento às questões de pesquisa:

- O estudo tem informações relevantes para a dissertação?
- O estudo possui detalhamento, referências e reprodutibilidade?

- Os dados apresentados pelo estudo podem ser validados e aproveitados na dissertação?
- O objetivo da pesquisa está claramente descrito?

Os estudos selecionados então foram quantificados nos critérios de qualidade e as pontuações refletiam os seguintes conceitos: 0 (não conformidade), 0,5 (parcialmente em conformidade) e 1 (totalmente em conformidade) levando ao final que cada estudo poderia chegar a receber nota 4 (no máximo) e no mínimo 0.

Tabela 1 - Quantificação dos Estudos Selecionados

A CONSIDERATION OF THE SOCIAL IMPACT OF CYBERCRIME: EXAMPLES FROM HACKING, PIRACY, AND CHILD ABUSE MATERIAL ONLINE (2016)				3.0
O estudo tem informações relevantes para a dissertação?	Sim	Parcialmente	Não	
O estudo possui detalhamento, referências e reprodutibilidade?	Sim	Parcialmente	Não	
Os dados apresentados pelo estudo podem ser validados e aproveitados na dissertação?	Sim	Parcialmente	Não	
O objetivo da pesquisa está claramente descrito?	Sim	Parcialmente	Não	

CRIMES CIBERNÉTICOS: A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO (2016)				3.0
O estudo tem informações relevantes para a dissertação?	Sim	Parcialmente	Não	
O estudo possui detalhamento, referências e reprodutibilidade?	Sim	Parcialmente	Não	
Os dados apresentados pelo estudo podem ser validados e aproveitados na dissertação?	Sim	Parcialmente	Não	
O objetivo da pesquisa está claramente descrito?	Sim	Parcialmente	Não	

TOWARDS DIGITAL ORGANIZED CRIME AND DIGITAL SOCIOLOGY OF ORGANIZED CRIME (2022)				3.0
O estudo tem informações relevantes para a dissertação?	Sim	Parcialmente	Não	
O estudo possui detalhamento, referências e reprodutibilidade?	Sim	Parcialmente	Não	
Os dados apresentados pelo estudo podem ser validados e aproveitados na dissertação?	Sim	Parcialmente	Não	
O objetivo da pesquisa está claramente descrito?	Sim	Parcialmente	Não	

3.1.7 RESULTADOS DOS PROCEDIMENTOS DE BUSCA SISTEMÁTICA

Após a realização das buscas nas bases de dados, os estudos encontrados passaram por um processo de avaliação onde foram usados os critérios de inclusão, exclusão e qualidade.

Inicialmente foram encontrados no total 94 estudos (Quadro1), e após a realização da análise, apenas 3 foram selecionados para leitura por preencherem os critérios preestabelecidos (Quadro 2).

Quadro 1 - Resultados da Pesquisa Inicial

Base de Conhecimento	Resultados Iniciais	Aproveitamento
ACM	1	0
Google Scholar	84	3
Science@Direct	2	0
Scopus	6	0
Web Of Science	1	0

Quadro 2 - Estudos Selecionados

Título	**Autores**
A CONSIDERATION OF THE SOCIAL IMPACT OF CYBERCRIME: EXAMPLES FROM HACKING, PIRACY, AND CHILD ABUSE MATERIAL ONLINE	Mary Aiken, Ciaran McMahon, Ciaran Haughton, Laura O'Neill & Edward O'Carroll (2014)
CRIMES CIBERNÉTICOS: A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO	Ana Luiza Siepierski (2022)
TOWARDS DIGITAL ORGANIZED CRIME AND DIGITAL SOCIOLOGY OF ORGANIZED CRIME	Andrea Di Nicola (2022)

3.1.8 ANÁLISE E DISCUSSÃO DOS ARTIGOS SELECIONADOS

Em Aiken et al., (2014), os autores examinam os impactos sociais do mundo real e cibernético em relação ao cibercrime, dando ênfase a necessidade de se estudar esse fenômeno devido principalmente ao ambiente em que o mesmo ocorre, o ciberespaço e as implicações no mundo virtual e no mundo real.

Inicialmente ao apresentar o conceito sobre o que seria “impacto social”, a autora traz para discussão a necessidade de se considerar o alcance e a escala sobre o conceito e

apresenta fatores a serem usados como ferramental exploratório para compreensão desse contexto e que devem ser considerados ao se analisar o ambiente em que o mesmo ocorre.

No ciberespaço, a interação embora seja realizada em um ambiente de isolamento físico, se torna quase imediatamente público e permanente, como se os usuários estivessem sozinhos e hiperconectados ao mesmo tempo, e nesse contexto, o cibercrime acaba apresentado propriedades relacionadas ao impacto social com características próprias com convergência de fenômenos físicos e virtuais. Essa convergência indica então um novo problema para o estudo de comportamentos ambientais como o crime, necessitando foco no estudo dos problemas como eles existem de fato no cotidiano, o que é um desafio ao se considerar os cibercrimes e seu contexto ambiental.

Esses desenvolvimentos teóricos acabam trazendo questões metodológicas como consequência. Por exemplo, Aiken et al., (2014) afirmam que 'a metodologia de pesquisa tradicional…está começando a parecer pitoresca' à luz dos rápidos desenvolvimentos na tecnologia da comunicação da informação e como isso afeta o processo de pesquisa em ciências sociais. Surgem então questões importantes sobre as quais os pesquisadores devem refletir, como o nível de alfabetização digital, a fonte de sua orientação ética, o evangelismo que envolve as mensagens públicas sobre o uso da tecnologia e quão perto o pesquisador pode ou deve chegar da realidade e experiência vivida do objeto da pesquisa.

Essas reflexões são particularmente úteis no contexto do impacto social do cibercrime, mas igualmente em uma abordagem mais ampla sobre o tratamento acadêmico de seu contexto social. Os autores baseando-se em uma leitura de Vishik (2014) observam que "a natureza multidisciplinar dos ataques à cibersegurança é importante, e que os ataques ocorrem por diferentes razões, apenas algumas das quais são técnicas, outras razões incluem, por exemplo, questões socioeconómicas".

Além da interdisciplinaridade, nesse texto os autores destacam a importância da construção da transdisciplinaridade no ciberespaço concordando com (SULER, 2013) e afirmando que existe uma longa tradição disso no contexto do crime cibernético, sob a forma de estudos aplicados, como os realizados em psicologia forense e investigativa e os que recentemente vem sendo apresentados no contexto das humanidades digitais.

No trabalho de Siepierski (2022) a abordagem do estudo foi da observação da evolução da internet e suas tecnologias e vantagens trazendo evoluções também de práticas ilícitas conhecidas como crimes cibernéticos.

De forma geral, o trabalho resume a questão da dificuldade em se encontrar um autor de um crime cibernético, o que gera uma espécie de sensação de impunidade e que poderia ser justificada por ser baseada principalmente na facilidade tecnológica de se realizar tais atos e no anonimato que existe em boa parte das ações no ciberespaço. Só que sendo o anonimato um direito fundamental, quais os mecanismos e formas de coibir os cibercrimes podem ser criados, mas que se mantenham equilibradas com o Direito e com a liberdade de expressão?

Finalmente, no trabalho de Di Nicola (2022), o autor após contextualizar a tecnologia e seus impactos evolutivos na sociedade como um todo, gerando uma sociedade digital, demonstra então que a sociedade digital também tem um forte impacto no mundo do crime, que mudam, em termos de tipologias e modus operandi, suas características, suas interações sociais e seus relacionamentos com as potenciais vítimas. Onde há novos fatos sociais, novos hábitos, novas formas de conhecer, comprar, pagar, economizar, proteger, transferir ativos, novas identidades digitais, novos sistemas de coleta de informações, auto-organização, lazer e viagens, é natural que novos crimes e novas formas de combater o crime também surjam. A tese é que, para compreender a nova dimensão do crime organizado digital, será cada vez mais necessária uma sociologia digital do crime organizado, estudando o impacto da sociedade digital no crime organizado e nas respostas digitais, formais e informais.

Ainda conforme Di Nicola (2022), a sociologia digital do crime organizado precisará tentar desenvolver novos conceitos e novos paradigmas teóricos criminológicos sobre o crime organizado digital e a resposta social a ele. Será necessário testar velhas teorias criminológicas sobre o crime organizado em domínios digitais e desenvolver e testar novas explicações criminológicas para as causas do crime organizado digital. Tendo de desenvolver e testar novas ideias sobre a estruturação do crime organizado e como ele atua na sociedade digital, adotando uma abordagem interdisciplinar e multidisciplinar da pesquisa em segurança e do crime como fenômeno em diálogo profundo com muitas outras disciplinas científicas, incluindo direito, estatística, matemática, ciência da computação, engenharia, economia e ciência cognitiva, para melhor entender e responder ao crime organizado na sociedade digital.

4 COLETA E ANÁLISE DE DADOS

Neste capítulo apresentamos as fases de condução da coleta e análises qualitativa e quantitativa de dados desse estudo, identificando a classificação e abordagens discutidas em sua sustentação teórica.

4.1 PROCEDIMENTOS INICIAIS DE COLETA DOS DADOS

Diante da rápida difusão do cibercrime, a estratégia brasileira de enfrentamento a esse tipo de crime não pode ficar anacrônica. Resta, contudo, compreender se ela tem atendido às expectativas do momento e se protege de forma suficiente os cidadãos e empresas.

Frente a essa percepção, iniciamos o desenvolvimento da pesquisa, considerando justamente a amplitude do país, a descentralização da responsabilidade e da heterogeneidade dos atores envolvidos na segurança pública, da complexidade do tema e da abrangência do assunto, sendo necessário fazer uma delimitação de um escopo que permitisse a identificação não somente dos aspectos tecnológicos envolvidos no cibercrime e a atuação das unidades de segurança pública responsáveis pelo enfrentamento, mas também que permitisse algum nível de análise quanto ao contexto legal e o nível de suporte existente para as forças de segurança.

Durante o ano de 2021, desenhamos uma proposta de ação e iniciamos um levantamento de dados junto as Secretarias de Segurança Pública do país. Nessa atividade foi possível identificar que todas indicavam ter unidades de combate ao cibercrime conforme a determinação da lei Nº 12.735/2012 e somados a isso, ainda apareceram estruturas especializadas em cibercrimes no Ministério Público e até mesmo em empresas privadas, o que indicava que eles em conjunto seriam fontes potenciais de dados relevantes para essa dissertação.

Para que fosse possível melhor identificar qual o foco da pesquisa a ser desenvolvida e buscar informações mais detalhadas junto as estruturas de Segurança Pública, foi elaborado um questionário com questões do tipo abertas com três domínios específicos para produção de conhecimento, sendo suas perguntas direcionadas sobre as unidades especializadas em crimes digitais, suas formações, especializações e infraestrutura, sobre os crimes digitais propriamente ditos, os dados existentes até a

posição de acompanhamento e prevenção dos mesmos e finalmente, sobre os aspectos jurídicos envolvidos no assunto.

Frente à impossibilidade logística de visitar as instituições e das restrições advindas da pandemia de COVID-19, a coleta de dados foi conduzida através de questionários emitidos pelos canais digitais oficiais através do uso do Serviço de Informações ao Cidadão e acesso similares via ouvidorias, fundamentando o pedido via Lei de Acesso à Informação (Lei nº 12.527, sancionada em 18 de novembro de 2011) e Decretos Estaduais de Regulamentação para contato junto às unidades de análise da área de Segurança Pública. Os questionários enviados para as unidades estão disponíveis no ANEXO 1.

Ao todo 30 questionários foram enviados e as Unidades de Análise foram:

- Ministério Público Federal;
- Secretaria Nacional de Segurança Pública;
- Departamento de Polícia Federal;
- Secretarias de Segurança Pública e/ou de Defesa Social dos Estados (Direcionamento para as unidades especializadas da Polícia Judiciária Estadual).

No quadro 3 é apresentada a unidade de análise por Estado e o status da apreciação dos pedidos de informação e na sequência, um descritivo inicial dos dados obtidos:

Quadro 3 – Estados, Unidades de Análise e Status das Respostas Recebidas

Estados	**Órgão**	**Status**
Acre (AC)	SEPC - Secretaria de Estado da Polícia Civil	Atendido
Alagoas (AL)	SESP - Secretaria de Estado de Segurança Pública	Atendido
Amapá (AP)	DGPC - Delegacia Geral de Polícia Civil	Atendido
Amazonas (AM)	SSP - Secretaria de Segurança Pública	Atendido
Bahia (BA)	Ouvidoria Geral do Estado da Bahia	Atendido
Ceará (CE)	Controladoria e Ouvidoria Geral do Estado	Atendido

Distrito Federal (DF)	PCDF - Delegacia Especial de Repressão aos Crimes Cibernéticos	Atendido
Espírito Santo (ES)	Ouvidoria SSP - Redirecionada para a PCES - Polícia Civil	Indeferido
Goiás (GO)	Controladoria Geral do Estado	Atendido
Maranhão (MA)	SSP - Secretaria de Estado da Segurança Pública	Sem resposta
Mato Grosso (MT)	Ouvidoria Geral do Estado	Indeferido
Mato Grosso do Sul (MS)	SEJUSP - Secretaria de Estado de Justiça e Segurança Pública	Atendido
Minas Gerais (MG)	PCMG- Polícia Civil do Estado de Minas Gerais	Atendido
Pará (PA)	SEGUP - Secretaria de Estado de Segurança Pública - PCPA	Atendido
Paraíba (PB)	SEDS - Secretaria do Estado da Segurança e da Defesa Social - PCPB	Atendido
Paraná (PR)	Ouvidoria da PC-PR	Atendido
Pernambuco (PE)	Ouvidoria Geral do Estado	Atendido
Piauí (PI)	Secretaria de Segurança Pública	Atendido
Rio de Janeiro (RJ)	Instituto de Segurança Pública e Delegacia de Repressão aos Crimes de Informática	Atendido
Rio Grande do Norte (RN)	Controladoria Geral do Estado	Atendido
Rio Grande do Sul (RS)	Secretaria de Segurança Pública	Atendido
Rondônia (RO)	Secretaria de Segurança Pública	Atendido
Roraima (RR)	Secretaria de Segurança Pública	Atendido
Santa Catarina (SC)	Ouvidoria Geral do Estado	Atendido
São Paulo (SP)	Secretaria de Segurança Pública	Atendido
Sergipe (SE)	Secretaria de Segurança Pública	Atendido
Tocantins (TO)	Secretaria de Segurança Pública	Atendido
Ministério Público Federal	Procuradoria da República no Estado do Rio de Janeiro	Atendido

Secretaria Nacional de Segurança Pública	Diretoria de Gestão e Integração de Informações - DGI	Atendido
Departamento de Polícia Federal	Diretoria de Investigação e Combate ao Crime Organizado	Indeferido

