People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Ibn Khaldoun University of Tiaret

Faculty of Law and Political Science

Department of Law

Proving Cyber-Crime Using Modern Technology: Artificial Intelligence as A Model

Dissertation submitted in Partial fulfillment for Master's Degree in Criminal Law

Submitted by:

- **Mr.** Abdelkader **BENSAID**
- **Ms.** Hafidha **DRAOUI**

Supervised by:

- **Dr.** Samir BERDAL

Board of examiners:

- **Prof.** Leila **KAID**	**Professor**	**Ibn Khaldoun University of**
- **Dr.** Kheira **ABDELSADOUK**	**Doctor**	**Ibn Khaldoun University of**
- **Dr.** Farid **BOUABDELLAH**	**Doctor**	**Ibn Khaldoun University of**

Academic Year: 2023/2024

Dedication

I express my gratitude.

To all those who have supported me throughout this educational journey.

With heartfelt memories,

I dedicate the fruits of my hard work to my beloved parents and extended family. To the companions who walked alongside me, contributing to our shared success, and to my friends and colleagues during my university studies, I extend my deepest appreciation. Lastly, to all those who have positively impacted my life, my heart holds gratitude, and my pen gifts you this graduation.

Thank you.

Acknowledgments

We would like to express our special thanks of gratitude to our teacher

Mr. Samir Berdal who gave us the Golden opportunity to do this wonderful work, we are really thankful to him, secondly, we would also like to thank our parents and friends who helped us a lot to finalizing this work

Thank you

Abstract

Artificial intelligence (AI) is rapidly reshaping the landscape of cybercrime, presenting a complex scenario with both immense promise and chilling peril. On the one hand, AI algorithms hold the potential to revolutionize criminal justice. By analysing vast datasets, AI can offer a more precise and objective analysis of criminal risk, potentially predicting cyberattacks before they occur. Imagine a future where AI can identify patterns in criminal behaviour, allowing authorities to intervene proactively and prevent crimes from happening in the first place, this optimistic vision is tempered by a harsh reality: cybercriminals themselves are turning to AI. These malicious actors can leverage AI to craft more sophisticated scams and malware, making it even harder for traditional security measures to keep pace. Malicious actors can exploit AI to personalize phishing attacks, create deepfakes to spread misinformation, or even automate the process of launching cyberattacks across a vast network of compromised devices, this study delves into the intricate relationship between AI and cybercrime. We will explore the potential benefits of AI for both law enforcement and cybersecurity professionals. AI-powered systems can become powerful tools for Crime Prediction, Cybersecurity Enhancement, Privacy Concerns, Algorithmic Bias and The Human Element.

Keyword's: Artificial intelligence; Cybercrime; modern technology; Cybersecurity; phishing attacks; deepfakes.

ملخص

لقد أعاد الذكاء الاصطناعي رسم مشهد الجريمة المعلوماتية بسرعة، فقد أصبح هذا الأخير يقدم سيناريو معقدا يجمع بين الوعود الهائلة من ناحية والأخطار الجسمية من ناحية أخرى. وتتمتع خوارزميات الذكاء الاصطناعي بإمكانية إحداث ثورة في العدالة الجنائية من خلال تقديم تحليل أكثر دقة وموضوعية للمخاطر الإجرامية، مما يسمح بالتنبؤ بالهجمات الإلكترونية قبل وقوعها. إن الاعتماد على الذكاء الاصطناعي في تحديد أنماط السلوكات الإجرامية سيسمح للسلطات بالتدخل الاستباقي ومنع حدوث الجرائم في المقام الأول، لكن هذا التصور المتفائل يعتريه واقع قاس حينما يتجه المجرمون إلى الذكاء الاصطناعي واستغلاله والاستفادة منه لارتكاب عمليات احتيال وانشاء برامج ضارة أكثر تعقيدا مما يصعب على إجراءات الأمن التقليدية مواكبة هذا التطور؛ بحيث يعمد هؤلاء المجرمون إلى استعمال الذكاء الاصطناعي لارتكاب المزيد من جرائم الاحتيال وانشاء مقاطع فديو مزيفة لنشر المعلومات المضللة وشن هجمات الكترونية عبر شبكة واسعة من الأجهزة المخترقة. وتتعمق هذه الدراسة في العلاقة بين الذكاء الاصطناعي والجريمة المعلوماتية للكشف عن المزايا المحتملة لهذا الأخير في مساعدة أجهزة انفاذ القانون وخبراء الأمن الالكتروني. يمكن أن تصبح الأنظمة التي تعمل بالذكاء الاصطناعي أدوات قوية للتنبؤ بالجريمة وتعزيز الأمن المعلوماتي وحماية الخصوصية.

Table of Contents

Dedication I

Acknowledgments II

Abstract III

ملخص IV

Table of Contents V

List of figures IX

List of tables X

General Introduction 1

Chapter. 1 Definition of cybercrime: 9

1.1 Introduction 9

1.2 Defining cybercrime 9

1.3 Characteristics of Electronic Crime 11

1.4 Objectives of Cybercrime: 13

1.5 Definitions of cybercrime from various sources 14

1.6 Classification of Electronic Crimes: 15

1.7 Types and motives for Cybercrime 16

1.8 Characteristics of cybercriminals: 19

1.9 The Legal Nature of Cybercrime 20

1.10 Conclusion 20

Chapter. 2 Definition of Artificial intelligence: 22

2.1 Linguistic Definition of Artificial Intelligence: 22

2.2 Technical Defining of Artificial Intelligence 23

2.3 Definition of Artificial Intelligence (AI) 24

2.4 Characteristics of Artificial Intelligence Technologies 28

2.5 Importance of Artificial Intelligence: 30

2.6 Types of Artificial Intelligence 31

2.7 Conclusion..... 32

Chapter. 1 The Impact of Artificial Intelligence on Methods of Committing Cybercrime 23

Introduction: 23

1.1.1 Harmful uses of artificial intelligence 23

1.1.2 AI in Cybersecurity:..... 24

1.1.3 AI-driven cyberattacks:..... 25

1.1.4 Among what artificial intelligence can do: 28

1.2 Traditional cybercrimes and modern cybercrimes committed by artificial intelligence: 28

1.2.1 The crime of illegal entry and stay in automated data processing systems: 28

1.2.2 The crime of stealing credit card numbers in Algerian penal code: 39

1.3 The crime of stealing credit card numbers committed by Ai: 42

1.3.1 Types of Credit Card Fraud and Precautionary Measures:..... 45

1.3.2 Types of Credit Card Fraud: 46

1.4 Artificial Intelligence as a vector of crime: 49

1.4.1 Approaches of malevolent artificial intelligence: 49

1.4.2 Astroturfing: 53

1.4.3 Generation: 55

1.4.4 Cyber security: 56

1.4.5 Vulnerability discovery: 56
1.4.6 Exploitation: 58
1.4.7 Post-Exploitation & Data Theft: 59
1.4.8 Exploitation of deployed artificial intelligence: 60
1.4.9 Poisoning of artificial intelligence systems: 62
1.5 Conclusion 62
Chapter. 2 Mechanism to combat cybercrime using artificial intelligence. ... 63
2.1 Introduction: 63
2.2 Proactive policing: 63
2.2.1 The Four Categories of Proactive Policing: 64
2.3 Digital police: 66
2.3.1 Purpose, materials, methods, and objectives: 67
2.3.2 Buffer overflow: 69
2.3.3 Viruses, Trojan horses, mail worms, sniffers, rootkits and other special programs: 69
2.3.4 Network intelligence: 69
2.3.5 IP spoofing: 70
2.3.6 Man-in-the-Middle: 70
2.3.7 Injection: 71
2.3.8 XPath injection: 71
2.4 Digital investigation: 72
2.4.1 AI and crime detection: 73
2.4.2 A taxonomy of AI capabilities: 73

2.5 Challenges facing the use of artificial intelligence in Combating cybercrime and proposed solutions: 84

2.5.1 Ethical challenges: 84

2.5.2 Effectiveness challenges: 84

2.5.3 Procurement challenges: 87

2.5.4 Appropriation challenges: 89

2.6 Conclusion: 90

General Conclusion: 92

BIBLIOGRAPHY 30

List of figures

Figure 1. Revenues from the artificial intelligence software market worldwide from 2018 to 2025, by region Source: Own results based on Liu (2019) 67

Figure 2. Pixel Data Diagram of Abraham Lincoln 75

List of tables

Table 1: Table summarizing the different definitions of AI 24

List of abbreviations and Acronyms

AGI: General Artificial Intelligence

AI : Artificial intelligence

AIC : Artificial intelligence crimes

ANI: Narrow Artificial Intelligence

CNP: card not present

DoS: Denial of service attacks

GAI: Generative Artificial Intelligence

ICT: information and communication technology

ML: machine learning

PC: Penal code

UNODC: United Nations Office on Drugs and Crime

US: united states

General Introduction

General Introduction

We stand at the precipice of a new era, one driven by the transformative power of artificial intelligence (AI). Emerging as the cornerstone of the fourth industrial revolution, AI's reach extends far and wide, influencing various sectors from military operations and industrial automation to economic development, healthcare, education, and even the service industry. It's a technology poised to unlock a universe of innovation, potentially ushering in further industrial revolutions that will fundamentally alter the way we live. In the years to come, AI promises to be a potent engine of progress and prosperity.

