Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

CENTRO UNIVERSITÁRIO PROCESSUS
Prática Extensionista

- **PROJETO (2024.1)**

- **1. Identificação do Objeto**

Atividade Extensionista:

( ) PROGRAMA
(x) PROJETO
( ) CURSO
( ) OFICINA
( ) EVENTO
( ) PRESTAÇÃO DE SERVIÇOS
( ) AÇÃO DE EXTENSÃO SOCIAL

Área Temática: Direito Digital

Linha de Extensão: Direito

Local de implementação (Instituição parceira/conveniada): Centro de Ensino Fundamental 12 da Ceilândia

Título Geral: Inteligência Artificial no mundo do crime.

2. Identificação dos Autor(es) e Articulador(es)

Curso: Direito/ Serviços Jurídicos e Cartoriais

Coordenador de Curso: Adalberto Nogueira Aleixo
Articulador(es)/Orientador(es): Prof. Alberto Carvalho Amaral
Aluno(a)/Equipe:

Nome Completo	Curso / Matrícula	Telefone
Jannyne Rodrigues de Medeiros de Souza	Direito 2313180000115	(61) 999976554
Giúlia Silva de Souza	Direito 2313180000111	(61) 983256187
Alana Almeida Ribeiro	SJC	(61) 996251484

	2327200000037	
Ana Luiza da Silva Daher	SJC 2327200000024	(61) 982771206
Paulo Victor de Lima Gomes	Direito 2313180000104	(61) 998788063
Julia de Araújo Simões	Direito 2313180000175	(61) 985525885
Artur Leonardo Massari Rosa	Direito 2317200000047	(61) 993063353

3. Desenvolvimento

Apresentação: Hodiernamente, observa-se que o avanço das tecnologias tem sido cada vez mais rápido sendo dificultoso acompanhar a rápida evolução. A Inteligência Artificial (IA) se popularizou nos últimos anos, sendo muito utilizada para aumentar a eficiência e produtividade em diversos setores, inclusive no cotidiano de diversas pessoas. Contudo, tal avanço traz consigo também os aspectos negativos. Infelizmente é cada vez mais comum a utilização da IA como uma ferramenta para o mundo do crime, facilitando fraudes digitais, crimes cibernéticos, deep fakes, etc. Portanto, a conscientização e alerta sobre a má utilização da IA acaba sendo fundamental para prevenção de mais pessoas serem vítimas.

Fundamentação Teórica

O que é uma Inteligência Artificial (IA)?

A inteligência artificial é um campo da ciência da computação onde se estuda o desenvolvimento de máquinas e programas computacionais, tais programas são capazes de reproduzir o comportamento humano na tomada de decisões e na realização de tarefas, desde as mais simples até as mais complicadas.

Seu maior desenvolvimento se deu a partir da década de 1950, a inteligência artificial já faz parte da vida cotidiana das pessoas por meio dos assistentes de voz, dos mecanismos de pesquisa, dos carros autônomos e das redes sociais. Apesar de trazerem inúmeros benefícios e avanços importantes em diversas áreas, muito se debate a respeito dos limites éticos da inteligência artificial e do papel que elas desempenham na nossa sociedade.

Como funciona a inteligência artificial?

Seu funcionamento acontece por meio da coleta e da combinação de um grande volume de dados, seguido da identificação de determinados padrões nesse conjunto de

informações. Com esse processo, que geralmente se dá mediante a utilização de algoritmos pré-programados, o software consegue tomar decisões e realizar tarefas de maneira autônoma.

Existe uma série de diferentes métodos por meio dos quais uma IA pode reproduzir o comportamento humano. Os dois principais são:

Machine learning: chamado de aprendizado de máquina, é o processo que acontece de maneira automatizada. O reconhecimento e a reprodução de padrões são feitos pela IA com base na sua experiência prévia, adquirida pela utilização de algoritmos. Um dos principais exemplos são os mecanismos de pesquisa na internet.

Deep learning: Subcampo do machine learning, utiliza-se de redes neurais (unidades conectadas em rede para a análise de bancos de dados e informações) para imitar o cérebro humano.

No dia a dia algumas funções tecnológicas da IA são usadas para a facilitar e auxiliar em diversas áreas.

- Assistentes de voz: presentes em celulares e dispositivos como caixas de som inteligentes (smart speakers), os assistentes são um modelo de IA que reconhece e executa comandos feitos por meio da voz, como realizar ligações, programar alarmes, dar informações, tocar música e fazer pesquisas online. Os mais famosos assistentes de voz são o Google Assistente (integrado ao sistema Android); Siri, da Apple; e Alexa, da Amazon.

