UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Gabriel Zeitoum dos Santos

Observatório de cibercrimes: prototipação e desenvolvimento do painel web interativo

Uberlândia, Brasil

2025

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Gabriel Zeitoum dos Santos

Observatório de cibercrimes: prototipação e desenvolvimento do painel web interativo

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Rodrigo Sanches Miani

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Ciência da Computação

Uberlândia, Brasil

2025

Gabriel Zeitoum dos Santos

Observatório de cibercrimes: prototipação e desenvolvimento do painel web interativo

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Ciência da Computação.

Prof. Dr. Rodrigo Sanches Miani
Orientador

Prof. Dr. Pedro Franklin Cardoso Silva

Uberlândia, Brasil
2025

Resumo

O crescimento de delitos praticados no ambiente digital tem pressionado o poder público e a academia a desenvolver ferramentas que tornem os dados de cibercrimes mais acessíveis e interpretáveis. Este trabalho apresenta o desenvolvimento de um painel web interativo para análise de decisões judiciais classificadas como cibercrimes no Estado de São Paulo. O sistema consome uma API pública de processos, filtra apenas registros marcados como cibercrimes e realiza o tratamento dos dados (padronização de datas, normalização de nomes de municípios e agregações por ano, assunto e distrito). A interface, construída em *Angular* e *ECharts*, disponibiliza um mapa coroplético (*heatmap*) dos municípios paulistas, gráficos de barras por ano, gráfico de pizza por assunto, ranking de temas e uma tabela de processos com busca e paginação. As faixas do mapa são calculadas dinamicamente: quando o máximo de casos no mapa for ≤ 4 utiliza-se degraus inteiros (1, 2, 3, 4) e, em cenários mais volumosos, quebras por percentis (25%, 50% e 75%), evitando sobreposição e reforçando a legibilidade. O painel é responsivo, oferece modo claro/escuro e um seletor de estado preparado para futuras bases. Resultados mostram que a solução permite explorar padrões temporais e espaciais com baixo tempo de resposta, preservando a privacidade por meio de dados públicos agregados. O trabalho contribui com um *pipeline* replicável de geovisualização de dados judiciais e um protótipo funcional, abrindo caminho para ampliar a cobertura para outros estados e fontes.

Palavras-chave: cibercrime; visualização de dados; geovisualização; ECharts; Angular; decisões judiciais; mapa coroplético.

Abstract

The growth of crimes committed in the digital environment has pressured public authorities and academia to develop tools that make cybercrime data more accessible and interpretable. This work presents the development of an interactive web dashboard for analyzing judicial decisions classified as cybercrimes in the State of São Paulo. The system consumes a public API of legal cases, filters only records marked as cybercrimes, and performs data processing (date standardization, normalization of municipality names, and aggregations by year, subject, and district). The interface, built with Angular and ECharts, provides a choropleth map (heatmap) of São Paulo municipalities, bar charts by year, a pie chart by subject, a ranking of topics, and a searchable, paginated table of cases. Map ranges are calculated dynamically: when the maximum number of cases on the map is ≤ 4, integer steps (1, 2, 3, 4) are used, and in larger scenarios, breakpoints by percentiles (25%, 50%, and 75%) are applied, avoiding overlap and reinforcing readability. The dashboard is responsive, offers light/dark mode, and includes a state selector prepared for future datasets. Results show that the solution enables the exploration of temporal and spatial patterns with low response time, preserving privacy through aggregated public data. This work contributes a replicable pipeline for geovisualization of judicial data and a functional prototype, paving the way to extend coverage to other states and data sources.

Keywords: cybercrime; data visualization; geovisualization; ECharts; Angular; court decisions; choropleth map.

Lista de ilustrações

Sumário

1 Introdução

Com a digitalização de diversos aspectos da vida diária e o surgimento da Internet, é imprescindível a necessidade do desenvolvimento de observatórios de cibercrime para apoio a análise e visualização de dados de segurança para ir contra as novas oportunidades de práticas ilícitas. Através de tais análises, é possível visualizar com clareza através de demonstrações gráficas de quais atos ilícitos cibernéticos ocorreram com suas determinadas frequências. Tais crimes podem variar, desde fraudes financeiras até invasões de sistemas governamentais e espionagem cibernética.

É de suma importância um observatório voltado à análise de crimes cibernéticos na sociedade contemporânea. A partir de 2020, com o início da pandemia, muitas empresas foram obrigadas a acelerar seus processos de digitalização, muitas vezes sem a devida implementação de medidas de segurança adequadas. Esse cenário resultou em um aumento significativo de fraudes, crimes e ataques cibernéticos de diversas naturezas (BARBOSA et al., 2021). Além disso, há registros de casos emblemáticos, como o ataque a instituições financeiras em que hackers roubaram mais de 1 bilhão de dólares em ataques que começaram em 2013 e acontecem até os dias de hoje, evidenciando a magnitude do problema no cenário global (BRASIL, 2015). Na academia, o estudo desses crimes é crucial para o desenvolvimento de novas ferramentas de mitigação e políticas de segurança, além de fortalecer a base teórica necessária para uma legislação mais eficaz.

Há diversos trabalhos que contribuem para a análise de crimes cibernéticos. Alguns empregam ferramentas específicas para a coleta de dados de segurança. Por exemplo, (LABAKI, 2023) apresenta uma solução promissora para otimizar e acelerar a coleta de informações em fóruns especializados em segurança cibernética por meio de web scrapers. Da mesma forma, (COSTA, 2017) destaca, em seus estudos, a importância de analisar vulnerabilidades em portais de governos eletrônicos, evidenciando como falhas nesses sistemas podem comprometer tanto a integridade dos dados quanto a segurança dos cidadãos.

O código do *front-end* foi desenvolvido utilizando *HTML*, *CSS* e *TypeScript* (JavaScript), tendo o *Angular* como *framework* para a construção da interface. A visualização de dados foi implementada com a biblioteca *ECharts*, integrada ao Angular, por oferecer gráficos interativos de alto desempenho (mapas, barras, pizza, entre outros) e boa capacidade de customização. O *front-end* funciona como um microsserviço do tipo *SPA* (*Single Page Application*) que se comunica com o microsserviço de *back-end* por meio de uma API REST, responsável por prover os dados (com paginação, ordenação e busca) a partir da base de dados.

1.1 O observatório proposto e o ecossistema de observatórios

O presente trabalho se insere no conceito de observatório enquanto instrumento de produção e compartilhamento de conhecimento para apoiar a tomada de decisão. Em termos gerais, observatórios são espaços organizados — frequentemente em ambientes acadêmicos ou governamentais — dedicados a reunir informações, avaliar sua relevância, estruturar os dados com coerência e comunicar os achados de forma clara ((UFSC), 2019; MARCIAL, 2009). Na literatura, discute-se que a noção de observatório abrange um conjunto de práticas para identificar, acompanhar e analisar fenômenos (em geral sociais), produzindo evidências úteis para políticas públicas e gestão ((UFSC), 2019).

No Brasil, encontram-se iniciativas variadas de observatórios — como o Observatório da Saúde Pública (Umane, 2021), o Observatório ACATE de Empresas de Tecnologia (ACATE, 2025) e o Observatório da Fiocruz (Fundação Oswaldo Cruz (Fiocruz), 2016) — que ilustram abordagens temáticas distintas e diferentes arranjos institucionais para monitoramento contínuo e suporte à decisão.

O observatório proposto tem foco na visualização e análise de decisões judiciais marcadas como cibercrimes no Estado de São Paulo. A plataforma opera como um painel público que coleta, recorta, agrega e explora tais dados, a fim de transformá-los em uma visualização gráfica consistente e de fácil interpretação.

1.2 Objetivos

1.2.1 Objetivo geral

Desenvolver e avaliar um painel web interativo para análise e visualização de dados públicos de decisões judiciais classificadas como cibercrimes no Estado de São Paulo, permitindo exploração temporal e espacial por meio de mapa coroplético e gráficos complementares, com foco em legibilidade, responsividade, usabilidade e extensibilidade para outros estados.

1.2.2 Objetivos específicos

1. Levantar requisitos e definir escopo, público-alvo e métricas de sucesso do painel.
2. Projetar a arquitetura do *frontend* em Angular e os serviços de dados.
3. Integrar a API pública, aplicar filtros essenciais para verificação de cibercrimes (`isCyberCrime = true`) e normalizar dados (datas, distritos e nomes de municípios compatíveis com o GeoJSON de SP[1]).

4. Construir as visualizações principais: mapa coroplético, séries anuais e distribuição por assunto, além de ranking de temas.

5. Implementar interação e navegação: seletores (ano e estado), busca, paginação e tabela de processos.

6. Garantir responsividade (layout fluido e adaptação para *mobile*, sem rolagem horizontal) e acessibilidade, assegurando boa leitura em modo claro/escuro.

[1]Fonte do GeoJSON (municípios de SP) utilizado no projeto: <https://github.com/tbrugz/geodata-br/blob/master/geojson/geojs-35-mun.json>

2 Fundamentação Teórica

Este capítulo tem por objetivo apresentar os fundamentos que sustentam o desenvolvimento do painel proposto. A Seção 2.1 apresenta uma contextualização sobre os crimes cibernéticos, abordando suas definições, evolução histórica, tipologias e o arcabouço jurídico brasileiro. Já a Seção 2.2 descreve as tecnologias utilizadas no desenvolvimento do painel, destacando linguagens, frameworks, bibliotecas e ferramentas de apoio. A Seção 2.3 discute o papel dos dashboards na análise e visualização de dados, trazendo fundamentos teóricos e relacionando-os à construção do painel proposto.

2.1 Crimes Cibernéticos

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) foi pioneira ao definir cibercrime em 1983 como “qualquer conduta ilegal, não ética ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados”. Porém, esse conceito admite interpretações variadas, como a de Daoun e Lima (2020), que caracteriza cibercrime como “ação típica, antijurídica e culpável cometida contra ou pela utilização de sistemas informáticos”. Assim, embora existam definições distintas, a essência permanece: o uso de tecnologia para ações que violam normas legais.

Os Crimes cibernéticos têm se tornado cada vez mais frequentes, apesar de já existirem registros de delitos cibernéticos desde a década de 1960. Naquele período, os primeiros casos documentados na imprensa e na literatura científica dos Estados Unidos envolveram atividades como sabotagens e espionagem realizadas por meio de computadores. A partir de 1980, as atividades ilícitas evoluíram, abrangendo crimes mais graves, como manipulação de dados bancários e disseminação de pornografia infantil (BARROS, 2006).

Através do crescimento da Internet e da conectividade, os crimes cibernéticos se tornaram uma ameaça global com ataques de grande escala, mudando o foco para roubo de dados financeiros, espionagem cibernética e ataques a infraestruturas críticas (LACERDA, 2023). No Brasil, possui-se uma estrutura jurídica sólida para lidar com cibercrimes, através de leis, como a Lei 12.965/2014, o "Marco Civil da Internet", a qual estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL, 2014) e a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann", a qual tipifica crimes cibernéticos, especialmente relacionados à invasão de dispositivos eletrônicos e à divulgação não autorizada de dados pessoais (BRASIL, 2012).

2.1.1 Tipologia dos crimes cibernéticos

Os processos utilizados neste trabalho vêm etiquetados por *assunto* (`subject`) no provimento judicial e, após o filtro `isCyberCrime = true` (verificação de cibercrimes), observam-se alguns grupos recorrentes. A tipologia abaixo não exaure o tema, mas descreve, de forma operacional, algumas das classes mais presentes no conjunto analisado e como elas se manifestam no ambiente digital.

2.1.1.1 Bancários.

Reúne casos em que instituições financeiras, canais de atendimento ou meios de pagamento são explorados de forma fraudulenta. No contexto digital, a dinâmica mais frequente envolve *phishing* (páginas ou mensagens que imitam bancos), engenharia social por chamadas falsas, sequestro de contas após comprometimento de credenciais, golpes relacionados a *internet/mobile banking* e fraudes com PIX ou boletos.

2.1.1.2 Falsificação de documento público.

Abrange condutas voltadas à criação ou alteração indevida de documentos públicos (físicos ou digitais) — por exemplo, RG/CNH digitais, certidões, comunicações oficiais, atestados e documentos com QR Code/assinatura eletrônica. No ambiente cibernético, os documentos podem ser gerados ou manipulados por software de edição, uso indevido de certificados ou adulteração de metadados digitais, frequentemente com a finalidade de abrir contas, contratar serviços, obter crédito ou viabilizar outras fraudes on-line.

2.1.1.3 Furto qualificado.

Refere-se a tirar bem móvel de outra pessoa com agravantes previstos em lei. Costuma aparecer em situações "híbridas", quando o digital entra depois do furto: por exemplo, furtar um celular ou notebook, desbloquear o aparelho e usar aplicativos bancários; ou usar dispositivos e senhas furtados para movimentar dinheiro.