This revolution finds its roots in the digital revolution and mobile internet boom of the early 21st century. From there, advancements in areas like remote sensors, biotechnology, robotics, automation, and digital technologies paved the way for smarter systems and intelligent machines. But AI stands out as the true game-changer. Its ability to learn, adapt, and make independent decisions – even without constant human supervision – sets it apart. These very capabilities empower AI to become a critical force in streamlining processes and accelerating production. By analysing vast amounts of data and identifying optimal solutions, AI can react to changing circumstances with remarkable speed and flexibility, ultimately boosting efficiency and output.

Recognizing the immense potential of AI, many nations are now actively implementing comprehensive strategies to integrate this technology into the fabric of their societies. Understanding the importance of forward-thinking solutions, these states are fostering innovative working environments that optimize energy expenditure and elevate performance. Furthermore, some countries have gone a step further by establishing dedicated ministries solely focused on AI development and implementation across various sectors.

The impact of AI extends beyond industry and economics. For law enforcement and security services, AI presents a powerful tool for evidence

gathering and criminal investigations. By harnessing cutting-edge technologies, security forces can address security threats and solve problems with greater ease. Integrating AI can significantly improve crime prevention and control by enabling proactive measures to be taken before criminal activity unfolds. This proactive approach, already adopted by security services in many countries, highlights the crucial role AI technologies can play in ensuring public safety and combating crime in all its forms. It is a technology with the potential to safeguard society and promote peace and order.

The problem of the study: Our topic is about the following problem: To what extent does AI impact the preparedness for and evidence of cybercrime?

It also includes the following sub-questions: " What is AI"? What is the concept and characteristics of cybercrime? What is the interrelationship between AI and cybercrime and the most important challenges in tackling it?

Hypotheses

While the introduction does not explicitly state the hypotheses, they can be inferred from the research questions and objectives. Hypotheses are typically formulated based on the research questions and the aims of the study. Here are some potential hypotheses based on the provided content:

1. Hypothesis 1: AI significantly enhances the preparedness of law enforcement agencies in handling cybercrime.

2. Hypothesis 2: AI improves the accuracy and efficiency of evidence collection in cybercrime investigations.

3. Hypothesis 3: There is a significant relationship between the deployment of AI technologies and the reduction of cybercrime incidents.

4. Hypothesis 4: The integration of AI into cybercrime prevention strategies faces significant challenges that need to be addressed for optimal performance.

Research Importance:

The significance of this study lies in:

- Understanding the concepts of cybercrime and artificial intelligence.
- Defining artificial intelligence and the limitations of its applications.
- Highlighting the procedures followed in the various stages of investigation, prediction, and detection of traditional and emerging cybercrimes.
- Addressing the challenges of artificial intelligence in combating cybercrime.

Research Objectives:

- Based on the research problem, this study aims to:
- Define the concept of artificial intelligence.
- Understand the nature of cybercrime.
- Investigate the existence of a significant relationship between artificial intelligence and cybercrime.
- Identify methods for combating cybercrime.
- Examine the position of Algerian law on artificial intelligence.
- Shed light on the emerging topic of confronting computer crimes using artificial intelligence techniques.
- Provide a general overview of the subject.

Reasons for choosing the subject:

The most important reasons why we choose this topic are novelty, modernity and an urgent desire to keep abreast of modern technological renaissance with judicial legislation to prove and reduce cybercrime of various kinds in view of the difficulty of proving it.

The objective reasons are to search and investigate the procedures and penalties for cybercrime that AI contributes to in whole or in part.

Limits of study:

This study is based mainly on all the legislation that we find relevant to the field of study, including the following countries: Qatar, UAE, Libya, Saudi Arabia, France, Egypt, United States of America, United Kingdom, Zambia, Jordan, and by reference to Algerian legislation, no law or order has been specified except under conventions and penal law.

Study difficulties:

Our studies on this topic were fraught with difficulty due to a complex interplay of factors.

Firstly, we encountered a significant lack of references and existing literature on the subject. This meant we had a limited foundation of prior research to build upon and consult.

Secondly, the ongoing discussions surrounding the establishment of cybercrime legislation in Algeria further complicated matters. Since the use of artificial intelligence in the legal field hinges on this legislation, the lack of a definitive framework created uncertainty and made it difficult to assess the current state of affairs.

PLAN OF WORK

Part One: Navigating the Digital Frontier: Unraveling the Nexus of Cybercrime and Artificial Intelligence

This part will lay the groundwork for understanding the complex relationship between cybercrime and artificial intelligence.

- **Chapter 1: Definition of Cybercrime**
    - This chapter will delve into the concept of cybercrime.
        - We will explore various definitions of cybercrime from authoritative sources.
        - We will then define cybercrime in our own words, providing a clear and concise understanding of the term.
        - Finally, we will explore the different types of cybercrime and the motivations behind them, giving context to the various forms these crimes can take.
- **Chapter 2: Definition of Artificial Intelligence**
    - This chapter will focus on artificial intelligence (AI).

        - Similar to Chapter 1, we will begin by examining definitions of AI from different sources.
        - Following that, we will offer a clear definition of AI from our perspective.
        - To solidify our understanding, we will categorize different types of AI, highlighting their functionalities.
        - Lastly, we will explore the characteristics of AI technologies, giving a deeper insight into how they operate.

Part Two: The Impact of Artificial Intelligence on Criminal Justice

This section will explore the two-sided coin of AI: its potential for both criminal activity and crime prevention.

- **Chapter 1: The Impact of Artificial Intelligence on Methods of Committing Cybercrime**
    - This chapter will delve into the dark side of AI, examining its role in facilitating cybercrime.
        - We will discuss how AI can be used to commit cybercrimes, outlining the specific ways criminals leverage this technology.
        - To illustrate this point, we will explore specific crimes committed with the aid of AI. This might include examples like illegal access to data systems or the theft of financial information.
- **Chapter 2: The Impact of Artificial Intelligence on Methods of Combating Cybercrime**
    - This chapter will shift the focus to the positive side of AI, exploring its potential in combating cybercrime.
        - We will discuss how AI can be used as a powerful tool for proactive policing, outlining concepts like digital police and digital investigation.

- Since no technology is without its challenges, we will conclude the chapter by examining the obstacles faced when using AI in cybercrime prevention. Additionally, we will propose solutions to overcome these challenges.

PART ONE

Navigating the Digital Frontier: Unraveling the Nexus of Cybercrime and Artificial Intelligence

Chapter 01:

Definition of cybercrime

Chapter. 1 Definition of cybercrime:

1.1 Introduction

In order to understand the nature of cybercrime, assess its differences from traditional crime, examine its goals and types, and reveal motives for its implementation, further investigation of the phenomenon of cybercrime itself is needed.

1.2 Defining cybercrime

Electronic or cybercrime is composed of two parts: These topics are crime and cyber. The term cyber is also used to refer to the computer or information age in the current world. [1] The scope of detailing electronic crime has been varying hence within the context of establishing the legal vantage. Some jurists have a restricted meaning when referring to the aforesaid provision, whereas, others have a wider meaning when referring to the aforesaid provision. Some of the nuances included in the definitions offered by theorists supporting the main approach are that electronic crime is “any offense that can only be perpetrated, and prosecuted, using specialized knowledge of computer systems. [2]

In the same context, Professor Mass sees information technology as: cyber legal criminal activities that are performed with human intent to gain some form of benefit. [3] According to the German jurist Tie de man, electronic crime refers to “all Illegal and detrimental conduct that is unlawful to the society and is perpetrated via

[1] Dhaib Musa Al-Badaniyah, "Cybercrimes: Concept and Causes, Emerging Crimes in Light of Regional and International Changes and Transformations," Amman - Hashemite Kingdom of Jordan, 2014, p. 3.

[2] RaziyaAymour, "Cybercrime and Mechanisms for Combating It in Algerian Legislation," Academic Journal of Legal and Political Research, University of Laghouat, No. 1, 2022, p. 91.

[3] Baara Saeed, "Cybercrime in Algerian Legislation," Master's Thesis, University of Mohamed Kheider - Biskra, 2016/2015, p. 11.

the use of the computer" [1], with reference to the method applied when perpetrating the crime.

What is remarkable is that these definitions have reduced the meaning of Electronic Crime since many of the crimes that may involve the use of the computer, the electronic crime word does not extend its meaning to cater for such types of crimes. [2]

However, there are definitions that have endeavored towards developing a broader view of what Cyber Crime is due to the criticisms that the first approach attracted. Some have defined it as:" they defined any intentional act or omission for unlawful purpose that seeks to assail material or moral, goods and assets and as: "the utilization of the computer as an instrumentality in the commission of the crime in addition to situations of unauthorized access of other's computer or data". [3]

The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders adopted the following definition of electronic crime:

Every crime which it is possible to execute in the computer system or a network and such crime encompass, at least as a principle, all the crimes that in the electronic environment.[4]

As for the Algerian legislator, he did not define electronic crime and adopted the term "crimes related to information and communication technology", defining

[1] MassoudChahira, "Cybercrime in Algerian Legislation," Master's Thesis, University of Abdelhamid Ben BadisMostaganem, 2021/2020, p. 6.

