

الموضوع البحث

دور الذكاء الاصطناعي في ارتكاب الجرائم المعلوماتية ومكافحتها

The Role of Artificial Intelligence in Committing and Combating Cybercrime

الاسم: ريناد حسن عثمان ششه

التخصص: ماجستير القانون الرقمي

الجامعة: جامعة ميدأوشن

الباحث المعتمد للمراسلة: (253002271@st.midocean.edu.km)

الملخص

هدفت هذه الدراسة إلى بيان دور الذكاء الاصطناعي في ارتكاب الجرائم المعلوماتية ومكافحتها، مع تحليل طبيعته المزدوجة كأداة يمكن استخدامها في النشاط الإجرامي أو في مكافحته. وقد أدى التطور التقني المتسارع إلى ظهور أنماط جديدة من الجرائم المعلوماتية تعتمد على تقنيات الذكاء الاصطناعي، مثل الهجمات الاحتيالية المتطورة، وتقنيات التزييف العميق، والاختراقات المؤتمتة.

واعتمدت هذه الدراسة المنهج التحليلي المقارن من خلال تحليل النصوص القانونية والدراسات الحديثة، ومقارنة بعض التجارب الدولية في استخدام الذكاء الاصطناعي في مواجهة الجرائم المعلوماتية. كما تناولت الدراسة أبرز التطبيقات الإجرامية للذكاء الاصطناعي، إلى جانب دوره في تعزيز الأمن السيبراني وتحليل الأدلة الرقمية.

وتوصلت الدراسة إلى مجموعة من النتائج، من أهمها أن الذكاء الاصطناعي أسهم في تعقيد الجرائم المعلوماتية وزيادة صعوبة اكتشافها، في الوقت الذي يوفر فيه أدوات متقدمة للجهات الأمنية في التنبؤ بالجرائم وتحليلها.

وخلصت الدراسة إلى ضرورة تطوير التشريعات القانونية لمواكبة هذه التحديات، وتعزيز التعاون الدولي، وتبني حلول تقنية متقدمة لضمان الاستخدام الآمن للذكاء الاصطناعي.

Abstract

This study aimed to examine the role of artificial intelligence in both committing and combating cybercrime, highlighting its dual nature as a tool that can be used for criminal activities or for prevention. Rapid technological development has led to the emergence of new forms of cybercrime that rely on artificial intelligence technologies, such as advanced fraud attacks, deepfake techniques, and automated hacking

The study adopted a comparative analytical approach by analyzing legal texts and recent studies, as well as comparing selected international experiences in using artificial intelligence to combat cybercrime. It also addressed major

criminal applications of artificial intelligence alongside its role in enhancing cybersecurity and digital forensic analysis

The study found that artificial intelligence has contributed to increasing the complexity of cybercrimes and making them more difficult to detect, while at the same time providing advanced tools for authorities to predict and analyze crimes.

The study concluded that there is a need to develop legal frameworks to keep pace with these challenges, strengthen international cooperation, and adopt advanced technological solutions to ensure the safe use of artificial intelligence.

المقدمة

شهد العالم في السنوات الأخيرة تطورًا هائلًا في تقنيات الذكاء الاصطناعي، مما أدى إلى تغييرات جذرية في مختلف المجالات، بما في ذلك المجال القانوني والأمني. وقد ساهم هذا التطور في تحسين كفاءة الأنظمة الرقمية، إلا أنه في المقابل أتاح فرصًا جديدة لارتكاب الجرائم المعلوماتية بطرق أكثر تعقيدًا واحترافية.

وأصبحت الجرائم المعلوماتية المدعومة بالذكاء الاصطناعي تشكل تهديدًا حقيقيًا للأفراد والمؤسسات، حيث يستخدم المجرمون تقنيات متقدمة مثل التزييف العميق والهجمات الاحتيالية الذكية، مما يزيد من صعوبة اكتشافها أو تتبع مرتكبيها.