2.1.1.4 Estelionato.

É quando alguém engana outra pessoa para obter dinheiro ou vantagem, causando prejuízo (art. 171 do Código Penal). No ambiente digital, isso aparece com frequência em falsas "centrais de atendimento", anúncios de produtos que não existem em plataformas, golpes de investimento, clonagem de perfis e outras fraudes feitas por sites, aplicativos ou mensagens.

2.2 Tecnologias utilizadas para desenvolver o painel

2.2.1 JavaScript

Linguagem de programação essencial do *frontend* web, também utilizada em ambientes *backend*, *desktop* e *mobile*. No projeto, é o alicerce executado pelo navegador, sobre o qual o Angular e as bibliotecas operam.

2.2.2 TypeScript

Superset de JavaScript que adiciona tipagem estática e recursos de orientação a objetos (interfaces, tipos, classes abstratas). A tipagem forte ajuda a detectar erros em tempo de desenvolvimento, melhora o preenchimento automático e a manutenção do código.

2.2.3 Angular

Framework (conjunto de ferramentas e bibliotecas) baseado em componentes, mantido pelo Google, usado para construir aplicações web modernas. Esse tipo de aplicação costuma ser uma *SPA* (*Single Page Application*, ou seja, uma aplicação de página única, onde o usuário navega entre telas sem precisar recarregar toda a página, tornando a experiência mais rápida e fluida).

O Angular oferece recursos importantes como:

- **Vinculação de dados** (*data binding*): permite que as informações exibidas na tela estejam sempre sincronizadas com os dados internos da aplicação;
- **Injeção de dependências**: facilita a organização e o reaproveitamento de código;
- **Roteamento**: possibilita a navegação entre diferentes telas/páginas dentro da mesma aplicação;
- **Formulários reativos**: ajudam no tratamento e validação de dados digitados pelo usuário;
- **Ecossistema maduro**: possui grande comunidade, bibliotecas e suporte.

No projeto desenvolvido, foram utilizados:

- Componentes *standalone* (independentes, que não precisam ser declarados em módulos) para as páginas de Home, Processos, e também para o cabeçalho (*Header*) e rodapé (*Footer*);

- Serviço `CibercrimeService`, responsável por centralizar as chamadas à API e implementar lógicas de busca e paginação;
- *Angular CLI*, uma ferramenta de linha de comando que auxilia na criação da estrutura do projeto, na geração de código base e também no processo de execução e construção da aplicação.

2.2.4 ECharts e ngx-echarts

ECharts é uma biblioteca de visualização de dados de alto desempenho, que permite criar diferentes tipos de gráficos (como mapas, colunas, linhas e setores), além de oferecer recursos como *tooltips* (caixas de informação que aparecem ao passar o mouse em cima de um município do mapa, por exemplo), *zoom* e personalização por temas.

O pacote `ngx-echarts` integra o *ECharts* de forma nativa ao Angular, facilitando sua utilização dentro dos componentes da aplicação.

2.2.5 HTML e CSS

O HTML é a linguagem usada para estruturar o conteúdo das páginas, como cartões, tabelas e grades (*grid*). O CSS é responsável pela parte visual, definindo o estilo, cores, botões e tornando o *layout* (disposição dos elementos na tela) adaptável a diferentes tamanhos de dispositivos. Neste projeto, foram aplicadas boas práticas de organização do *layout* com uso de `grid` e *media queries* (regras que permitem ajustar a aparência para celulares e computadores).

2.2.6 Bootstrap / ng-bootstrap

O Bootstrap é um conjunto de ferramentas pronto para criar interfaces visuais mais bonitas e padronizadas. Já o ng-bootstrap é a versão adaptada especificamente para Angular, que facilita o uso desses componentes dentro da aplicação. Um exemplo é o módulo `NgbPaginationModule`, usado para criar a paginação (navegação entre páginas de dados). O uso dessas ferramentas ajuda a manter consistência visual e garante que a aplicação seja responsiva.

2.2.7 HTTP Client (Angular)

Módulo oficial do Angular para requisições *REST* (`HttpClient`), com configuração de cabeçalhos, parâmetros e *observables* (fluxos de dados que podem ser acompanhados em tempo real) tipados para respostas (`CibercrimeResponse`).

2.2.8 GeoJSON

Formato aberto para dados geoespaciais. O GeoJSON do estado de SP foi utilizado para desenhar o mapa e correlacionar municípios com as contagens agregadas.

2.2.9 Node.js e NPM

Ambiente de execução e gerenciador de pacotes utilizados pelo Angular CLI para desenvolvimento, *build* e instalação de dependências.

2.2.10 Git e GitHub

O Git é um sistema de controle de versão distribuído amplamente utilizado para gerenciar o histórico de alterações de projetos de software, permitindo trabalho colaborativo e seguro. O GitHub, por sua vez, é uma plataforma de hospedagem baseada em Git que facilita a colaboração, revisão de código e integração com ferramentas de desenvolvimento.

2.3 Dashboards

De acordo com Few (2006), um *dashboard*, também conhecido como painel, pode ser definido como uma tela que apresenta dados, presentes e históricos, e que auxilia no processo de tomada de decisão (YIGITBASIOGLU; VELCU, 2012). Dito isso, é de suma importância utilizá-los nas análises de crimes cibernéticos, visto que as mesmas são complexas e necessitam de entendimento adequado para que analistas de segurança consigam tirar conclusões e, além disso, pessoas leigas possam acessar e obter uma visão correta do tema para fins pessoais. Os *dashboards* têm como ideia principal traduzir dados complexos para os tomadores de decisão por meio da visualização — representações gráficas (muitas vezes interativas) de dados abstratos —, o que facilita a compreensão (CARD; MACKINLAY; SHNEIDERMAN, 1999).

A razão para se utilizar visualização em *dashboards* pode ser explicada pela teoria do ajuste cognitivo, que analisa a compatibilidade entre as habilidades de decisão do usuário, o formato de apresentação das informações e a tarefa em questão. Essa teoria oferece orientações valiosas sobre qual formato utilizar (VESSEY; GALLETTA, 1991). Por exemplo, gráficos são ideais para tarefas que exigem previsões e comparações, bem como análises multidimensionais. Por outro lado, tabelas são mais indicadas para tarefas simbólicas e para usuários com um perfil numérico, como contadores e analistas financeiros (VELCU-LAITINEN; YIGITBASIOGLU, 2012).

No contexto deste trabalho, o painel foi construído em Angular e ECharts, combinando visualizações complementares para cobrir dimensões espacial, temporal, temática

e tabular. A seguir, detalha-se o papel de cada componente.

Mapa coroplético (municípios de SP): Representa a dimensão espacial agregando o número de processos por município no ano selecionado. O mapa é registrado a partir de um GeoJSON estadual e recebe, para cada *feature* (município), a contagem de casos daquele ano. Os nomes dos municípios obtidos pelo banco de dados são normalizados (remoção de acentos, padronização de caixa, tratamento de hífens) para casar com os nomes do GeoJSON, reduzindo perdas de correspondência. O mapa possui faixas sem sobreposição, tratados da seguinte maneira: quando o máximo de casos no mapa é menor ou igual a 4, aplica-se degraus inteiros (1, 2, 3, $\geq$4); quando maior, adotam-se quebras aproximadas por percentis (25%, 50%, 75%). Ao passar o *mouse* em cima de cada município, é exibido seu nome e a quantidade de cibercrimes ocorridos no mesmo; o usuário pode dar zoom e navegar. A legenda mostrada no cartão é personalizada e reflete exatamente os cortes aplicados.

Barras por ano (Crimes ao longo do tempo): Sintetiza a dimensão temporal: soma-se, para cada ano presente na base filtrada (somente cibercrimes), o total de processos, exibindo-se uma barra com rótulo de valor no topo para leitura imediata. Esse gráfico favorece a identificação de tendências (crescimento/queda), pontos fora da curva e impactos de eventos externos. A paleta e os textos acompanham o tema (claro/escuro), garantindo contraste; o eixo X lista os anos disponíveis e o eixo Y mostra a quantidade agregada.

Pizza e ranking por assunto (Dimensão temática): Os dois gráficos abordam a composição por assunto (`subject`) no ano selecionado:

- **Pizza (distribuição)**: mostra a participação relativa de cada assunto. Para preservar legibilidade em grandes quantidades de dados, aplica-se um `Top N` configurável, o qual limita a quantidade de assuntos que irão aparecer no gráfico e agrega-se o restante na categoria "Outros". Rótulos percentuais têm limiar mínimo (2%), evitando poluição visual com fatias muito pequenas, enquandrando os assuntos com quantidade menor que 2% em "Outros"também.
- **Ranking (barras horizontais)**: lista os assuntos mais incidentes em ordem decrescente, com valores numéricos à direita. Esse arranjo lida melhor com rótulos textuais longos e permite comparar magnitudes de forma mais precisa.

Em conjunto, pizza e ranking permitem ver proporção e ordem de grandeza, complementando-se na interpretação.

Tabela pesquisável (consulta pontual): Oferece detalhamento tabular para buscas específicas. O usuário informa um termo livre (`search`) e aciona a busca por Enter ou pelo botão "Buscar". O *frontend* consolida todas as páginas retornadas pela API,

filtra por dados marcados como cibercrime e aplica paginação no cliente, o que evita páginas vazias. As colunas incluem campos operacionais para conferência e leitura do caso: `ID Processo` (`processCode`), `Classe` (`className`), `Assunto` (`subject`), `Relator` (`rapporteur`), `Comarca` (`district`), `Órgão Julgador` (`judgingBody`), `Data Julgamento` (`judgmentDate`), `Data Publicação` (`publishDate`), `Ementa` (`headnote`, com ver mais/ver menos) e `Link` (`pdfUrl`, quando disponível). Em telas pequenas, a tabela adota o padrão *stacked*, o qual "empilha"o conteúdo, preservando legibilidade.

Essa combinação cobre tarefas de visão geral e de aprofundamento, alinhando-se às recomendações clássicas de visualização para suporte à decisão.

3 Trabalhos Relacionados

Nesta seção serão discutidos trabalhos relacionados a desenvolvimento de sistemas para apoio a análise e visualização de crimes cibernéticos além de iniciativas de observatórios que inspiram o desenho e a comunicação dos dados.

(BRAR; KUMAR, 2018) investigaram e analisaram uma proposta de taxonomia para cibercrimes, com foco na crescente disponibilidade de dados pessoais na internet e nos crimes que exploram essas informações. Os autores apresentaram uma nova taxonomia baseada em princípios fundamentais da segurança cibernética — confidencialidade, integridade e disponibilidade — para a categorização de incidentes, utilizando pesquisas recentes e proeminentes como base. Essa abordagem visa proporcionar uma visão estruturada e sistemática dos diferentes tipos de cibercrimes. Além disso, o estudo destaca os desafios impostos pelos avanços tecnológicos, como os ataques mistos, nos quais cibercriminosos constantemente desenvolvem novas variantes de ciberataques já existentes, dificultando a implementação de uma solução única capaz de proteger completamente os dados e informações na internet. Essa classificação é particularmente relevante no contexto deste trabalho, pois oferece um modelo inicial para categorizar cibercrimes de forma clara e estruturada, facilitando a organização e a visualização dos dados no projeto em desenvolvimento.

Além disso, (BUCZAK; GUVEN, 2016) realizaram uma ampla revisão dos métodos de *Data Mining* e *Machine Learning* aplicados à detecção de intrusões em segurança cibernética. O estudo aborda tanto técnicas clássicas quanto modernas, como redes neurais, árvores de decisão, algoritmos baseados em clustering e métodos híbridos, detalhando suas vantagens e limitações em diferentes cenários. Os autores dissertam sobre como essas abordagens podem ser aplicadas e quais os melhores métodos — dependendo das características do problema cibernético — para a identificação de padrões de comportamento malicioso em grandes volumes de dados, para contribuir na antecipação e mitigação de ciberataques. A relevância desse trabalho para o projeto proposto está na possibilidade de integrar esses métodos em sistemas interativos de análise e visualização, o qual facilita a detecção de anomalias e melhora a tomada de decisão na segurança cibernética.