- Reconhecimento facial: empregada na confirmação da identidade de uma pessoa ao acessar seus dispositivos pessoais, como smartphones, ou ainda em aplicativos financeiros, como os bancos virtuais. Mais recentemente, o reconhecimento facial tem sido aperfeiçoado para a sua adoção ampla em sistemas de segurança pública.

- Redes sociais: os conteúdos das redes sociais que utilizamos todos os dias, como Instagram, Twitter e Facebook, não são apresentados da mesma maneira para todos os usuários. Isso porque existe um algoritmo que analisa os padrões da atividade dos indivíduos e personaliza qual tipo de postagem aparecerá para cada um, de acordo com os seus interesses.

A Inteligência Artificial como ferramenta para o crime

O uso de Inteligência Artificial (IA) para o cometimento de crimes é uma preocupação crescente à medida que a tecnologia se torna mais sofisticada e acessível. A IA pode ser mal utilizada para realizar uma variedade de atividades criminosas, desde ataques cibernéticos até fraudes financeiras e manipulação de informações.

Em primeiro lugar, é crucial estabelecer que a inteligência artificial por si só não é o problema. A tecnologia é uma extensão do potencial humano, uma ferramenta neutra que reflete os valores e ética de quem a utiliza.

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

O verdadeiro cerne da questão reside nos indivíduos que, de maneira maliciosa, exploram essa tecnologia para criar conteúdo pornográfico artificial, cometer crimes de cunho financeiro, gerar desinformação e assim sucessivamente. A verdade é que a artificialidade acaba sendo um recurso que não representa a realidade desejada ou experienciada pelas vítimas.

A IA pode ser usada como ferramenta para a criminalidade de várias maneiras, aproveitando sua capacidade de automatizar e melhorar tarefas complexas. Aqui estão alguns exemplos de como criminosos podem utilizar IA:

1. Phishing e Engenharia Social Automatizada: Os criminosos têm a possibilidade de empregar inteligência artificial para elaborar e-mails de phishing (é uma referência à forma como os golpistas usam "iscas" para enganar as vítimas) com um alto nível de personalização. Utilizando algoritmos de aprendizado de máquina, esses ataques podem ser adaptados conforme dados pessoais obtidos de redes sociais e outras fontes disponíveis ao público, o que eleva as chances de eficácia. A IA também pode reproduzir conversas em tempo real para enganar as vítimas, utilizando "chatbots" ou assistentes virtuais fictícios.

2. Deep Fakes: Deep Fakes referem-se a vídeos, áudios e imagens criados por inteligência artificial que replicam a aparência e a voz de indivíduos reais, falsificando falas, diálogos ou comportamentos. Essa tecnologia pode ser utilizada para extorsão, disseminação de informações erradas ou fraudes, como a elaboração de vídeos manipulados de personalidades públicas fazendo comentários prejudiciais ou enganando sistemas judiciais. Utiliza-se muita a IA generativa.
   A IA generativa é um tipo de inteligência artificial que pode gerar conteúdo original, como texto, imagens e áudio, sem intervenção humana. Ela usa grandes conjuntos de dados para “aprender” sobre linguagem, estilos e padrões, e depois pode aplicar esse conhecimento para criar novos conteúdos parecidos com o que foi treinada. Os cibercriminosos estão aproveitando o poder da IA generativa para escalar e automatizar seus ataques de maneira mais eficiente e inteligente.

3. Ataques Cibernéticos Automatizados: A inteligência artificial pode ser empregada para automatizar e aprimorar ataques cibernéticos. Os hackers têm a capacidade de programar IA para localizar vulnerabilidades em sistemas de maneira mais ágil do que seria possível para humanos. Um exemplo disso é a utilização de malware inteligente, que se adapta ao ambiente da vítima, conseguindo burlar sistemas de segurança e aprendendo a esquivar-se de medidas de proteção.

4. Ransomware Evoluído: A inteligência artificial pode otimizar o ransomware (um tipo de malware que sequestra dados e solicita um pagamento para a liberação) ao detectar os arquivos mais valiosos e relevantes em um sistema. Isso torna os ataques mais focados, elevando as chances de que a vítima ceda e

pague o valor do resgate. Além do mais, a IA pode aumentar a eficácia do malware em evitar soluções de segurança.

5. Fraude em Transações Monetárias: Ferramentas de IA têm a capacidade de examinar padrões em transações financeiras, identificando fraudes como lavagem de dinheiro ou fraudes em plataformas de pagamento digital. Delinquentes podem empregar IA para simular comportamentos que se assemelham a transações legítimas, tornando a identificação por sistemas antifraude convencionais mais complexa.