[2] Si Hamdi Abdel Momen, Kira Saad, "Cybercrime and Mechanisms to Combat It in Algerian Law," Journal of Legal and Political Studies, University of Mohamed Bachir Ibrahim, Bordj BouArreridj, Algeria, No. 01, June 2022, p. 61.

[3] BelaidMansouriya, "The Procedural System of Cybercrime in Algerian Legislation," Master's Thesis, University of Abdelhamid Ben BadisMostaganem, 2020/2019, p. 9.

[4] MerabetRamissa, "Cybercrime: Between the Limits of Danger and the Necessities of Confrontation," Journal of Governance and Economic Law, Faculty of Law and Political Sciences Sousse/Tunisia, No. 01, 2023, p. 61.

it under the provisions of Article 02 of Law 09-01 22 [1] as: That is, “criminal attacks against the processing systems of the data determined in the Penal Code, and other crimes committed by using information system or electronic communication system.

The law which regulates electronic crime is The Penal Code and there is no legal definition of the term ‘electronic crime’. [2]

1.3 Characteristics of Electronic Crime

Electronic crime, as mentioned in the definition, has properties that set it out of the category of traditional crime. These include:

a. Cross-border crime: Such type of crime is extraterritorial and unaccepted as it spans across more than one nation, thus inviting questions such as jurisdiction, process, and inquiry.

b. A crime that is difficult to detect and prove: It is extremely difficult to conceal information crime and, should it get noticed, it is normally through happenstance since the culprit does not leave external signs of his culminating or tends to obliterate the evidence adroitly[3].

c. A soft crime: The old type of crime involves the application of tools and force, occasionally as exemplified by terrorisms and drug offenses. Nonetheless, electronic crime is defined as a digital crime that does not require the use of force usually. Getting information from one computer system to another or simply

[1] Law No. 09 - 04 issued on August 5, 2009, which includes the special rules for the prevention and fight against crimes related to information and communication technologies, J.R. No. 47.

[2] Si Hamdi Abdel Momen, Kira Saad, same reference and same page.

[3] Ferj Hussein, "Electronic Crime and Its Repercussions on National and Citizen Security Between Legal Combat and Detection and Investigation Devices," Journal of Public Administration, Law and Development, Hassiba Ben Bouali University, El-Oued, Algeria, No. 01, 2022, p. 76.

stealing electronically from an account does not involve a shoot-out with security guard[1].

d. Underreporting of crime: Because of the nature of these types of crimes and the stigmatization that a person involved in the act may receive in case they report the incident, reporting the crime is rare, and most cases are discovered accidentally. This may be done long after the crime has taken place, or even in areas far from the scene of the crime[2].

e. Lack of a common concept of cybercrime: Another important feature of this crime is the absence of a clear common understanding or a single legal definition of this given type of crime, because this field is not very developed at the international level and there are no international agreements here – the mention should be made of the differences in juridical systems.

f. Occurrence of cybercrime during data processing: This is the premise that must hold in order to examine the possibility or impossibility of cybercriminal elements …with regards to the attack on the data processing system. Criminal operations cease to exist in cyberspace when this occurs.

g. Cybercrime is an emerging crime: It can be said that if a crime is associated with computers or if those devices are used to commit a crime, then such criminal acts are referred to as emerging crimes[3].

[1] Dhaib Musa Al-Badaniyah, "Electronic Crime and Its Repercussions on National and Citizen Security Between Legal Combat and Detection and Investigation Devices," Journal of Public Administration, Law and Development, Hassiba Ben Bouali University, El-Oued, Algeria, No. 01, 2022, p. 20.

[2] Yamina Mankhrifis, "Electronic Crimes on Social Media Sites with Social and Moral Dimensions," Journal of Law and Human Sciences, University of Algiers 3, Faculty of Information and Communication Sciences, No. 01, 2023, p. 1304.

[3] Si Hmadi Abdel Momen, Kira Saad, "Electronic Crime and Its Repercussions on National and Citizen Security Between Legal Combat and Detection and Investigation Devices," Journal of Public Administration, Law and Development, Hassiba Ben Bouali University, El-Oued, Algeria, No. 01, 2022, p. 62-63.

1.4 Objectives of Cybercrime:

Cybercrime can be broadly categorized into the following objectives:

a. Unauthorized Access to Information:

In this method, the criminal steals, views or deletes information so that it can be used beneficial to him or her.

This encompasses entering personal details, finances and other secrets such as product formulas and designs that are not open to the public domain.

b. Disrupting Information Systems:

Interference with computer networks, servers or websites; the destruction of all the software or any data contained within it.

This can be achieved through hacking techniques, through injection of malware, or in through denial-of-service attacks.

c. Extortion and Financial Gain:

Performing an unauthorized access to a computer system to obtain a valuable information and then blackmailing the owner to provide him some money or else this information will be leaked.

This can be targeted at the persons, corporations, or the government.

Other examples of financial gains are credit card fraud whereby people steal credit card details to purchase items, identity theft whereby people’s identity is stolen with the intension of embezzling funds and scams that are conducted online.

d. Espionage and Political Influence:

Sneaking into a department and issuing a fire to prevent spying or taking sensitive data for political purposes.

This can involve the attack on government departments, military, or other business entities that may hold rather valuable information.

e. Personal Gratification and Vandalism:

Conducting cyber-terrorism like, changing layout and color of website, posting wrong information or information which can create disturbance just for some fun or to take revenge. This can be done in the form of accessing account information, posting spam, phishing or cyber bullying.[1]

1.5 Definitions of cybercrime from various sources

SpringerLink: As the study of cybercrime has evolved, researchers have explored how to best define the term. To date, no universal definition of cybercrime has been developed.

Cybercrime can be conceptualized as either traditional criminal activity, deviant behavior, a legal issue, a political issue, a white-collar crime, the product of a social construction, or a technological problem. It is best understood through a multidisciplinary lens.[2]

Oxford Learner's Dictionary: Cybercrime refers to crime committed using the Internet, such as stealing personal or bank details or infecting computers with viruses.[3]

Cambridge Learner's Dictionary: Cybercrime is illegal activity done using the Internet, often associated with hackers and other cybercriminals.[4]

UNODC (United Nations Office on Drugs and Crime): Cybercrime is an act that violates the law, perpetrated using information and communication

[1] Cybercrime: "Objectives, Causes, Methods, and Treatment" by Esraa Gabriel Rashad Murree (05/12/2023, 14:03) https://democraticac.de/?p-35426

[2] SpringerLink definitions of cybercrime link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3 - time 3:53 / 26/02/2024.

[3] Oxford Learner's Dictionary definitions of cybercrime www.oxfordlearnersdictionaries.com/definition/american_english/cybercrime - time 3:53 / 26/02/2024.

[4] Cambridge Learner's Dictionary of cybercrime dictionary.cambridge.org/dictionary/learner-english/cybercrime - time 3:53 / 26/02/2024.

technology (ICT) to target networks, systems, data, websites, and/or technology, or to facilitate a crime.[1]

Cybercrime, the use of a computer as an instrument to further illegal ends, such as committing fraud,traffickingin childpornography and intellectual property, stealing identities, or violating privacy. Cybercrimed, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

1.6 Classification of Electronic Crimes:

It is difficult, therefore, to classify electronic crimes based on the levels of technology, computer usage, and dependence on this machinery in various aspects of life in different societies. The European Convention project of 2001 has divided Computer and Internet crimes as a whole into a new classification of four categories although it does not include the privacy related crime as these are excluded being of a different European Convention altogether.[2]

Crimes Targeting the Integrity and Confidentiality of Data and Systems:

This includes features like access to services and data for which the user is not entitled, interception of services and data, deletion of services and data, and obstructing the Services.

[1] UNODC (United Nations Office on Drugs and Crime) https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html - time 3:53 / 26/02/2024.

[2] YasminaBounaara, "Cybercrime," Al-Mi'yar, University of Amir Abdelkader of Islamic Sciences Constantine - Algeria, No. 39, June 2015, p. 289.

Computer-Related Crimes:

This category covers computer Forging and Fraud related to computer products.[1]

Content-Related Crimes:

This category involves crimes that are likely to involve nude and lewd acts.

Crimes Against Persons and Property:

This includes theft, fraud, forgery, unauthorized access to persons' data (identity theft), spreading of false information, violations of privacy rights, wrong use of information, hacking, illegal dissemination of information from unknown sources, cyber-terrorism, and any other form of unlawful activities.[2]

1.7 Types and motives for Cybercrime

The motives of cybercrime can be divided into four main categories[3]:

A. Economic Motives

The largest group of cyber terrorism motives is economic. Cybercriminals who are motivated by money may use a variety of methods to steal money or valuables, such as cybercriminals who are motivated by money may use a variety of methods to steal money or valuables, such as:

Phishing: Phishing is a type of social engineering where the attacker uses fake email, to text messages or fake websites to lure people into properly authenticating, and thereby disclose to the attacker their credit card details or their user names and passwords.