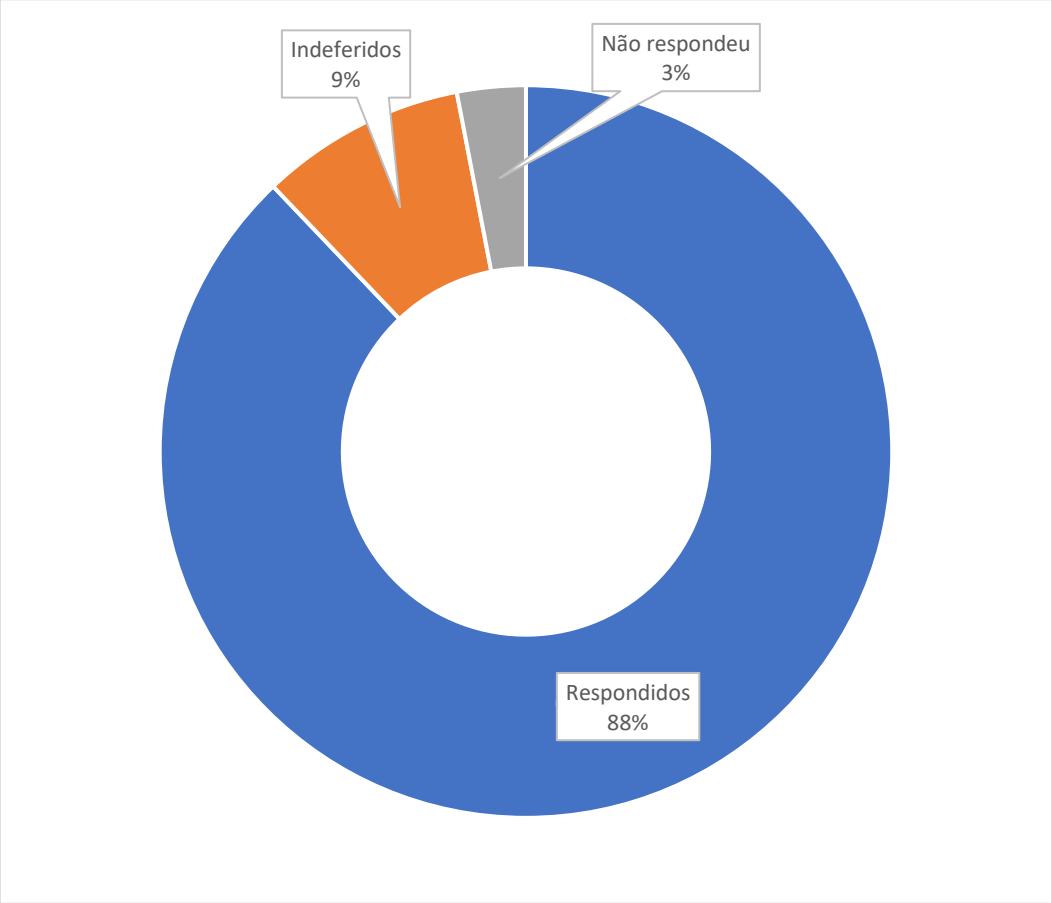
De todas as unidades de análise, a grande maioria apresentou apenas dados parcialmente consolidados de natureza descritiva e qualitativa, com apenas sete unidades apresentando dados quantitativos de números de ocorrências, somando cerca de 354.000 registros de crimes com um espaço temporal que foi do ano de 2006 até o ano de 2021.

Nesse ponto, ao se considerar as respostas dos Estados, é possível afirmar que existe a identificação da necessidade de formação e especialização das forças policiais para a investigação do cibercrime, e isso se materializou inicialmente através da criação de delegacias ou unidades especializadas nesse ambiente, além das declarações de elaboração de sistemas e futuros protocolos para investigação.

4.2 ANÁLISE QUALITATIVA DOS DADOS DOS QUESTIONÁRIOS

Com relação as respostas iniciais dos questionários, tivemos as seguintes distribuições: 29 foram respondidos pelos destinatários, 3 foram indeferidos e apenas 1 não respondeu. Além dessa abordagem, desenvolvemos uma avaliação preliminar de natureza qualitativa sobre cada questionário respondido, com as principais observações resumidas de acordo com as respostas emitidas pelos órgãos (Gráfico 2).

Gráfico 2 - Respostas dos Unidades da Federação e Órgãos de Segurança Pública



4.3 ANÁLISE QUANTITATIVA DOS DADOS DOS QUESTIONÁRIOS

Com relação as respostas iniciais dos questionários, realizamos uma análise quantitativa e para fins de organização, nesta seção apresentaremos as análises considerando as regiões demográficas e os seus respectivos estados.

Região Norte

Acre:

Em linhas gerais, frente ao apresentado como resposta pelo estado, pode-se resumir que ele ainda não possui unidade especializada em crime digital, que possui infraestrutura de TI e realiza treinamentos, mas não possui trabalhos estatísticos sobre crimes digitais, além de não citar nenhum caso de grande repercussão ou quaisquer cooperações com a iniciativa privada nesse aspecto.

Amazonas:

O Estado possui unidade especializada em crime digital, que foi criada pela portaria normativa N.º 010/2021-GDG/PC, que regulamenta, no âmbito da Polícia Civil do Estado do Amazonas, as atribuições da DELEGACIA ESPECIALIZADA EM REPRESSÃO A CRIMES CIBERNÉTICOS – DERCC e define principalmente o seguinte escopo de atuação:

Art. 2º. Serão apuradas pela Delegacia Especializada em Repressão a Crimes Cibernéticos - DERCC as seguintes infrações penais ocorridas no ambiente cibernético com autoria desconhecida:

I. Os crimes cibernéticos próprios tipificados na lei nº 12.737/2012;

II. Os crimes tipificados no artigo 218-C do CPB;

III. Os crimes de extorsão cometidos por meio da Internet;

IV. Os crimes de falsa identidade cometidos por meio da Internet;

V. Os crimes de estelionato e outras fraudes quando o valor do prejuízo for igual ou superior a 10 (dez) salários-mínimos, praticados por *sites* de vendas *online,* conhecidos por *e-commerce*; desde que iniciados e consumados em ambiente virtual, com autoria desconhecida, assim como cometidos através de páginas falsas;

VI. Os crimes cometidos contra crianças ou adolescentes, nas hipóteses dos artigos 241-A, 241-B, 241-C e 241-D da Lei nº 8.069/1990 (Estatuto da Criança e Adolescente), desde que por autoria desconhecida;

VII. Os crimes de ameaça, calúnia, difamação e injúria praticados por meio da internet e em face de Funcionário(s) Público(s) pertencente(s) ao Poder Executivo, Legislativo, Judiciário, Ministério Público ou Tribunal de Contas do Estado do Amazonas, em razão de suas funções;

A delegacia possui infraestrutura de TI e realiza ações de prevenção através de divulgação de cartilhas e alertas para a sociedade.

Não possui trabalhos estatísticos sobre crimes digitais, mas indicou sem apresentar números, que os crimes de maior frequência seriam os crimes contra a honra

que ocorrem em ambientes cibernéticos, os golpes cibernéticos como Estelionato (Art. 171 do CPB) e de Falsa Identidade (Art. 307 do CPB).

A unidade não citou nenhum caso de grande repercussão, e afirmou existir cooperações com a iniciativa privada sem maiores detalhamentos.

Amapá:

O Estado possui unidade especializada em crimes digitais, que é a Delegacia de Repressão aos Crimes Cibernéticos (DR-CCIBER) que foi acrescentada à estrutura da Polícia Civil do Estado do Amapá por meio da Lei Estadual n. 2.507/20, mas que ainda aguarda sua sede física e a lotação de profissionais tendo nesse meio tempo, suas atribuições e delegações distribuídas entre todas as unidades policiais já em operação.

A Secretaria de Segurança Pública do Estado possui trabalhos estatísticos sobre crimes digitais e disponibilizou dados para análise na forma de uma planilha com o título de "CRIMES OCORRIDOS EM AMBIENTE VIRTUAL NOS ANOS 2019 A 2021* REGISTRADOS NO ESTADO DO AMAPÁ" com 150 registros.

Nas respostas ao questionário não foi apresentado nenhum tempo de duração de investigação, nem houve a citação de casos de grande repercussão ou cooperação com a iniciativa privada.

No gráfico 3 são representadas as ocorrências de maior frequência e seus respectivos valores de incidência por ano, enquanto no gráfico 4 são apresentados os totais de ocorrências de cibercrimes por ano, merecendo citação que os dados referentes ao ano de 2021 contemplam apenas o primeiro semestre do ano.

Gráfico 3 - Cibercrimes de Maior Frequência – Amapá (2019 a 2021)

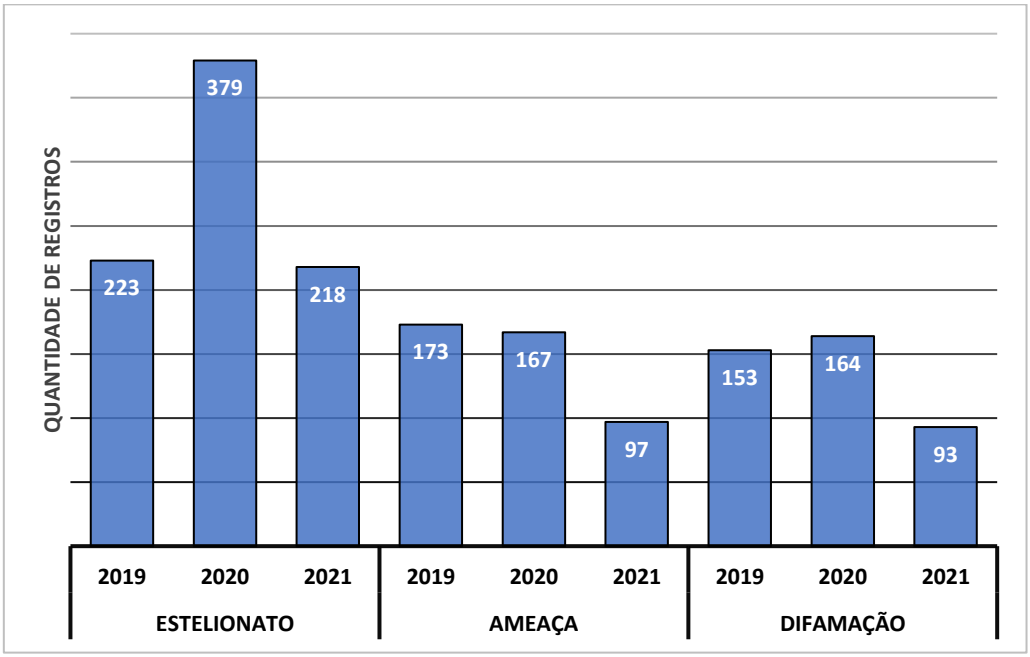
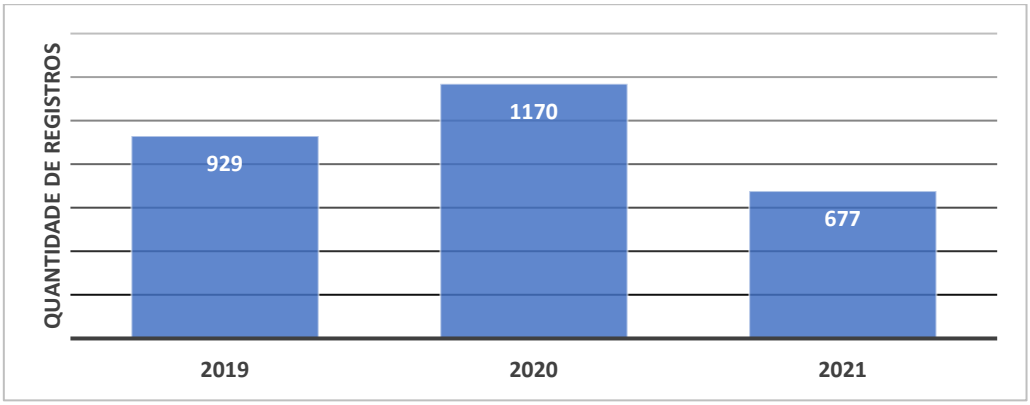


Gráfico 4 - Total de Registros de Cibercrimes por Ano - Amapá



Pará

O Estado criou no ano de 2020 a Diretoria Estadual de Combate a Crimes Cibernéticos, atual DECCC, composta pelas seguintes divisões: DCDI (Divisão de Combate a Crimes Contra Direitos Individuais Praticados por Meios Cibernéticos), DCCV (Divisão de Combate a Crimes Contra Vulneráveis Praticados por Meios Cibernéticos) e DCEP (Divisão de Combate a Crimes Econômicos e Patrimoniais Praticados por Meios Cibernéticos).

Possui trabalhos estatísticos sobre crimes digitais, mas não os disponibilizou e indicou sem apresentar números, que os crimes de maior frequência seriam os contra

patrimônio (fraude, estelionato, extorsão), os contra a honra (difamação, calúnia, injúria) e o crime de pornografia infantil.

Citou como casos de grande repercussão as operações CIBERMARKETING que foi contra crimes do tipo de fraudes bancárias e a operação LUZ NA INFÂNCIA que foi contra pornografia infantil.

Rondônia

Possui unidade especializada que é o Laboratório de Tecnologia de combate a Crimes Cibernéticos - CIBER-LAB e que foi criado através da lei 4.630 de 31 de outubro de 2019 na estrutura da Polícia Civil, entretanto a unidade em questão ainda está em fase de implantação.

Roraima

Possui unidade especializada que é o Distrito Estadual de Repressão à Crimes Cibernéticos – DERCC e que foi criado através do Decreto n. 29.637-E de 03 de dezembro de 2020, com a regulamentação de suas atribuições feita por Resolução do Conselho Superior de Polícia (Resolução n.002/2021-CONSUPOL, de 21 de abril de 2021).

Não possui trabalhos estatísticos sobre crimes digitais e citou cooperação com a iniciativa privada sem apresentar maiores detalhes e nem citar as iniciativas ou empresas.

Tocantins

Possui unidade especializada que é Delegacia de Repressão a Crimes Cibernéticos e que foi criada através da PORTARIA SSP Nº 350, DE 19 DEABRIL DE 2017. Atualmente, passou a ser chamada de Divisão Especializada em Repressão a Crimes Cibernéticos – DRCC e está subordinada à Diretoria de Repressão à Corrupção e ao Crime Organizado – DRACCO.

A unidade afirmou que o tempo médio de uma investigação é de cerca de 3 meses sendo o crime de estelionato, extorsão e furto mediante fraude os mais frequentes.

Foram citadas as operações OSTENTAÇÃO como exemplo de operação contra o crime de furto e a PERFIL OCULTO contra o crime de extorsão.

Região Nordeste:

Alagoas:

A estrutura de segurança pública possui unidade especializada em crimes digitais que foi criada em 2016 chamada de Seção de Crimes Cibernéticos.

Possuem dados estatísticos, mas não disponibilizaram nenhuma informação, inclusive sobre tempo de investigação.

Adicionalmente, não citou nenhum caso de grande repercussão e nem cooperação com a iniciativa privada ou forneceu detalhes adicionais.

