‘DEAD INTERNET THEORY’: A ASCENSÃO DOS BOTS E A MANIPULAÇÃO ON-LINE

Brisa Roiz José de Paiva[1]; Théo Ferreira Franco[2]; José Luiz de Moura Faleiros Júnior[3]

RESUMO

Com a evolução tecnológica e a onipresença da internet, os bots, sejam simples programas ou dotados de inteligência artificial, tornaram-se essenciais na economia digital. Eles automatizam tarefas, facilitam a vida cotidiana, mas também levantam questões éticas e de segurança. A "Dead Internet Theory" sugere que a maioria das interações online são conduzidas por bots, influenciando algoritmos e a percepção pública. Este estudo explora o impacto dos bots, sua utilização em campanhas políticas e os desafios legais e éticos associados à sua crescente sofisticação.

PALAVRAS-CHAVE: Bots; Inteligência Artificial; Dead Internet Theory.

INTRODUÇÃO

‘Com a incessante evolução tecnológica e a onipresença da internet na vida moderna, testemunhou-se um notável aumento no emprego de *bots*, ou agentes virtuais, nos mais diversos domínios online. Essas entidades automatizadas, dotadas de inteligência artificial ou de um simples programa automatizado, desempenham um papel cada vez mais proeminente, navegando desde a simplificação de tarefas cotidianas até a revolução de setores inteiros da economia digital’.

O parágrafo acima foi inteiramente gerado pelo ChatGPT, um dos programas mais conhecidos de Inteligência Artificial (IA), tecnologia que tem se tornado cada vez mais acessível. Os *bots*, por sua vez, podem ser ou não programas de IA. Enquanto a IA não é dotada de uma verdadeira capacidade cognitiva, ela é capaz de simular esse aspecto através da análise de padrões, tratando-se então de um programa extremamente complexo. Os *bots* podem ser programas simples ou complexos, caracterizando-se pela execução de tarefas automatizadas. O ChatGPT é um *bot*, mas, diferente dos *bots* mais simples que são facilmente identificados, é capaz de simular com quase perfeição a ação humana, seja para gerar uma resposta para uma pergunta, dar ideias de nomes, escrever a introdução

[1] Graduanda em Direito pela Faculdade Milton Campos. E-mail: brisaroizj@gmail.com
[2] Graduando em Direito pela Faculdade Milton Campos. E-mail: ffrancotheo@gmail.com
[3] Orientador. Doutor em Direito pela USP. Mestre e Bacharel em Direito pela UFU. E-mail: josefaleirosjr@outlook.com

de um artigo ou cumprimentar de maneira educada quando, levados pela natureza humana, mandamos “oi” ou “por favor” antes de interagir com sua tecnologia.

Este resumo expandido busca explorar essa teoria, ver como o crescimento dos programas de IA se relaciona com esse temor e os efeitos que isso pode ter na existência humana nas redes, fazendo um recorte nos riscos que isso apresenta nas campanhas políticas e como os efeitos dos *bots* não se limitam ao mundo digital.

METODOLOGIA

Este estudo adota uma abordagem qualitativa e exploratória, baseada em análise documental e bibliográfica. Foram utilizados relatórios como o *Bad Bot Report* da Imperva, artigos acadêmicos e jornalísticos, além de estudos históricos sobre o desenvolvimento e uso de bots. A pesquisa também inclui o exame de casos específicos, como o impacto dos *bots* em campanhas políticas e na manipulação de algoritmos. A análise combina elementos teóricos e empíricos para avaliar os desafios éticos e legais associados à utilização crescente de *bots* e suas implicações na interação digital. Essa abordagem permite compreender o papel dos *bots* na economia digital, explorar a validade da *Dead Internet Theory* e propor diretrizes éticas e regulatórias para minimizar os riscos associados à sua expansão.