Malware: Malware is a type of program that is built with ill intentions that aims to put a computer system in a detrimental state. The result of having a virus could be

[1] YaminaMankhrifis, Reference previously cited, p. 1305.
[2] Yasmina Bounaara, Same reference and same page.
[3] 6 Motivations of Cyber Criminals, Mar 3, 2022 11:15:00 AM, Visit date: 13-05-2024, Visit time: 00:03, https://www.coretech.us/blog/6-motivations-of-cyber-criminals

to steal information, locked files or just gain unauthorized control of a computing system.

Ransomware: That encouraging message leads to the definition of ransomware, which is a type of malware that encrypts the files in a computer system and then asks the user to pay a certain amount of money to be given the decryption key.

Denial-of-service (DoS) attacks:

Denial of Service (DoS) attacks encompass all those scripts that attempt to flood a targeted website or online service with traffic so that real users are locked out.

B. Individual Motives

The motivation behind the crime in the cyber world is more than just related to green from technologically enabled crime. Cybercriminals who are motivated by individual factors may engage in cybercrime for a variety of reasons, such as cybercriminals who are motivated by individual factors may engage in cybercrime for a variety of reasons, such as:

Revenge: Cybercriminals may want to seek retaliation on people or organizations they perceived as having offended them.

Threatening others: A subgroup within cybercriminals might engage in cybercrime with the purpose intent of coercing a certain behaviour.

Seeking pleasure: There is evidence that certain computer criminals may engage in hacking with intent and motivation due to excitement of the challenge.

Love of destruction: Some hackers may have ill intentions for attacking systems or databases that are in place to cause as much havoc as possible.

A grandiose sense of self-importance: The social factors can include the perception that some cybercriminals are arrogant and think they are more intelligent than their targets and can therefore get away with it.

C. Political Motives

Cybercrimes motivated by political agendas are typically used in an attempt to manipulate the population as well as to weaken an opponent. Cybercriminals who are motivated by political factors may engage in cybercrime to cybercriminals who are motivated by political factors may engage in cybercrime to:

Defame individuals and institutions: Another trick of cybercriminals is to get unauthorized access to personal accounts or organizations' databases in order to post fake or scandalous information about the owner of the account or company to slander them.

Damaging reputations: internet criminals can compromise computer networks to siphon off and desegregate such an individuals or organizations' data with the intention of denigrating them.

Spreading misinformation: This misfortune bears the potential of being managed by cybercriminals especially since they are well known to disseminate messages that contain false or misleading information so as to cause confusion.

D. Strategic motives are normally aiming at the achievement of objectives such as enhancing competitive advantage or protecting the nation's security:

Cybercriminals who are motivated by strategic factors may engage in cybercrime to:

Damage to the Internet: The hacktivist group that hacked computer systems around the world recently released data explaining that hacker tries to minimize people's capability; Hack and sabotage to minimize the effectiveness of others.

Espionage in all its forms: Burglars may eavesdrop on people or firms with an aim of robbing them of their essential or privy info or to obtain undue advantage. It

is vital to explain that goals of cybercriminals should not necessarily have one major motive; the motives can overlap. [1]

For instance, a cybercriminal who is both, financially driven and vindictive, may decide to install the malware in an organization they feel has crossed them; and the malware's main target may be to extract credit card information from the organization in question.

1.8 Characteristics of cybercriminals:

Cybercriminals can be summarized by the following characteristics:

Specialized criminals: They possess great technical knowledge and skills, employing these in order to penetrate into different networks.

Recidivist criminals: Cyber criminals are often known by their capacity to commit streamline crimes. They know the way around computers and may not use the knowledge to harm computer systems but will hack for the mere purpose of personally bringing out the ability in them.

Professional criminals: It point them to have requisite technical skills and competence that enable them to apply of their specialization in hacking, thefts, and other unlawful activities.

Intelligent criminals:

These criminals are experienced and capable of developing and manipulating the security systems with a view of evading the cookies.[2]

Alas, it is crucial to mention that cyber criminals, based on their nature, are often hard to apprehend and discover, no matter the fact that the victim and the offender are in different geographical locations and adverse effects are narrated in a different country.

[1] LattarchFairouz, Hatem Ben Azouz, "Cybercrime in Algeria: From Individual Crime to Organized Crime," Afak for Sciences, University of Djelfa, No. 01, 2016, p. 328.

[2] Mahmoud Ragab Fatah Allah, the cybercrime criminal and his motives, 2023/05/13, Visit date: 13-05-2024, Visit time: 00:03, https://www.ahewar.org/debat/show.art.asp?aid-608845

1.9 The Legal Nature of Cybercrime

Cybercrimes fall within the scope of study of the special section of the Penal Code, which is a branch specialized in studying each crime individually, dealing with its basic elements and the prescribed penalty. However, cybercrimes represent a criminal phenomenon of a special nature related to criminal law, as the special legal nature of these crimes through the field in which they can be committed or on which the assault occurs.

The nature of the rapid development in the field of information technology necessitates its inclusion in the scope of the special criminal law, due to the inability of criminal texts to keep pace with electronic development or what it contains of a legislative vacuum in this field, Therefore, updating criminal laws for high-tech crimes.[1]

1.10 Conclusion

This is an ever-growing menace that exists in the shadows and thus requires constant attention. These days, as we use the technology significantly for important activities in life no doubt that criminals will also look for good chances to misuse this technology. If we are knowledgeable of the new strategies in the world wide web, observing responsible computing, and endorsing strong cyber security systems we will be able to fashion out a tighter world web for the future.

[1]Abdulrazzaq, Rana Mesbah Abdel Mohsen, "The Impact of Artificial Intelligence on Cybercrime," Journal of King Faisal University, Vol. 22, No. 1 (2021), p. 431.

Chapter 02:

Definition of Artificial intelligence (AI)

Chapter. 2 Definition of Artificial intelligence:

A Glimpse into the Future of Artificial Intelligence:

Will Machines Surpass Human Intelligence?

A question that often arises in our minds is whether we can imagine computers becoming as intelligent as humans. If the answer is yes, do we expect these machines to eliminate humanity or marginalize their main role in life? Before delving into answering these two questions, it is necessary for me to address the definition of artificial intelligence, both linguistically and technically, as will be explained below.

2.1 Linguistic Definition of Artificial Intelligence:

The Merriam-Webster[1] dictionary has provided a comprehensive definition of artificial intelligence as:

A branch of computer science concerned with simulating intelligent behaviour in computers.

The ability of a machine to mimic human intelligent behaviour.

The Oxford Dictionary defines it as "the theory and development of computer systems capable of performing tasks that typically require human intelligence, such as perception, speech recognition, decision-making, and language translation."[2]

And the Britannica Encyclopaedia defines it as "a field of computer science that gives machines the ability to seem like they have human intelligence, or the power of machines to replicate human intelligent behaviour."[3]

---

[1]The capability of a machine to imitate intelligent human behavior https://www.merriam-webster.com/dictionary/artificial%20intelligence Visit date: 19-05-2024, Visit time: 11:03

[2]Christian Youssef, Civil Liability for Artificial Intelligence Acts, Al-Halabi Legal Publications, First Edition, Beirut, Lebanon, 2022, p26.

[3]Britannica dictionary definition of artificial intelligence, https://www.britannica.com/dictionary/artificial-intelligence Visit date: 12-05-2024, Visit time: 13:23

2.2 Technical Defining of Artificial Intelligence

There are numerous definitions of artificial intelligence (AI), and there is no single, universally accepted definition. Information technology companies have described AI as "the science of creating intelligent machines that can perform tasks in record time at the level of a person programmed for AI." Others have defined it as "a rapidly developing field of computer science." In the mid-1950s, John McCarthy, considered the father of AI, defined it as "the science and engineering of making intelligent machines." Conceptually, AI is the ability of a machine to perceive and respond to its environment independently and perform tasks that typically require human intelligence and decision-making, but without direct human intervention. It is also defined as "the science of building machines that perform tasks that require some degree of human intelligence when performed by humans."

Numerous hypotheses and theories have raised many controversial issues about the nature of the human mind and how to simulate the human mind in an electronic machine. AI systems have also sparked debate about their ability to think logically parallel to natural human thinking, as well as machine learning, knowledge, planning, sensory perception, and the tremendous capabilities that rival humans.

AI is also defined as "programs that allow computers to simulate some of the functions of the human brain in limited ways. These programs are implemented on large mainframe computers, mid-range computers, or personal computers."