Bahia:

Não possui unidade especializada em crime digital e nem respondeu nenhum dos questionamentos apresentados

Maranhão:

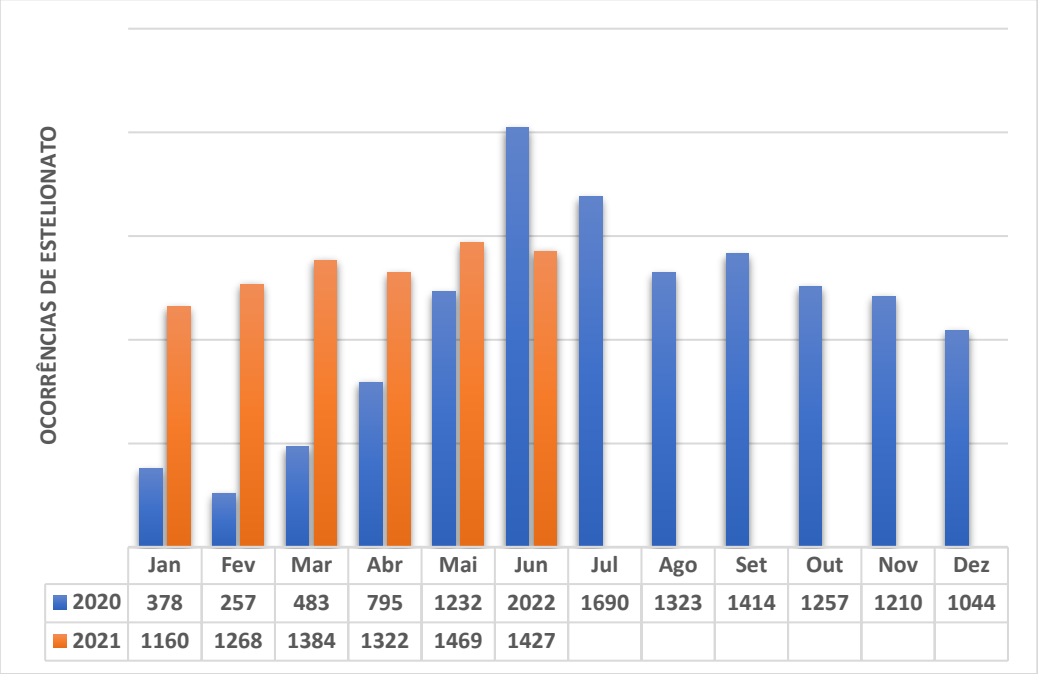
Não respondeu a solicitação de informações via LAI/Ouvidoria

Ceará:

Não possui unidade especializada em crime digital, mas reconhece a importância e tal demanda está em fase de criação e formação.

Possui trabalhos estatísticos sobre crimes digitais e disponibilizou dados para análise na forma de um arquivo em formato pdf com uma tabela chamada “NÚMERO DE OCORRÊNCIAS DE ESTELIONATO EM AMBIENTE VIRTUAL (INTERNET) NO ESTADO DO CEARÁ” por mês referente aos anos 2020 e 2021.

Gráfico 5 - Estelionato via Internet 2020 2021 - Ceará



	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
2020	378	257	483	795	1232	2022	1690	1323	1414	1257	1210	1044
2021	1160	1268	1384	1322	1469	1427						

No gráfico 5 são apresentados os dados de estelionato em ambiente virtual (internet) que foram extraídos do Sistema de Informações Policiais – SIP da Polícia Civil do Estado do Ceará pela Gerência de Estatística e Geoprocessamento da Superintendência de Pesquisa e Estratégia de Segurança Pública (SUPESP) que é a unidade responsável por produzir, analisar e disponibilizar estatísticas e informações relacionadas à Segurança Pública e Defesa Social.

Paraíba

Possui unidade especializada em crime digital, criada em 10/06/2021 por força do Decreto Estadual de nº 41.333 e chamada de Delegacia Especializada de Crimes Cibernéticos.

Não apresentou mais nenhuma informação em resposta ao questionário enviado.

Pernambuco

A Delegacia de Repressão aos Crimes Cibernéticos, surgiu através da Lei Estadual Nº 15.026, DE 20 DE JUNHO DE 2013, em cumprimento ao Art. 4º da Lei Federal nº 12.735/2012, com a finalidade de prevenir e reprimir, com exclusividade no Município do Recife, a prática de crimes tecnológicos, virtuais e eletrônicos, que envolvam delitos praticados com o uso da tecnologia, sobretudo através da internet; e que a posterior foram

estabelecidas as atribuições através da Portaria GAB/PCPE nº 050 de 15/02/2017 e atualizadas com a Portaria GAB/PCPE nº 24 de 15/02/2019.

Afirmam possuir trabalhos estatísticos sobre crimes digitais, mas não disponibilizou nenhum dado para análise, salvo a informação que no trimestre inicial de 2021 tiveram aproximadamente 186 registros de ocorrência presencialmente e 5.000 boletins registrados através da internet.

Citou um caso de grande repercussão, a chamada operação 404 contra pirataria e com várias fases de execução em todo o país, e afirmam que os crimes de estelionato e fraude são os mais frequentes sem, entretanto, detalhar esses dados

Piauí

Respondeu apenas que possui uma unidade especializada em cibercrimes, a Delegacia de Repressão aos Crimes de Informática DRCI. Não enviou dados.

Rio Grande do Norte

Não possui unidade especializada em crime digital e as investigações de cibercrimes são conduzidas pelas outras delegacias distritais.

Não possui trabalhos estatísticos sobre crimes digitais e basicamente não responderam mais nada do questionário enviado.

Sergipe

Possui unidade especializada em crime digital, a Delegacia Especial a Crimes Cibernéticos – DRCC que foi criada no ano de 2013 por meio da Portaria nº 01/2013 do Delegado Geral de Polícia Civil, com atribuição para apuração dos fatos enquadrados como condutas típicas, antijurídicas e culpáveis contra sistemas de informática ou praticadas com a utilização destes, desde que com autoria desconhecida e ocorrido nos limites da circunscrição da Coordenadoria de Polícia Civil da Capital

Afirmam existir trabalhos estatísticos sobre crimes digitais, mas não disponibilizaram nenhum dado

Citou caso de grande repercussão e eventuais cooperações com a iniciativa privada, mas sem mais dados.

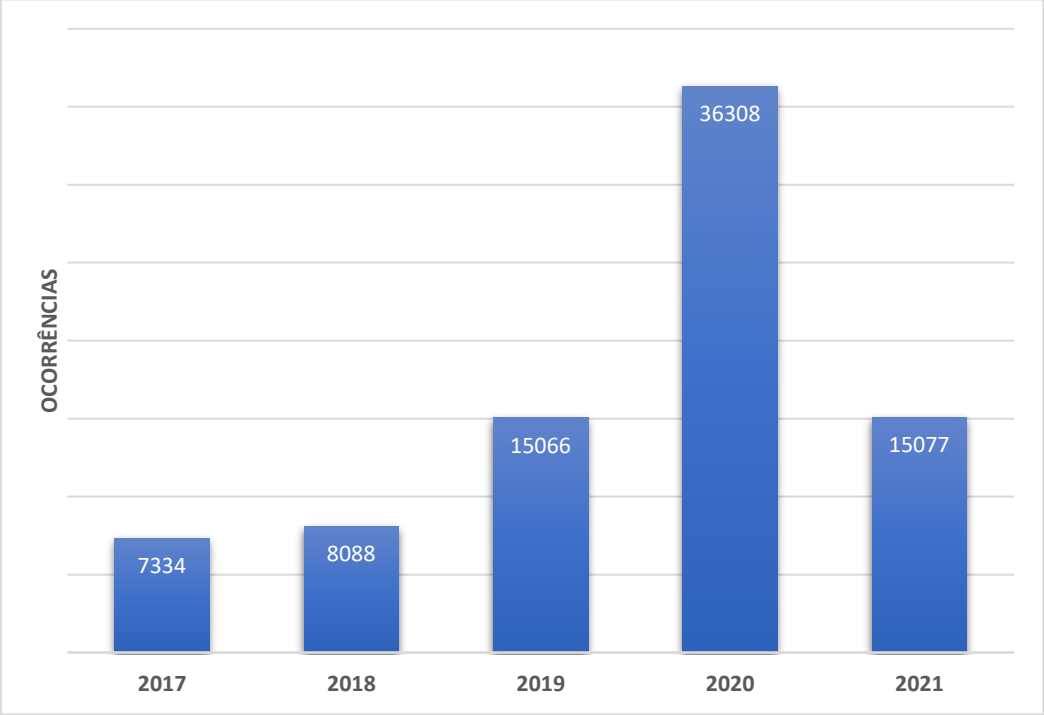
Região Centro-Oeste:

Distrito Federal

Possui unidade especializada em crime digital, a Delegacia Especial de Repressão aos Crimes Cibernéticos.

Possui trabalhos estatísticos sobre crimes digitais e disponibilizou dados para análises na forma de uma planilha com o título "NATUREZAS DE CRIMES PRATICADOS PELA INTERNET NO DISTRITO FEDERAL" contendo três pastas com cerca de 82000 registros, além do Perfil dos autores e Mapa de Calor.

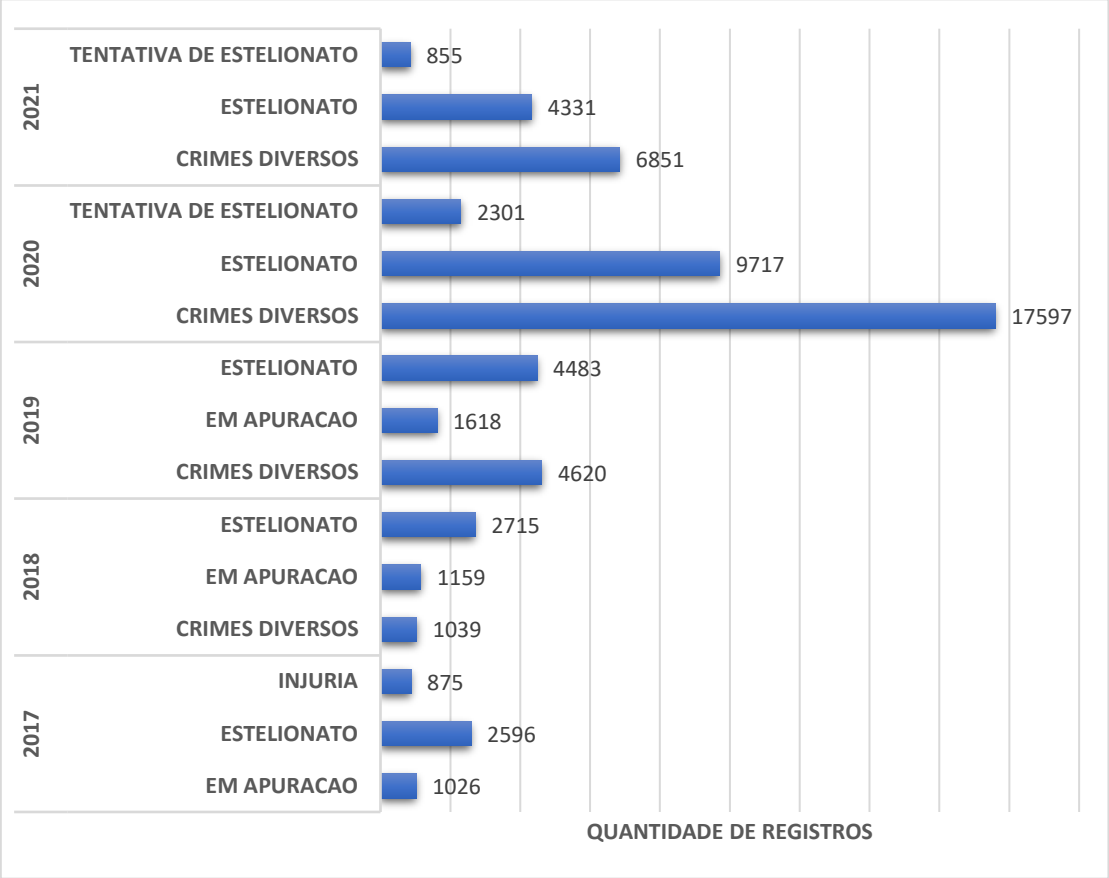
Gráfico 6 - Cibercrimes por Ano - Distrito Federal



No gráfico 6 é possível identificar o total de cibercrimes registrados no Distrito Federal por ano e numa primeira avaliação, seria viável correlacionar o crescimento de ocorrências a partir de 2019 com a necessidade de isolamento social por conta da pandemia da COVID-19 e a crescente demanda de serviços de internet.

No gráfico 7 são apresentados os cibercrimes de maior frequência registrados no DF e entre as ocorrências chama a atenção o título "CRIME DIVERSOS" que em uma explicação superficial seriam as ocorrências declaradas na delegacia, mas cujo crime apesar de estar sendo denunciado, ainda não é possível classificar entre as várias opções de titulação criminal.

Gráfico 7 - Ocorrências de Maior Frequência por Ano - DF



Goiás

Possui unidade especializada em crime digital, a Delegacia Estadual de Repressão a Crimes Cibernéticos - DERCC que foi criada pela Lei Estadual 19907/17 – publicada em 17/12/2017 e com o efetivo início das atividades em 01/03/2018.

A unidade possui infraestrutura de TI e realiza treinamentos, mas não os detalhou, também não apresentou dados estatísticos ou tempos de duração de investigação.

Citou casos elucidados de Pornografia Infantil, envolvendo exploração sexual infantil, onde o tráfico de dados dos arquivos com conteúdo criminoso foi monitorado pelos sistemas/agentes e posterior rastreio do autor. Também afirmam existir casos resolvidos envolvendo a venda/consulta de dados privados, onde criminosos criavam portais/sites expondo banco de dados com dados pessoais e corporativos de milhares de usuários sem a devida autorização ou ciência deles.

Mato Grosso do Sul

Possui unidade especializada em crime digital criada em 2006 pelo decreto nº 12.218, a Delegacia Virtual do Estado de mato Grosso do Sul – DEVIR é responsável pelo registro de Boletim de ocorrência on-line, pela instauração de procedimento para apuração de crimes virtuais e apoio a outras unidades policiais.

Possui trabalhos estatísticos sobre crimes feita por uma outra área da segurança, entretanto disponibilizou apenas alguns dados para análise, na forma de uma tabela com a quantidade total de registros mensais de ocorrências de janeiro a abril de 2021 sem detalhamento de títulos ou outras informações mais relevantes.

Citou casos de grande repercussão envolvendo elucidação de crime de estelionato e o desenvolvimento e liberação para acesso público de uma ferramenta de pesquisa de vazamento de dados na internet além de informações sobre como se proteger na web (https://crasp.gov.br/admpro/site/materias-em-destaque/privacidade-em-risco)

Mato Grosso

Não respondeu ao questionário alegando necessidades adicionais de análise, interpretação ou consolidação de dados e informações.