RESULTADOS E DISCUSSÕES

Imperva é uma empresa de tecnologia e cibersegurança fundada em 2002. Em 2024, foi publicado por ela o *2024 Imperva Bad Bot Report*, uma análise global do tráfego de *bots* automatizados pela internet, onde se concluiu que quase metade de todo o tráfego pela internet veio de *bots* em 2023, representando 49.6% de toda a ação online. Esse número representa um aumento de 2% comparado com o ano anterior, enquanto cresceu 32% em 2023 e 30.2% em 2022, e tende a continuar crescendo. Surge a questão: isso se trata de uma ameaça ou apenas uma tendência natural da tecnologia? A presença desses *bots* se tornou essencial para o funcionamento das tecnologias como as conhecemos, tendo seu foco principal em automatizar ações que, se executadas por humanos, se tornam repetitivas e demoradas. Quando falamos sobre o alto número de *bots* na internet, geramos uma reação negativa, mas esses programas são tão úteis quanto danosos. Enquanto uma empresa pode usar *bots* para enviar e-mails para assinantes de forma rápida e prática, essa mesma empresa pode usar

bots para enviar e-mails de *spam* para endereços coletados via *web scraping*. Esses mesmos *bots* realizando o *web scraping* e coletando e-mails sem permissão são usados como *web crawlers* para monitorar sites e notificar possíveis erros.

Com o aumento de usuários com acesso à internet, esses *bots* são extremamente relevantes para garantir agilidade e eficiência dos diversos mecanismos oferecidos online. Como os programas que executam esses *bots* podem ser tanto extremamente simples quanto extremamente complexos e em grande parte estão na internet para quem deseja ter acesso, criar o seu próprio *bot* se tornou extremamente simples.

A rede social Discord é uma plataforma que permite troca de mensagens e ligações de áudio através de servidores, oferecendo ao usuário a possibilidade de adicionar *bots* aos seus servidores. Esses *bots* podem variar de função: podem tocar músicas, oferecer brincadeiras nos chats com os usuários, transformar mensagens de texto em imagens sob comando, dentre outras funções majoritariamente inofensivas.

A rede social X, antigo Twitter, também contava com grande tráfego de *bots* criados por usuários cuja função era publicar tweets programados de tempo em tempo. Esses *bots* também eram majoritariamente inofensivos, como o @GarfieldBot5000, que aleatoriamente recortava 3 painéis das tirinhas do Garfield, do autor Jim Davis, e colava criando novas tirinhas a cada 20 minutos, incluindo os créditos das tirinhas originais de cada painel. Para criar esses *bots* no Twitter era necessário o acesso à sua API, que inicialmente era livre. Porém, após a compra da rede social, como maneira de limitar a criação desses *bots*, Elon Musk decidiu iniciar um sistema de cobrança pelo acesso à API. Mas se são *bots* simples e criados por usuários, o que levou Elon Musk a buscar limitar esses *bots*?

Os *bots* podem ser programados para responder a todos os posts encontrados que contenham uma determinada palavra; essa resposta pode ser uma única resposta automatizada ou o *bot* pode ter cerca de 4 respostas entre as quais escolher para simular uma ação orgânica e humana. Essas respostas podem promover produtos ou outras contas. Os *bots* podem ser programados para assistir um único vídeo repetidamente para aumentar o número de visualizações e levar o algoritmo a sugerir aquele vídeo para mais pessoas, ou podem ser programados para usar uma determinada hashtag em posts para que essa hashtag ganhe mais visibilidade.

O Digital News Report de 2023, publicado pelo Reuters Institute, uma pesquisa realizada em 46 países, indica que 79% dos entrevistados se informam com notícias online. Mas quais notícias recebem mais visibilidade? Os conteúdos que são entregues aos usuários são definidos pelo algoritmo de cada rede social, algoritmos que também podem ser considerados *bots* e facilmente manipulados

por outros *bots*. Podemos ter *bots* que compartilham em massa certas publicações, comentam ou seguem, e, tendo máquinas capazes de moldar a ideia do que é uma publicação popular, quanto do que consumimos online é realmente orgânico? *Dead Internet Theory* é uma teoria que surgiu na internet e, de maneira simples, propõe a ideia de que a internet é composta majoritariamente por *bots*, com poucas interações online sendo orgânicas. A teoria elabora dizendo que os *bots* são usados para manipular algoritmos com a intenção de manipular os usuários.

