ISSN: 2358-8829

INTELIGÊNCIA ARTIFICIAL E CIBERCRIMES: um estudo dos desafios da Linguística Forense na era das mídias sociais

Sinthia Moreira Silva[1]
Eliana Crispim França Luquetti [2]
Emanoelly Carvalhal Ferreira [3]
Raquel França Freitas [4]

RESUMO
Vive-se na era das comunicações eletrônicas e a cada dia que passa, o mundo digital está mais presente na sociedade. Com isso, diversos mecanismos são desenvolvidos para otimizar os processos em geral. Dessa forma, dentre as novas possibilidades para suprir tais demandas, tem-se a criação da Inteligência Artificial (IA) que são capazes de criar, simular capacidades humanas, processamento de linguagem natural, entre outros, sendo usadas cada vez mais em todas as áreas de conhecimento. Com essa evolução, aumentaram-se os crimes virtuais e muitos utilizam da IA na utilização como ferramenta para a criminalidade na criação de uma figura, voz ou criação de um texto falso controlado pela IA. O objetivo desta pesquisa é fazer um estudo bibliográfico dentre os desafios que a linguística forense encontra mediante o mundo tecnológico em que se encontra, no qual muitas pessoas utilizam deste recurso para praticar crimes virtuais, uma vez que se torna mais complexo detectar e impedir esse tipo de técnica que trabalha com evidências que podem ser encontradas e analisadas para se compreender o contexto que a envolve, implicando numa reformulação de várias áreas forenses. Para sua construção, utilizou-se pesquisas bibliográficas, de natureza básica e abordagem qualitativa, tendo como principais teóricos Levy (2017), Machado (2022), Rosa (2002), (Colares, 2016), dentre outros, cujas fontes teóricas embasam na busca de respostas sobre o tema abordado. Percebe-se que devido as transformações na era digital, uma das áreas bastante impactada é a linguística forense, que está ligada à investigação criminal.

Palavras-chave: Inteligência Artificial, Linguística Forense, Cibercrimes, Desafios.

INTRODUÇÃO

Nos últimos tempos, o mundo testemunhou um avanço tecnológico sem precedentes, que trouxe uma revolução nas interações humanas e na maneira como as atividades são conduzidas. Entre essas transformações notáveis, está a ascensão da

[1] Doutoranda no Curso de Cognição e Linguagem pela Universidade Estadual do Norte Fluminense Darcy Ribeiro, sinthia_moreira@hotmail.com.
[2] Doutora e Mestra em Linguística pela Universidade Federal do Rio de Janeiro (UFRJ), elinafff@uenf.br.
[3] Mestranda no Curso de Cognição e Linguagem pela Universidade Estadual do Norte Fluminense Darcy Ribeiro, emanoellycarvalhal.ferreira@gmail.com.
[4] Doutoranda no Curso de Cognição e Linguagem pela Universidade Estadual do Norte Fluminense Darcy Ribeiro, raquelfreitas_@hotmail.com.

ISSN: 2358-8829

inteligência artificial (IA), que promete transformar vários setores e enfrentar desafios complexos em diversos campos.

No entanto, à medida que a inteligência artificial se torna uma presença mais proeminente em nossa sociedade, suas aplicações não estão isentas de dilemas e riscos, com um dos campos mais impactados sendo o da segurança cibernética. Outrossim, a intersecção da inteligência artificial com crimes cibernéticos apresenta um cenário complexo e em evolução, onde as implicações das aplicações de IA para fins maliciosos levantam preocupações significativas para a segurança digital, privacidade e integridade das informações.

Portanto, identificar uma deficiência legislativa significativa no Brasil, onde muitos desses comportamentos ainda não são definidos pela lei e encontram muitas brechas nela, a qual dá origem a uma forte sensação de impunidade no ambiente online. Ao mesmo tempo, o Legislativo não consegue acompanhar os desenvolvimentos cibernéticos, resultando em uma estrutura legal cada vez mais desatualizada e ineficaz.