وفي المقابل، برز دور الذكاء الاصطناعي كأداة فعالة في مكافحة هذه الجرائم من خلال تحليل البيانات الضخمة، والتنبؤ بالهجمات، وتعزيز قدرات التحقيق الجنائي الرقمي

Introduction

In recent years, the world has witnessed significant advancements in artificial intelligence technologies, leading to fundamental changes across various fields, including the legal and security sectors. This development has contributed to improving the efficiency of digital systems; however, it has also created new opportunities for committing cybercrimes in more complex and sophisticated ways

AI-powered cybercrimes have become a real threat to individuals and institutions, as criminals use advanced techniques such as deepfakes and intelligent fraud attacks, making them more difficult to detect or trace

On the other hand, artificial intelligence has emerged as an effective tool in combating such crimes through big data analysis, prediction of cyberattacks, and enhancing digital forensic investigations

مشكلة الدراسة

تتمثل مشكلة الدراسة في تزايد استخدام الذكاء الاصطناعي في ارتكاب الجرائم المعلوماتية، مقابل قصور التشريعات القانونية الحالية عن مواكبة هذا التطور.

Research Problem

The research problem lies in the increasing use of artificial intelligence in committing cybercrimes, alongside the inadequacy of current legal frameworks to keep pace with this rapid development

أسئلة الدراسة

- ١- ما مفهوم الذكاء الاصطناعي وعلاقته بالجرائم المعلوماتية؟
- ٢- ما أبرز صور الجرائم المعلوماتية المرتكبة باستخدام الذكاء الاصطناعي؟
- ٣- ما دور الذكاء الاصطناعي في مكافحة الجرائم المعلوماتية؟
- ٤- ما التحديات القانونية المرتبطة باستخدام الذكاء الاصطناعي؟
- ٥- ما الحلول المقترحة لتعزيز مكافحة هذه الجرائم؟

Research Questions

What is the concept of artificial intelligence and its relationship to cybercrime?

What are the main forms of cybercrimes committed using artificial intelligence?

What is the role of artificial intelligence in combating cybercrime?

What are the legal challenges associated with the use of artificial intelligence?

What are the proposed solutions to enhance the fight against such crimes?

أهداف الدراسة

- بيان مفهوم الذكاء الاصطناعي والجرائم المعلوماتية
- تحليل دور الذكاء الاصطناعي في الجريمة
- توضيح دوره في مكافحة
- إبراز التحديات القانونية
- تقديم حلول وتوصيات

Research Objectives

- To define artificial intelligence and cybercrime
- To analyze the role of artificial intelligence in crime
- To clarify its role in combating cybercrime
- To highlight legal challenges
- To propose solutions and recommendations

منهجية الدراسة

اعتمدت الدراسة على المنهج التحليلي المقارن من خلال تحليل النصوص القانونية والدراسات الحديثة ومقارنتها.

Research Methodology

The study adopted a comparative analytical approach by analyzing relevant legal texts and recent studies and comparing them

الخطوة البحثية

المبحث الأول: الذكاء الاصطناعي والجرائم المعلوماتية

المطلب الأول: مفهوم الذكاء الاصطناعي

الفرع الأول: تعريف الذكاء الاصطناعي

هو مجموعة من التقنيات التي تمكن الأنظمة من محاكاة الذكاء البشري.

الفرع الثاني: خصائصه

السرعة، الدقة، التعلم الذاتي.

المطلب الثاني: الجرائم المعلوماتية

الفرع الأول: تعريفها

هي الجرائم التي ترتكب باستخدام الحاسب أو الإنترنت.

الفرع الثاني: خصائصها

عابرة للحدود وصعبة الإثبات.

المبحث الثاني: دور الذكاء الاصطناعي في الجريمة والمكافحة

المطلب الأول: دور الذكاء الاصطناعي في ارتكاب الجرائم

• التزييف العميق (Deepfake)

• الاحتيال الإلكتروني الذي

• الهجمات السيبرانية المؤتمتة

وقد أظهرت الدراسات أن الذكاء الاصطناعي يُستخدم في إنشاء هجمات تصيد احتيالي دقيقة جدًا يصعب اكتشافها، كما تُستخدم تقنيات التزييف العميق في الإساءة للأفراد وانتحال الهوية الرقمية.