Here is a table summarizing the different definitions of AI:

Definition	Source
"The science of creating intelligent machines that can perform tasks in record time at the level of a person programmed for AI."	Information technology companies
"A rapidly developing field of computer science."	General definition
"The science and engineering of making intelligent machines."	John McCarthy, father of AI
"The ability of a machine to perceive and respond to its environment independently and perform tasks that typically require human intelligence and decision-making, but without direct human intervention."	Conceptual definition
"The science of building machines that perform tasks that require some degree of human intelligence when performed by humans."	Another conceptual definition
"Programs that allow computers to simulate some of the functions of the human brain in limited ways. These programs are implemented on large mainframe computers, mid-range computers, or personal computers."	Technical definition

Table 1: Table summarizing the different definitions of AI

2.3 Definition of Artificial Intelligence (AI)

There are multiple definitions of AI, and in fact, there is no single, universally accepted definition. Information technology companies have described AI as "the science of creating intelligent machines that can perform tasks in record time at the level of a person programmed for AI."[1] Others have defined it as "a rapidly evolving field of computer science."[2] In the mid-1950s, John McCarthy, who is considered the father of AI, defined it as "the science and engineering of making intelligent machines." [3]

Conceptually, AI is the ability of a machine to perceive and respond to its environment independently and perform tasks that typically require human intelligence and decision-making, but without direct human intervention. It is also defined as "the science of building machines that perform tasks that require a degree of human intelligence when performed by humans."[4]

Many hypotheses and theories have raised many controversial issues about the nature of the human mind and how the electronic machine can simulate the human mind. AI systems have also raised debate about their ability to think logically parallel to natural human thinking, as well as machine learning, knowledge, planning, sensory perception, and the enormous capabilities that match humans.[5] It is also defined as "programs that allow the computer to simulate some of the functions of the human brain in limited ways. These programs are implemented on mainframes, mid-range computers, or personal computers."

However, I can lean towards defining it for some as 'software systems and perhaps hardware designed by humans with a complex goal, operating in the real or digital world by perceiving the environment, by obtaining information, and by

---

[1]Ayman Mohamed Sayed Mustafa Al-Asyuti, The Impact of Artificial Intelligence Technology on Law, published in a book entitled "Collective Book - The Impact of Technological Development on Law, Institute of Palestine Ahliya University for Studies and Research, Palestine, without year of publication, p. 367.

[2]Christopher Rigano, Using Artificial Intelligence to Address Criminal Justice Needs, National Institute of Justice, NIJ Journal / Issue No. 280, January 2019, Page 1.

[3]Abdullah Saeed Abdullah Al Wali, Civil Liability for Damages Caused by Artificial Intelligence Applications in UAE Law, Analytical and Comparative Study, Dar Al Nahda Al Arabiya, Cairo, 2021, p. 27.

[4]Christian Youssef, previous reference, p. 26.

[5]Abdellah Ibrahim Al Faqi, Artificial Intelligence and Expert Systems, Dar Al Thaqafah for Publishing and Distribution, First Edition, Jordan, 2012, p. 58.

interpreting structured or unstructured data collected, applying analysis to knowledge or processing information derived from that data, and deciding the best action or actions to take in order to achieve a specific goal. AI systems can either use symbolic rules or learn a digital model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions, as has been rightly said in the context of describing AI as "allowing a machine or system to behave intelligently in a way that mimics human behavior."[1]

It is worth noting what a study published in 2004 stated that the memory capacity of the human brain is about 100 trillion powers, which can be estimated at about one million billion bits. In 1998, one billion bits of RAM (128 MB) cost around $200 and memory capacity doubles every 18 months. Thus, by 2023, one million billion bits will cost around $1000. However, the silicon equivalent will work over a billion times faster than the human brain, and the study pointed out that there are techniques for trading memory for speed, so that human memory can be effectively matched much sooner, considering that it is reasonable to estimate that a $1000 computer will match the computing speed and capacity of the human brain by 2020, especially for the neural network calculations that make up the bulk of the computation in the human brain.[2]

Industrial supercomputers are up to ten thousand times faster than personal computers, so this study expected to reach 20 million calculations per second before a decade of 2010, as well as expected the creation of artificial intelligent characters, which are expected to have knowledge and thinking power far greater than humans. For example, it may be possible to create an entity with the

[1]Mohamed Mohamed Abdel Latif, Liability for Artificial Intelligence between Private Law and Public Law, Paper presented to the Conference on the Legal and Economic Aspects of Artificial Intelligence and Information Technology, May 23-24, 2021, Faculty of Law, Mansoura University, 2021, p. 3-4.

[2]A. D. (Dory) Reiling, Courts and Artificial intelligence, International Journal for Court Administration, 2020, Page 4.

intelligence and personal skills of a high school teacher, providing individualized education on a standard curriculum, with the size and cost of a Walkman device.[1]

AI is a comprehensive concept for a set of advanced technologies. Many technologies have emerged that have swept the world and we may find them clearly in our smartphones without the slightest realization that they contain artificial intelligence. It is a technology that is synchronized with other technologies to make our daily tasks easier.

Digital algorithms can be considered the foundation of artificial intelligence (AI), which plays a central role in merging AI with human cognition. Based on this, this technology is considered algorithmic intelligence that mimics the human mind and can match it in many fields and sciences, including physics, mathematics, and engineering. However, it falls short in some other sciences, such as the humanities and social sciences, because it is not possible to be certain about many of the applications of these sciences. It can be said that these sciences are often shrouded in mystery, or in other words, they have their own special characteristics, as is the case with legal sciences. Thus, the application of AI in these sciences remains somewhat limited due to its lack of full readiness for human analysis of philosophical and social concepts that conflict in human society, including legal issues and their complex philosophy. However, in terms of quantity or information storage, AI surpasses human capabilities in an unbelievable way.[2]

AI has two basic forms according to the draft law of US Senator Maria Cantwell and also the report of the National Consultative Committee on Ethics in France: either partial AI, or as it is called narrow or partial AI, whose tasks focus on allowing the machine to understand and apply commands. The second form is

[1]Frank wells Sudia, Artificial Intelligence, sooner than you think. – A Jurisprudence of Artilects: Blueprint for a Synthetic Citizen, Al Tamimi & Company, Westlaw Middle East, Thomson Reuters, August 1, 2004, Page 2 – Page 3.

[2]Mohammed Irfan Al Khatib, Artificial Intelligence and Law, A Critical Comparative Study in French and Qatari Civil Legislation in Light of the European Rules in the Civil Law of Humanity for 2017 and the European Industrial Policy for Artificial Intelligence and Humanity for 2019, Journal of Legal Studies, Arab Beirut University, 2020, p. 4-5.

known as full AI, which uses machine learning technology to match human intelligence and learn from natural humans. AI does not need to be integrated into a robot to function properly. According to the French Consultative Committee on Ethics, a robot is "a machine capable of influencing the physical and sensory reality that surrounds it and interacting with humans and their environment. It can be endowed with artificial intelligence."[1]

2.4 Characteristics of Artificial Intelligence Technologies

The most important characteristics of artificial intelligence are:

Use of an approach similar and somewhat equivalent to the human approach in solving complex problems. This is characterized by simultaneity, accuracy, and high speed in receiving and addressing hypotheses, the ability to find a solution to each problem, as well as the ability to process non-digital data of a symbolic nature. Artificial intelligence (AI) is also difficult to prepare, as it requires the representation of large quantities of specialized knowledge in specific fields. Among its goals are to simulate the human way of thinking and his style of perception or response, and to create new creative and innovative ideas.[2]

Artificial intelligence (AI) works to preserve human experiences and provide multiple alternatives for the system, which allows for dispensing with experts and compensating for their expertise. The absence of feelings of tiredness and boredom, and reducing dependence on human energies are among the other most important characteristics of artificial intelligence.[3]

Reduction and prediction: This are the ability of artificial intelligence to act independently. Artificial intelligence systems are capable of performing complex

[1] Christian Youssef, previous reference, p. 27-28.

[2] Abdel Nour, Adel (2017). Expert Systems, Publications of the Department of Electrical Engineering, King Saud University. Kingdom of Saudi Arabia

[3] Abdel Nour, previous reference, p. 128

tasks, such as driving a car and building an investment portfolio, without effective human control or even supervision. There are great prospects for the economic challenges and disruptions to the labor market caused by artificial intelligence applications, and how these applications are likely to accelerate progress.[1]

Monitoring: The risks arising from the independence of artificial intelligence do not include only predictability problems, but also control problems. It may be difficult for humans to maintain control over machines programmed to work with a high degree of self-reliance. There are many problems that occur in the mechanisms that cause loss of control: malfunctions, such as a corrupted file or physical damage to input equipment, security breaches, and here the great response from these applications appears with a superior response time compared to humans. If artificial intelligence is designed with features that allow it to learn and adapt. These are the characteristics that make artificial intelligence a potential source of general risks on a scale that far exceeds the familiar forms of general risks that arise solely from human behaviour.[2]

Extreme speed and accuracy:

High efficiency in data management, in addition to having a great deal of flexibility in responding to the user, and not being controlled by its uncontrolled emotions and motives unlike humans. These systems operate according to a logical, organized, and practical way of thinking that is far from mood swings. This improves its ability to make sound decisions within a short period of time.