O objetivo desta pesquisa é fazer um estudo bibliográfico dentre os desafios que a linguística forense encontra mediante o mundo tecnológico em que se encontra, no qual muitas pessoas utilizam deste recurso para praticar crimes virtuais, uma vez que se torna mais complexo detectar e impedir esse tipo de técnica que trabalha com evidências que podem ser encontradas e analisadas para se compreender o contexto que a envolve, implicando numa reformulação de várias áreas forenses. Para sua construção, utilizou-se pesquisas bibliográficas, de natureza básica e abordagem qualitativa, tendo como principais teóricos Levy (2017), Machado (2022), Rosa (2002), (Colares, 2016), dentre outros, cujas fontes teóricas embasam na busca de respostas sobre o tema abordado

Inteligência artificial e cibercrimes

A tecnologia está avançando e se tornando cada vez mais indispensável no dia a dia. Sua facilidade e rapidez têm promovido grandes revoluções, pois o indivíduo não precisa se deslocar para tal fim. Uma vez que com essa ferramenta, é possível se comunicar com outras pessoas e até mesmo realizar suas atividades básicas, como efetuar pagamento de contas, realizar compras online, estudar, reservar hotéis, entre outros. conforme aponta Levy (1997), que por meio dos canais de comunicação, tem-se a capacidade de replicar e difundir símbolos de maneira automática. Pois, esse modelo

ISSN: 2358-8829

comunicativo serviu como fundamento para as revoluções científica, industrial, democrática e várias outras.

Com isso, o panorama dos crimes cibernéticos avançou significativamente nas últimas décadas, transitando de ataques isolados de hackers para operações criminosas altamente sofisticadas, geralmente organizadas em redes globais. Assim, a inteligência artificial, com sua habilidade de reconhecer padrões complexos, processar grandes quantidades de dados e realizar tarefas de forma autônoma, oferece uma nova perspectiva a esses crimes.

Além disso, a produção de deepfakes - conteúdos multimídia sintéticos e extremamente realistas gerados por algoritmos de IA - resultou em um aumento na propagação de desinformação e calúnias. A capacidade de gerar vídeos ou áudios autênticos de pessoas fictícias ou reais fazendo declarações que nunca proferiram pode comprometer a confiança nas informações disponíveis online e danificar reputações de maneira sem precedentes, conforme aponta Machado (2022).

Outrossim, De acordo com o autor, embora a principal ênfase do deepfake seja a substituição de rostos em vídeos, é um equívoco acreditar que essa prática se limite apenas a essa aplicação. Essa técnica é igualmente utilizada na manipulação de áudios, permitindo a criação de gravações que imitam a voz de indivíduos específicos. Esse tipo de deepfake pode ser facilmente disseminado através de aplicativos de mensagens, como o WhatsApp (Machado, 2022).

Além disso, o autor afirma que já pode ser observado a ascensão dos deepfakes textuais, nos quais a inteligência artificial é empregada para gerar textos; os deepfakes em redes sociais, que originam perfis falsos na internet; e até mesmo os deepfakes em tempo real, que possibilitam a modificação de rostos durante transmissões ao vivo. Um exemplo notável dessa técnica é o software DeepFaceLive (Machado, 2022).

Dessa forma, no Brasil, os cibercrimes tornaram-se uma preocupação crescente, em razão do rápido avanço tecnológico e da crescente digitalização da sociedade, no qual pode ser encontrado desde as fraudes financeiras e ataques de phishing, até a disseminação de malware e invasões de sistemas, uma variedade de atividades ilegais que ocorre no ambiente digital do país.

Em consonância com Rosa (2002), a internet trata-se de um conjunto de redes de computadores interconectadas globalmente, que compartilham um conjunto de protocolos e serviços, caracterizando-se pela operação por meio do sistema de troca de pacotes, onde as mensagens são divididas em pacotes, e cada pacote pode seguir uma rota

ISSN: 2358-8829

diferente para alcançar o mesmo destino. A autora afirma a operação em função dos protocolos ou sistemas de intercomunicação de programas, sendo os protocolos mais relevantes o TCP (Protocolo de Controle de Transferência) e o IP (Protocolo Internet), o que possibilita o uso da internet por computadores com qualquer sistema operacional (Rosa, 2002).