Ainda sobre o tema de detecção de anomalias, o artigo de (AKOGLU; TONG; KOUTRA, 2015) apresenta uma pesquisa abrangente sobre a detecção de anomalias baseada em grafos, discutindo como os grafos podem ser utilizados para identificar comportamentos atípicos em grandes conjuntos de dados. A pesquisa tem como objetivo principal oferecer uma visão abrangente e organizada dos métodos utilizados para detectar anomalias em dados que são representados por meio de grafos. O estudo analisa métodos como

(1) detecção de anomalias em grafos estáticos, (2) detecção de eventos em grafos dinâmicos e (3) detecção de fraudes em cenários do mundo real. Os dois primeiros grupos envolvem definições gerais de anomalias e as técnicas de detecção propostas, em grande parte, pela comunidade de mineração de dados. Já o terceiro grupo foca em técnicas especializadas, voltadas para fraudes específicas observadas em cenários reais, utilizando abordagens principalmente baseadas em aprendizado de máquina. Os principais resultados indicam que a análise de grafos é eficiente para detectar padrões incomuns de atividade em grandes volumes de dados interconectados. A relevância desse trabalho para o projeto proposto de análise e visualização de crimes cibernéticos está no uso dos grafos para representar relações entre eventos de segurança, permitindo a identificação de comportamentos suspeitos, o que facilita a visualização de tais anomalias em sistemas interativos.

3.1 Outras iniciativas de observatórios

O ecossistema brasileiro reúne iniciativas que ilustram diferentes recortes temáticos e arranjos institucionais de observatórios, reforçando seu papel como espaços de coleta, organização e comunicação de evidências ((UFSC), 2019; MARCIAL, 2009). Exemplos incluem:

- **Observatório de Inovação Social de Florianópolis** (Observatório de Inovação Social de Florianópolis, s.d.): plataforma para mapear, articular e acompanhar atores do ecossistema de inovação social da cidade, com foco em dados e narrativas que apoiam políticas locais. A Figura 1 apresenta a página inicial deste observatório, destacando sua interface de acesso público.

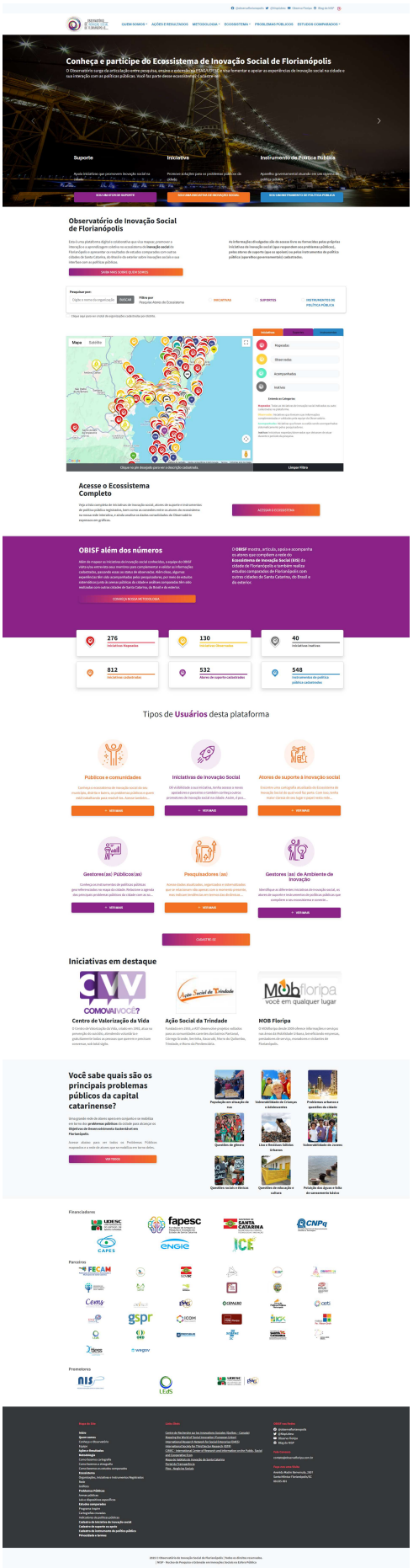

Figura 1 – Página inicial do Observatório de Inovação Social de Florianópolis.

- **Observatório ACATE de Empresas de Tecnologia** (ACATE, 2025): acompanha indicadores do setor de tecnologia em Santa Catarina, oferecendo séries e análises para posicionamento competitivo. A Figura 2 mostra a página inicial da plataforma, ilustrando sua proposta de comunicação de dados estratégicos.

Figura 2 – Página inicial do Observatório ACATE.

- **Observatório Blockchain RNP** (RNP, s.d.): dedicado ao levantamento sistemático de iniciativas acadêmicas, governamentais e empresariais que empregam blockchain no Brasil, com o objetivo de oferecer uma visão abrangente do ritmo de expansão e da diversidade de usos da tecnologia no país. Sua página inicial é exibida na Figura 3, evidenciando o esforço de centralização das informações sobre o tema.

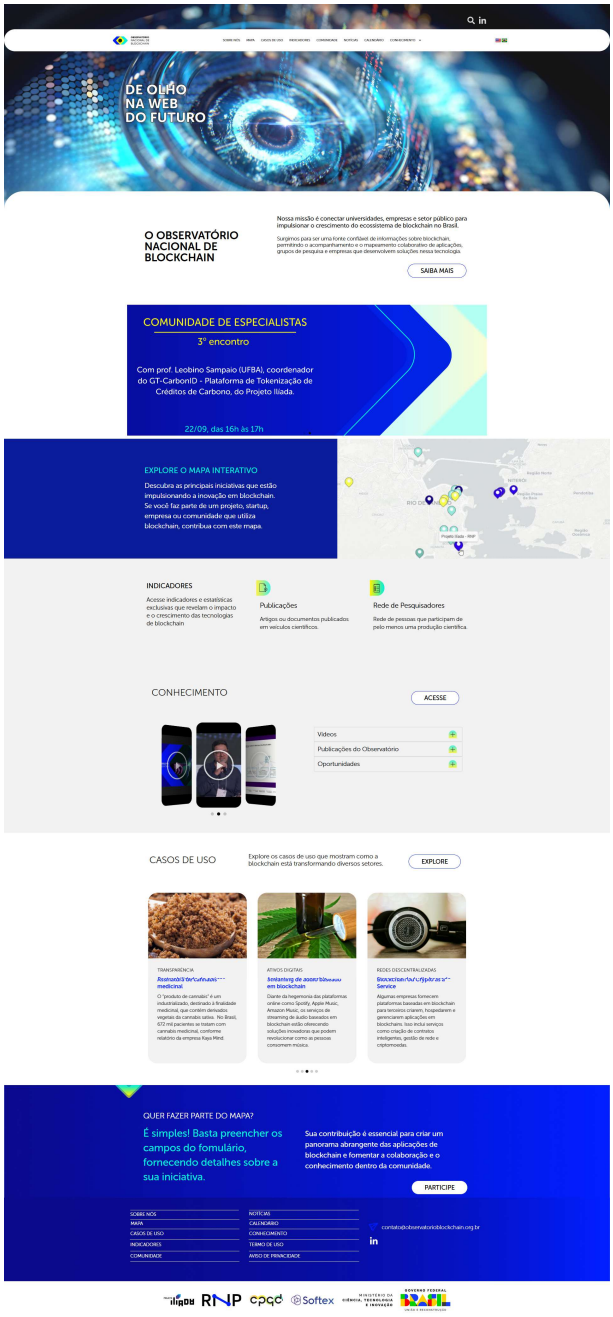

Figura 3 – Página inicial do Observatório Blockchain RNP.

Tais exemplos evidenciam que observatórios eficazes combinam seleção e organização de dados, métodos de análise e comunicação clara — princípios que orientaram o observatório proposto neste trabalho. No contexto brasileiro, não foram identificadas iniciativas públicas ou acadêmicas que proponham um observatório dedicado a cibercrimes, o que reforça a relevância desta proposta.

4 Desenvolvimento

Este capítulo integra a perspectiva metodológica e a implementação do painel, descrevendo como o painel foi planejado, quais dados alimentam as visualizações e como cada parte da interface foi construída no *Angular* e no *ECharts*. O código-fonte do painel está disponível publicamente em: <https://github.com/Zeitoum/Observatorio-de-cibercrimes> na pasta "frontend". A disponibilização do repositório facilita a verificação independente dos resultados, a reprodução do ambiente e a evolução colaborativa do projeto.

4.1 Visão geral e etapas metodológicas

Com o intuito de estruturar o desenvolvimento do painel, esta seção apresenta uma visão geral de sua concepção e das etapas metodológicas que orientaram sua implementação. O objetivo é explicitar o fluxo de transformação dos dados, desde a coleta bruta até a disponibilização em visualizações interativas, destacando os procedimentos intermediários que asseguram a consistência, clareza e usabilidade do sistema.

A aplicação foi concebida como uma *Single Page Application* (SPA) em *Angular*, com foco em exploração visual de dados judiciais. O fluxo segue cinco etapas encadeadas:

1. **Coleta**: obtenção de dados judiciais a partir da API pública em <http://cyber-crime-tracker.sa-east-1.elasticbeanstalk.com/v1/legal-process>, com suporte a parâmetros como `pageSize`, `pageNumber`, `orderBy` e `search`, os quais são utilizados para paginação, ordenação e busca na página de processos.

2. **Filtragem de escopo**: uso exclusivo de registros marcados como cibercrimes.

3. **Preparação**: limpeza e normalização dos campos necessários às análises (especialmente datas e `district`), além de agregações por ano, assunto e município.

4. **Visualização**: construção do mapa coroplético (municípios de SP), barras por ano, pizza por assunto e ranking (Top N assuntos), com legendas, *tooltips* e rótulos.

5. **Interação**: seletor de estado (preparado para futuras bases), seletor de ano, alternância claro/escuro, busca e paginação na página de Processos.

4.1.1 Arquitetura geral do observatório

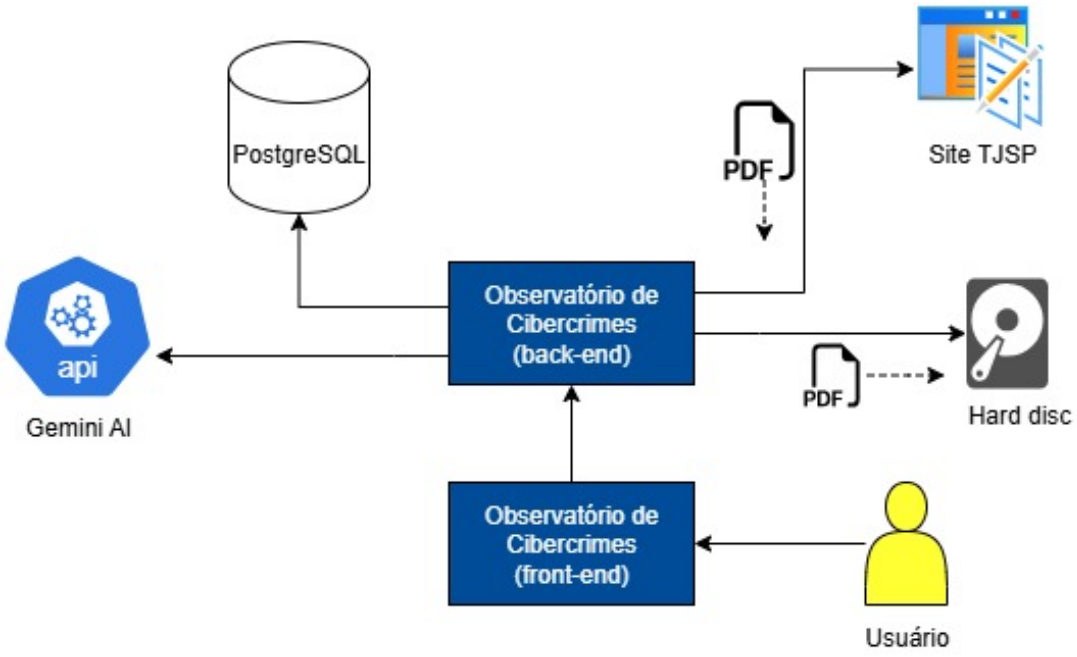

Figura 4 – Arquitetura geral do Observatório de Cibercrimes.

A Figura 4 resume a arquitetura do Observatório de Cibercrimes. No topo direito, o site do TJSP é a fonte primária dos documentos (acórdãos em PDF). O *backend* do observatório coleta e processa esses PDFs, podendo armazenar os arquivos em *hard disk* (para auditoria/reprocessamento) e persistir metadados e conteúdos estruturados em um PostgreSQL. Um módulo de IA (Gemini) assiste a classificação das decisões: a partir do texto dos acórdãos (ementa), aplica modelos de linguagem para inferir se o caso deve ser ou não marcado como cibercrime.

Este trabalho concentra-se na camada de apresentação (o painel), detalhando como os dados expostos pela API são filtrados para o escopo de registros marcados como cibercrimes, tratados (normalizações e agregações) e transformados em visualizações interativas, enquanto as camadas de coleta, processamento e armazenamento são utilizadas como provedoras de dados.