"From the above, the researcher observes that the application of artificial intelligence has lots of benefits such as the super speed, accuracy and efficiency of handling with data. Moreover, it has huge flexibility in dealing the user, or rather it

[1] Shekhar. 2019. Artificial Intelligence in Automation. International Journal of Multidisciplinary, 4(6), pp.13-17

[2] Ahmed Adel Jameel, Othman Hussein (2018). The Possibility of Using Artificial Intelligence in Internal Audit Quality Control. Amman, Without Publisher, p. 112

does not have ability to contain its anger and other violent intentions while making decisions as like human, because such systems work in very systematic, logical and structural manner of thinking and free from any sort of moods which in turn enhance its capability to take proper and fine decisions in short time period."

2.5 Importance of Artificial Intelligence:

However, it important to consider the contribution that Artificial intelligence (AI) is likely to have on the destiny of human beings. In my case, computers can do much more through the concepts of AI and can solve most problems and issues, carry out the industrial work and do specialization in engineering, medical, military, educational sectors, etc. The study of artificial intelligence involves defining the concept of intelligence by being able to create programs to generate like human beings and designing different systems in various disciplines to attain the level of intelligence similar to humans or even surpass their level.[1]

Improves Efficiency and Productivity: A major advantage of artificial intelligence is that it can contribute a lot in the increase of productivity to different business fields. For instance, in production, the intelligent robots can help in areas that require one to spend a lot of time and energy in doing and leave the more challenging roles to be finished by human beings. It is the same with the application of the AI in the healthcare sector where patients will have better results through the reduction of the administrative work that occupies most of the time of the health practitioners allowing for actual physical care for the patient.

Personalized Recommendations: One of the beneficial ways in which AI technology can be implemented is to help organizations in offering recommendations relevant to the user. This is especially true in the sectors that involve the provision of online products and services; this includes sectors aspects such as e-commerce, digital marketing and entertainment sectors where clients can

[1] Mamdouh Hassan Manea Al-Adwan, Criminal Responsibility for Illegal Acts of Artificial Intelligence Entities, Journal of Law and Technology, Jordan University, No. 4, 2021, p. 151.

be encouraged to purchase more products or engage in other activities relating to loyalty to the greatest extent possible through product recommendation. For instance, the leading e-commerce stores like Amazon and the entertainment streaming platforms like Netflix employ the application of artificial intelligence to offer their customers a recommendation of the product or content they are likely to be interested in based on their past activity. This plays a crucial role in supporting the effective development of qualified leads and helping to increase conversions.

Predictive Analytics: After that, using big data and machine learning, AI also supports businesses by making the necessary decisions for better futures. This way, data on larger datasets is analyzed and the AI algorithms are capable of identifying patterns and trends that are not immediately noticeable in the larger population by a human mind and thus it offers business insights to the business people that they would not be able to notice on their own. Similar to the survey conducted by PwC, a majority of business executives predicted that AI will likely affect industries in a significant manner with 63% agreeing with the statement. For example, applications of predictive analytics are valuable in the finance field because it first enables the determination of possible risks and gains for a particular stock in the market so investments can be made more securely and with higher accuracy.[1]

2.6 Types of Artificial Intelligence

Artificial intelligence can be classified based on scope into:

a. General Artificial Intelligence (AGI): This type refers to computers with human-level intelligence in all areas, meaning they can perform any intellectual task that a human can. Creating this type of intelligence is much more difficult than the previous type, and we have not yet reached this level.[2]

---

[1] The Importance of Artificial Intelligence in Today's World By Nextech3D.ai on May 11, 2024 14:53

[2] Tahir Abu Al-Eid, A Guide to Artificial Intelligence for Law Students and Researchers, Journal of Law and Technology, Cairo, No., 2023, p. 10.

b. Narrow Artificial Intelligence (ANI): This is artificial intelligence that specializes in a single area and is actually the most widespread in practice, and perhaps the only one that is used to our knowledge. It has also seen progress in recent years. For example, there are AI systems that can beat a chess champion, which is the only thing they do.[1]

c. Superintelligence: Oxford philosopher Nick Bostrom defines superintelligence as "intelligence that is far superior to the best human minds in virtually every domain, including scientific creativity, general wisdom, and social skills." This type makes the field of artificial intelligence a fascinating area to delve into.

d. Generative Artificial Intelligence (GAI): This type of AI focuses on generating new content, such as text, images, or music. GAI has the potential to revolutionize many industries, such as art, design, and entertainment.[2]

2.7 Conclusion

AI has steadily risen in sophistication and significance in many aspects of people's everyday existence. Yet the potential benefits of empowering communities with secure, reliable, and affordable access to information remain vast and though the possibilities are largely positive, there are considerable ethical implications that must be seriously considered are real and that when handled responsibly and appropriately the positive transformation of communities is possible with the help of access to Information technology. Challenges with AI will therefore arise as researchers and developers, governments and citizens collectively seek to harness AI technologies for the benefit of all mankind.

[1] Ahmed Ali Hassan Osman, Reflections of Artificial Intelligence on Civil Law, Journal of Law and Technology, Zagazig University, No. 76, June 2021, p. 1534.

[2] Tahir Abu Al-Eid, Same reference and same page.

PART TWO

The impact of artificial intelligence on criminal justice

Chapter 01:

The Impact of Artificial Intelligence on Methods of Committing Cybercrime

Chapter. 1 The Impact of Artificial Intelligence on Methods of Committing Cybercrime

Introduction:

The rapid evolution of information and communication technologies and the diversity of interconnection networks have been significant factors in broadening the application do-mains of such technologies. Consequently, so-called artificial intelligence crimes (AIC) have emerged involving a corresponding rise in criminality figures, affecting individuals' rights and freedoms. The emergence of AI-related crimes has triggered many challenges for the judiciary nationally and internationally. Thereby, jurisprudence and the judiciary must consider whether the existing provisions of law are sufficient to confront these crimes, or is there a need to strengthen international, regional, and national legislation to cover such cases. Such peculiarities characterizing AI crimes have complicated dealing with criminal activities, and they are usually dealt with using traditional criminal provisions, which may be compromised by the principle of criminal legality and the limited interpretation of a criminal provision. Accordingly, legislative steps must be taken to combat such crimes by enforcing legal provisions intended to criminalize the newly introduced criminal acts.[1]

1.1 The role of artificial intelligence in committing cybercrime

1.1.1 Harmful uses of artificial intelligence

We have now demonstrated that AI is established to the point were any dedicated developer is able to enter the field using publicly available resources.

As mentioned, such accessibility is generally a positive thing, however, it also potentially allows malicious actors to leverage the technology. There are several properties of AI which might make it attractive for malicious actors. Like many technologies, it can serve dual purposes and can be used both for beneficial and

[1] Ibrahim Suleiman Al Qatawneh UAE, Artificial Intelligence Crimes, Academic Journal of Interdisciplinary Studies, p143

harmful ends. AI can emulate many acts performed by humans, and in some cases even exceed human performance in terms of efficiency and scalability. This means that crimes that previously required human skills and time can be performed on a much larger scale, targeting thousands of victims simultaneously.[1] AI can also increase the distance between the offender and the victims. This could make criminals harder to track and decrease psychological inhibitions.[2] Additionally, artificial intelligence, like any technological system, is bound to suffer from a number of technical vulnerabilities that will inevitably be exploited by criminal interests. Therefore, there are three impending consequences regarding the risks posed by AI:

1. Existing threats could expand: due to the scalability of artificial intelligence, offenders could use the technology to target an increasing number of victims;

2. Entirely new threats could be introduced: AI is able to generate data such as audio files mimicking the voice of real people. These could be used to carry out entirely new types of attacks and be exploited for novel criminal activities;

3. The nature of threats could change: due to the capabilities of artificial intelligence, crimes could become more effective, targeted and difficult to attribute.[3]

Artificial intelligence therefore significantly changes the kinds and the amount of harm that can be directed against computer users.

1.1.2 AI in Cybersecurity:

As we navigate the modern digital era, AI has emerged as a transformative tool, making significant inroads into various sectors, including healthcare, finance,

[1] Supra note 71 at 16-17.
[2] Same reference at 17.
[3] Same referenceat 18-22.

supply chain, and agriculture. AI is a powerful tool that can be used for both defensive and offensive purposes in cybersecurity[1]. On the one hand, AI can be used by defenders to develop new and more effective ways to detect and prevent cyberattacks[0]. In other words, defenders are increasingly using AI tools to improve intrusion detection, anomaly identification, and other preventive measures, with the goal of proactively thwarting unauthorized access and malicious activities. On the other hand, AI can also be used by cyber criminals to develop new and more sophisticated attack vectors. Thus, the growing symbiotic relationship between AI and Ethics and cybersecurity, as explored by **Error! Reference source not found.**[2], and many others, warrants closer scrutiny.