Região Sudeste

Espírito Santo

Indeferiu o pedido citando a complexidade da demanda e falta de estrutura e tempo para atender a requisição.

São Paulo

Possui unidade especializada em crime digital, a Divisão de Crimes Cibernéticos (DCCIBER) que é subordinada ao Departamento Estadual de Investigações Criminais (DEIC) e conta com quatro delegacias especializadas: 1ª Delegacia de Polícia sobre Fraudes contra Instituições Financeiras praticadas por meios Eletrônicos; 2ª Delegacia de Polícia sobre Fraudes contra Instituições de Comércio Eletrônico praticada por meios Eletrônicos; 3ª Delegacia de Polícia sobre Violação de Dispositivos Eletrônicos e Redes de Dados; 4ª Delegacia de Polícia de Lavagem e Ocultação de Ativos Ilícitos por Meios

Eletrônicos; além de um Centro de Inteligência Cibernética (CIC) e um Laboratório Técnico de Análises Cibernéticas (Lac-TAC).

Possui trabalhos estatísticos sobre crimes digitais, mas não disponibilizou dados para análise, se limitando a indicar o site da Secretaria de Segurança Pública como local a ser avaliado para acesso aos dados.

Minas Gerais

Possui uma Divisão criada em 2008 com duas delegacias especializadas em crime digital, apresentou trabalhos estatísticos sobre crimes digitais e disponibilizou dados para análise na forma de duas planilhas, sendo uma sobre os crimes cibernéticos com quatro pastas e com cerca de 106000 registros, e as outras pastas com análises por título, ano e origem. A outra planilha é sobre as vítimas com um total de 125000 registros

Citou casos de grande repercussão como a Operação "defacement" – desencadeado pela 1ª DEICC – Que em resumo foi um jovem de 23 anos natural de Uberlândia que teve encerrada sua rotina de invasão de sites de empresas varejistas e de órgãos públicos ao tentar violar a página da Polícia Civil de Minas Gerais. Natural de Uberlândia, no Triângulo Mineiro, ele vinha atuando pelo menos desde 2013 e chegou a penetrar nas defesas de sites como o do Exército do Brasil, do Ministério Público de Minas Gerais, do Governo de Minas, do Tribunal de Justiça de Minas Gerais, de várias prefeituras e de particulares.

A prisão ocorreu no dia 18/11/2019, depois de uma investigação da 1ª Delegacia Especializada em Investigação de Crimes Cibernéticos (DEICC) que conseguiu rastrear o jovem que segundo a polícia tinha origem humilde, aparentava agir sozinho e se vangloriava de suas ações criminosas.

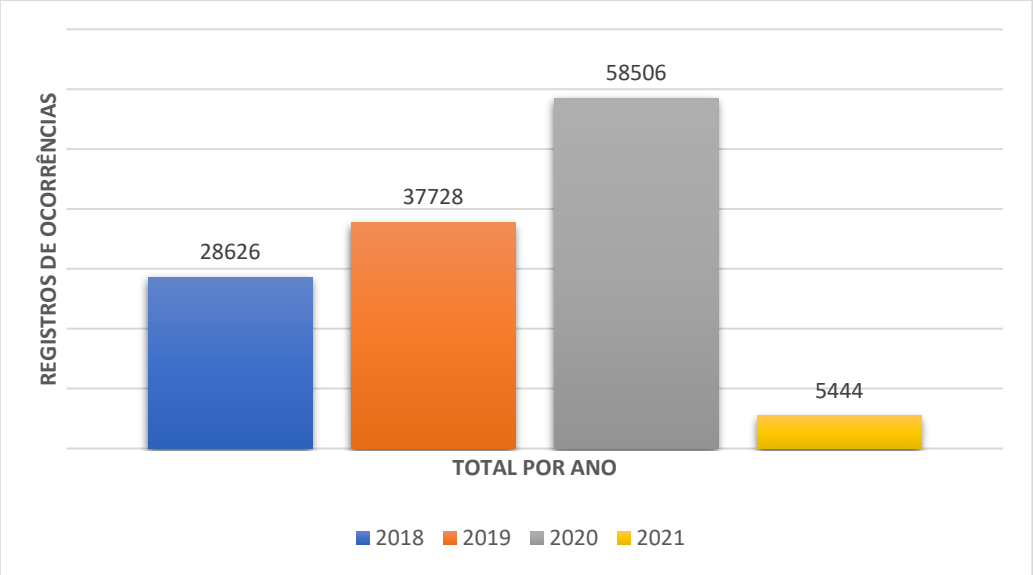
Outra Operação citada foi a chamada "Sodoma" – desencadeado pela 2ª DEICC – Onde um homem foi preso suspeito de estuprar e cometer crimes contra a dignidade sexual contra mais de 100 mulheres em 13 estados diferentes. Ele exigia que vítimas assinassem contrato de escravidão e gravassem vídeos dizendo estar de acordo com o documento. Ele foi detido no dia 2/10/2019, no sítio que alugava em Juatuba, na Grande BH.

A ação ocorria desde 2015 e os policiais precisaram de grande dedicação para comprovar os crimes, chegando a mais de 15 horas diárias de investigação. Além dos

vídeos comprometedores que o suspeito obrigava as vítimas a fazer, muitas vezes envolvendo cães e outros animais, era uma parte do jogo mental que ele fazia, com a criação de vários perfis onde se passava por outras pessoas para ganhar a confiança das vítimas e as atormentar. A unidade também destacou que seria inexistente qualquer cooperação com a iniciativa privada.

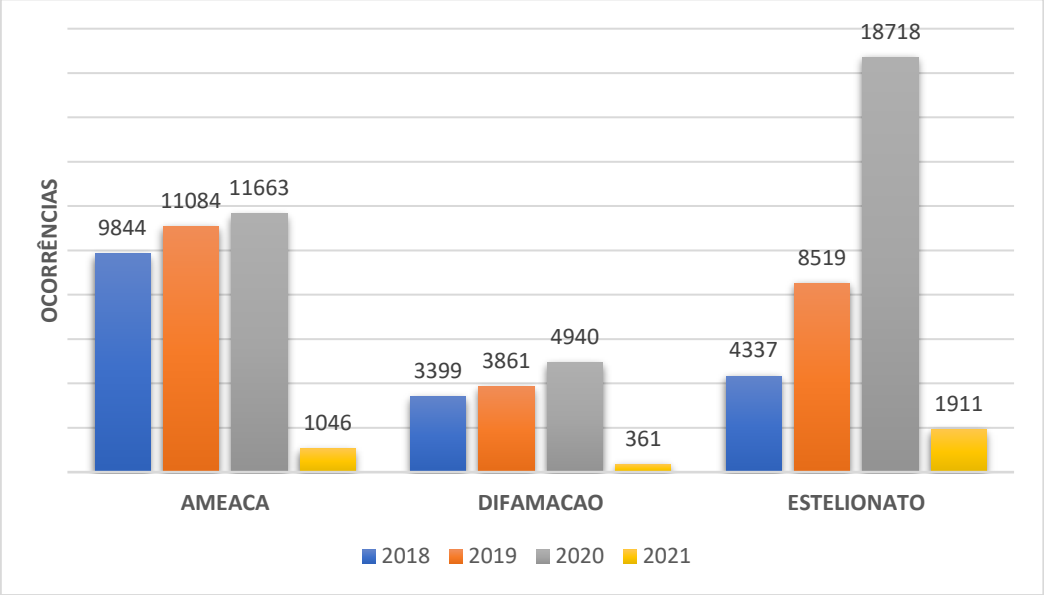
No gráfico 8 são apresentados os totais de ocorrências registradas por ano e é possível inferir que o crescimento ocorrido sequencialmente de 2019 até 2020 é um indicativo de potencial relação com a necessidade de isolamento social por conta da pandemia da COVID-19 e a crescente demanda de serviços de internet.

Gráfico 8 - Cibercrimes por Ano – Minas Gerais



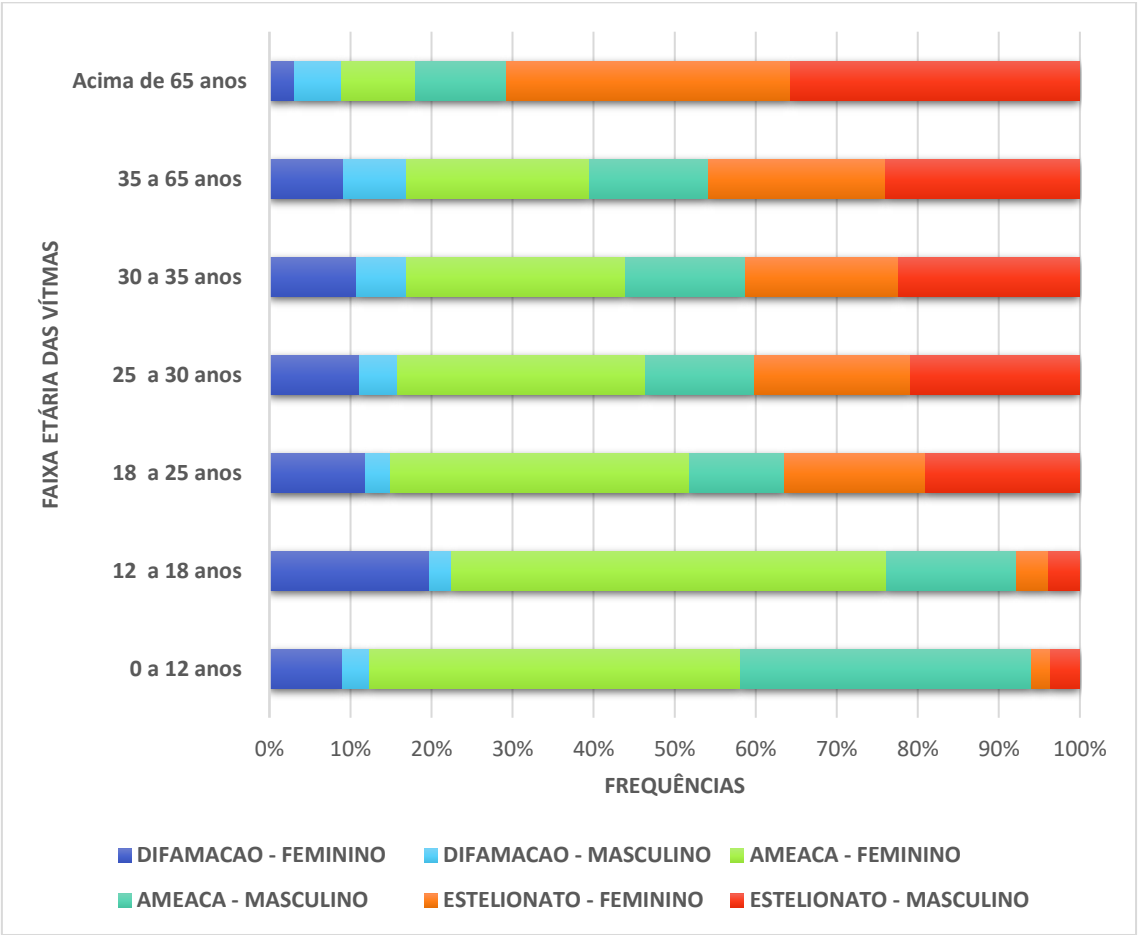
No gráfico 9 são apresentados os três cibercrimes mais frequentemente denunciados, com a ressalva que os dados referentes ao ano de 2021 são limitados até o mês de janeiro.

Gráfico 9 - Ocorrências Criminais de Maior Frequência por Ano – Minas Gerais



No gráfico 10 são apresentadas as faixas etárias e sexo das vítimas dos cibercrimes de maior ocorrência e é possível identificar que tais títulos de crimes (DIFAMAÇÃO, AMEAÇA E ESTELIONATO) são ocorrências também declaradas por outros estados, mesmo sem apresentar dados que corroborem tal afirmativa.

Gráfico 10 - Cibercrimes de Maior Frequência por Faixa Etária e Sexo – Minas Gerais



Rio de Janeiro

Possui unidade especializada em crime digital, A Delegacia de Repressão aos Crimes de Informática – DRCI, criada pela resolução 1047/2017 da SSP/RJ. A DRCI apresentou trabalhos estatísticos sobre crimes digitais através do Instituo de Segurança Pública do RJ – ISP, e disponibilizou uma planilha com um total de 22925 registros além de dados sobre cibercrimes. Também apresentou tempo de duração de investigação de cerca de 1 ano, mas sem possibilidade de verificação dos dados pela cobertura do sigilo necessário nesse tipo de informação.

Frente aos dados obtidos junto ao ISP na tabela 2 é possível identificar que os cibercrimes de DIFAMAÇÃO, ESTELIONATO E INJÚRIA são os mais frequentemente registrados na unidade especializada.

Tabela 2 - Ocorrências de Maior Frequência – DRCI RJ

DRCI	Anos				
Ocorrências	2017	2018	2019	2020	Total Geral
Ameaça	138	121	89	50	398
Calúnia	84	86	78	81	329
Difamação	239	259	159	128	785
Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia		6	59	81	146
Estatuto da Criança e do Adolescente	81	73	67	26	247
Estelionato (outros)	305	259	371	255	1190
Extorsão (outros)	58	78	64	40	240
Falsa Identidade	161	98	51	54	364
Furto outros	25	47	44	30	146
Injúria (outros)	338	398	386	247	1369
Invasão de Dispositivo Informático	198	108	39	22	367
Total Geral	**1627**	**1533**	**1407**	**1014**	**5581**

No gráfico 11 é possível identificar a totalização de registros de cibercrimes por ano feitos na delegacia de repressão aos crimes de informática, e no gráfico 12 é demonstrado a evolução especificamente do crime de ESTELIONATO, tanto em sua forma "tradicional", como também o cibercrime executado pela internet durante o período de isolamento social frente a pandemia de COVID-19.