4.1.2 Origem e características dos dados

Os dados são obtidos pela API REST <http://cyber-crime-tracker.sa-east-1.elasticbeanstalk.com/v1/legal-process>. Entre os campos utilizados, destacam-se:

- `processCode` (identificador processual), `className` (classe), `subject` (assunto), `rapporteur` (relator), `district` (comarca), `judgingBody` (órgão julgador);

- `judgmentDate` e `publishDate` (datas), `headnote` (ementa), `pdfUrl` (link, quando disponível);
- `isCyberCrime` (indicador — usado aqui conceitualmente como "marcado como cibercrime").

A base é dinâmica e pode conter lacunas pontuais (por exemplo, datas ausentes ou variações ortográficas em `district`). Por isso, o painel aplica sanitização (descarta registros sem data/comarca) e normalização textual do município para casar com o *GeoJSON* utilizado no mapa. A exibição preserva a privacidade, pois trabalha com dados públicos agregados e sem informações pessoais sensíveis.

4.2 Arquitetura do *frontend*

Esta seção descreve a estrutura do *frontend*, indicando as responsabilidades de cada componente principal (Home, Processos, Header e Footer) e a forma como se articulam para oferecer ao usuário uma experiência unificada e responsiva.

A aplicação é organizada em componentes independentes (*standalone*):

- **Header** e **Footer**: navegação, identidade visual e utilidades.
- **Home**: painel analítico com mapa, barras, pizza, ranking, seletor de estado/ano e a seção "Sobre o projeto".
- **Processos**: tabela pesquisável/paginada (apenas registros marcados como cibercrimes) com expansão de ementa.

A camada de dados é centralizada em `CibercrimeService`, responsável por requisitar a API, consolidar múltiplas páginas (quando necessário) e fornecer coleções já filtradas pelo escopo do estudo.

4.3 Implementação das etapas

Esta seção descreve a implementação prática do painel desenvolvido, apresentando de forma detalhada as etapas que transformam os dados brutos em visualizações interativas. A estrutura segue o fluxo metodológico definido anteriormente — coleta, filtragem, preparação, visualização e interação —, evidenciando como cada uma dessas fases foi traduzida em código e recursos técnicos dentro do *framework* Angular e da biblioteca ECharts.

O objetivo desta seção é, portanto, demonstrar de maneira clara e transparente como as escolhas metodológicas se materializaram em soluções computacionais, garantindo a rastreabilidade entre o planejamento do trabalho e sua execução.

4.3.1 Coleta (API REST)

A coleta usa `HttpClient` (Angular) com cabeçalhos JSON e parâmetros: `pageSize`, `pageNumber`, `orderBy` e `search`. Na Home, quando o conjunto completo é necessário para agregações, o serviço percorre as páginas e concatena os itens. Na página Processos, a busca (`search`) é acionada pelo usuário (*Enter*/botão).

4.3.2 Filtragem e preparação

Aplicam-se as seguintes transformações:

1. **Escopo**: mantém-se apenas registros marcados como cibercrimes.
2. **Sanitização**: excluem-se itens sem `judgmentDate` ou `district`.
3. **Normalização de municípios**: remoção de acentos, hífens/pontuação, compressão de espaços e caixa alta para casar `district` (comarca/município do banco de dados) com o nome da *feature* do GeoJSON estadual.

4.3.3 Visualização (ECharts)

4.3.3.1 Mapa coroplético (SP).

Registra-se o GeoJSON do Estado de São Paulo no ECharts (`registerMap`). Cada município recebe a contagem do ano selecionado:

- Baixos volumes (max ≤ 4): degraus discretos (1, 2, 3, $\geq$4), além do 0 (sem casos).
- Volumes maiores: cortes aproximados em 25%, 50% e 75%, formando faixas (Baixo/Médio/Médio-alto/Alto) sem sobreposição.

A legenda no cartão é personalizada no *HTML* e espelha os limites aplicados pelo *ECharts*. *Tooltips* mostram município e quantidade, além de ser habilitado o zoom com limites adequados ao recorte estadual.

Através das Figuras 5 e 6 é possível visualizar o Mapa de Calor de São Paulo com suas respectivas legendas nas versões escura e clara. Já nas Figuras 7 e 8 são apresentados dois exemplos: a *tooltip* do município de São Paulo e a representação do mapa para poucos casos de cibercrimes, respectivamente.

Figura 5 – Mapa coroplético de SP com legenda customizada (modo escuro).

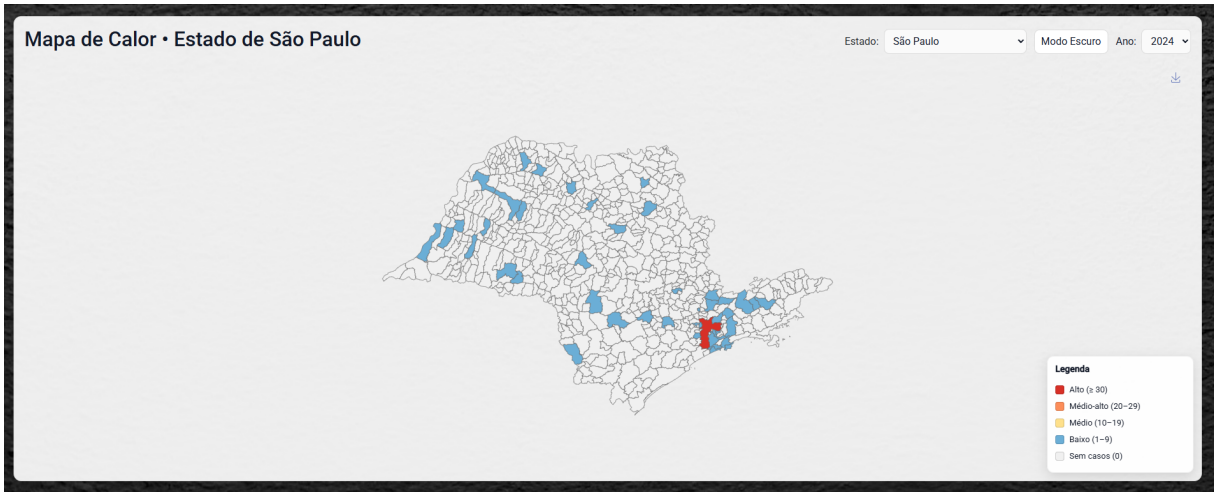

Figura 6 – Mapa coroplético de SP com legenda customizada (modo claro).

Figura 7 – Exemplo *Tooltip* de São Paulo .

Figura 8 – Exemplo de 2015 com número de crimes menor ou igual a 4.

4.3.3.2 Barras (crimes por ano).

Para cada ano presente na base filtrada (marcados como cibercrime), computa-se o total anual e exibe-se uma barra com rótulo de valor no topo. O eixo X mostra os anos;

o eixo Y, a quantidade. O gráfico atualiza automaticamente quando o usuário alterna o tema (claro/escuro).

As Figuras 9 e 10 apresentam a evolução anual dos crimes classificados como cibercrimes.

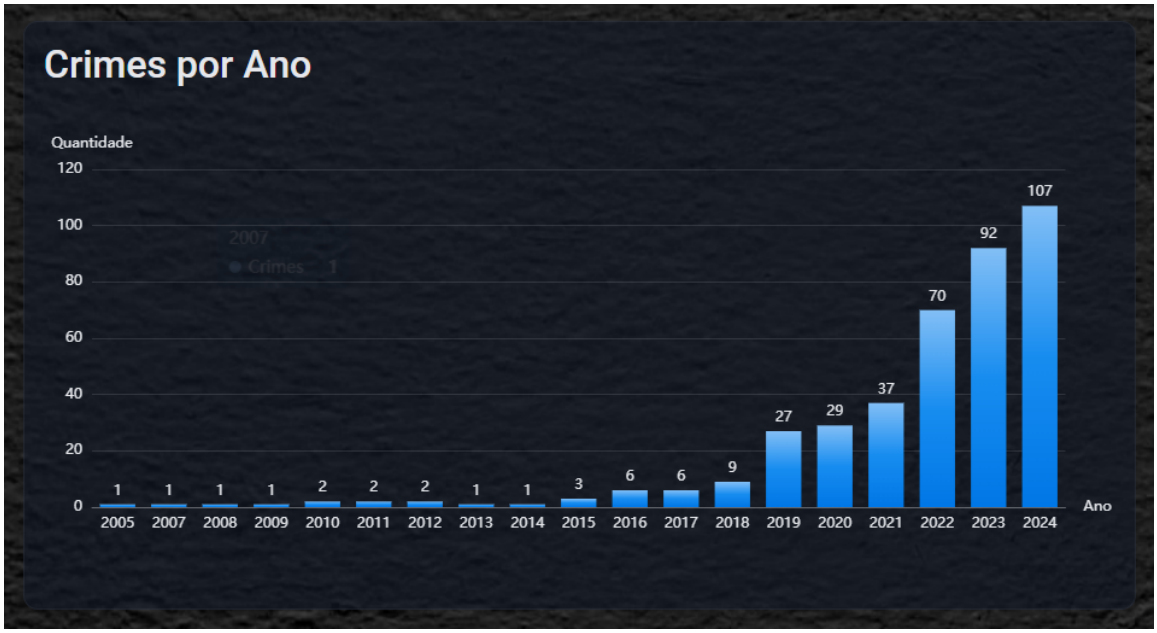

Figura 9 – Crimes por ano (modo escuro).

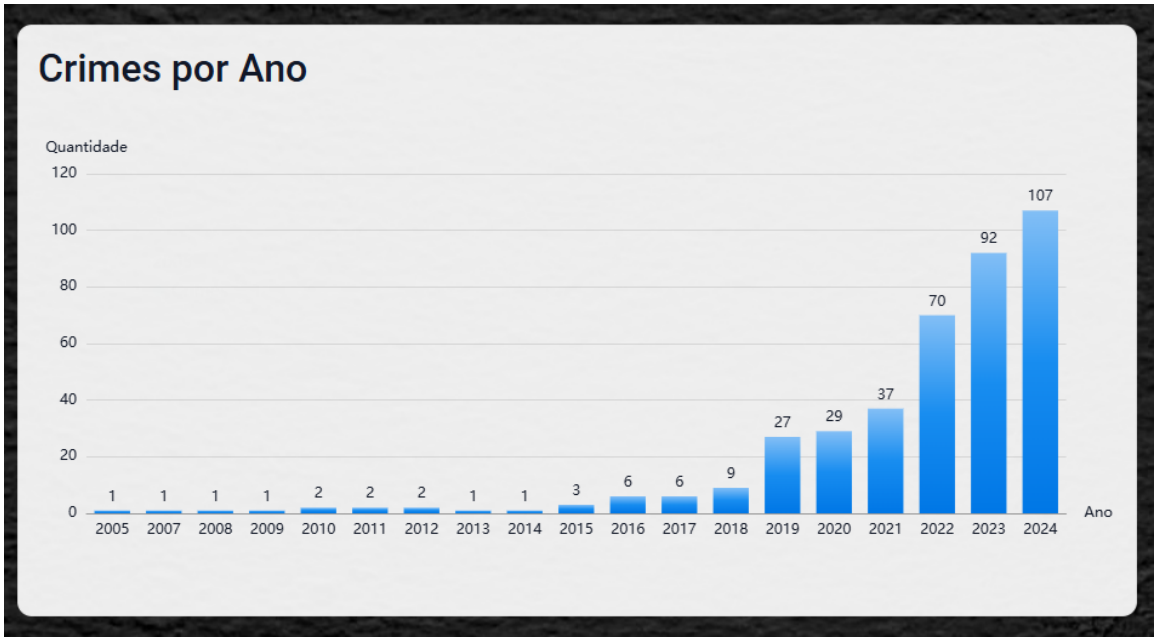

Figura 10 – Crimes por ano (modo claro).

4.3.3.3 Pizza (distribuição por assunto).

O gráfico mostra a distribuição dos assuntos (`subject`) no ano selecionado. Para manter legibilidade, é aplicado um `Top N` (configurável) e o excedente é agregado em "Outros". Os rótulos de % têm limiar mínimo (2%) para evitar poluição visual.

As Figuras 11 e 12 ilustram a proporção de assuntos jurídicos relacionados aos cibercrimes.