المطلب الثاني: دور الذكاء الاصطناعي في مكافحة الجرائم

• تحليل البيانات الضخمة

• كشف الجرائم

• التنبؤ بالهجمات

وتساعد تقنيات الذكاء الاصطناعي في تحليل الأدلة الرقمية وتحسين كفاءة التحقيقات الجنائية.

كما يتم استخدامه في أنظمة أمنية متقدمة للتنبؤ بالجريمة وتحليلها .

Research Plan

Chapter One: Artificial Intelligence and Cybercrime

Section One: Concept of Artificial Intelligence

First Branch: Definition of Artificial Intelligence

Artificial intelligence refers to a set of technologies that enable systems to simulate human intelligence

Second Branch: Its Characteristics

Speed, accuracy, and self-learning

Section Two: Cybercrime

First Branch: Definition

Cybercrime refers to crimes committed using computers or the internet

Second Branch: Characteristics

They are transnational and difficult to prove

Chapter Two: The Role of Artificial Intelligence in Crime and Prevention

Section One: The Role of AI in Committing Crimes

Deepfake

Intelligent online fraud

Automated cyberattacks

Studies have shown that artificial intelligence is used to create highly sophisticated phishing attacks that are difficult to detect. Additionally, deepfake technologies are used to harm individuals and impersonate digital identities

Section Two: The Role of AI in Combating Crimes

Big data analysis

Crime detection

Attack prediction

Artificial intelligence technologies help in analyzing digital evidence and improving the efficiency of criminal investigations

They are also used in advanced security systems to predict and analyze crimes.

الخاتمة

وفي الختام، يتضح من هذه الدراسة أن الذكاء الاصطناعي يمثل سلاحًا ذا حدين في مجال الجرائم المعلوماتية، إذ يُستخدم في ارتكاب جرائم متطورة مثل الاحتيال والتزييف العميق، وفي الوقت ذاته يساهم في مكافحتها من خلال تحليل البيانات والكشف المبكر عن التهديدات. كما أظهرت الدراسة وجود تحديات قانونية في مواكبة هذا التطور التقني.

وعليه، تبرز أهمية تطوير التشريعات وتعزيز التعاون الدولي، إلى جانب توظيف تقنيات الذكاء الاصطناعي في المجال الأمني، للحد من هذه الجرائم وتحقيق بيئة رقمية آمنة

Conclusion

In conclusion, this study shows that artificial intelligence represents a double-edged sword in the field of cybercrime. It is used in committing advanced crimes such as fraud and deepfake, while also contributing to combating them through data analysis and early threat detection. The study also highlighted legal challenges in keeping up with technological developments

Accordingly, there is a need to develop legal frameworks, strengthen international cooperation, and employ artificial intelligence technologies in the security field to reduce cybercrimes and ensure a safe digital environment.

النتائج

- الذكاء الاصطناعي سلاح ذو حدين
- يزيد من تعقيد الجرائم
- يساهم في مكافحتها
- وجود قصور تشريعي

Results

- Artificial intelligence is a double-edged sword
- It increases the complexity of cybercrimes
- It contributes to combating cybercrimes
- There is a legislative gap

التوصيات

- تطوير التشريعات
- تعزيز التعاون الدولي
- نشر الوعي
- استخدام تقنيات حديثة في الأمن السيبراني

Recommendations

- Develop legal frameworks
- Strengthen international cooperation
- Raise public awareness
- Use modern technologies in cybersecurity

قائمة المراجع

- الشمري، ف. (٢٠٢٣). دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية. مجلة الدراسات الأمنية، ١٢ (٢)، ٧٧-١٠٢.
- الحربي، س. (٢٠٢١). الجرائم المعلوماتية في ظل التطور التقني. الرياض: مكتبة القانون.
- الهيئة الوطنية للأمن السيبراني. (٢٠٢٣). إطار الأمن السيبراني السعودي.

References

- Al-Shammari, F. (2023). The Role of Artificial Intelligence in Combating Cyber Crimes. Journal of Security Studies, 12(2), 77-102
- Al-Harbi, S. (2021). Cyber Crimes in Light of Technological Development Riyadh: Law Library
- National Cybersecurity Authority. (2023). Saudi Cybersecurity Framework