Gráfico 11 - Total de Ocorrências Ano – DRCI RJ

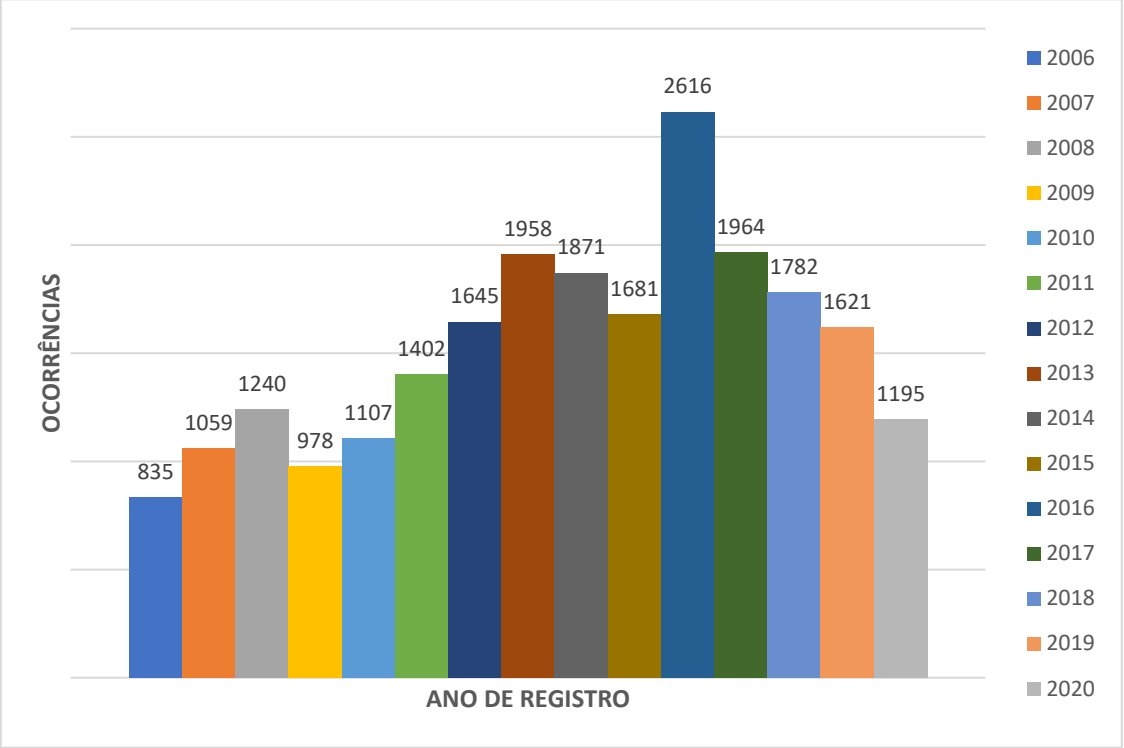
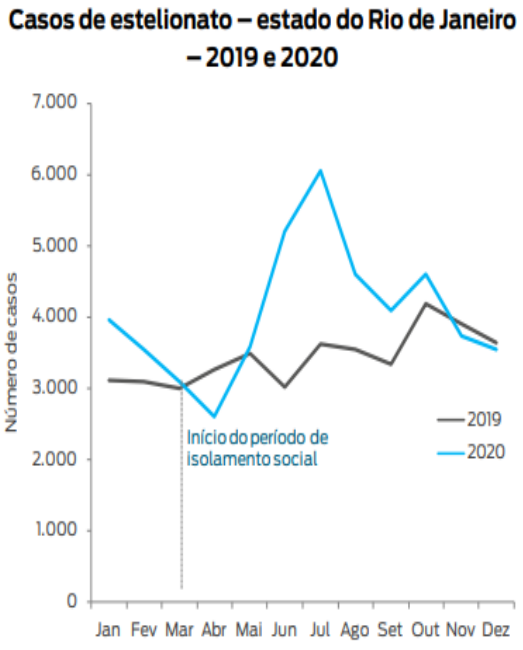
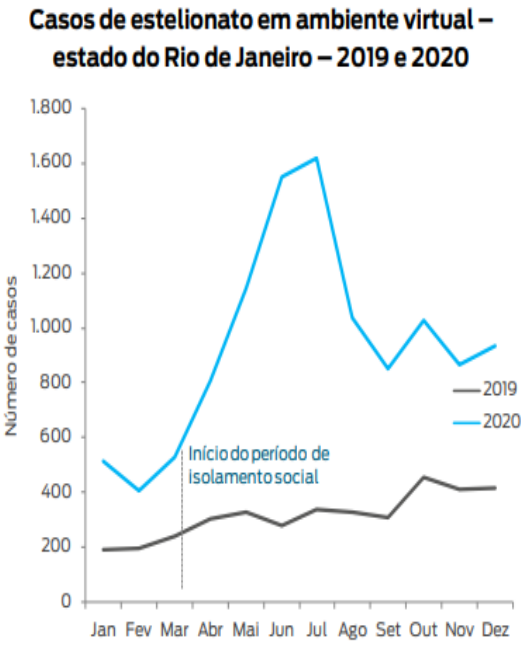


Gráfico 12 - Evolução de Registros de Estelionato - RJ



Fonte: Elaborado pelo ISP com base em informações da Secretaria de Estado de Polícia Civil.



Fonte: Elaborado pelo ISP com base em informações da Secretaria de Estado de Polícia Civil.

Região Sul

Paraná

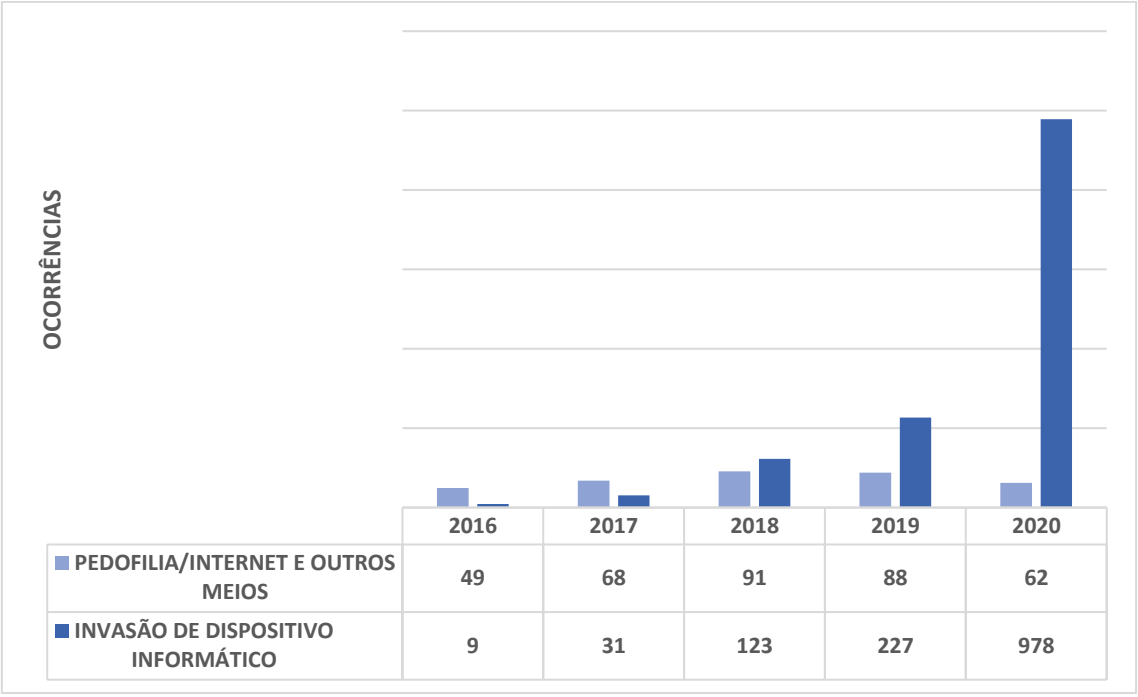
Possui unidade especializada em crime digital, criado em 2005 pela resolução SESP 293/05 o Núcleo de Combate aos Cibercrimes – NuCiber, órgão de atividade especial, com atribuições de polícia administrativa e judiciária em todo o Estado do Paraná. Destacamos que os dados coletados sobre o estado do Paraná não nos permitiram fazer

Não possui trabalhos estatísticos sobre crimes digitais e citaram casos de grande repercussão como as Operações 404 e LUZ NA INFÂNCIA.

Rio Grande do Sul

Possui unidade especializada em crime digital, a Delegacia de Repressão aos Crimes Informáticos e Defraudações. Destacamos que os dados encaminhados pelo estado do Rio Grande do Sul não possibilitaram desenvolver trabalhos estatísticos sobre crimes digitais, mas o estado disponibilizou dados para análise referentes a crimes de pedofilia na Internet e Outros Meios e de Invasão de Dispositivo de 2016 e 2020 (Gráfico 13).

Gráfico 13 - Ocorrências Rio Grande do Sul



	2016	2017	2018	2019	2020
PEDOFILIA/INTERNET E OUTROS MEIOS	49	68	91	88	62
INVASÃO DE DISPOSITIVO INFORMÁTICO	9	31	123	227	978

Santa Catarina

Possui unidade especializada em crime digital como parte da estrutura da Diretoria Estadual de Investigações Criminais (DEIC). O DEIC afirma possuir trabalhos estatísticos sobre crimes digitais, mas não disponibilizou dados para nossa análise, apresentando apenas a tabela 3 com as informações de ocorrências registradas sem maiores detalhamentos referentes ao solicitado.

Tabela 3 - Ocorrências Santa Catarina

	2019							
REG - Sistema de Origem	mai	jun	jul	ago	set	out	nov	dez
Totais	1684	2186	2806	2820	3022	3426	3199	2852
Delegacia Virtual (online)	1		4	2		9	7	1
Delegacias de Polícia (precencial)	1683	2186	2802	2818	3022	3417	3192	2851

	2020											
REG - Sistema de Origem	jan	fev	mar	abr	mai	jun	jul	ago	set	out	nov	dez
Totais	3910	3656	2315	677	1016	1440	1256	1236	3287	6361	6622	5792
Delegacia Virtual (online)	3	4	32	178	181	231	187	120	1731	4228	4299	3944
Delegacias de Polícia (precencial)	3907	3652	2283	499	835	1209	1069	1116	1556	2133	2323	1848

	2021					
REG - Sistema de Origem	jan	fev	mar	abr	mai	jun
Totais	6288	6395	7075	6892	7207	325
Delegacia Virtual (online)	4186	3995	4680	4325	4173	180
Delegacias de Polícia (precencial)	2102	2400	2395	2567	3034	145

Outras Unidades de Análise

Ministério Público Federal

O MPF possui unidade especializada em crime digital que conta com infraestrutura de TI e realiza treinamentos para seus membros. Eles possuem trabalhos estatísticos sobre crimes digitais dentro de seu escopo de atuação e disponibilizaram documentos em formato pdf como atos e normativos, doutrinas, eventos e treinamentos, notas técnicas, palestras, pareceres e relatórios.

Departamento de Polícia Federal

Indeferiu o pedido alegando necessidade de tratamento adicional de dados

4.4 AVALIAÇÃO COMPARATIVA SOBRE OS DADOS DO RJ, DF E MG

Após a análise qualitativa e quantitativa dos dados obtidos das estruturas de segurança pública, é possível identificar que somente alguns possuem informações detalhadas suficientes ou que permitam algum tipo de comparação e análise especificamente sobre os cibercrimes. Esta seção apresenta um estudo comparativo que ficou restrito apenas as três unidades federativas que ofereceram dados mais detalhados, a saber: Estados de Minas Gerais, Distrito Federal e Rio de Janeiro.

Rio de Janeiro

O estado apresentou dados em uma planilha com faixa temporal de 2006 até 2020, específicos da delegacia especializada e com um total de 22954 registros, formatados em 263 títulos de ocorrências discriminadas e listadas na coluna “TÍTULO”.

Distrito Federal

Apresentou dados de 2017 até 2021 de crimes praticados pela internet em uma planilha com 81.873 registros, sendo 23 títulos de ocorrências discriminadas e listadas na coluna “NATUREZA PADRONIZADA”.

Minas Gerais

O estado apresentou dados de 2018 até 2021 de informações sobre crimes cibernéticos em duas planilhas, totalizando 105.911 registros com 269 títulos de ocorrências discriminadas e listadas na coluna “NATUREZA PRINCIPAL” da planilha recebida.

Observando os crimes mais registrados por estado, e atribuindo que a ausência de grafia correta ainda permitiria a identificação e comparação dos dados, foi realizado um recorte dos 15 crimes mais registrados além da padronização dos termos, como por exemplo, o que foi encontrado no título do crime “AMEAÇA”, que contava com a escrita “AMEAÇA” E “AMEACA”, resultando a sequencia em ordem decrescente de número de registros de ocorrências:

Rio de Janeiro:

1. AMEAÇA
2. CALÚNIA
3. DIFAMAÇÃO

4. DIVULGAÇÃO DE CENA DE ESTUPRO OU DE CENA DE ESTUPRO DE VULNERÁVEL, DE CENA DE SEXO OU DE PORNOGRAFIA
5. ESTATUTO DA CRIANÇA E DO ADOLESCENTE
6. ESTELIONATO (OUTROS)
7. ESTELIONATO (OUTROS) - TENTATIVA
8. EXTORSÃO (OUTROS)
9. FALSA IDENTIDADE
10. FATO ATÍPICO
11. FURTO OUTROS
12. INJÚRIA (OUTROS)
13. INJÚRIA POR PRECONCEITO
14. INVASÃO DE DISPOSITIVO INFORMÁTICO
15. MEDIDA ASSECURATÓRIA DE DIREITO FUTURO

Minas Gerais:

1. AMEAÇA
2. CALÚNIA
3. DIFAMAÇÃO
4. ESTELIONATO
5. FALSIDADE IDEOLOGICA
6. INJÚRIA
7. INVASÃO DE DISPOSITIVO INFORMATICO
8. OUTRAS AÇÕES DEFESA SOCIAL
9. OUTRAS DENUNCIA RECLAMAÇÕES SOLICITAÇÕES DEF SOCIAL
10. OUTRAS INFRAÇÕES CONTRA DIGNIDADE SEXUAL E A FAMILIA
11. OUTRAS INFRAÇÕES CONTRA O PATRIMONIO
12. OUTRAS INFRAÇÕES DEMAIS LEIS ESPECIAIS
13. OUTROS INFRAÇÕES C/ A PESSOA
14. PERTURBAÇÃO DA TRANQUILIDADE
15. PERTURBAÇÃO DO TRABALHO OU DO SOSSEGO ALHEIOS

Distrito Federal:

1. AMEAÇA
2. CONTRAVENÇÕES
3. CRIME CONTRA O CONSUMIDOR
4. CRIMES DIVERSOS
5. EM APURAÇÃO
6. ESTELIONATO
7. EXTORSÃO
8. FURTOS DIVERSOS
9. INJÚRIA
10. LEI MARIA DA PENHA (Lei 11.340/06)
11. PORNOGRAFIA
12. TENTATIVA DE CRIMES DIVERSOS
13. TENTATIVA DE ESTELIONATO
14. TENTATIVA DE EXTORSÃO
15. VIOLAÇÃO DE DIREITO AUTORAL

Frente a esses dados, e buscando pontos em comum dos tipos de crimes registrados em cada unidade da federação, os crimes de ameaça, estelionato e injúria aparecem como sendo os títulos em comum de maior número de ocorrências nos três estados analisados com os dados sendo apresentados na tabela 4.