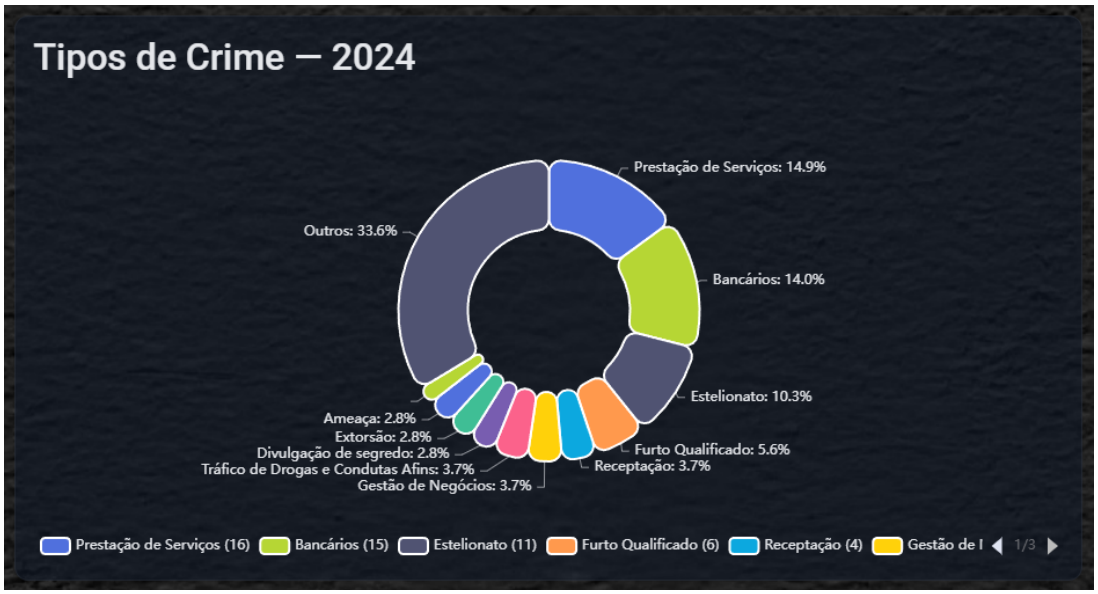

Figura 11 – Distribuição por assunto no ano selecionado (modo escuro).

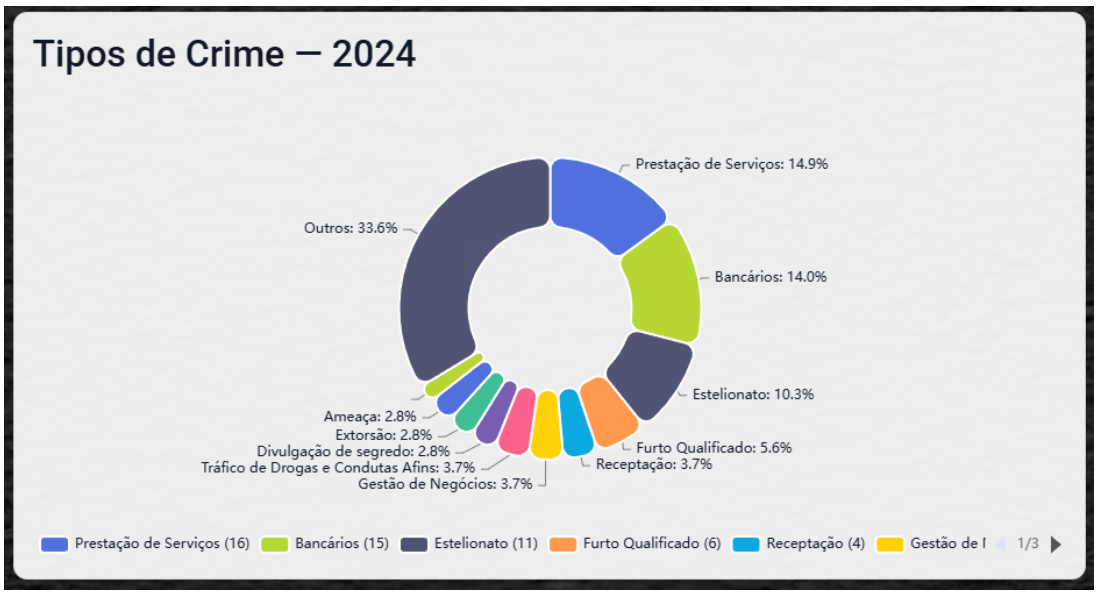

Figura 12 – Distribuição por assunto no ano selecionado (modo claro).

4.3.3.4 Ranking (Top N por assunto)

Exibe os assuntos mais recorrentes do ano em barras horizontais (ordenadas), com rótulo de valor à direita. Esse arranjo favorece a leitura de categorias textuais longas.

As Figuras 13 e 14 exibem os 5 assuntos mais recorrentes, ordenados de forma decrescente.

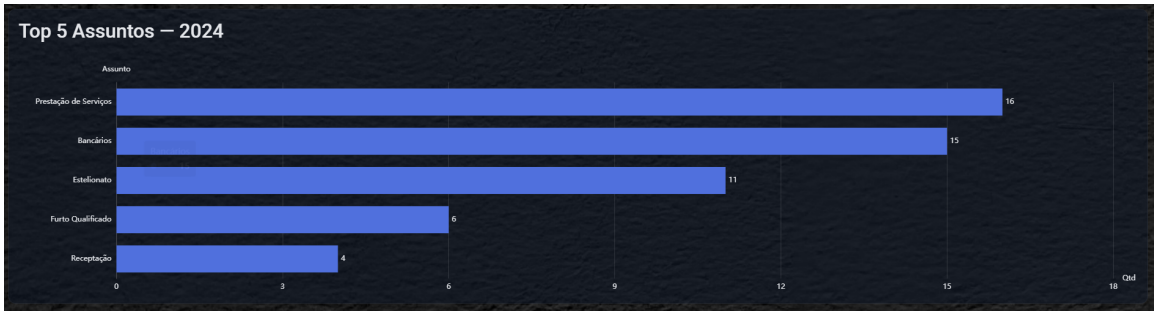

Figura 13 – Ranking dos assuntos mais incidentes no ano selecionado (modo escuro).

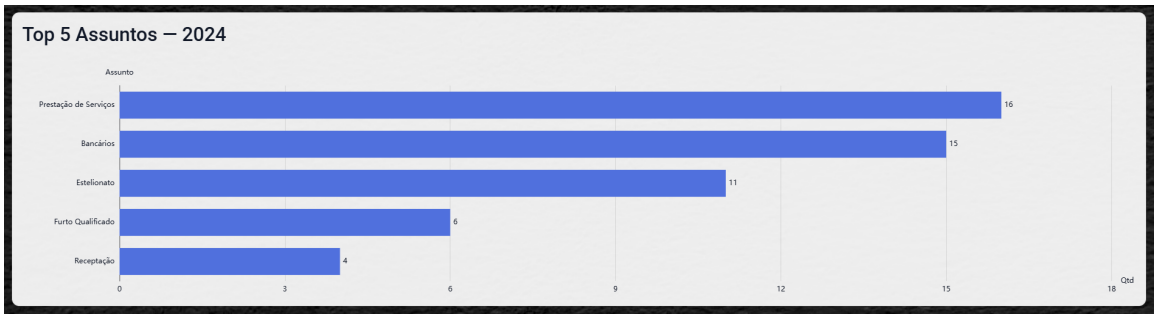

Figura 14 – Ranking dos assuntos mais incidentes no ano selecionado (modo claro).

4.3.4 Interação e usabilidade

A experiência do usuário foi planejada para que a navegação no painel seja simples, fluida e acessível em diferentes dispositivos. Foram incorporados elementos de interação que permitem personalizar a visualização (como seletores e tema), bem como recursos de usabilidade voltados à clareza na busca de informações e adaptação a diversos formatos de tela.

- **Seletor de estado**: posicionado no cabeçalho do cartão do mapa; atualmente disponibiliza SP, mas a arquitetura está preparada para receber outras malhas (ex.: RJ, MG) no futuro.
- **Seletor de ano**: atualiza mapa, pizza e ranking de forma sincronizada.
- **Tema claro/escuro**: alternância via variáveis CSS.

- **Busca (Processos)**: termo livre em `search`, acionado por *Enter* ou botão "Buscar". A páginação é feita no lado do cliente sobre o vetor já filtrado, evitando páginas vazias.
- **Exportação de visualizações**: todos os gráficos e mapas oferecem ao usuário a possibilidade de download em formato de imagem, por meio de um botão de exportação embutido no canto superior direito. Esse recurso contribui para a transparência e a reprodutibilidade das análises, permitindo que os dados processados e suas representações visuais sejam reutilizados em relatórios, apresentações ou estudos posteriores.
- **Responsividade**: suporte a dispositivos móveis, empregando a variação de tabela *stacked* (empilhada) para melhor visualização em telas menores.

4.4 Páginas e componentes

Esta seção apresenta a organização das principais páginas e componentes do painel, detalhando suas funções e como contribuem para a experiência do usuário. A divisão em páginas busca separar as áreas analíticas (como a Home, que concentra as visualizações gráficas) da parte de consulta detalhada (a página Processos, voltada à pesquisa e exploração dos registros).

Além disso, são descritos os componentes estruturais que garantem a navegação e a identidade visual da aplicação, como o *Header* e o *Footer*.

4.4.1 Home

Reúne as quatro visualizações (mapa, barras, pizza, ranking), além dos seletores (estado/ano) e da seção “Sobre o projeto”, que apresenta o total de processos filtrados, período coberto, ano selecionado e cartões explicativos (o que é cibercrime, fontes e tratamento de dados, como ler o mapa, privacidade & ética). Os *cards* usam variáveis CSS para harmonizar claro/escuro.

As Figuras 15 e 16 ilustram a tela inicial com os temas escuro e claro, respectivamente, evidenciando a adaptação visual do painel conforme a preferência do usuário.

A seção “Sobre o projeto” está destacada nas Figuras 17 e 18, apresentando indicadores como o total de processos filtrados, o período coberto, o ano selecionado e cartões explicativos sobre cibercrimes, fontes de dados, metodologia de tratamento, leitura do mapa e aspectos de privacidade.

Já os seletores, que possibilitam alterar o estado e o ano analisados, estão representados nas Figuras 19 e 20 (seletor de estado nos modos escuro e claro) e nas Figuras 21

e 22 (seletor de ano em ambos os modos). Esses componentes asseguram a personalização da análise e a navegação fluida dentro do painel.

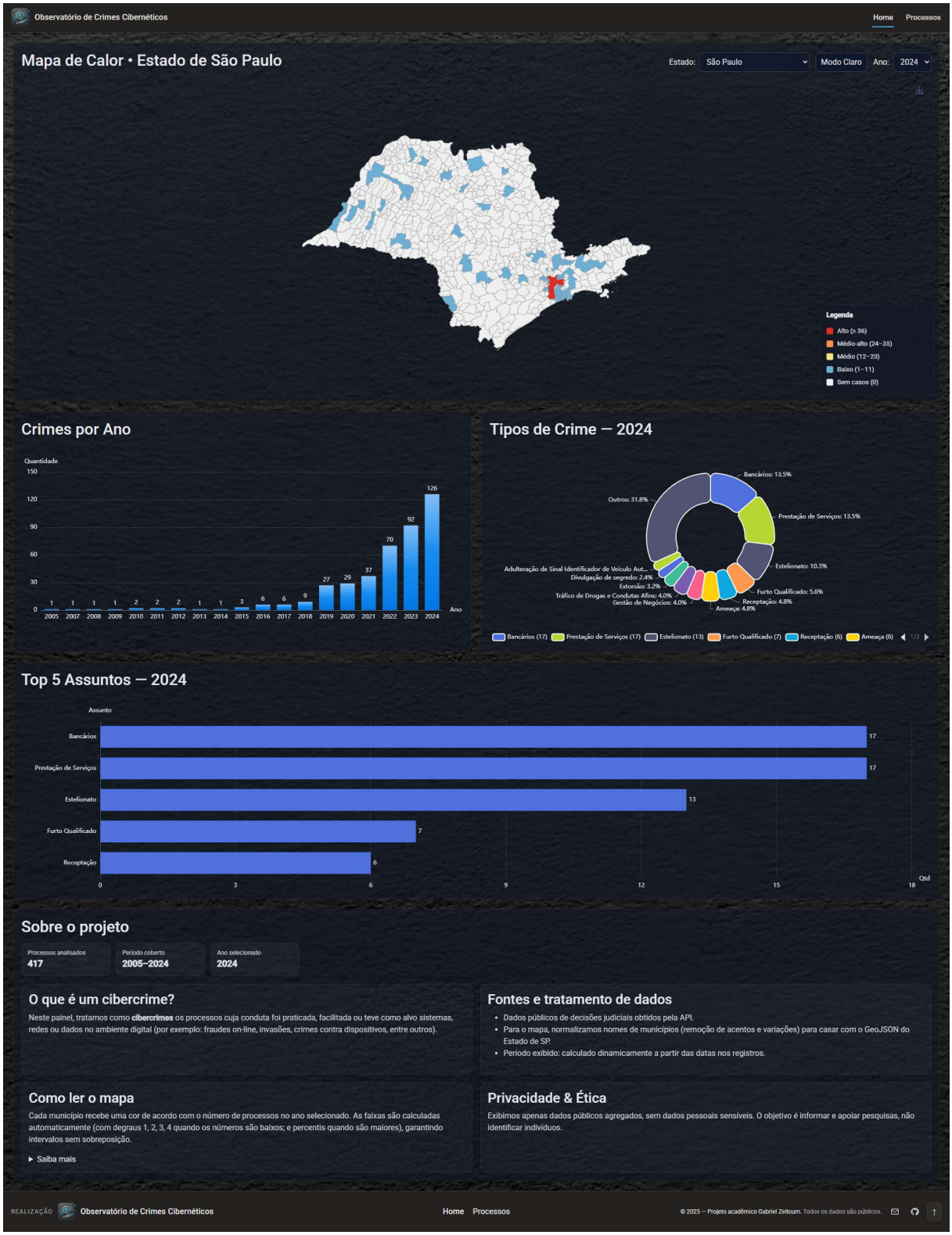

Figura 15 – Home com tema escuro.