Entretanto, o que tem ocorrido de forma cada vez mais contínua é a utilização da internet de maneira imprópria pelas pessoas, sendo necessário reconhecer que, nesse contexto, ela gera “enormes riscos em termos de concentração e controle social”. daí porque a autorregulação do setor não é suficiente. Em que os direitos socialmente relevantes devem ser protegidos pelo Estado, que tem a função de agente assegurador das liberdades públicas e do mercado de consumo (Castro, 2003).

Em definição análoga, Cassanti (2014, p. 3) afirma que crime cibernético é toda a atividade de um computador ou uma rede de computadores utilizada como uma ferramenta, base de ataque ou como meio de crime, conhecida como crime cibernético. Em outros termos, que se referem a essa atividade é: crime informático, crimes eletrônicos, crime virtual ou crime digital.

Em consonância com Almeida (2015, p. 224), os crimes cibernéticos são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual utiliza o computador como sistema tecnológico sendo usado como objeto e meio para execução do crime.

Portanto, essas condutas ilícitas afetam bens jurídicos já protegidos, o que se trata de crimes tipificados, agora consumados com o uso de computadores e da rede. Assim, o sistema de informática e seus componentes servem como mais um meio para a prática do delito, diferenciando-se pela não essencialidade do computador para a concretização do ato ilícito, o qual pode ocorrer de outras maneiras, não necessariamente por meio da informática, para se atingir o resultado almejado (Almeida, 2015).

Destarte, em épocas no qual tudo se torna alvo de legislações punitivas, é essencial agir com bom senso e cautela ao considerar a criação de novos delitos. Todos estão exauridos de analisar a enxurrada de tipos penais em nosso ordenamento, os quais não trazem efetiva contribuição para o convívio harmonioso e para a promoção da paz social.

Logo, isso ocorre pela incriminação indiscriminada de condutas que, na maioria das vezes, deveriam ser tratadas por políticas sociais mais cuidadosas e nas esferas civil e administrativa, relegando o âmbito penal à ultima ratio, sempre debatida cientificamente, mas que, na prática, não é respeitada (Crespo, 2011).

ISSN: 2358-8829

Linguística Forense e crimes virtuais

A Linguística Forense é um campo que integra aspectos da linguagem, da comunicação e do direito. Sua importância tem crescido nas investigações criminais, pois contribui para a resolução de questões jurídicas, para a análise de provas e para a formulação de táticas de defesa ou acusação. Para os profissionais do direito, ter um entendimento profundo dos princípios e das utilizações da Linguística Forense pode ser essencial para uma atuação precisa em casos onde a comunicação verbal ou escrita é fundamental.

A partir das obras de Virginia Colares, é possível perceber como a Linguística Forense tem ganhado relevância no contexto judicial e de investigações. A autora busca promover a conscientização da sociedade sobre essa disciplina, explorando sua aplicação em situações que envolvem comunicação verbal ou escrita.

Assim, a Linguística Forense se destaca como um campo da linguística aplicada na análise de diversos casos, como bilhetes de suicídio, chamadas de emergência, mensagens ameaçadoras, cartas anônimas, verificação de plágio e textos legais, em resposta ao crescente número de crimes cibernéticos, incluindo mensagens e interações em redes sociais.

Outrossim, a investigação é realizada a partir dos traços linguísticos deixados, com a exclusão de unificando características comuns da língua, além dos aspectos normativos, o uso de nomes que caracterizam uma linguagem usuária de determinado grupo, ou que pretende parecer de algum indivíduo, como no caso de muitos bilhetes suicidas, que em muitos casos, quando pesquisados a fundo, são investigados como homicídio.

De acordo com Saussure (2006), a linguística é entendida como a ciência que tem como foco a linguagem humana, abrangendo seus aspectos fonéticos, morfológicos, semânticos, sintáticos, lexicais e pragmáticos, incluindo a descrição geral. Observa-se que a fala ocorre exclusivamente nos seres humanos e a linguagem é “um produto social da faculdade da linguagem e um conjunto de convenções necessárias adotadas pelo corpo social para permitir o exercício dessa faculdade nos indivíduos.