Tabela 4 – Volume de Ocorrências dos Crimes de AMEAÇA, ESTELIONATO e INJÚRIA

TÍTULOS DE OCORRÊNCIAS	DF	MG	RJ	Total Geral
AMEACA	4.762	33.637		38.399
AMEAÇA			1.377	1.377
AMEAÇA - LEI 11.340/06			13	13
AMEACA/COAGE/P/ EXPOR AO RIDICULO P/QUITAR		13		13
ESTELIONATO	23.842	33.485		57.327
ESTELIONATO (OUTROS)			4.121	4.121
ESTELIONATO (OUTROS) - TENTATIVA			192	192
ESTELIONATO COM EMPREGO DE CARTÃO DE CRÉDITO			37	37
ESTELIONATO COM EMPREGO DE CARTÃO DE CRÉDITO - TENTATIVA			5	5

ESTELIONATO ENVOLVENDO VEÍCULO			2	2
ESTELIONATO POR DEFRAUDAÇÃO DE PENHOR			1	1
ESTELIONATO POR FRAUDE NA ENTREGA DE COISA			22	22
EXIBE/VEIC INFOR/IMAGEM DEPREC/INJURI. IDOSO		9		9
INJURIA	4.748	4.983		9.731
INJÚRIA (OUTROS)			5.101	5.101
INJÚRIA (OUTROS) - TENTATIVA			1	1
INJURIA ALGUEM NA PROPAGANDA ELEITORAL		11		11
INJÚRIA POR PRECONCEITO			142	142
INJÚRIA REAL			7	7
TENTATIVA DE AMEACA	3			3
TENTATIVA DE ESTELIONATO	4.154			4.154
TOTAL GERAL	**37.509**	**72.138**	**11.021**	**120.668**

Durante o processo de análise dos dados obtidos junto aos estados, ficou latente que existia uma falta de uma padronização dos títulos de ocorrências, o que dificultaria qualquer trabalho de comparação dos dados e na sequência a análise e suas conclusões.

Um outro evento que chamou a atenção foi o entendimento que as tipificações apresentadas nos dados foram apenas as interpretações iniciais feita pela autoridade policial frente a narração do delito pela vítima, e que justamente por isso podem vir a ser alteradas no percurso da investigação.

Uma última observação sobre o conjunto dos dados, foi o fato de que alguns títulos possuíam valores muito altos de frequências, mas a falta da possibilidade de identificação ao que se referiam inviabilizou qualquer análise no contexto dessa pesquisa. Por exemplo: No Distrito Federal, o título indicado como “CRIMES DIVERSOS” possuía uma grande taxa de crescimento entre os anos de 2019 e 2021 sendo inclusive mais frequente que a maioria dos outros títulos do estado, só que por não ser possível analisar tal titulação acabou por excluir essa informação desse estudo.

Esses três fatores previamente apresentados ao serem combinados demonstram a necessidade de um desenvolvimento e integração entre as áreas de segurança pública no

país, com foco em tentar unificar suas titulações e aprimorar a geração de dados e informações para planejamento e estatística.

4.5 CONSIDERAÇÕES SOBRE AS DEFINIÇÕES LEGAIS E CRIMES MAIS IDENTIFICADOS NAS TRÊS UNIDADES FEDERATIVAS

Nesse ponto, torna-se prudente e relevante discutir as definições jurídicas desses crimes anteriormente apresentados para nivelar o entendimento sobre o que seriam e de que forma são identificados e/ou tratados na justiça.

4.5.1 INJÚRIA

O derradeiro crime contra a honra é o crime de Injúria. A tipificação penal está descrita no artigo 140 do Código Penal vigente, que tem a redação:

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa. § 1º - O juiz pode deixar de aplicar a pena: I - quando o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria. § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes: Pena – detenção, de três meses a um ano, e multa, além da pena correspondente à violência. § 3] Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência: (Redação dada pela Lei nº 10.741, de 2003) Pena – reclusão de um a três anos e multa.

Desta forma, Rogério Greco, eminente estudioso sobre o tema, faz a afirmação de que entre todas as infrações penais tipificadas no Código Penal que visam proteger a honra, a injúria, na sua modalidade fundamental, é a considerada menos grave. Entretanto, por mais paradoxal que possa parecer, a injúria se transforma na mais grave infração penal contra a honra quando consiste na utilização de elementos referentes à raça, cor, etnia, religião, origem ou à condição de pessoa idosa, ou portadora de deficiência, sendo denominada, aqui, de injúria preconceituosa (...) (GRECO, 2016, p.433).

E ainda nesse contexto continua explicando (GRECO, 2016, p.433) “já a injúria se difere dos outros crimes contra a honra, pois tutela a honra subjetiva do indivíduo, ou seja, a autoestima da pessoa, e como ela mesma vê seus atributos físicos, morais ou

intelectuais". A ofensa, neste caso, é direcionada à dignidade ou autoestima de um indivíduo e tal prática passou a ser muito comum no ciberespaço pois, acreditando na segurança de um falso ou precário anonimato, o agressor desfere contra suas vítimas ações e conteúdos ofensivos. Pelo ensinamento de Rogério Greco, citado acima, percebe-se que se trata de um crime que pode ser realizado de forma livre, algo que se mostra muito comum na internet, especificamente em redes sociais ou sites que divulgam imagens, frases, ou qualquer conteúdo que atribuam qualidades negativas a alguém, incluindo também as variações relacionadas as injúrias raciais, aos posicionamentos políticos ou por qualquer tipo de preconceito.

4.5.2 ESTELIONATO

A pandemia global de COVID-19 com a recomendação do isolamento social, o avanço tecnológico que trouxe a massificação do acesso da internet em suas várias apresentações, além da falta de conhecimento e treinamento da população nesse ecossistema, permitem inferir que ao serem considerados em conjunto teriam relação no crescimento dos índices desse cibercrime no período de 2019 até o atual.

O crescimento do comércio eletrônico, as oportunidades de negócios que seriam "imperdíveis", os descontos avassaladores e os romances baseados em relacionamentos virtuais são os vetores básicos para os estelionatos digitais.

O crime de estelionato se tipifica no artigo 171 do Código Penal que possui a redação: "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". Rogério Grego (2009, p.228), afirma que: "desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas"

Merece atenção que o crime de estelionato não se utiliza de furto ou mesmo de violência, quer seja física ou moral, sendo basicamente o uso de uma ilusão da vítima que coopera com o ato, mediante uso de meios fraudulentos. Partindo dessa linha de raciocínio, é possível encontrar inúmeros exemplos desse tipo de crime que é comum no mundo "analógico" com sua versão no ciberespaço, tais como as famosas ofertas de falsos empregos, que só se efetivariam mediante o pagamento de uma taxa para conseguir o posto de trabalho, e o atualmente mais comum de todos; a pirâmide financeira baseada

em ativos conhecidos ou chamados de criptomoedas, com rentabilidades absurdas e com promessas de enriquecimento rápido e fácil.

4.5.3 AMEAÇA

O crime de ameaça conforme descreve o Artigo 147, do Código Penal e aquele onde por meio de palavra, escrita ou gesto, ou qualquer outra forma simbólica, prenunciar a outro a prática de mal injusto e grave contra ele ou contra terceiro, com pena de detenção de 1 a 6 meses ou multa.

Conforme apresentado por Capez (2012, p. 360), essa lei quis deixar claro o tipo penal na modalidade genérica de ameaça, uma vez que pode acontecer de modo falado, escrito, real ou simbólico. O objeto material desse delito é a pessoa que sofre a ameaça e o bem jurídico ou o objeto jurídico protegido pelo tipo penal de ameaça é a liberdade pessoal. O elemento subjetivo é o dolo (direto/eventual), ou seja, a intenção de provocar medo de intimidar a vítima.

Esse crime basicamente é sobre a conduta de amedrontar, intimidar e assustar, por meio de palavras, escritos e gestos. No caso dos cibercrimes, esse crime pode vir a ocorrer por meio de comentários intimidadores nas redes sociais por exemplo.

5 PROPOSTA DE ELABORAÇÃO DE UM AMBIENTE COMPUTACIONAL DE REGISTRO DE OCORRÊNCIAS DE CIBERCRIMES PARA O BRASIL

Nesse capítulo, apresentamos uma proposta de natureza conceitual para a elaboração de um ambiente computacional embasado nos elementos estudados e discutidos ao longo desta dissertação. Dado o escopo desta dissertação e a natureza do nosso programa de pós-graduação, destacamos que a proposta não visa abarcar todos os tecnicismos, requisitos funcionais e não funcionais e regramentos de um projeto de software e bancos de dados ou algoritmos de inteligência artificial tradicionais da Ciência da Computação, pelo contrário trata-se de uma primeira contribuição, uma visão geral de um ambiente computacional e que não pretende esgotar o assunto por si só.

Observando que no caso do Brasil ainda inexistente um canal digital de registro unificado de ocorrência de cibercrimes, a proposição de criação de um artefato computacional ou plataforma concentradora para facilitar a denunciação de cibercrimes por parte dos cidadãos (nos moldes utilizados ou recomendados por outras nações), com

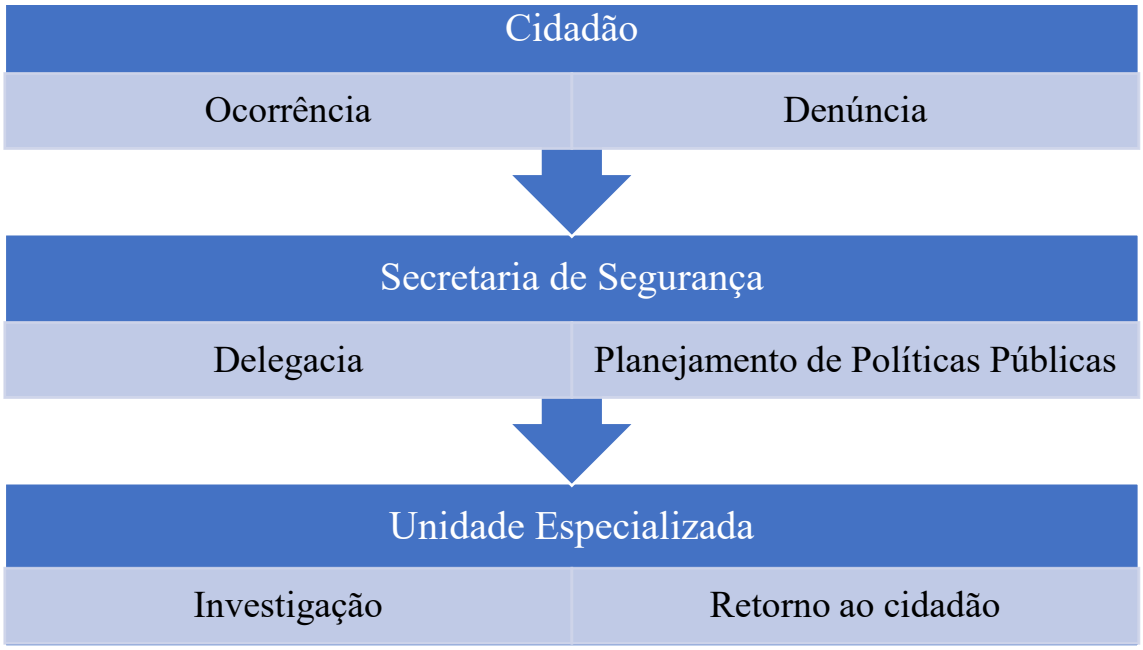
posterior direcionamento para as forças policiais especializadas em cibercrimes pode ser uma contribuição inicial para mitigá-los, fornecendo um ambiente mais automatizado para as forças de segurança pública.

Devido a ampla heterogeneidade de características sociais, educacionais, etárias e demográficas da população brasileira, aliado com as desigualdades estruturas organizacionais da segurança pública estadual, aqui se estima que um artefato digital assemelhado a um formulário online permitiria ao cidadão (vítima ou declarante) fazer um registro inicial e anexar imagens, mensagens ou telas ou outras informações sobre o ambiente computacional onde o fato ocorreu. Adicionalmente, optou-se por este tipo de artefato já que poderia ser executado pelos interessados tanto em computadores pessoais quanto em dispositivos móveis de baixo custo.

As informações seriam fornecidas diretamente pelos cidadãos seriam armazenadas em um repositório seguro de dados, esses dados representam um diferencial que além de ajudar nas investigações. Essa interação inicial permitiria a diminuição do trabalho de recepção das denúncias em uma unidade policial, possibilitando o abastecimento de um grande repositório de dados unificado que serviria de base para a elaboração de processos analíticos e criação de indicadores ou relatórios mais precisos sobre as ocorrências de cibercrimes, apoiando em possíveis futuras ações de planejamento ou até mesmo norteando os investimentos da segurança pública.

Nossa proposta de artefato computacional pode ser ilustrada como sendo um conjunto de camadas, onde cada camada teria um objetivo e um público-alvo distinto. O fluxo de informações produzidas pelo artefato inicialmente pela vítima ou declarante de um cibercrime, sendo direcionada e acessível pela polícia e por responsáveis por elaborar estudos e políticas públicas de combate ao crime e criar atividades de planejamento e inteligência policial conforme apresentado na figura 8.

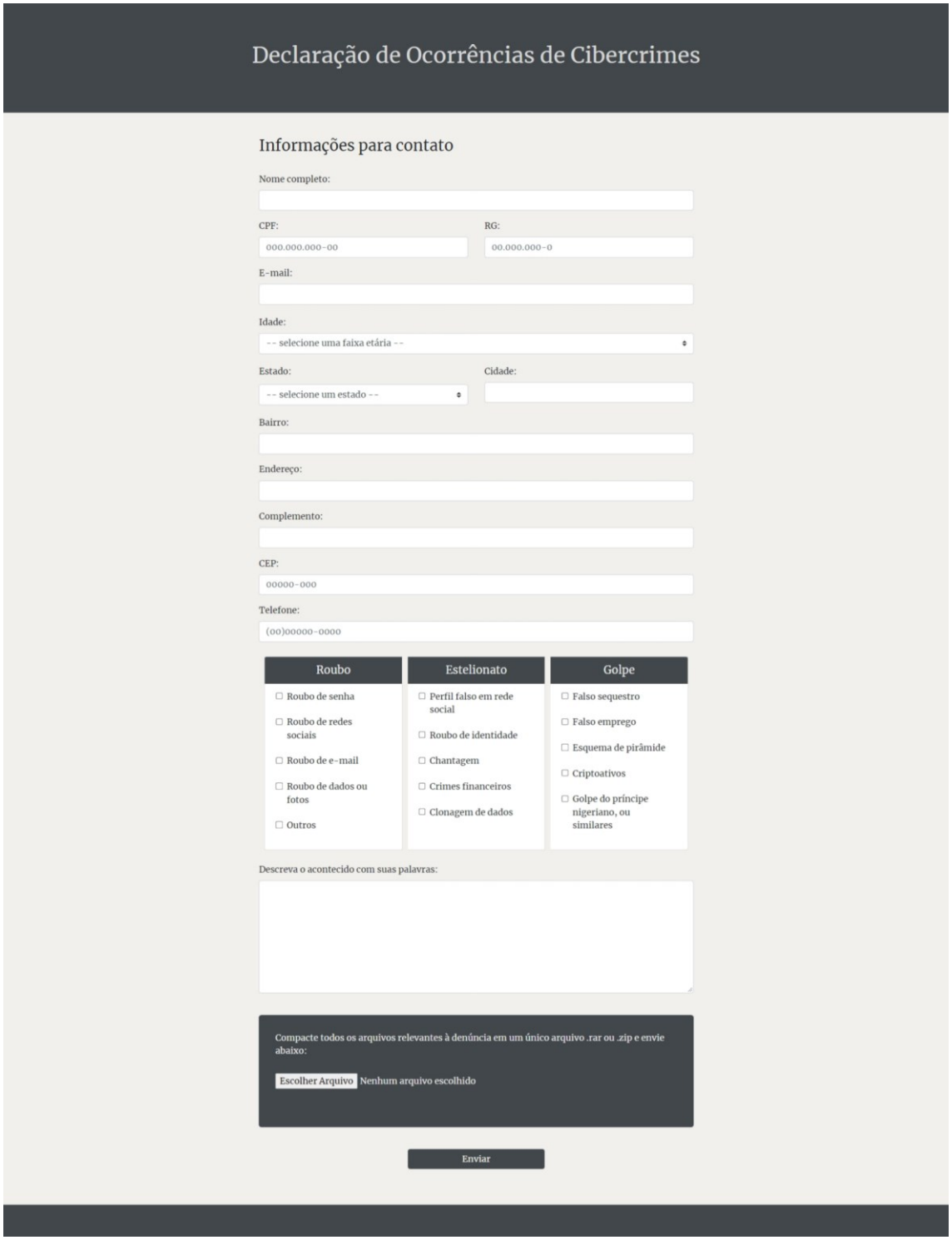
Figura 8 - Fluxo de Sistematização de Informação Sobre Cibercrimes



O resultado do processamento inicial para a vítima ou declarante, seria a geração de um protocolo para um atendimento presencial com indicação de procedimentos e documentos a serem levados para a unidade especializada em cibercrimes, quando convocada ou quando se apresentasse pessoalmente visando buscar informações.