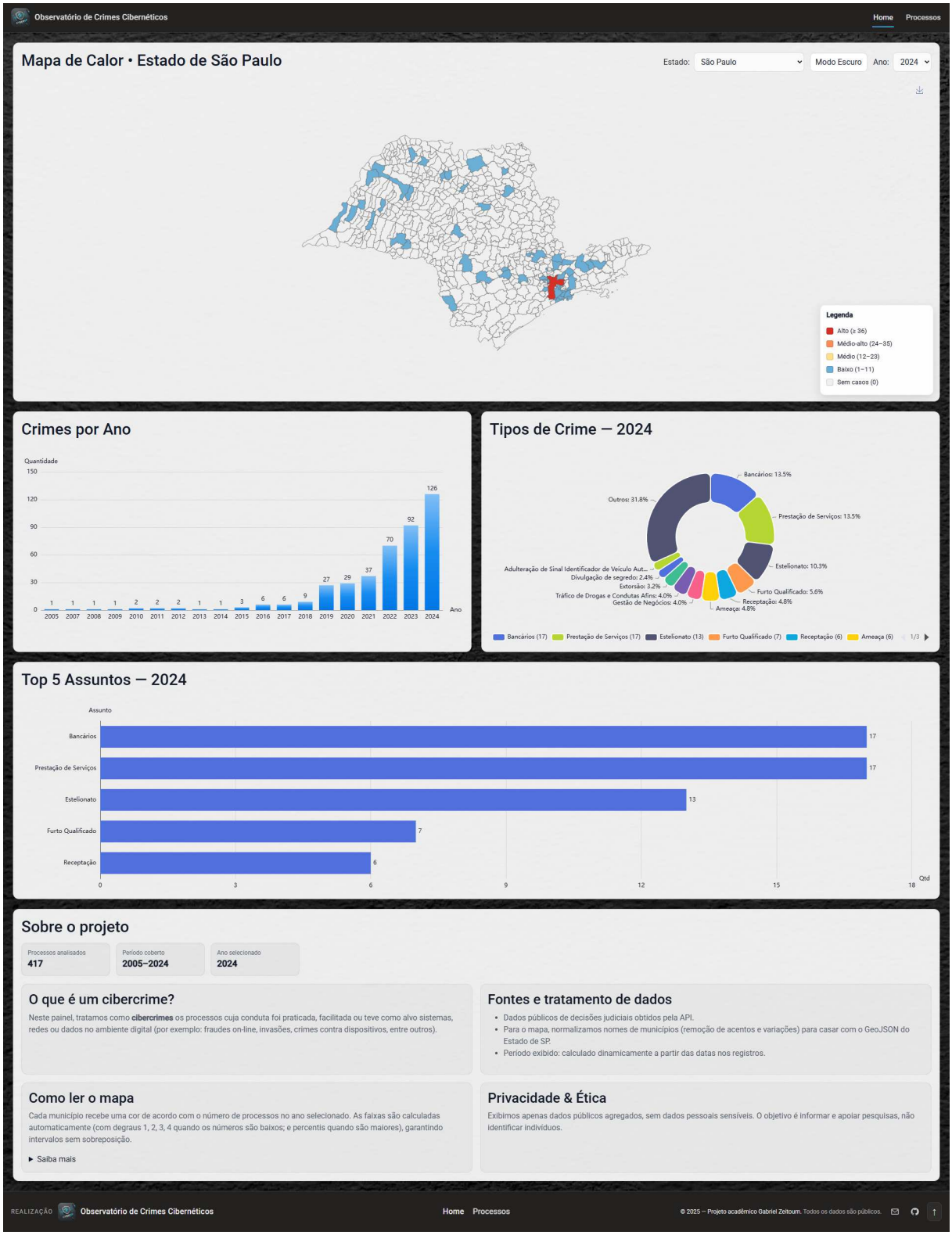

Figura 16 – Home com tema claro.

Figura 17 – Seção "Sobre o projeto" (modo escuro).

Figura 18 – Seção "Sobre o projeto" (modo claro).

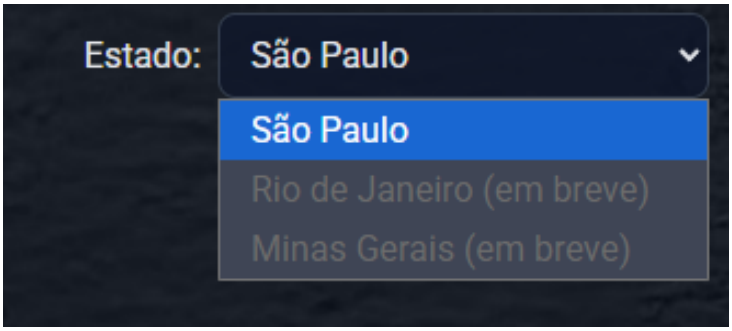

Figura 19 – Seletor de Estado (modo escuro).

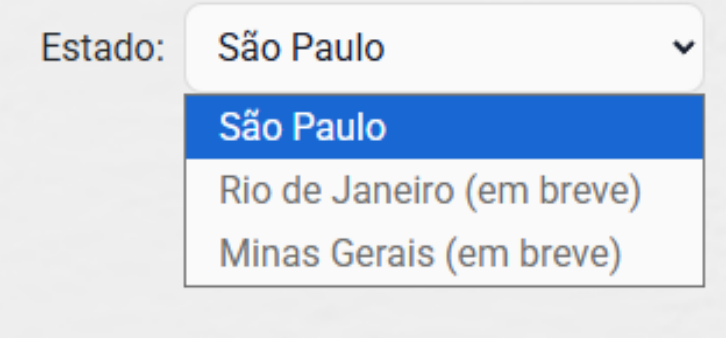

Figura 20 – Seletor de Estado (modo claro).

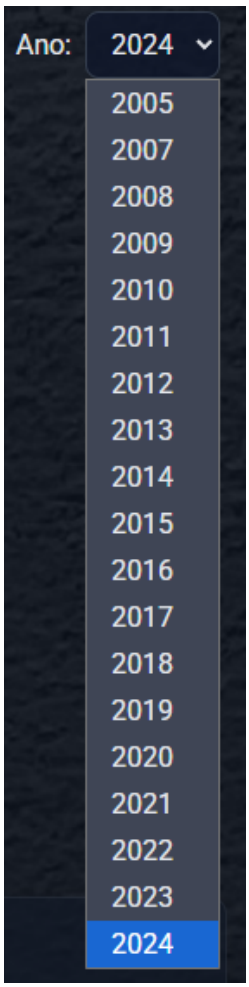

Figura 21 – Seletor de Ano (modo escuro).

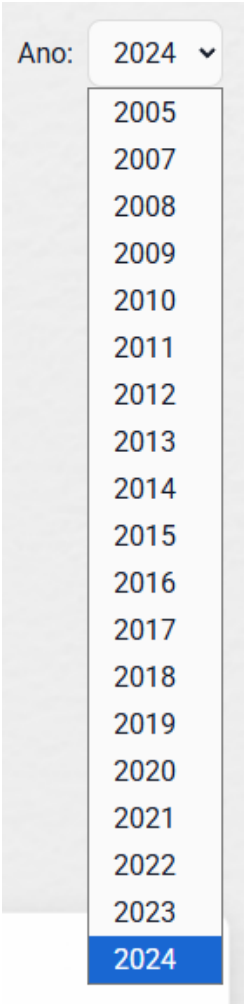

Figura 22 – Seletor de Ano (modo claro).

4.4.2 Processos

A página Processos apresenta uma tabela responsiva com os campos: `ID Processo`, `Classe`, `Assunto`, `Relator`, `Comarca`, `Orgão Julgador`, `Data Julgamento`, `Data Publicação`, `Ementa` e `Link` todas buscadas no banco de dados. Caso ocorra algum erro durante esta busca, o mesmo será informado no front-end através de uma mensagem de erro informando que nenhum processo foi encontrado. O *card* é claro (sem alternância de tema), sobre o mesmo *background* da página Home.

A Figura 23 ilustra a visualização geral da página Processos, evidenciando a tabela e seus campos principais.

Para demonstrar a interação do usuário com o recurso de busca, foram realizados testes com diferentes filtros. A Figura 24 apresenta o resultado de uma consulta por **ID do Processo**, enquanto a Figura 25 mostra uma pesquisa pelo campo **Classe**. Já a Figura 26 exemplifica a busca por **Assunto**, e a Figura 27 exibe uma consulta pelo campo **Relator**.

Esses exemplos reforçam a flexibilidade da página Processos, que permite ao usuá-

rio explorar os registros de acordo com diferentes critérios de interesse, sem perda de legibilidade ou consistência visual.

4.4.2.1 Definição das colunas da tabela

A Tabela de processos exibe, para cada registro retornado pela API, os seguintes campos:

`ID Processo` : Identificador processual exibido ao usuário (campo `processCode` na API). Em geral corresponde ao número CNJ do processo e serve para referência e conferência no sistema de origem.

`Classe` : Categoria processual (`className`), por exemplo: "Apelação", "Habeas Corpus", "Agravo Interno Cível". Ajuda a distinguir a natureza do procedimento.

`Assunto` : Tema jurídico principal do processo (`subject`), como "Estelionato", "Roubo Majorado", etc. É a base para as análises por assunto (pizza e ranking).

`Relator` : Magistrado relator do acórdão (`rapporteur`), responsável pelo voto condutor no órgão colegiado.

`Comarca` : Comarca de origem (`district`), isto é, a circunscrição judiciária (normalmente associada ao município) de onde o caso se origina. É o campo usado no *matching* com os municípios do GeoJSON do Estado para o mapa.

`Órgão Julgador` : Colegiado que proferiu a decisão (`judgingBody`), como "Xª Câmara de Direito Criminal" ou "Turma Julgadora".

`Data Julgamento` : Data em que o colegiado julgou o caso (`judgmentDate`). No front-end é formatada como `dd/mm/aaaa`.

`Data Publicação` : Data da publicação do acórdão (`publishDate`) no Diário de Justiça ou equivalente. Também formatada como `dd/mm/aaaa`.

`Ementa` : Síntese textual da decisão (`headnote`). Para manter a legibilidade, exibe-se apenas um trecho inicial; o usuário pode expandir via "Ver mais" e recolher via "Ver menos".

`Link` : Hiperlink para o documento PDF do acórdão (`pdfUrl`), quando disponível. Abre em nova aba e pode não aparecer se a API não fornecer o endereço.