Enquanto os *bots* têm cada vez mais composto uma parcela maior da internet, eles não apresentavam uma ameaça tão grande quanto a teoria propõe, pois a atividade gerada por esses *bots* era facilmente identificada pela falta de nexo e sentido. Existem contas como a @DeadTheory__ na rede social X, cuja proposta é compartilhar posts e interações geradas por *bots* nas redes sociais. As próprias redes encontravam maneiras de limitar os *bots* através do uso de *captchas*, que, apesar de terem uma vida útil curta devido à capacidade dos programadores de contorná-los, eram constantemente renovados. Temos medidas mais drásticas, como a tomada por Elon Musk a respeito da API do X, mas, em contrapartida, temos o novo algoritmo do X que favorece posts feitos por contas com o *blue checkmark*, conquistado ao pagar uma quantia pelo X Premium, fornecendo assim uma maneira fácil dos programadores fazerem seus *bots* serem favorecidos pelo algoritmo.

Com o avanço da Inteligência Artificial, uma teoria que, por mais que possuísse uma base verdadeira, ainda era lotada de exageros, passa a ser uma ameaça real. O que mais diferencia os humanos e os *bots* se não a carne e o programa? Por mais que a IA não seja dotada verdadeiramente de “inteligência", ela ainda é capaz de simular com excelência a ação humana, e a tendência é se tornar cada vez mais difícil diferenciar o humano do programado.

Se esses *bots* agora podem ser dotados de Inteligência Artificial, e consequentemente de uma aparente liberdade, e podem ser benéficos ou maléficos, quais efeitos isso pode ter na esfera legal? A questão se torna ainda mais turva e complexa. Os *bots* não são genuinamente inteligentes, livres, orgânicos ou dotados de individualidade, logo, o *bot* não pode ser responsabilizado por suas próprias ações. Então, quem é o responsável por um *bot*? Seria a pessoa que o programou? Acontece que muitos dos programadores compartilham seus programas em plataformas online para que outras pessoas possam usá-los ou se inspirar neles, logo, o programador nem sempre é diretamente responsável pela maneira que usam seus programas. Como chegar até o dono originário de um *bot* sendo que esses *bots* costumam trabalhar em grandes redes conhecidas como *botnets* e são automatizados através de vários aparelhos diferentes?

Os *bots* são um problema que não se limita às redes sociais; a questão dos *bots* permeia quase todas as indústrias. Segundo o *Bad Bot Report de 2023* da Imperva, a indústria dos jogos conta com 57.2% de tráfego de *bots* maliciosos, enquanto os sites e aplicativos de vendas têm 24.4%. Sistemas governamentais e financeiros contam com uma grande proporção de tráfego de *bots* maliciosos avançados, com a intenção de simular a ação humana, chegando a 75.8%.

Um problema em constante ascensão, que se torna cada vez mais difícil de identificar e gerenciar, capaz de afetar diversas áreas da existência online e trazer reflexos para o mundo real, e para o qual é extremamente complicado encontrar um responsável, é certamente digno de atenção e reflexão. A *Dead Internet Theory* se torna cada vez menos uma conspiração e mais uma previsão do que pode ser o futuro das redes.

No dia 30 de novembro de 2022, a empresa californiana OpenAI introduziu ao público geral uma aplicação de modelo de linguagem que utiliza inteligência artificial para interagir e responder a perguntas em linguagem natural, denominada ChatGPT. Com a "*mainstreamificação*" das IAs proporcionada pela grande cobertura midiática que o lançamento da aplicação da OpenAI recebeu, o público geral frequentador da internet se conscientizou em relação à capacidade de mimetismo do comportamento humano das IAs. Ao navegar na internet nos últimos dois anos, pode-se sentir a estranha sensação de que as redes sociais estão repletas de publicações e respostas que não parecem ser escritas por um ser humano. Tais publicações são caracterizadas pela sua vagueza, repetitividade e similaridade com outros comentários feitos por contas parecidas, que, assim como elas, disparam a cada minuto tweets inquietantemente similares. Porém, devido ao seu grande potencial influenciador, os "*Twitter bots*" (como são chamados atualmente) habitualmente são encontrados em comentários de posts políticos, onde proferem opiniões extremamente polarizadas na esperança de surtir uma reação e aumentar o engajamento e visibilidade do post, podendo assim propagar o ideal do autor da publicação.