Em consonância com Magalhães e Oliveira (2016), o termo “forense” tem origem latina forenses, que significa foro ou fórum. Assim, ao entrar no vocabulário inglês, o conceito tornou-se mais voltado à área de investigação criminal.

ISSN: 2358-8829

Diante disso, quando os serviços de um linguista forense são solicitados no âmbito de uma investigação, é certo que o material a ser analisado é aquele que levanta dúvidas sobre o autor ou a mensagem pretendida pelo autor através daquele texto, normalmente curto e com poucas informações (Colares, 2016).

Na verdade, trata-se de uma investigação à parte, pois não analisa apenas as palavras nelas contidas, mas também examina o formato das letras, utiliza a grafologia, destaca termos e períodos, para chegar a uma conclusão excluindo certas informações e enfatizando outras. Não é tarefa do linguista forense decifrar palavras, mas sim interpretá-las. Assim, o significado de sentenças ou mesmo de palavras individuais pode ser de crucial importância em certos julgamentos (Colares, 2016).

Portando, é importante ressaltar que a análise da linguagem se baseia nos rastros deixados num modo interativo de comunicação. Esta análise baseia-se em estudos dos idioletos falados e escritos do contexto que requer exame. Geralmente estes idioletos são breves, exceto no caso de depoimentos que ocasionalmente podem ter uma duração mais longa. Os idioletos são uma forma de individualidade linguística, onde as particularidades de cada indivíduo variam de acordo com o seu contexto social e geográfico (Figueiredo, 2015).

De acordo com o autor, é necessária uma lupa para ampliar objetos, lápis, caderno para organização de dados; e o cérebro para se tornar um especialista, uma vez que o fator humano na expertise é essencial (Figueiredo, 2015).

Assim, tendo em vista o leque de possibilidades de técnicas e mecanismos de atribuição de autoria gerenciados pela Linguística Forense, articulados ao perfilamento criminal e considerando o cenário nacional de obstáculos à identificação de cibercriminosos, sempre há um vestígio deixado pelo indivíduo que praticou o crime, uma vez que cada pessoa tem suas características própria, ou seja, a sua identidade, no qual é possível identificar com a análise do linguista forense.

Portanto, o “Princípio da Transferência”, cunhado por Edmond Locard no início do século XX, afirmando que “todo contato deixa um rastro”, serviu de base para o desenvolvimento da Ciência Forense moderna (Chisum; Turvey, 2000). Estabelecendo que cada interação entre dois agentes – indivíduos, objetos e locais – produz alguma forma de evidência que pode ser identificada e examinada para compreender o contexto circundante.

Logo, os vestígios deixados no mundo físico, também se aplica ao mundo virtual, no qual o que antes havia vestígios como impressões digitais, pegadas ou sangue, agora

ISSN: 2358-8829

também entram em cena fotos, clipes de áudio/vídeo, postagens em mídias sociais, transações bancárias, registros de localização GPS, entre outros.

Condutas delituosas perpetradas através da Internet

Segundo a empresa de segurança na internet Symantec, 54 pessoas são vítimas de crimes cibernéticos no Brasil a cada minuto. Segundo relatório da Norton Cyber Security, em 2017, o Brasil se tornou o segundo país com maior número de casos de crimes cibernéticos, afetando aproximadamente 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões (Jusbrasil, 2014). Dado esse que tem ampliado a cada dia.

Perante este cenário, tornou-se essencial compreender não só o fenômeno dos crimes cibernéticos, virtuais ou informáticos, mas também as razões do aumento exponencial da criminalidade cibernética, seja a nível internacional ou nacional.

Em virtude do princípio da legalidade ou anterioridade do direito penal, a insuficiência ou ausência de disposições penais que tipifiquem os crimes digitais limita a função punitiva do Estado, pois afeta o sentimento de insegurança e impunidade, com repercussões negativas para a sociedade brasileira e, especificamente, para o comunidade internacional, que há mais de uma década chama a atenção para a necessidade e urgência de controlar e prevenir condutas criminosas no ciberespaço (Kunrath, 2017).