O processo consistiria inicialmente na coleta de dados cadastrais e do evento criminoso de forma simples com linguagem "fácil e acessível", para permitir a contextualização de forma mais organizada e que poderá ser descrita na sequência do formulário na forma de texto livre, conforme apresentado na figura 9.

Figura 9 - Protótipo de Tela Cibercrimes



A finalização da declaração da ocorrência soma-se a possibilidade de anexar outras evidências digitais que a vítima ou declarante entenda como relevante ao caso, resultando em um documento de protocolo que seria enviado as secretarias de segurança e unidades especializadas em cibercrimes do país para o devido tratamento e análise.

Na camada seguinte, ocorre a recepção da ocorrência nas secretarias de segurança, onde esses dados seriam remetidos a unidade especializada para averiguação e ações cabíveis, além de terem papel potencialmente relevante nas ações de planejamento e apoio as políticas públicas quando consolidados por exemplo em trabalhos estatísticos, análises preditivas e de apoio a tomada de decisão.

Na recepção da delegacia designada pela secretaria de segurança, o policial teria a possibilidade de interagir com o cidadão para solicitar complementação das informações e ao resgatar os dados declarados no formulário teriam a disposição um pré-registro de ocorrência que aceleraria a parte inicial do procedimento policial frente a investigação de um crime.

Em uma visão mais ampla, a sistematização das ocorrências traria ferramental para levantamento de dados que indicariam por exemplo, se denúncias apresentadas possuem o mesmo padrão ou vitimologias em comum, algo que seria utilizado para a investigação e para o planejamento em ações de combate e repressão ao cibercrime, além de permitir a criação de indicadores estratégicos para o aprimoramento de políticas públicas referentes a cibercriminalidade.

Um exemplo de desdobramento da proposta de sistematização inicial das ocorrências que seria estruturante para as unidades de segurança pública, seria a criação de um serviço centralizado de cruzamento de dados de várias bases relacionadas a investigação policial, onde o foco seria um processo de produção de conhecimento em inteligência que consolidaria automaticamente relatórios analíticos em apoio a identificação de eventuais movimentações, tendências e desenvolvimentos por parte de cibercriminosos tendo por base não só os arquivos existentes mas também essa nova corpora de dados em cibercrimes.

Com relação ao repositório de dados da plataforma, vislumbra-se que para a efetivação dessa proposta, poderia ser criada uma base de dados tipo federada com um *schema* relacional capaz de armazenar os dados e metadados para atender geração de consultas, produção de relatórios e análises para todos os tipos de usuários das camadas da plataforma.

Cada unidade de força de segurança pública teria acesso a um nó do repositório, gerando com o passar do tempo uma fonte relevante de informações a serem estudadas em nível local, regional ou nacional. Esse repositório seria viável de ser correlacionado

com outros já existentes da área de segurança pública já que uma base de dados federada é relativamente simples de ser configurada e mantida ao longo do tempo e assim poderia suportar recursos analíticos tradicionais da área de Ciência de Dados apoiando as ações de produção de conhecimento para tomada de decisão por parte das autoridades e até mesmo da academia.

Finalizamos esse capítulo ressaltando que implementação tecnológica desse artefato foge ao escopo dessa dissertação, mas é possível inferir que a proposta envolvida seria de desenvolvimento, hospedagem e manutenção simplificados justamente por se basear basicamente em formulários digitais e repositórios concebidos para a captação de dados declarados, tendo como principal desafio suplantar a limitações de coordenação na distribuição entre os Estados e as suas respectivas unidades policiais especializadas em cibercrimes.

6 CONCLUSÃO

A quarta revolução industrial e os processos de transformação digital não apenas influenciam significativamente a maneira como vivemos e trabalhamos enquanto sociedade digital, mas também como os criminosos evoluem suas formas de atuação na busca de ilícitos.

Concluímos que a rápida evolução dos recursos tecnológicos trouxe inegáveis ganhos para a humanidade e isso se reflete em quase tudo que fazemos em nosso dia a dia, mas, no entanto, devido a sua incompletude agregou uma série de efeitos colaterais que merecem novos olhares da área de Humanidades Digitais, como por exemplo aprofundar os estudos sobre os aspectos sociais e éticos dos cibercrimes. Adicionalmente, verifica-se que a transformação digital se reflete assimetricamente nas organizações sociais, sendo elas lícitas ou não, e nesse contexto, também afeta os tipos e formatos de crimes.

É importante destacar que esta pesquisa foi totalmente concebida e conduzida durante o período da pandemia de COVID-19 e do conflito entre a Ucrânia e a Rússia e por esses motivos, ponderamos que as conclusões deste estudo devem ser consideradas dentro deste recorte temporal, com potencial de que possam ser extrapolados para outros períodos.

Dentro do que estudamos através da revisão sistemática da literatura e nas análises de dados reais originados pelas forças de segurança públicas no contexto da realidade brasileira, estima-se que o cibercrime cresceu nas mesmas proporções da adoção das novas tecnologias digitais, onde é possível estimar que existem lacunas referentes a criação e implementação de legislação penal especifica para tratar das condutas ilícitas praticadas no ambiente virtual, e que isso atuou como um catalisador e estimulador desses crimes, que em uma última instância, afeta potencialmente o papel do Estado na prevenção criminal e da persecução penal, levando ao descontrole e à impunidade.

Ainda com foco em legislação, merece atenção que o princípio da legalidade previsto no art. 5.º, XXXIX, da Constituição Federal enuncia que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Este princípio constitucional, corresponde ao art. 1º do Código Penal que possui dois princípios distintos: o da reserva legal e o da anterioridade. De tal modo, respectivamente, somente

a lei em sentido estrito pode criminalizar uma conduta (reserva legal), ao tempo em que, a lei penal deve ser anterior ao fato pretende incriminar (princípio da anterioridade) e esse princípio seria um dos fatores que dificultam o combate ao cibercrime, já que sem uma clara e inequívoca definição, um ato ilícito ou criminoso não pode ser corretamente tipificado e punido.

Verificamos que em um debate sobre interpretações dos fenômenos e atores envolvidos em segurança pública é importante promover um olhar amplo sobre vários campos do conhecimento ante a complexidade dos objetos de estudo, não se podendo prescindir dos conceitos, definições e princípios que regem as áreas correlatas e que, de um modo ou de outro, se ocupam do crime e seus efeitos jurídicos e sociais. Assim, o Direito, a Ciência Política, a Sociologia, a Criminologia e a Tecnologia da Informação entre outros são potenciais fontes de informações para a realização de estudos transdisciplinares em Humanidades Digitais e viabilizam uma melhor compreensão do fenômeno criminal identificado como cibercrime.

Nesta pesquisa foi identificado que o Estado brasileiro vem buscando reagir aos cibercrimes ao implementar políticas e mecanismos legais de persecução criminal especializada nesse tipo de delito. Tal reação é uma resposta contra o cibercriminoso que conta com a velocidade da evolução e adoção da tecnologia sem as devidas precauções de segurança em seu favor, com a falta de fronteiras físicas entre seus potenciais vítimas e até mesmo com uma falta de coordenação ou concentração eficiente das ações de combate e repressão por parte do Estado que lhe traz uma sensação de impunidade. O somatório desses fatores indica a necessidade de sistemas digitais mais resilientes e serve como indicador do potencial fragilidade e insegurança em que os cidadãos estão expostos e que no limite ainda se mostram como sendo o grande desafio a ser encarado pela sociedade e governo dentro desse contexto de resposta ao cibercrime.

Finalmente, informamos que dentre as contribuições acadêmicas complementares a esta pesquisa e ao texto da dissertação, obtivemos:

- A realização da Revisão Sistemática da Literatura (RSL) que apoiou a concepção e moldou a estratégia para coletar dados públicos das estruturas de segurança pública brasileira relacionados a cibercrimes.
- O aceite e apresentação do trabalho intitulado “Investigando os Cibercrimes no Brasil Através Da Perspectiva Das Humanidades Digitais”

no III Congresso Internacional em Humanidades Digitais (HDRio2023) realizado na Universidade Federal do Estado do Rio de Janeiro (UNIRIO) em abril de 2023

- O aceite e apresentação do trabalho intitulado “Cybercrime Analysis Keeping the Digital Humanities in Perspective” no 1st International Conference Data & Digital Humanities (DDHUM2023) realizado Universidade do Minho, Braga – Portugal em março de 2023.
- Por se tratar de um produto inovador houve o registro do protótipo da arquitetura junto ao Instituto Nacional de Propriedade Industrial INPI em 25/2/2023 sob o número BR 51 2023 000436 7 e com o nome de PRIC - Plataforma de Registro e Informação de Cibercrimes.
- A criação de um repositório público no GitHUB com todos os dados abertos desta pesquisa, que se encontra disponível em https://github.com/emersonbd/cibercrimes. O compartilhamento desses dados tem por objetivo permitir que outros pesquisadores do tema ou as estruturas de segurança pública tenham acesso gratuito ao material elaborado durante essa dissertação.

Como limitações desta pesquisa destacamos que os dados dos *datasets* poderiam ter menor granularidade, o que permitiria análises mais refinadas. Os dados fornecidos pelas estruturas de segurança pública não eram padronizados e não continham metadados ou descritores, isso poderia ter sido contornado se fosse franqueado a este pesquisador os acessos aos bancos de dados.

Como trabalhos futuros, é possível indicar que as implementações da plataforma poderiam ser baseadas no paradigma da Ciência Aberta, observando-se as peculiaridades da área de segurança pública e do estado brasileiro. Além disso, se sugere a agregação de novos módulos ou serviços de Inteligência Artificial. Estes poderiam pré-avaliar ou classificar as ocorrências e mesmo acompanhar mais dinamicamente as variações das novas ameaças e legislações sobre o tema.

Ao agregar recursos mais inteligentes se estima que eles permitirão uma compreensão melhorada sobre como esses crimes ocorrem, como são perpetuados, quais as técnicas utilizadas, quais as vulnerabilidades são exploradas, qual sua frequência, localização ou potenciais alvos. Os recursos inteligentes poderiam ser usados como

ferramental mais resiliente para produção de novos conhecimentos para que autoridades e legisladores aprimorem seus mecanismos de análise, predição, mitigação ou mesmo combate às ameaças digitais ou aos cibercrimes de forma mais efetiva e eficaz trazendo benefícios para os cidadãos e organizações.

7 REFERÊNCIAS

ACHA, F. R. (2019). **Crimes Digitais: Uma Necessária Releitura Do Direito Penal À Luz Das Novas Tecnologias**. LINKSCIENCEPLACE - Interdisciplinary Scientific Journal, v. 5, n. 6, p. 199–220.

Aiken, Mary & Mc Mahon, Ciarán & Haughton, Ciaran & O'Neill, Laura & O'Carroll, Edward. (2015). **A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online**. Contemporary Social Science. 11. 1-19. 10.1080/21582041.2015.1117648.

AUTORIA COLETIVA. **Manifesto das Humanidades Digitais**. THATCamp (2010). Disponível em: https://humanidadesdigitais.files.wordpress.com/2011/10/poster_manifesto_hd_portugues.pdf. Acesso em: 10 out. 2021

BAUMAN. Z. 2000. **Globalização: as Consequências Humanas**. Rio de Janeiro, Zahar.

BERRY, DAVID M. **Understanding Digital Humanities**. [S. l.]: Palgrave Macmillan, 2012. 318 p. ISBN 978-0-230-37193-4. E-book

BEZERRA et al. (2021). **Cibercrime e cibersegurança - Desafios da IV revolução industrial.** Disponível em: http://www.api.org.br/conferences/index.php/ISTI2021/ISTI2020/paper/viewFile/1393/695. Acesso em 15/11/2021

BLATT, Erick Ferreira. **Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal**. In: BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso (Org.). **Combate ao crime cibernético: doutrina e prática (a visão do Delegado de Polícia)**. 1. ed. Rio de Janeiro: Mallet Editora, 2016. p. 67-86.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: senado Federal, 1988.

BRYNJOLFSON, E.; McAFEE, A. (2014). **The second machine age: work, progress and prosperity in a time of brilliant technologies**. New York: W. W. Norton & Company, Inc.

CAPEZ, Fernando. **Curso de Direito Penal** – Volume 2 – Parte Especial: 12. ed. São Paulo: Editora Saraiva, 2012

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 25 out. 2021.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 2011.

CASTELLS, Manuel. **Fim de milênio**. SÃO PAULO: PAZ E TERRA, V. 3, 1999

CAVALCANTE, Waldek Fachinelli. **Crimes cibernéticos: noções básicas de investigação e ameaças na internet Conteudo Juridico**, Brasilia-DF: 16 out 2015, 04:15. Disponivel em: https://conteudojuridico.com.br/consulta/Artigos/45322/crimes-ciberneticos-nocoes-basicas-de-investigacao-e-ameacas-na-internet. Acesso em: 27 fev 2022.

JÚNIOR, J. C. A. (2019). **Cibercrime: Um Estudo Acerca Do Conceito De Crimes Informáticos**. Revista Eletrônica da Faculdade de Direito de Franca, v. 14, n. 2, p. 341–351.