6. Manipulação dos Mercados Financeiros: Os algoritmos de inteligência artificial têm a capacidade de serem utilizados na manipulação do mercado financeiro. Indivíduos mal-intencionados podem desenvolver "bots de negociação" que efetuam transações fraudulentas em velocidades extremamente rápidas, distorcendo preços ou aproveitando mínimas oscilações de mercado para realizar ganhos ilegítimos, tudo isso sem despertar a atenção.Esses casos exemplificam como a utilização inadequada da IA pode elevar a complexidade e os efeitos de atividades ilícitas, frequentemente dificultando sua detecção e enfrentamento.

Casos reais da utilização da IA em crimes

- Advogada aposentada Karla Pinto

Poucas horas depois de ver a filha sair de casa para trabalhar, a advogada aposentada Karla Pinto recebeu uma chamada de vídeo em seu celular. Do outro lado do vídeo, sua filha, a advogada criminalista Hanna Gomes, pedindo uma transferência via pix de R$600.

Três fatores fizeram a aposentada desconfiar da situação: na chamada de vídeo sua filha estava com uma blusa diferente da que havia saído de casa; a conta para a qual o dinheiro deveria ser transferido seria de uma amiga da filha e não a dela própria e, principalmente, a filha não havia chamado a mãe pelo apelido carinhoso que as duas comumente usam entre elas.

Ao notar essas situações desconexas, a aposentada decidiu checar se realmente era Hanna que aparecia no vídeo e perguntou qual era o nome do cachorro da família e do vizinho que mora em frente à casa delas. Depois disso, a chamada foi desligada.

“Era o meu rosto, o meu cabelo e a minha voz. O único detalhe é que a voz estava um pouco em descompasso com o vídeo, mas sabemos que isso pode acontecer devido à conexão com a internet. É assustador ver a evolução desse tipo de golpe”, diz Hanna à BBC News Brasil.

- Ceo Britânico(ICEV)

O Wall Street Journal noticiou o primeiro caso de fraude de voz baseada em inteligência artificial (IA) – também conhecido como vishing (abreviação de “voice

phishing") – que custou a uma empresa alemã US$243 mil. O caso é um sinal que a falsificação de áudio está se tornando muito precisa e cada vez mais profissional.

Para conseguir o feito, os criminosos recorreram a um software de IA de geração de voz para se passar pelo chefe de uma companhia proprietária de uma empresa de energia sediada no Reino Unido. Eles convenceram o presidente-executivo da companhia de energia a transferir urgentemente fundos para um fornecedor húngaro em uma hora, com garantias de que a transferência seria reembolsada imediatamente.

Segundo o jornal que apurou o caso, o CEO britânico disse que não desconfiou da voz, pois reconheceu o sotaque alemão e achou que realmente se tratava de seu chefe.

- Taylor Swift

A cantora norte-americana Taylor Swift foi vítima de deep fake em janeiro de 2024. Uma foto compartilhada por um usuário no X (antigo Twitter) foi visualizada 47 milhões de vezes antes de a conta ser suspensa na última. A foto, gerada por IA, generativa, criou uma imagem de teor sexual da cantora. Por ser figura pública o potencial de ferramentas generativas são violentas e cerceantes, não apenas para sua reputação e no que tange a moral e segurança de imagem, mas também, para sua integridade física e emocional.

Regulamentação e Fiscalização de Inteligência Artificial

Como o aumento de crimes com a utilização da IA, o legislativo brasileiro vem discutindo projetos de leis para a regulamentação desta tecnologia. O projeto de lei (PL) 2.338/2023 busca regulamentar o desenvolvimento e uso da inteligência artificial (IA). Proposto pelo presidente do Senado, Rodrigo Pacheco, esse projeto cria o Sistema Nacional de Regulação e Governança de Inteligência Artificial, que será a autoridade responsável por fiscalizar e regular o setor. Atualmente, está sendo debatido na Comissão Temporária Interna sobre Inteligência Artificial no Brasil, e sua aprovação é amplamente apoiada.

A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020, já regula o tratamento de dados pessoais, incluindo aqueles utilizados por sistemas de IA, assegurando direitos aos cidadãos e exigindo que as empresas adotem práticas de proteção de dados.

A Autoridade Nacional de Proteção de Dados (ANPD) foi designada como coordenadora do Sistema Nacional de IA. Além de fiscalizar a aplicação da LGPD, a ANPD terá um papel fundamental na supervisão do uso da IA, especialmente no que se refere à proteção de dados pessoais.