O mapeamento entre os rótulos mostrados ao usuário e os campos da API é apresentado a seguir:

Tabela 1 – Mapeamento de rótulos (UI) para campos da API

Rótulo (UI)	**Campo na API**
ID Processo	`processCode`
Classe	`className`
Assunto	`subject`
Relator	`rapporteur`
Comarca	`district`
Órgão Julgador	`judgingBody`
Data Julgamento	`judgmentDate`
Data Publicação	`publishDate`
Ementa	`headnote`
Link	`pdfUrl`

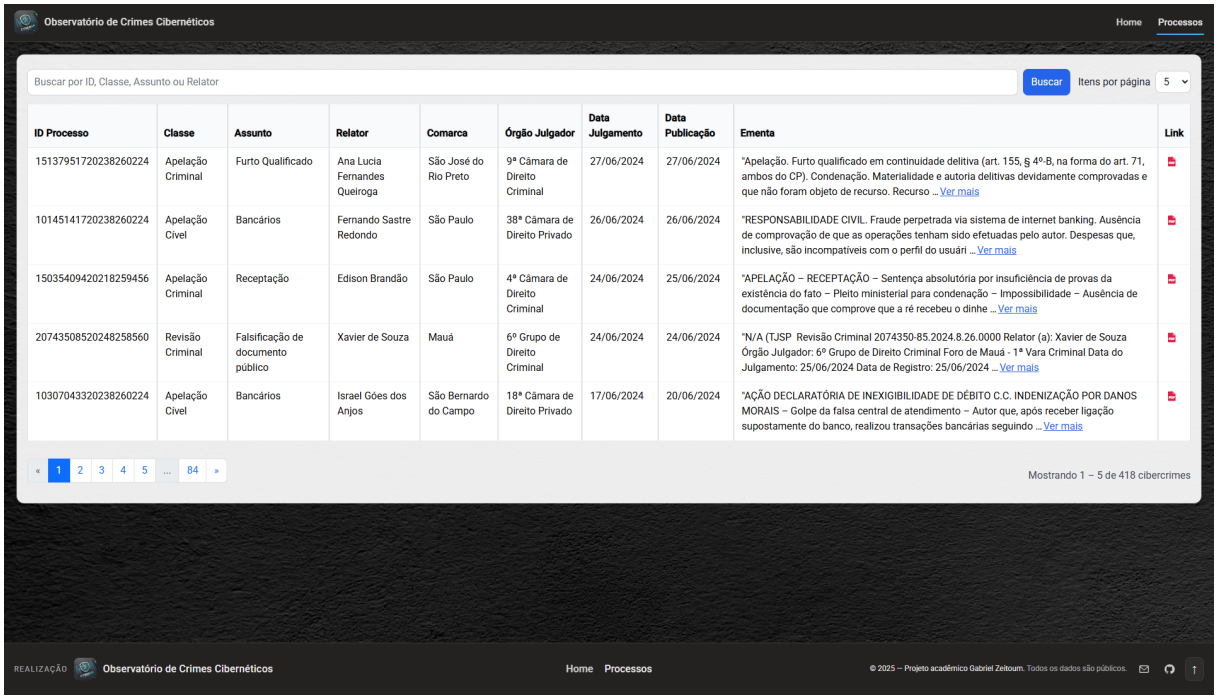

Figura 23 – Página de Processos.

Figura 24 – Exemplo de busca por ID do Processo.

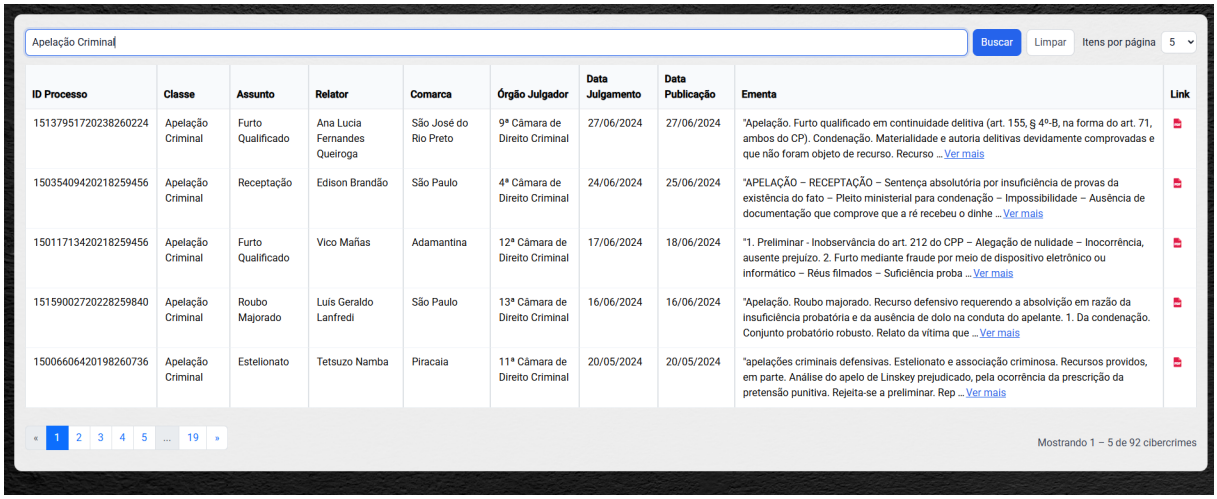

Figura 25 – Exemplo de busca por Classe.

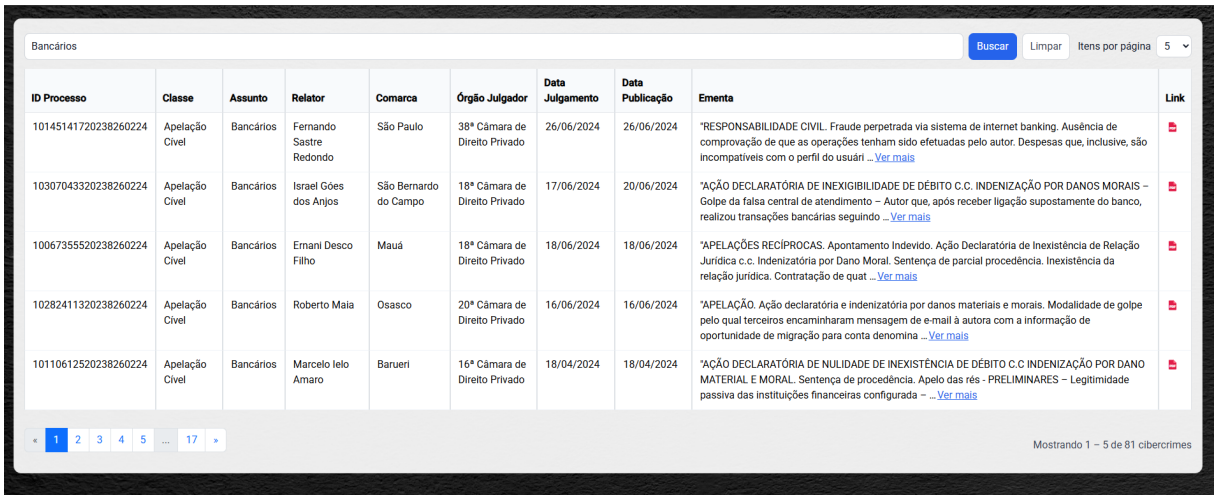

Figura 26 – Exemplo de busca por Assunto.

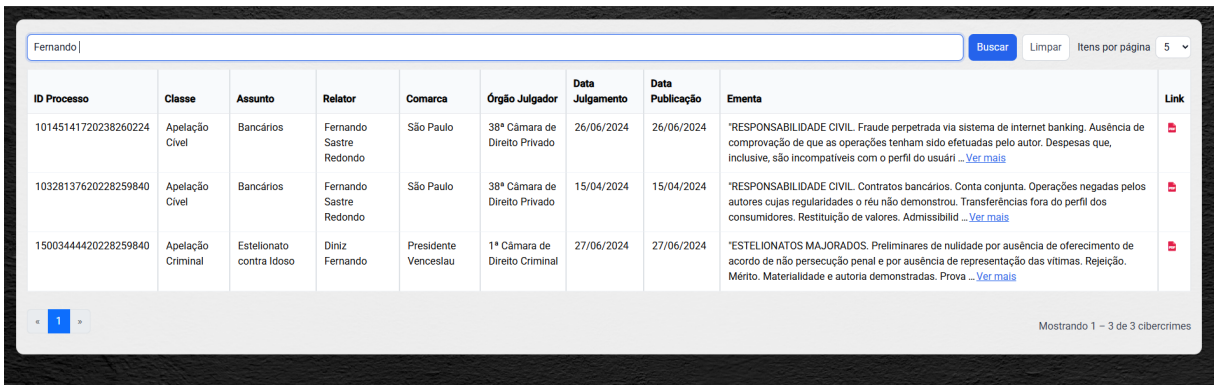

Figura 27 – Exemplo de busca por Relator.

4.4.3 Header e Footer

4.4.3.1 Header

O cabeçalho desempenha um papel essencial na identidade visual e na navegação do painel. Ele apresenta a logomarca criada para este trabalho e os links de acesso às páginas Home e Processos. Além disso, utiliza fundo cinza-escuro e tipografia clara para proporcionar alto contraste, com estados de *hover* que auxiliam na usabilidade.

A Figura 28 mostra a versão do Header em ambiente desktop, destacando a disposição dos elementos em tela cheia. Já a Figura 29 apresenta a versão adaptada para dispositivos móveis, evidenciando a fluidez do *layout* para diferentes larguras de tela.

Figura 28 – Header Desktop.

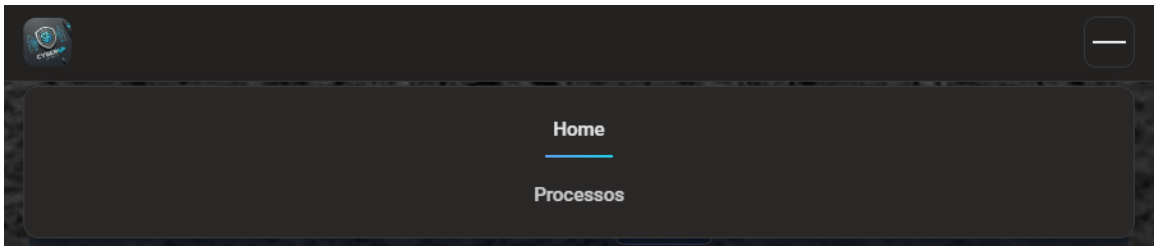

Figura 29 – Header Mobile.

4.4.3.2 Footer

O rodapé adota o mesmo padrão visual do cabeçalho, reforçando a identidade gráfica do painel. Ele inclui uma seção de "Realização", a navegação entre Home e Processos, além de elementos adicionais como identificação, ícones para contato por e-mail e acesso ao repositório no GitHub, e um botão de scroll que leva o usuário ao topo da página.

Na Figura 30, observa-se a versão do Footer para desktop, onde todos os elementos estão dispostos horizontalmente. Já a Figura 31 ilustra a versão para dispositivos móveis, em que o conteúdo é reorganizado para garantir legibilidade e acessibilidade em telas menores.

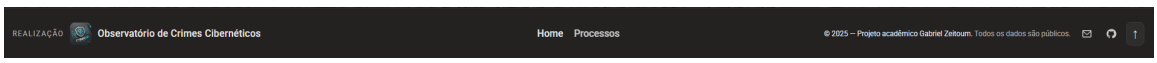

Figura 30 – Footer Desktop.

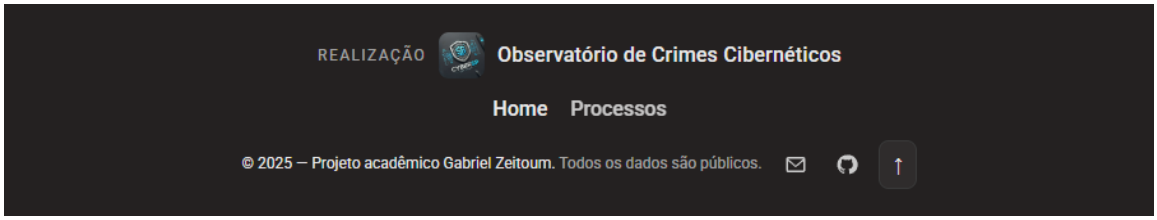

Figura 31 – Footer Mobile.

4.5 Serviços e requisitos de interface

O desenvolvimento do painel também exigiu a implementação de serviços auxiliares e a adoção de boas práticas de usabilidade. Esta seção descreve, portanto, o serviço de dados utilizado para integrar a API e o tratamento de informações, bem como as medidas aplicadas para garantir responsividade e acessibilidade na interface.

4.5.1 Serviço de dados: `CibercrimeService`

O `CibercrimeService` encapsula a integração com a API e o pré-processamento das informações, centralizando a lógica de acesso e filtragem dos dados. Suas principais rotinas incluem:

- `getProcessos(termo, pagina, limite)`: retorna lista paginada de processos, útil em cenários gerais;
- `getAllProcessosWithSearch(search)`: percorre todas as páginas disponíveis, concatenando os itens;
- `getAllCyberProcessos(search)`: reaproveita a rotina anterior, mas retorna apenas registros marcados como cibercrimes.

4.5.2 Responsividade e acessibilidade

Foram aplicadas práticas de interface voltadas à adaptação do painel para diferentes dispositivos e à inclusão de usuários. Entre elas, destacam-se:

- **Layout**: uso de *grid* responsivo, tabelas no formato *stacked* (empilhadas) em telas menores e cartões com espaçamento adequado;
- **Acessibilidade**: contraste adequado no tema escuro, além de rótulos e *tooltips* legíveis em diferentes resoluções.