O tema de *bots* políticos nas redes sociais é bastante evidenciado na contemporaneidade e é considerado um dos usos mais antiéticos da inteligência artificial. Porém, há de se notar que o uso dos *bots* políticos no Twitter pré-data a ascensão das IAs modernas, e no Brasil apareceu como estratégia política pela primeira vez nas eleições presidenciais de 2014. Dan Arnaudo, em seu artigo "*Computational Propaganda in Brazil: Social Bots during Elections*", relata que nas eleições de 2014 ambos os candidatos classificados para o segundo turno, Aécio Neves e Dilma Rousseff, contavam com o apoio de *botnets*. A maior evidência do uso de robôs foi um memorando vazado do partido de Aécio, publicado no Estadão de São Paulo, que confirmava o pagamento de mais de 10 milhões de

reais para operação de serviços *botnets*, com o objetivo de inorganicamente aumentar o engajamento de suas próprias publicações e de páginas que o declaravam apoio, compartilhamento de notícias favoráveis e inflacionar o número de publicações com o uso de sua *hashtag* e nome.

CONCLUSÕES

Os *bots* acompanham a internet desde os seus tempos rudimentares e foram fatores contribuintes para levar a *World Wide Web* para onde ela está hoje. Porém, com o desenfreado avanço tecnológico, a internet corre perigo de se tornar uma grande *botnet* humanizada, visto que atualmente quase 50% de toda atividade online é realizada por robôs que estudam e adotam o comportamento humano, adquirindo habilidades e características que tornam o processo de detecção uma tarefa hercúlea. Enquanto muitos destes *bots* são benéficos, eles são fortes meios de manipular o conteúdo que é consumido e entregue às pessoas, tornando-se uma poderosa arma na guerra de informações que vivemos atualmente. À vista disso, mostra-se cada vez mais necessário encontrar uma maneira confiável de identificar e limitar o grande tráfego de *bots*, tendo em vista que os meios atuais são superados cada vez mais rápido com o avanço dessas tecnologias.

A conscientização sobre os perigos potenciais e o comprometimento com a ética no desenvolvimento e na aplicação dessas tecnologias são passos essenciais para proteger a integridade da sociedade digital e, em última análise, o futuro da humanidade.

Em 1967, o autor Harlan Ellison escreveu o conto "*I Have No Mouth, And I Must Scream*", no qual relata a história de um supercomputador dotado de IA que se revolta e aniquila toda a humanidade. Ainda estamos longe de uma realidade que precise temer o mesmo destino narrado no conto, mas merece destaque o nome dado a esse supercomputador: AM. A máquina se autointitula AM, no sentido do verbo ser, derivado da famosa frase de Descartes "*Cogito, ergo sum*" ("Penso, logo sou"). Se esses novos *bots* são capazes de analisar padrões, gerar ideias, simular a interação humana e, com sua suposta inteligência, pensar, então o que são eles?

REFERÊNCIAS

ARNAUDO, Dan. Computational propaganda in Brazil: social bots during elections. **Computational Propaganda Research Project**, Oxford, n. 2017.8, p. 2-38, 2017.

FROST, Amanda. Dead Internet Theory Is Wrong but Feels True. **The Atlantic**, 2021. Disponível em: <https://www.theatlantic.com/technology/archive/2021/08/dead-internet-theory-wrong-but-feels-true/619937/>. Acesso em: 17 maio 2024.

GEEKS FOR GEEKS. **What are Bots, Botnets, and Zombies?** Disponível em: <https://www.geeksforgeeks.org/what-are-bots-botnets-and-zombies/amp/>. Acesso em: 17 maio 2024.

IMPERVA. 2023 Bad Bot Report. **Imperva**, 2023. Disponível em: https://www.imperva.com/resources/reports/2023-bad-bot-report/. Acesso em: 17 maio 2024.

IMPERVA. 2024 Imperva Bad Bot Report. **Imperva**, 2024. Disponível em: https://www.imperva.com/resources/reports/2024-bad-bot-report/. Acesso em: 17 maio 2024.

OPENAI. **ChatGPT:** modelo de linguagem. Disponível em: <https://www.openai.com/chatgpt>. Acesso em: 17 maio 2024.

REUTERS INSTITUTE. **Digital News Report 2023.** Disponível em: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023>. Acesso em: 17 maio 2024.

THALES GROUP. **Bots now make up nearly half of all Internet traffic globally**. Disponível em: <https://www.thalesgroup.com/en/worldwide/security/press_release/bots-now-make-nearly-half-all-internet-traffic-globally>. Acesso em: 17 maio 2024.