Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Engenharia de Software

Título: Inteligência Artificial em Cidades Inteligentes: Estratégias para Enfrentar Delitos Informáticos.

Orientador – Sidney Marlon Lopes de Lima (sidney.lima@ufpe.br)

Descrição:

As cidades inteligentes constituem um campo interdisciplinar que busca utilizar metodologias avançadas e dados para melhorar a qualidade de vida dos cidadãos e aumentar a eficiência dos seus serviços. Um metamodelo de cidades inteligentes é uma abstração conceitual que busca capturar os elementos essenciais e as interconexões que caracterizam uma cidade inteligente. A proteção de dados íntimos nas cidades inteligentes é de extrema importância de modo a evitar a perda da dignidade, finanças e até da saúde mental da vítima. Entretanto se observa uma discrepância entre os metamodelos e a realidade do cenário nacional. Um exemplo emblemático é o fato de que o Anuário Brasileiro de Segurança Pública evidencia que diversos agentes estatais cometem improbidade administrativa ao negar informações sobre crimes, sejam eles cibernéticos ou convencionais, ao órgão nacional responsável pela consolidação das estatísticas (PÚBLICA, 2023). No que diz respeito aos crimes cibernéticos no Brasil, os dados disponíveis são, em grande parte, provenientes de empresas transnacionais, como a desenvolvedora de antivírus Kaspersky. Segundo esses registros, entre 2017 e 2021, com exceção de 2019, o Brasil foi o país mais atingido por golpes de cyber-estelionato (*phishing*) (KASPERSKY, 2018)(KASPERSKY, 2023). Porém é importante destacar que tais informações são fornecidas por uma empresa privada, e não por órgãos de segurança pública. Mediante essa lacuna de dados, torna-se inviável a formulação de um metamodelo de cidades inteligentes no Brasil de forma convencional. A primeira etapa para qualquer planejamento estratégico é compreender o ponto de partida, ou seja, diagnosticar a situação atual. Consequentemente, a construção de metamodelos de cidades inteligentes fica comprometida. Diante desse cenário, o objetivo desta proposta é não se guiar por dados estatísticos consolidados até porque eles não existem. Propõe-se inverter a forma de aquisição dessas informações. A ideia é consultar diretamente os operadores do sistema de segurança pública, como magistrados, delegados, comissários, agentes e outros profissionais envolvidos no combate aos crimes cibernéticos. Dessa forma, será possível auditar a aplicação das leis sobre crimes cibernéticos, além de identificar eventuais aumentos na ocorrência desses delitos nos últimos anos. Com a adoção de metodologias mais eficientes, será possível esboçar um metamodelo de cidades inteligentes no Brasil, quanto ao combate de cibercrimes.

Requisitos necessários dos(as) candidatos(as)

- Ter inserção na área de segurança pública (ex.: pesquisador do tema, profissional de segurança pública, servidores públicos de delegacias ou divisões, dentre outros).
- Ter conhecimento na área do Direito e das leis quanto à Segurança da Informação: (Lei Geral de Proteção de Dados LGPD, Marco Civil da Internet, dentre outras) .
- Ter conhecimento na área de Segurança da Informação e Direito Digital.

Requisitos desejados dos(as) candidatos(as)

- Ser profissional da área de inteligência em segurança pública ou institucional de órgãos públicos.
- Ter conhecimento em investigação, prevenção e combate a fraudes digitais.
- Ter disponibilidade em qualquer horário diurno para encontros com o orientador e realizar pesquisas em órgãos públicos pertinentes ao tema da proposta.

Referências Bibliográficas

[Pública 2023] PúBLICA, F. de S. Anuário Brasileiro de Segurança Pública. 2023. 84 p. Disponível em: <https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf >.
[KASPERSKY 2018] KASPERSKY. Spam and phishing in 2017. 2018. Disponível em: <https://securelist.com/spam-and-phishing-in-2017/83833/ >.
[KASPERSKY 2019] KASPERSKY. Spam and phishing in 2018. 2019. Disponível em:

<https://securelist.com/spam-and-phishing-in-2018/89701/ >.
[KASPERSKY 2020] KASPERSKY. Spam and phishing in 2019. 2020. Disponível em:
<https://securelist.com/spam-report-2019/96527/ >.
[KASPERSKY 2021] KASPERSKY. Spam and phishing in 2020. 2021. Disponível em:
<https://securelist.com/spam-and-phishing-in-2020/100512/ >.
[KASPERSKY 2022] KASPERSKY. Spam and phishing in 2021. 2022. Disponível em:
<https://securelist.com/spam-and-phishing-in-2021/105713/ >.
[KASPERSKY 2023] KASPERSKY. Spam and phishing in 2022. 2023. Disponível em:
<https://securelist.com/spam-phishing-scam-report-2022/108692 />.