5 Conclusão

Este trabalho partiu de uma motivação simples, mas atual: como tornar dados de cibercrimes mais acessíveis, compreensíveis e exploráveis por qualquer pessoa—de pesquisadoras e analistas a usuários interessados que queiram enxergar padrões de uma forma visual e direta. O resultado foi um painel web construído em Angular utilizando também sua biblioteca ECharts para a construção do mapa e dos gráficos, que integra dados públicos via API, a qual filtra somente registros marcados como cibercrimes e apresenta diferentes recortes: espacial (mapa coroplético do Estado de São Paulo), temporal (barras por ano) e temático (pizza e ranking de assuntos), além de uma página de consulta com busca e paginação.

Do ponto de vista técnico, a proposta se mostrou viável e consistente. A arquitetura em *SPA* (*Single Page Application*) ajudou a manter a experiência fluida: quem usa navega entre *Home* e *Processos* sem recarregar a página, interage com filtros e vê os gráficos se atualizando em tempo real através da alteração do ano. O *ECharts* foi um ótimo aliado—oferece performance, uma API flexível e componentes visuais que conversam bem com as necessidades de um painel analítico (tooltips, legendas, exportação, mapas, etc.).

Mais do que montar gráficos visualmente agradáveis, o painel se propôs a criar um caminho de leitura dos dados: o usuário inicia pelo mapa (visão espacial), valida percepções com o gráfico de barras (visão temporal), aprofunda-se nos assuntos relacionados através dos gráficos de pizza e ranking (visão temática) e, se for de preferência do mesmo ter um conhecimento mais a fundo a partir de tais processos, é possibilitado o acesso aos registros na página *Processos*. A seção "Sobre o projeto" fecha o ciclo explicitando premissas, fontes, limites e escolhas de visualização. O conjunto forma um pipeline replicável para geovisualização de dados judiciais.

5.1 Limitações e aprendizados

Naturalmente, existem limites. O principal é a cobertura dos dados: no momento, a aplicação trabalha com estado de São Paulo e depende do que a API fornece. Se a base tem lacunas (datas faltando, nomes de municípios divergentes, `pdfUrl` ausente), isso se reflete no que é possível mostrar. Quanto ao filtro de escopo, houve uma evolução durante o desenvolvimento: inicialmente o sistema consumia todos os registros da API; posteriormente, o back-end passou a disponibilizar o campo/parâmetro `isCyberCrime` para identificar e filtrar decisões de cibercrime diretamente no servidor. Por falta de experiência prévia com desenvolvimento web e dado o cronograma reduzido, optei por implementar a filtragem no *front-end* (após o carregamento) em vez de já acionar o

novo filtro da API. Como o volume de dados não era grande, o impacto de desempenho foi aceitável e isso permitiu priorizar outras partes do projeto. Para versões futuras, a melhoria natural é migrar a filtragem para o *back-end*, aproveitando `isCyberCrime=true` na própria consulta para reduzir tráfego, tornar a paginação mais fiel e acelerar o tempo de resposta.

No front-end, alguns detalhes renderam bons aprendizados práticos:

- **GeoJSON e mapas coropléticos**: houve a compreensão prática do uso de arquivos GeoJSON no *ECharts* (`registerMap`) e da necessidade de normalização de nomes de municípios (remoção de acentos, padronização de caixa, tratamento de hífens e espaços) para garantir o *matching* (correspondência) consistente entre o campo `district` da base e as *features* do mapa.

- **Arquitetura em Angular**: a implementação consolidou o entendimento de componentes *standalone*, *data binding* (`ngModel`) e serviços injetáveis para comunicação com a API. O projeto evidenciou a importância da separação de responsabilidades (camadas de visualização e de dados) para facilitar manutenção, testes e evolução do código.

- **ECharts/ngx-echarts**: o trabalho com a biblioteca aprofundou a configuração de gráficos reativos (mapa, barras, pizza e ranking) — `tooltips`, rótulos, legendas e escalas. A prática levou à adoção de estratégias distintas de classificação: degraus inteiros quando as contagens são baixas e cortes por percentis em volumes maiores. Em cenários com muitas categorias, consolidou-se o uso de uma variável `pieTopN`, a qual era um valor inteiro (12) o qual limitava a quantidade de assuntos que poderia aparecer no gráfico de pizza, mostrando somente os 12 assuntos com maior porcentagem de ocorrências e os que nao se encaixavam nesses 12, eram agrupados em "Outros" para preservar legibilidade.

- **Integração com API REST**: a camada de dados sedimentou práticas de consumo de API com `HttpClient`, incluindo cabeçalhos, paginação/ordenação (`pageSize`, `pageNumber`, `orderBy`) e busca (`search`), além de tratamento de erros. Optou-se por busca explicitamente acionada (tecla Enter/botão), evitando requisições redundantes e melhorando a experiência.

- **Boas práticas de visualização**: o processo reforçou princípios de contraste adequado no modo escuro, equilíbrio entre detalhe e síntese (`Top N`/"Outros"), e definição de faixas de cor sem sobreposição, contribuindo para clareza, comparabilidade e reprodutibilidade das análises.

5.2 Trabalhos futuros

A aplicação foi pensada para crescer com segurança. Algumas frentes consideradas promissoras:

1. **Ampliar cobertura geográfica**: incorporar novos GeoJSONs (ex.: RJ, MG) ao seletor de estado, habilitando a análise e comparação entre múltiplos estados.
2. **Indicadores por habitante**: integrar dados populacionais (IBGE) para calcular taxas por 100 mil habitantes, permitindo comparações mais justas entre municípios.
3. **Filtros avançados**: criar filtros por faixa temporal, órgão julgador, classe, e um *quick filter* de assuntos frequentes.
4. **Acessibilidade**: adaptar para internacionalização (ex.: versão em inglês) e adaptar também para pessoas com deficiência visual, como o daltonismo.
5. **Mudança de gráficos**: substituir o gráfico de pizza por representações mais adequadas — como gráficos de barras ou de linhas — visando melhorar a proporção visual e a interpretação dos dados.

5.3 Considerações finais

Em suma, o projeto mostrou como um bom encadeamento de coleta, filtro, preparo e visualização pode transformar uma base crua em uma história navegável. Ao traduzir processos em camadas visuais coerentes, o painel ajuda a responder perguntas reais, como onde os cibercrimes se concentram, quando crescem ou diminuem, em que temas aparecem mais, sempre preservando a privacidade (dados públicos e agregados) e mantendo a porta aberta para evoluções.

Em termos acadêmicos, o trabalho entrega três contribuições principais: (i) um protótipo funcional e responsivo, com boa experiência de uso; (ii) um *pipeline* replicável de geovisualização em Angular + ECharts; e (iii) um ponto de partida concreto para ampliar a cobertura para outros estados, métricas e fontes. Em termos práticos, oferece um caminho para que órgãos, pesquisadoras e a sociedade possam enxergar o fenômeno dos cibercrimes com mais nitidez, saindo do abstrato para o explorável/palpável.

Referências

ACATE. **Observatório ACATE 2025**. 2025. Acesso em: 17 de setembro de 2025. Disponível em: <https://www.observatorioacate.com.br/>. Citado 2 vezes nas páginas 9 e 21.

AKOGLU, L.; TONG, H.; KOUTRA, D. Graph based anomaly detection and description: a survey. **Data Min. Knowl. Discov.**, Kluwer Academic Publishers, USA, v. 29, n. 3, p. 626–688, maio 2015. ISSN 1384-5810. Disponível em: <https://doi.org/10.1007/s10618-014-0365-y>. Citado na página 18.

BARBOSA, J. S. et al. A proteção de dados e segurança da informação na pandemia covid-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, 2021. Disponível em: <https://dx.doi.org/10.33448/rsd-v10i2.12557>. Citado na página 8.

BARROS. **Conheça a evolução dos crimes cibernéticos**. 2006. Acesso em: 29 de outubro de 2024. Disponível em: <https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos>. Citado na página 11.

BRAR, H.; KUMAR, G. Cybercrimes: A proposed taxonomy and challenges. **Journal of Computer Networks and Communications**, v. 2018, p. 1–11, 04 2018. Disponível em: <https://doi.org/10.1155/2018/1798659>. Citado na página 18.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos**. 2012. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 29 out. 2024. Citado na página 11.

_____. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. 2014. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 29 out. 2024. Citado na página 11.

BRASIL, B. **Hackers roubam mais de 1 bilhão de dólares em ataques a bancos**. 2015. <http://www.bbc.com/portuguese/noticias/2015/02/150216_gch_quadrilha_hackers_lk>. [Online; accessed 15-Dezembro-2016]. Citado na página 8.

BUCZAK, A. L.; GUVEN, E. A survey of data mining and machine learning methods for cybersecurity intrusion detection. **IEEE Communications Surveys & Tutorials**, IEEE, v. 18, n. 4, p. 1–35, 2016. Disponível em: <https://doi.org/10.1109/COMST.2015.2494502>. Citado na página 18.

CARD, S.; MACKINLAY, J.; SHNEIDERMAN, B. **Readings in Information Visualization: Using Vision To Think**. [S.l.]: Academic Press, 1999. ISBN 978-1-55860-533-6. Citado na página 15.

COSTA, J. V. **Análise de vulnerabilidades de segurança em portais de governos eletrônicos**. 46 f. p. Monografia (Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação)) — Universidade Federal de Uberlândia, Uberlândia, 2017. Citado na página 8.

DAOUN, A. J.; LIMA, G. Truzzi de. **Crimes Informáticos: O Direito Penal na Era da Informação**. 2020. <https://www.truzzi.com.br/wp-content/uploads/2020/07/Artigo1_CrimesInformaticos_GiseleTruzzi_AlexandreDaoun.pdf>. Acesso em: 17 de setembro de 2025. Citado na página 11.

FEW, S. **Information Dashboard Design: The Effective Visual Communication of Data**. O'Reilly Media, Inc., 2006. ISBN 0596100167. Disponível em: <https://dl.acm.org/doi/abs/10.5555/1206491>. Citado na página 15.

Fundação Oswaldo Cruz (Fiocruz). **Observatório da Fiocruz em Ciência, Tecnologia e Inovação em Saúde**. 2016. <https://observatorio.fiocruz.br/>. Acesso em: 15 set. 2025. Citado na página 9.

LABAKI, A. d. P. **Uso de web scrapers para coleta de dados em fóruns especializados de segurança**. 46 f. p. Monografia (Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação)) — Universidade Federal de Uberlândia, Uberlândia, 2023. Citado na página 8.

LACERDA, T. B. **Cibercrime no Brasil: A utilização da Inteligência Artificial como possibilidade de prevenção**. Monografia (Trabalho de Conclusão de Curso (Graduação em Direito)) — Centro Universitário Doutor Leão Sampaio (UNILEÃO), Juazeiro do Norte, CE, 2023. Acesso em: 29 de outubro de 2024. Disponível em: <https://sis.unileao.edu.br/uploads/3/DIREITO/D1223.pdf>. Citado na página 11.

MARCIAL, N. A. ¿qué son los observatorios y cuáles son sus funciones? **Innovación Educativa**, 2009. ISSN 1665-2673. Disponível em: <https://www.redalyc.org/articulo.oa?id=179414895002>. Citado 2 vezes nas páginas 9 e 19.

Observatório de Inovação Social de Florianópolis. **Observatório de Inovação Social de Florianópolis**. s.d. Acesso em: 15 de setembro de 2025. Disponível em: <https://observafloripa.com.br/is-home>. Citado na página 19.

RNP. **Observatório Blockchain RNP**. s.d. Acesso em: 15 de setembro de 2025. Disponível em: <https://observatorioblockchain.org.br/>. Citado na página 21.

(UFSC), V. E. C. **Observatórios como ferramentas de compartilhamento de conhecimento**. 2019. Acesso em: 15 de setembro de 2025. Disponível em: <https://via.ufsc.br/observatorios-como-ferramentas-de-compartilhamento-de-conhecimento/>. Citado 2 vezes nas páginas 9 e 19.

Umane. **Observatório da Saúde Pública**. 2021. <https://observatoriosaudepublica.com.br/>. Acesso em: 15 set. 2025. Plataforma que reúne dados, análises e pesquisas sobre saúde no Brasil. Citado na página 9.

VELCU-LAITINEN, O.; YIGITBASIOGLU, O. The use of dashboards in performance management: Evidence from sales managers. **International Journal of Digital Accounting Research**, Rutgers University, v. 12, p. 39–58, 2012. ISSN 1577-8517. Citado na página 15.

VESSEY, I.; GALLETTA, D. Cognitive fit: An empirical study of information acquisition. **Information Systems Research**, v. 2, n. 1, p. 63–84, 1991. Disponível em: <https://doi.org/10.1287/isre.2.1.63>. Citado na página 15.

YIGITBASIOGLU, O. M.; VELCU, O. A review of dashboards in performance management: Implications for design and research. **International Journal of Accounting Information Systems**, v. 13, n. 1, p. 41–59, 2012. Disponível em: <https://doi.org/10.1016/j.accinf.2011.08.002>. Citado na página 15.