Uma vez que muitas pessoas são pgas de surpresa no dia a dia, com ligações telefonicas ou mensagens via whatsaap, a fim de conseguirem praticar algum crime. A expemplo, a autora toma como posse o caso de sua maiga que se esqueceu de efetuar o pagamento de um boleto bancário e depois de alguns dias recebeu a ligação relatando ser o funcionário do banco, o qual lhe encaminhou um novo boleto com o cvalor atualizado, para pagamento via pix, onde o dinheiro cairia na conta de terceiros e não do banco/finaceira.

Sendo evidente que a necessidade de tipificação desses crimes cibernéticos, porém, a criação de novas leis deve ser analisada com cautela, a fim de garantir que não só sejam estabelecidos, mas também implementados. Em termos de crimes cibernéticos, a legislação brasileira não acompanha os avanços tecnológicos.

Inúmeras tentativas têm sido feitas pelo legislador para especificar regras que garantam direitos no mundo virtual. Um exemplo é o projeto de lei 84/1999, que vigorou por 13 (treze) anos e tratou da responsabilidade dos provedores de serviços de internet. Originalmente composta por quatro artigos, foi posteriormente reduzida a dois artigos por

ISSN: 2358-8829

sanção, passando a ser a lei nº. 12. 735/12. Esta lei introduziu duas modificações: a primeira determinou a criação de escritórios em cada estado para combater o crime cibernético, e a segunda teve como objetivo remover conteúdos racistas de qualquer meio de comunicação (Silva, 2017).

Nos últimos anos, o Brasil tem se apoiado nas seguintes regulamentações: Lei nº 12. 735/2012 (Lei Azeredo), Lei nº 12. 737/2012 (Lei Carolina Dieckmann) e Lei nº 12. 965/2014 (Internet Marco Civil). Esta, que veio com o intuito de ratificar as garantias constitucionais, não abordando qualquer conduta criminosa, visando apenas ser reconhecida como Constituinte da Internet brasileira. Seu amplo conteúdo abrange vários pontos relevantes sobre direitos e garantias (Silva, 2017).

De acordo com o G1, mais de 50 mil casos de estelionatos foram cometidos via WhatsApp e Instagram, apenas no estado de Minas Gerais, no ano 2022, tendo um prejuízo estimado de R$ 32 bilhões em todo o país (Zuba, 2023). O que traz um alerta para o Estado da necessidade em trazer maiores concretizações e atualizações das leis existentes com relação aos crimes virtuais a fim de estarem minimizando esses dados.

Ademais, a Linguística Forense parte de métodos convencionais de resolução de crimes revelam-se ineficazes quando aplicados aos cometidos exclusiva ou parcialmente através da linguagem, no âmbito virtual, surgindo como uma ferramenta particularmente significativa para a investigação destes crimes cibernéticos sendo uma área especializada que trata do assunto.

Logo, com base nos números apresentados relativos aos crimes cometidos total ou parcialmente através da linguagem, como calúnia, injúria, difamação, ameaça, fraude e extorsão, além de outros crimes, a Linguística Forense em todo o mundo é capaz de identificar o autor por meio de suas técnicas que envolve a linguística, trabalhando com a escrita e oralidade, identificando as identidades encontradas nas ligações e textos encaminhados pelos praticantes dos crimes.

Conclusão

Diante das análises apresentadas ao longo do trabalho, o tema abordado é de suma importância. Os crimes cibernéticos constituem um fenômeno jurídico recente. Essa modalidade criminosa vem se disseminando e causando diversos problemas. Consequentemente, o ordenamento jurídico brasileiro não acompanhou esse desenvolvimento, gerando perigosas lacunas legislativas que devem ser sanadas para

ISSN: 2358-8829

garantir maior segurança na abordagem punitiva desses crimes. Portanto, a dificuldade se torna aparente nesse âmbito virtual, pois a definição do crime se torna desafiadora para identificação, o território, ou melhor, o ciberespaço é vasto, sem limites territoriais, dificultando assim sua jurisdição, ou mesmo o autor, e ainda possibilitando que esses indivíduos utilizem o anonimato para atingir seu objetivo causando danos a terceiros, além de profissionais competentes para auxiliar nessa investigação/busca.