Os principais objetivos da regulamentação da IA incluem:

- Segurança: Proteger os usuários contra riscos potenciais associados à IA, como discriminação, violações de privacidade e decisões equivocadas.
- Transparência: Assegurar que os sistemas de IA sejam compreensíveis e que suas decisões possam ser auditadas.
- Responsabilidade: Definir quem é responsável por ações realizadas por sistemas de IA, especialmente em casos de danos.

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Além do Brasil, outros países da América Latina, como Argentina, Colômbia, Costa Rica, Chile, México e Uruguai, também apresentaram projetos de lei semelhantes. A maioria dessas iniciativas segue diretrizes da Lei de IA da União Europeia, que prioriza a segurança no desenvolvimento e uso dessa tecnologia em relação às oportunidades econômicas.

Tema Geral: Inteligência Artificial no mundo do crime.

Tema Específico do Grupo: Uso da Inteligência Artificial como uma ferramenta para a criminalidade.

Problema verificado:

Com a popularização da IA, os golpes digitais estão ficando cada vez mais eficientes. Atualmente o Brasil é o segundo país que mais sofre crimes cibernéticos da América Latina. Um relatório divulgado pela BioCatch (líder global em detecção de fraudes digitais e prevenção de crimes financeiros) retrata uma tendência preocupante e crescente, em que criminosos estão utilizando essa tecnologia para melhorar a qualidade, o alcance e o sucesso de golpes e fraudes bancárias digitais e esquemas de crimes semelhantes. Jonathan Daley, CMO da BioCatch alerta: "Não podemos mais confiar em nossos olhos e ouvidos para verificar identidades digitais".

"O Brasil está atualmente em um estágio de aprendizado no que diz respeito à aplicação efetiva da Inteligência Artificial (IA) e Machine Learning na prevenção de fraudes. Embora tenhamos visto avanços significativos, a adoção ainda é predominantemente básica ou pontual em comparação com a sofisticação dos métodos empregados pelos fraudadores. Enquanto as organizações brasileiras estão começando a explorar o potencial dessas tecnologias, muitas ainda enfrentam desafios na implementação de sistemas abrangentes e integrados de detecção de fraudes baseados em IA", disse Cassiano Cavalcanti, Diretor de Pre-Sales Latam da BioCatch

Objetivo geral:

Informar a sociedade sobre o uso da inteligência artificial como uma ferramenta para a criminalidade.

Objetivos específicos:

- Alertar e conscientizar sobre o uso da inteligência artificial para a aplicação de golpes.
- Orientar a população mostrando como os cibercriminosos atuam.
- Distribuir cartilhas com orientações sobre o tema abordado.
- Ressaltar a importância do conhecimento como forma de prevenção de fraudes.

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Justificativa:

A principal forma de evitar ser vítima de crimes que utilizam a Inteligência Artificial é conhecendo como os cibercriminosos atuam e conhecer as fraudes. Com a vulnerabilidade digital, muitas pessoas nunca ouviram falar sobre. Portanto, ao levar esse tema atual para a comunidade, é o melhor caminho para tentar atenuar o número de vítimas e também ajudar em eventuais situações que podem acabar acontecendo no cotidiano.

Metas:

- Alertar e conscientizar sobre o uso da inteligência artificial para a aplicação de golpes.
- Orientar a população mostrando como os cibercriminosos atuam.
- Distribuir cartilhas com orientações sobre o tema abordado.
- Ressaltar a importância do conhecimento como forma de prevenção de fraudes.

Hipótese / Resultado esperado:

É esperado que, com a aplicação do projeto, a sociedade se conscientize e procure obter mais conhecimento sobre o assunto a fim de evitar que caiam em golpes na internet. Espera-se que a população entenda a importância de conhecer como os cibercriminosos atuam, quais os meios, como a inteligência artificial funciona e o modo como podem se precaver de tais fraudes, reduzindo o número de vítimas.

Metodologia:

- Slides
- Cartilhas
- Palestra

Cronograma de execução:

Data de início: 11/09/2024

Data de término: 22/11/2024

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

Evento	Período	Observação
Visita técnica	12 de setembro	
Aula no laboratório de Informática	11 de outubro	Orientações sobre como realizar pesquisas para o projeto
Pesquisas para o projeto	11 a 18 de outubro	
Produção do Slide	25 de outubro	
Produção da Cartilha	01 de outubro	
Apresentação do projeto em sala de aula	08 de novembro	
Apresentação do projeto na comunidade	11 de novembro	Centro de Ensino Fundamental 12 da Ceilândia
Elaboração do relatório final	22 de novembro	

Referência Bibliográfica:

BALDISSERA, Olívia. Tipos de inteligência artificial que fazem (e que não fazem) parte do nosso dia a dia. Pós Digital – PUCPR. [S.I.]. Disponível em: https://posdigital.pucpr.br/blog/tipos-de-inteligencia-artificial. Acesso em: 11 out. 2024.