1.1.3 AI-driven cyberattacks:

AI-driven cyberattacks are emerging as a major threat, as they are becoming more sophisticated and diverse[3]. At the time of writing this paper, it is not yet clear how this will affect the future of cybercrime and warfare. However, the potential for AI-driven cyberattacks has become a serious concern[4]. AI can provide a powerful toolkit for cyber adversaries, to enhance all types of conventional cyber-attacks, including phishing, malware, password attacks, and even manipulation of AI models them-selves.

[1] AL-Dosari, K., Fetais, N., Kucukvar, M.: Artifcial intelligence and cyber defense system for banking industry: a qualitative study of ai applications and challenges. Cybern. Syst. (2024) 11:44. "https://doi.org/10.1080/01969722.2022.2112539"

[2] Ansari, M.J., Dash, B., Sharma, P., Yathiraju, N.: The impact and limitations of artifcial intelligence in cybersecurity: a literature review. Int. J. Adv. Res. Comput. Commun. Eng. (2024) 11:55. "https://doi.org/10.17148/IJARCCE.2022.11912"

[3] Chomiak-Orsa, I., Rot, A., Blaicke, B.: Artifcial intelligence in cybersecurity: the use of ai along the cyber kill chain. In: Nguyen, N.T., Chbeir, R., Exposito, E., Aniorté, P., Trawiński, B. (eds.) Computational collective intelligence Lecture Notes in Computer Science, pp. 406–416. Springer International Publishing, Cham (2019) 13:47

[4] Rickli, J.M., Mantellassi, F.: Artifcial intelligence in warfare: military uses of AI and their international security implications. In: The AI wave in defence innovation, pp. 12–36. Routledge, Cham (2023) 13:15

For example, AI techniques can be leveraged to create malware that can adapt to its environment, learn from its actions, and refine its methods to evade traditional detection mechanisms[1]. Polymorphic and metamorphic malware are stark examples of AI-enabled malware. These strains can self-alter their code to avoid signature-based detection and evolve in response to countermeasures, posing a significant challenge to cybersecurity defenses.

In addition, AI can make phishing attacks more effective; automate the generation of highly convincing fake websites and emails, making it more likely that people will fall for them. AI can also be used to create spear-phishing attacks, which are targeted at specific individuals or entities[2]. By analyzing large datasets, attackers can customize their messages to the target's personal or professional context, making them more likely to be successful.

AI is also making botnets more sophisticated by enabling them to launch more coordinated and targeted attacks, and with the possibility of unpredictable emergence and evolution.

Moreover, AI can make botnets more evasive, helping them circumvent traditional detection mechanisms more effectively. These advancements highlight the changing dynamics of the cyber threats landscape, where AI is becoming a force multiplier for both attackers and defenders[3]. These AI-driven cyber threats also pose a serious risk to privacy and security, and traditional cybersecurity mechanisms may not be able to keep up.

[1] Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K., Singh, S.: A review on cybercrimes on the internet of things. In: Makkar, A., Kumar, N. (eds.) Deep learning for security and privacy preservation in iot, in signals and communication technology, pp. 83–98. Springer, Singap 13:20

[2] Gilad, A., Tishler, A.: Mitigating the risk of advanced cyber-attacks: the role of quality, covertness and intensity of use of cyber weapons. Def. Peace Econ. (2023). https://doi.org/10.1080/ 10242694.2022.2161739 13:30

[3] Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., Sangaiah, A.K.: Classifcation of ransomware families with machine learning based onN-gram of opcodes. Futur. Gener. Comput. Syst..Gener. Comput. Syst. 90, 211–221 (2019). https://doi.org/ 10.1016/j.future.2018.07.052 14:05

Additionally, adversarial AI, which targets the vulnerabilities of AI models, is a distinct threat within the offensive AI umbrella.

AI-driven attacks can have a significant negative impact on society, including extended periods of systemic failures and downtime[1], disruption of emergency services potentially leading to loss of lives, economic and financial losses, social media manipulation potentially leading to political instability, and the possibility of malicious botnets existing indefinitely, with unpredictable emergent characteristics and unlimited potential for evolution[2].

To combat AI-driven cyberattacks effectively, it is essential to understand the attack vectors, vulnerabilities, and motivations of the attackers.

Various researchers have investigated this topic[3] revealing several common motivations that security professionals and organizations should be aware of.

However, these motivations can vary depending on the threat actor and attack type. For example, attackers may be motivated by financial gain, political or strategic goals, or the desire to cause harm. Understanding attacker motivations can also help incident response team's priorities strategies, adapt response tactics, anticipate attack techniques, improve detection capabilities, and develop security countermeasures. This empowers response teams and professionals to mitigate the immediate impact of an attack and minimize future incidents.

This growing complexity and diversification of AI-driven cyberattacks necessitate a thorough exploration to inform our understanding and response strategies.

---

[1] Rabiul Islam, Former Forbes Councils Member, Jun 23, 2023 https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/ 14:25, 12/02/2024.

[2] Rabiul Islam, Same reference.

[3] Jordan Smith, US Reporter, HCL Tech, https://www.hcltech.com/trends-and-insights/cybercriminals-utilizing-ai-commit-cybercrimes 14:35

1.1.4 Among what artificial intelligence can do:

- **Enhancing Existing Attacks:**

AI can make it more challenging for antivirus software and spam filters to detect threats. By leveraging AI, cybercriminals can fine-tune their attacks to evade traditional security measures.

- **Creating New Attacks:**

AI can manipulate or generate fake data, leading to confusion or impersonation. For instance, deep-fake technology powered by AI can create realistic but fabricated videos or audio recordings, potentially deceiving individuals or organizations.

- **Automating and Scaling Attacks:**

Cybercriminals can use AI to automate large-scale attacks with minimal effort. This includes spear-phishing campaigns, social engineering attacks, and even fake customer support chatbots.

- **Empowering Cybercrime Organizations:**

AI reduces the need for human involvement in various aspects of cybercriminal operations. For instance, it streamlines software development, scamming, extortion, and other activities. This efficiency lowers operational costs and minimizes the need for recruiting new members.

1.2 Traditional cybercrimes and modern cybercrimes committed by artificial intelligence:

In Algeria's Penal Code, cybercrime includes:

1.2.1 The crime of illegal entry and stay in automated data processing systems:

Abstract:

The Algerian legislator has dealt with crimes of prejudice to the automatic data processing systems in Chapter seven bis of the Penal Code. These crimes, according to the Penal Code, are the illegal entry and stay in the automatic data processing system, and the intentional assault on the functioning of the automatic data processing system, The legislator also linked some terrorist activities such as financing and recruitment to the use of information and communication technology under Law 16-02 supplementing the penal code, and created another form of information crime under Article 394 8 Duplicate created under Law 02-16, with penalties for these crimes as a whole, misdemeanor, except for what is related to terrorist activity. Felonies are considered according to Articles 87 Duplicate 11 and 87 Duplicate 12 introduced in Law 02-16.

1.2.1.1 The legitimate element of This crime :

There is no crime and no punishment except by a legal text that defines that criminal behavior for us and the appropriate punishment for it. The legislator has interfered with regard to information crime and stipulated it in the penal code in Section Seven bis under the heading of prejudice to automatic data processing systems, and it decided the special penalties for each crime, and the criminal legal texts for acts affecting information and communication technology are represented in Articles 394 Duplicate up to 394 duplicate 8, and part of these crimes dealt with Articles 87 duplicate11 and 87 Duplicate 12. On the basis that the automatic data processing system represents the primary condition, which must be fulfilled in order to search for the availability or non-availability of the elements of the crime of assault on this system, if it is proven that this initial condition is defective, then this research will not be possible. [1]

[1] Amal Kara, 2020, Computer Crime, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law and Political Science, University of Ben Aknoun, Algeria

1.2.1.2 The material element :

We will deal with all the crimes mentioned in the seventh section, bis, for crimes of infringing upon automatic data processing systems, and articles 87 duplicate 11 and 87 duplicate 12 of the code penal.

First: The illegal entry and stay in the automatic data processing system:

Article 394 duplicate of the Penal Code stipulates: “Anyone who enters all or part of a system for automatic data processing or attempts to do so shall be punished with imprisonment from three months to one year and a fine from 50,000 to 100,000 DZD. The aforementioned acts resulted in sabotaging the system’s operation system. "The penalty is imprisonment from six months to two years and the fine is from 50,000 to 150,000 dinars."

This crime through Article 394 bis, we note that it has two forms, the simple image is merely illegal entry or stay, and the aggravated image is achieved by the availability of the aggravating circumstance for it, and it is in the case in which the unlawful entry or stay results in either deletion or change System data or sabotage the system's operating system.

The first simple element:

represented in the mere illegal entry or stay in the automatic data processing system.