COSTA, M. A. R. **Crimes de informática**. Disponível em: <https://jus.com.br/artigos/1826/crimes-de-informatica >. Acesso em: 10 out. 2021.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal**. – Brasília: MPF, 2018. 275 p. – (Coletânea de artigos; v. 3)

BRYNJOLFSSON, Erik; MCAFEE, Andrew**. The second machine age: work, progress, and prosperity in a time of brilliant technologies**. London. UK; New York, USA: W. W. Norton & Company, 2014

DABI-SCHWEBEL (2018). **Transformation digitale (ou numérique).** Disponível em:https://www.1min30.com/dictionnaire-du-web/transformation-digitale-numerique. Acesso em: 12 set. 2021

DE LIMA FILHO, P. R. A. **O DIREITO PENAL NA QUARTA REVOLUÇÃO INDUSTRIAL: A expansão razoável frente aos crimes cibernéticos**. Delictae Revista de Estudos Interdisciplinares sobre o Delito, [S. l.], v. 6, n. 10, 2021. DOI: 10.24861/25265180.v6i10.150. Disponível em: https://www.delictae.com.br/index.php/revista/article/view/150. Acesso em: 28 nov. 2021.

DI NICOLA, A. **Towards digital organized crime and digital sociology of organized crime**. Trends Organ Crim (2022). https://doi.org/10.1007/s12117-022-09457-y

EISENHARDT, K. M. **Building Theories from Case Study Research. Academy of Management Review**, v. 14, n. 4, p. 532-550, 1989.

FEDERAL BUREAU OF INVESTIGATION. **Internet Crime Report. 2020.** Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. Acesso em: 20 set. 2021.

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

GIDDENS, A. (2001). **Em defesa da sociologia**. Unesp.

GIDDENS, A. (2001). **Sociology**. ISBN 10: 0745623115 / ISBN 13: 9780745623115 Published by Polity Press, United Kingdom, Oxford, 2001

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**. 5 ed. São Paulo: Atlas, 2007.

GODOY, A. S. **Introdução a pesquisa qualitativa e suas possibilidades**. Revista de Administração de Empresas. São Paulo, v. 35, n. 2, p. 57-63, Mar./Abr. 1995

GRECO, Rogério. **Curso de Direito Penal – parte geral**. 16. ed. Rio de Janeiro: Editora Impetus, 2014. v. I.

GRECO. Rogério. **Código Penal Comentado**. 10ª edição. Rio de Janeiro: Editora Impetus, 2016.

HERMANN, M.; PENTEK, T.; OTTO, B. **Design principles for industrie 4.0 scenarios. In: System Sciences (HICSS)**, 2016 49th Hawaii International Conference on. IEEE, 2016. p. 3928-3937.

HONN, J. **A guide to digital humanities: values & methods**. 2014. Disponível em: https:// https://researchguides.wcu.edu/digitalhumanities/toolsmethods. Acesso em: 10 out. 2021.

KIRSCHENBAUM, M. (2010). **Digital Humanities and what‟s It Doing In English Departments**. ADE Bulletin 150 55–61.

KITCHENHAM, B.; CHARTERS, S. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. EBSE Technical Report EBSE-2007-01. Disponível em: https://bit.ly/3o3EGsR

KRAPP, Peter. **Comunicação secreta e história da criptologia: um desafio para as Humanidades Digitais**. TECCOGS – Revista Digital de Tecnologias Cognitivas, n. 21, jan./jun. 2020, p. 146-165. Tradução de Eduardo Harry Luersen.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no cyberespaço**. – Feira de Santana: Universidade Estadual de Feira de Santana, 2017.

LEINER, Barry M., Vinton G. CERF, David D. CLARK, Robert E. KAHN, Leonard KLEINROCK, Daniel C. LYNCH, Jon POSTEL, Lawrence G. ROBERTS e Stephen S. WOLFF (1997). **The past and future history of the Internet**. Communications of the ACM, 40 (2): 102-108.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1997

LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. 5 C**ibercrimes e a legislação brasileira**: LORENZO, Larissa Papandreus. SCARAVELLI, Gabriela Piva. **Diálogos e Interfaces do Direito-FAG**, v. 4, n. 1, p. 104-122, 2021.

LUPTON, D. **Sociologia digital**. Londres: Routledge; 2015.

MARAS, Marie-Helen. (2014). **Computer Forensics: Cybercriminals, Laws, and Evidence** Jones and Bartlett; Chapter 12.

MCCARTY, Willard. **The big picture: where Digital Humanities has been & where you might take it**. Krasnoyarsk: Siberian Federal University, 25 de setembro de 2015 (Workshop Digital Humanities Conference). Disponível em: mccarty.org.uk. Acesso em: 17 jan. 2022.

MELLO, Janaina. (2021). **Cibersegurança em gestão de museus no século 21 nas Humanidades Digitais** (Boletim do Tempo Presente, v.10, n.7, 2021, p.12-28). 10. 12-28.

MELZER, N. **Cyber Warfare and International Law**. Genebra, Unidir Resources: 2011. Disponível em: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law382.pdf. Acesso em: 17 set. 2021

MINAYO, M. C. S. **Pesquisa Social: teoria, método e criatividade**. Petrópolis: Vozes,1994.

MOURA, M. A. (2019). **Ciência da Informação e Humanidades Digitais: mediações, agência e compartilhamento de saberes.** ***Perspectivas Em Ciência Da Informação***, *24*(spe), 57–69. https://doi.org/10.1590/1981-5344/3893. Acesso em: 1 out. 2021

NETO, M. F. AND GUIMARAES, J. A. C. (2003). **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Revista CEJ, 7(20). ISSN 2179-9857.

NOGUEIRA, Sandro D.'Amato. **Crimes de informática**. Leme: Editora BH, 2009.

NYE, JOSEPH S. Jr. **Bound to Lead: The Changing Nature of American Power**. New York: Basic Books, 1991b.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

PINHEIRO, R. C. **Os cybercrimes na esfera jurídica brasileira**. Disponível em: <http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira>. Acesso em: 20 out. 2021.

RIFKIN, J. (2011) **The third industrial revolution: how lateral power is transforming energy, the economy and the world**. New York: St. Martin's Griffin

SAUVAGE (2018) D**éfinition: transformation digitale en 2021 et ses enjeux + exemples**. Disponível em: <https://www.inboundvalue.com/blog/que-signifie-la-transformation-digitale-en-2000-mots>. Acesso em: 15/11/2021

SCHUMPETER, J. (1942) **Capitalismo, socialismo e democracia**. Rio de Janeiro: Zahar Editores, 1984.

SCHWAB, K. **A quarta revolução industrial**. São Paulo: Edipro, 2018.

SELLTIZ, C.; JAHODA, M.; DEUTSCH, M. **Métodos de Pesquisa nas Relações Sociais**. São Paulo: EDUSP, 1974.

SIDDAWAY, A. P.; WOOD, A. M.; HEDGES, L. V. **How to do a systematic review: a best practice guide for conducting and reporting narrative reviews, meta-analyses, and metasyntheses.** Annual Review of Psychology, v. 70, n. 1, p. 747–770, 2019.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo. Revista e atualizada (até a Emenda Constitucional n. 48, de 10.08.2005)**. 25. Ed. São Paulo: Malheiros, 2005.

SILVA, E. LUCIA; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4 ed. Florianópolis: UFSC, 2005.

SILVA, Ângelo Roberto Ilha da et al. **Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas**, Porto Alegre, Livraria do Advogado, 2018,2ª ed.,p. 90.

SIEPIERSKI, A. L. . **CRIMES CIBERNÉTICOS: A POSSIBILIDADE DE RELATIVIZAÇÃO DO ANONIMATO**. Portal de Trabalhos Acadêmicos, [S. l.], v.3, n.2, 2022. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/2204. Acesso em: 26 jun. 2022.

SOUZA, Michelle Licia. **Crimes digitais: quais são e quais leis existem. In: Aspectos Humanos e Sociais na Computação**. [S. l.], 11 set. 2019. Disponível em: http://link.medium.com/fp2CszvSheb. Acesso em: 14 maio 2021.

Suler, J. **Cyberpsychology as interdisciplinary, applied, and experiential**. Disponível em: http://cypsy.com/News/Cyberpsychology_as_Interdisciplinary. Acesso em:12 setembro 2021.

UNOSDC. United Nations Office on Drugs and Crime. **Comprehensive Study on Cybercrime**. 2013. Disponível em https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, Acesso em 20/05/2022.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 5. ed. São Paulo: Atlas, 2004.

VELLOZO, Jean Pablo Barbosa. **Crimes informáticos e criminalidade contemporânea**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 20, n. 4515, 11 nov. 2015. Disponível em: https://jus.com.br/artigos/44400. Acesso em: 6 jan. 2022.

VERHOEF, P., BROEKHUIZEN, T., BART, Y., BHATTACHARYA, A., QI-DONG, J., FABIAN, N. AND HAENLEI, M. (2019). **Digital transformation: A multidisciplinary reflection and research agenda**. Journal of Business Research, in press.

VENKATRAMAN V. **A matriz digital: novas regras para transformação de negócios por meio da tecnologia** Greystone Books, Vancouver, Canadá (2017)

VERHOEF et al., (2021). **Digital transformation: A multidisciplinary reflection and research agenda, Journal of Business Research**, Volume 122, 2021,Pages 889-901,

YIN RK. **Estudo de caso: planejamento e métodos**. 4ª ed. Porto Alegre (RS): Bookman; 2010.

ZAOUI, F.; SOUISSI, N. **Roadmap for digital transformation: A literature review**. *Procedia Comput. Sci.* 2020, *175*, 621–628.

APÊNDICE – QUESTIONÁRIO ENVIADO AS UNIDADES DE PESQUISA PARA COLETA DE DADOS

A) Texto utilizado na coleta dos dados junto aos órgãos de segurança pública:

Antecipadamente, agradeço o tempo e a disponibilidade em receber meu pedido de ajuda. Sou aluno do curso de mestrado em Humanidades Digitais na Universidade Federal Rural do RJ e minha área de pesquisa se concentra em métodos computacionais em políticas públicas e, em específico, busco informações sobre cibercrimes e crimes digitais ou virtuais. Basicamente meu contato é por necessitar de mais informações para entender essa tipificação de crimes combatidos pelo sistema de segurança pública e seus desafios.

Minha proposta é trazer a visão do agente de segurança pública e os desafios que o mesmo enfrenta na investigação e no combate aos crimes digitais/cibernéticos, dissertando inclusive sobre a questão da legislação envolvida e suas eventuais limitações.

Abaixo eu tomo a liberdade de apresentar uma série de perguntas que podem vir a me ajudar nesse estágio inicial de levantamento de informações que imagino possa ser respondida por vocês ou que possam me indicar a quem devo submeter esse desafio.

Sobre unidades especializadas no combate aos crimes cibernéticos:

1. Qual a história de criação da unidade?
2. Qual a formação e composição dos seus quadros funcionais? Existem apenas profissionais da segurança pública ou são contratados consultores?
3. Qual a infraestrutura, tecnologias e equipamentos disponíveis?
4. Quais os treinamentos (em tecnologia) necessários e/ou disponíveis para que sejam parte da unidade?
5. A unidade tem algum tipo de sistema “principal” para combate ao crime?
6. Existem ferramentas que tenham sido desenvolvidas internamente? Quem faz o apoio e suporte de TI?
7. Existe um perfil profissional específico ou desejado para se trabalhar numa unidade desse tipo?

8. Qual o número de registros de ocorrência por mês? Quantas são lavradas na própria unidade? Quantas são online? É possível ter uma ocorrência oriunda de outras unidades da estrutura de segurança pública?
9. Existe uma estatística sobre o tempo médio de uma investigação considerando a abertura de uma ocorrência e sua conclusão?
10. Existem trabalhos ou mapas de análise estatística do tipo "Mancha Criminal"? Talvez algum tipo de abordagem por tipo de crime e frequência de determinados tipos de ocorrência p.ex.?
11. Dentre os vários crimes elucidados certamente existem aqueles de maior destaque e que viraram casos de estudo e análise. Poderiam ser citados e resumidas algumas dessas ações?
12. A unidade faz ações educacionais ou patrocina ações de prevenção ou monitoração de crimes digitais ou cibercrimes?
13. A unidade faz consultoria para outros órgãos de governo ou da iniciativa privada na parte de segurança da informação ou na parte de tecnologia de prevenção a crimes digitais?

<u>Sobre Crimes Digitais:</u>

1. Existem dados (Bancos de dados ou microdados) que possam ser analisados para fins estatísticos? Como posso solicitar o acesso?
2. Quais são os Modus Operandi mais comuns? Quais os crimes mais denunciados?
3. Qual o típico perfil do criminoso?
4. Existem indicativos de organizações criminosas "tradicionais" migrando para atuar nesse tipo de crime?
5. Existe um levantamento sobre o perfil das vítimas?
6. Existe uma tabela com a tipificação dos crimes?
7. A tipificação (tipificação criminal de delitos informáticos –Lei nº 12.737, de 30 de novembro de 2012) é suficiente para os casos ou é necessário fazer também um trabalho de analogia com os outros tipos de crime previstos no código penal para a devida instrução processual e apresentação de denúncia?
8. Como se combatem as quadrilhas virtuais e como fica a tipificação criminal frente aos diferentes tipos de ações e responsabilidades? Existem casos que possam ser analisados (Por exemplo: Quem faz o vírus, quem faz o site ou

hospeda o site para golpes, quem compartilha, quem usa a máquina infectada, quem recebe e repassa o ganho ilícito)?

9. Como é tratada a divulgação de crimes realizados para recrutamento por facções ou por demonstração de força?
10. Qual é o protocolo de combate a divulgação, venda e entrega de armas, drogas e entorpecentes? Existem casos que possam ser analisados?

Sobre os aspectos jurídicos nos crimes via web:

1. Como é resolvida ou tratada a questão da jurisdição em investigações de crimes que são ou podem ser executados em vários locais pelo mundo (Estado/Brasil/Mundo)?
2. Existem acordos de cooperação policial no Brasil para esse tipo de crime? Qual o protocolo adotado para se acionar outras forças da área de segurança?
3. Caso o Brasil venha a aderir, qual a expectativa sobre a aplicação da "Convenção de Budapeste" no referente ao combate ao cibercrime e ao crime digital?
4. A lei 13.964/2019 (Lei Anticrime), que possibilitou a infiltração virtual de agentes policiais para obter dados de conexão e cadastrais de membros de organizações envolvidas com crimes cibernéticos já foi usada em algum caso? Podem ser resumidas para ilustração?
5. Imaginando que a unidade tem participação na Estratégia Nacional de Segurança Cibernética (batizada de "E-Ciber" por meio do decreto 10.222), já existem ações efetivas que possam ser destacadas?
6. Entre os casos de sucesso, existem histórias de ações conjuntas com outras unidades policiais do BRASIL ou do mundo em ações de combate ao cibercrime e crime digital?
7. Tendo as empresas privadas de tecnologia como a Google e Microsoft entre outras, além de ONGs (SaferNet p.ex.) exercido um papel expressivo no combate e sobretudo na denúncia de crimes pela internet, como é a cooperação com a iniciativa privada? Existem protocolos definidos?
8. Existem eventos do tipo "Lei 9099" (Baixo Potencial Ofensivo) que podem ser ou foram resolvidos por Termos Circunstanciados com o escopo dos crimes digitais?