CÂMARA DOS DEPUTADOS. Governo considera proposta de regulamentação de inteligência artificial em análise no Senado: madura e equilibrada. 2024. Disponível em: https://www.camara.leg.br/noticias/1086431-GOVERNO-CONSIDERA-PROPOSTA-DE-REGULAMENTACAO-DE-INTELIGENCIA-ARTIFICIAL-EM-ANALISE-NO-SENADO-MADURA-E-EQUILIBRADA. Acesso em: 18 out. 2024.

CONJUR. Regulamentação de inteligência artificial e seu destino em 2024. 2023. Disponível em: https://www.conjur.com.br/2023-dez-14/regulamentacao-de-inteligencia-artificial-e-seu-destino-em-2024/. Acesso em: 18 out. 2024.

COSSETTI, Melissa Cruz. O que é inteligência artificial? Tecnoblog, 2018. Disponível em: https://tecnoblog.net/responde/o-que-e-inteligencia-artificial/. Acesso em: 11 out. 2024.

ESET. Cinco formas com que cibercriminosos usam inteligência artificial para criar e aperfeiçoar ataques. 2023. Disponível em: https://www.eset.com/br/sobre/imprensa/comunicados-de-imprensa/comunicados-de-imprensa/cinco-formas-com-que-que-cibercriminosos-usam-inteligencia-artificial-para-criar-e-aperfeicoar-ataques/. Acesso em: 11 out. 2024.

Centro Universitário Processus

PORTARIA N. 282, DE 14 DE ABRIL DE 2022

EVOLUTIA TEC. Como criminosos estão usando IA generativa. 2023. Disponível em: https://evolutiatec.com.br/como-criminosos-estao-usando-ia-generativa/. Acesso em: 11 out. 2024.

FERNANDES, Flávia. O que é inteligência artificial? Veja como surgiu, exemplos e polêmicas. TechTudo, 03 mar. 2023. Disponível em: https://www.techtudo.com.br/guia/2023/03/o-que-e-inteligencia-artificial-veja-como-surgiu-exemplos-e-polemicas-edsoftwares.ghtml. Acesso em: 11 out. 2024.

GUITARRARA, Paloma. Inteligência artificial. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/inteligencia-artificial.htm. Acesso em: 18 out. 2024.

KOVACS, Leandro. Quais são os tipos de inteligência artificial? Tecnoblog, 2022. Disponível em: https://tecnoblog.net/responde/quais-sao-os-tipos-de-inteligencia-artificial/. Acesso em: 11 out. 2024.

ONODY, Roberto N. Teste de Turing e inteligência artificial. Portal IFSC – Universidade de São Paulo, 28 set. 2021. Disponível em: https://www2.ifsc.usp.br/portal-ifsc/teste-de-turing-e-inteligencia-artificial/. Acesso em: 11 out. 2024.

SENADO FEDERAL. Debatedores defendem regulamentação do uso de inteligência artificial. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/06/11/debatedores-defendem-regulamentacao-do-uso-de-inteligencia-artificial. Acesso em: 18 out. 2024.

SICHMAN, J. S. Inteligência artificial e sociedade: avanços e riscos. Estudos Avançados, São Paulo, v. 35, n. 101, p. 37-50. Disponível em: https://www.scielo.br/j/ea/a/c4sqqrthGMS3ngdBhGWtKhh/?lang=pt. Acesso em: 11 out. 2024.

SYOZI, Ricardo. O que é deep learning? Tecnoblog, 2022. Disponível em: https://tecnoblog.net/responde/o-que-e-deep-learning/. Acesso em: 11 out. 2024.

TENÓRIO, Augusto. Inteligência Artificial: origem, dilemas e contemporaneidade. Trabalho de Conclusão de Curso (Jornalismo) – Universidade Católica de Pernambuco, 2020. Disponível em: https://webjornalismo.unicap.br/inteligenciaartificial/. Acesso em: 11 out. 2024.

TERRA. Como a IA está sendo usada como ferramenta do cibercrime. 2023. Disponível em: https://www.terra.com.br/byte/seguranca-digital/como-a-ia-esta-sendo-usada-como-ferramenta-do-cibercrime,37f557299f82b0285824409cf6469589j1is5wj9.html. Acesso em: 18 out. 2024.