Dessa forma, é quase impossível identificar o indivíduo responsável pelo crime por meio de dispositivos eletrônicos. É evidente que a formação de profissionais nessa área é prioritária no contexto brasileiro; lamentavelmente, poucos estudantes optam por trilhar esse caminho, tanto no âmbito jurídico quanto no linguístico. O compartilhamento de conhecimento e experiências de ambas as áreas contribui significativamente para a educação das novas gerações, bem como para as práticas acadêmicas e profissionais.

Assim, a Linguística Forense serve como um canal crucial para a troca de conhecimento entre as duas áreas, e deve ser estudada com grande prioridade e respeito na sociedade contemporânea.

Portanto, pode-se concluir que a principal legislação que tipifica esses tipos de comportamentos ilícitos, os crimes cibernéticos, no Brasil, ainda são carentes, com muitas lacunas, devido ao fato de não ser constantemente atualizada com os avanços.

Assim, é necessário que nosso sistema jurídico comece a acelerar esses desenvolvimentos, pois a cada dia esses tipos de crimes são cada vez mais cometidos, permanecendo impunes. Por favor, reescreva o texto em um tom formal. Lembre-se de incluir duas quebras de linha quando necessário.

REFERÊNCIAS

ALMEIDA, Jéssica de Jesus. *et al*. Crimes cibernéticos. **Periódicos Grupo Tiradentes**, v. 2, n.3. p. 215-236, 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>. Acesso em: 24 set. 2024.

CASSANTI, Moises de Oliveira Cassanti. **Crimes Virtuais, Vítimas reais**. São Paulo: Brasport. 2014.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus aspectos processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2001.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

ISSN: 2358-8829

CHISUM, W. J.; TURVEY, B. Evidence dynamics: Locard's exchange principle & crime reconstruction. **Journal of Behavioral Profiling**, v.1, n.1, p.1-15, 2000.

JUSBRASIL. **Brasil registra 54 crimes virtuais por minuto**. 2014. Disponível em: https://www.jusbrasil.com.br/noticias/brasil-registra-54-crimes-virtuais-por-minuto/3125198. Acesso em: 18 out. 2024.

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

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

MACHADO, Amanda. **O que é deepfake e por que você deveria se preocupar**.2022. Disponível em: https://tecnoblog.net/responde/o-que-e-deep-fake-e-porque-voce-deveria-sepreocupar-com-isso/. Acesso em: 01 de agosto de 2024.

MAGALHÃES, Teresa; OLIVEIRA, Ricardo Jorge Dinis. **Introdução às ciências forenses**. *In*. MAGALHÃES, Teresa; OLIVEIRA, Ricardo Jorge Dinis. O que são as ciências forenses. Venda do Pinheiro: Pactor, 2016.

ROSA, Fabrizio. **Crimes de Informática**. Campinas, Bookseller, 2002.

SAUSSURE, Ferdinand de. **Curso de linguística geral**. 27ed. São Paulo: Cultrix, 2006.

SILVA, Rui. **Linguagem e Direito**: os eixos temáticos. Recife: ALIDI, 2017.

ALVES, Virgínia Colares Soares Figueiredo. **Inquirição na Justiça**: Estratégias Linguístico-Discursivas. Porto Alegre: Sérgio Antônio Fabris, 2003.

ZUBA, Fernando. Mais de 50 mil estelionatos foram cometidos por WhatsApp e Instagram em Minas Gerais, no ano passado, diz MP. **G1**. 2023. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2023/02/07/mais-de-50-mil-estelionatos-foram-cometidos-por-whatsapp-e-instagram-em-minas-gerais-no-ano-passado-diz-mp.ghtml. Acesso em: 12 out. 2024.