- The act of entering into this crime (which is the material pillar of the crime of assaulting the automatic data processing system). Entering here does not mean entering in the material sense, that is, entering a place, house or garden, but rather it must be seen as a moral phenomenon. The similarity to that which we know when we say entering into an idea or into the faculty of thinking in a person, i.e. entering into the mental processes carried out by the automatic data processing system, and the legislator did not specify the means of entry or the way in which to

enter the system, so the crime occurs by any means or method. It is equal to entry directly or indirectly.[1]

It is noticed through this article that the Algerian legislator considered the crime of unauthorized entry as a formal crime (in which the physical element is not required to achieve the criminal outcome), meaning that it is an offense merely to enter the system of automatic data processing, in whole or to only part of it, provided that it is actually to enter without a permit is intended and is not just a coincidence or a mistake.[2]

Remaining unauthorized in the automatic data processing system means continuing to be present within the processing system without permission from its owner or has control over it, meaning that a person remains inside the treatment system the property of others after entering into it by mistake or by chance, despite knowing that his / her stay there is unauthorized, and the crime of unauthorized survival is realized according to Article 394.

The aforementioned repeater has achieved its material pillar represented in the act of staying without a face of hatred, regardless of whether this survival was intended by the perpetrator or not intended, and the Algerian legislator considered the crime of the licentious baggage with this system of automatic data processing of formal crimes that do not require their occurrence to achieve a criminal result. To acknowledge the existence of the crime of complete existence and foundations its.[3]

The second aggravating element:

In order for the aggravating circumstances mentioned in Article 394 bis Paragraph 2 to be available, it is necessary to prove the existence of a causal relationship between the act of entering or remaining unauthorized, and the

[1] Amal Kara, 2020, Same reference.

[2] Jamal Brahimi, 2016, Combating Cybercrime in Algerian Legislation, The Critical Journal of Law and Political Science, Volume 2, Issue 2, Algeria.

[3] Jamal Brahimi, 2016, same reference.

criminal outcome specified by the article in the erasure and modification of the system data or sabotaging the operation of the system itself, otherwise we were in the process of a crime in its simple aforementioned form. In the text of Article 394 duplicate 1 of the Penal Code, and perhaps the goal of this strictness is to limit the aggravation of information crime.[1]

Second: Intentional attack on the automatic data processing system:

The Algerian legislator stipulated it in Article 394 duplicate 2 of the Penal Code: "Anyone who, by means of fraud, introduces data into the automated processing system, or removes or modifies, by means of fraud, the data it contains shall be punished with imprisonment from six months to three years and a fine from 500,000 to 2,000,000 dinars."

The first type:

Intentional attacks on the data within the system, The criminal activity in the crime of deliberate assault on data is embodied in one of the following three forms: Intrusion, Effacement, and Modification, and these images are not required to meet, rather it is sufficient for the perpetrator to issue one of them only in order for the material element to be available, and the acts of insertion, erasure and modification It involves manipulating the data contained in the automatic data processing system, whether by adding new incorrect data. Or erase or amend pre-existing data, which means that the criminal activity in this crime is only in response to a specific place or topic, which is the data or information that has been processed automatically, which has become mere signs or symbols that represent that information, and not the information in itself as One of the elements of knowledge, and the place of this criminal activity is limited to the data within the system, that is, those that are contained in the system and form part of it [2].

[1] Jamal Brahimi, 2016, same reference.

[2] Amal Kara, previous reference, 2001, p52

The second type: traditional attack on the system's external data:

The Algerian legislature provided criminal protection for the data in and of itself by criminalizing the following behaviors:

1-The text of Article 394 bis 2 aims to protect data as such, because it is not required that it be within the automatic data processing system or that it has been processed automatically, the subject of the crime is the data, whether it is stored on tapes or disks, or that is processed automatically, or that is sent through an information system, as long as it may be used as a means to commit the crimes stipulated in Section Seven bis of the Penal Code.

2- The text of Article 394 bis 2/2 criminalizes acts of possession, disclosure, publication, use, whatever the purpose of these acts that are contained in the data obtained, from one of the crimes mentioned in Section Seven bis of the Penal Code, with the objectives of unfair competition, espionage Terrorism, incitement to immorality...[1]

Intentional assault on the functioning of the automatic data processing system:

It was stipulated in Articles 05 and 08 of the International Convention on Information Crime, the Algerian legislator did not provide a provision for intentional attacks on the functioning of the system, and it was satisfied with the provision for the intentional attack on the data within the system, This may be explained by the fact that the abuse of data may affect the system's ability to perform its functions. This material behavior is the act of stopping the automated data processing system from performing its normal activity and what it is expected to do (such as introducing a virus program, or making the system slowdown in its performance of its functions. .), And either in the act of spoiling the activity or functions of this system, and it is not required that the act of disrupting or the act of

[1] Atta Allah Fashar, 2017, Confronting Cybercrime in Algerian Legislation, Research Presented to the Moroccan Conference on Law and Information Technology, Academy of Graduate Studies, Libya.

corruption occur on all the elements of the system altogether, rather it suffices that it affects only one of these elements, whether the physical, the computer itself, communication networks, and transport devices. As for the moral, such as programs and data.[1]

Crimes developed under Law 16-02 supplementing the Penal Code:

Certainly, criminal justice is clearly embodied when the penal policy aims to organize three sides: the prevention policy, the criminalization policy and the punishment policy. The first steps of the penal policy are criminalization, which is assumed to be a reflection of the social, political and economic reality within the state, it seems that crime with its methods is subject to development and growth, which requires the lawmaker to keep pace with this development in an attempt to confront it. Crime has taken on a global dimension by expanding its scope and introducing technology to its methods, and because crime fighting takes place at two levels: international and national, and it is certain that the issuance of Security Council resolutions similar to the resolution No. 1377 of 2001, and Resolution No. 2253 of 2015, associated with the development of terrorism crimes, had a legislative effect in Algeria, through the Algerian legislator's issuance of Law No. 02-16 on June 19, 2016, which complements Order No. 66-156 containing the Algerian Penal Code. By adding new articles, they are: 87 duplicate 11, 87 duplicate 12, and 394 duplicate 8.

This law also included strengthening the response to information crime due to its connection with the practice of many new crimes. In the year 2016, in the context of the legislator’s adaptation and updating of the provisions of the law related to information and communication technology, its legislative system, especially those related to combating terrorism, which is also known to be a remarkable development as the perpetrators of this type of terrorism crimes are

[1] Amal Kara, previous reference, 2001, p47

adopted. He denied carrying out his information and communication technology crimes, and this is in Articles 87 duplicate 11 and after.

This is through the criminalization of the act of transferring Algerians or foreigners residing in Algeria legally or illegally to another country to commit, incitement or training in terrorist acts using information and communication technology or any other means, and criminalizing acts of recruiting people for the benefit of associations, organizations, groups or organizations. This law criminalizes the phenomenon of combatants who move to other countries for the purpose of committing terrorist acts and prohibits the financing of these acts.

Whereas Article 394 duplicate 8 introduced under Amendment 16-02 includes the penalties imposed on the Internet service provider, who, despite being notified by the National Commission for the Prevention and Control of Crimes Related to Information and Communication Technology, does not perform an order or court ruling obligating him to intervene to withdraw or store the contents. Which allows access to it or makes access to it not possible when it constitutes crimes stipulated in the law, and the service provider is also punished if he fails to put in place technical arrangements that allow the withdrawal or storage of these contents?

1.2.1.3 The moral element of the crime :

Clarifying this element is considered one of the important matters in determining the nature of the behavior committed, and adapting it to determine the material texts that need to be applied, and the moral element in the various attacks affecting information systems takes the form of criminal intent in addition to the intention to cheat. Intentionally, where the moral element in it takes the form of criminal intent with its two components knowledge and will, as for the intention of fraud, it appears through fraud with which the entry is made from a breach of the

regulatory system that protects the system, as for survival, it is deduced from the operations that took place within the system.[1]

1.2.1.4 The forms of penalties imposed for crimes affecting information and communication technology:

Given the seriousness of the information crime, the Algerian legislator decided on the appropriate penalties for it, whether committed by a natural person or by a legal person, and each of them is subject to the penalty set for it. 2.1 penalties imposed on a natural person We will discuss the original penalties to which the natural person is exposed, as well as the complementary penalties.

First - Principal penalties:

We will deal with the punishment of each crime separately.

* The crime of unlawful entry and stay in the automated data processing system in its simple form is stipulated in Article 394 duplicate of the Penal Code, whereby it is punishable by imprisonment from six months to 2 years, and a fine from 60,000 to 200,000 DZD.

* As for the penalty for the aggravation of the crime of illegal entry and stay in the automatic data processing system, Article 394duplicate paragraphs 2 and 3 stipulated that "the penalty shall be doubled if this results in the deletion or change of the organization's data, and if the above-mentioned acts result in sabotaging the system's operating system, the penalty shall be detention. From a year three-year and the fine is from 100,000 to 300,000 dinars.

* Deliberate assaults on data, the Algerian legislator stipulated in Article 394 duplicate 1 of the Penal Code "shall be punished with imprisonment from a year to three years and a fine from 500,000 to 2,000,000 dinars. The data it contains.

[1] OuliOuld Rabah Safia, 2015, The Legal Nature of Cybercrime, National Conference on Cybercrime: Between Prevention and Combating, University of Mohamed Kheider, Biskra, November 15-16, Algeria.

* As for the punishment prescribed for the use of data in committing one of the crimes affecting the information systems, as well as the possession, disclosure, publication or use of data obtained from one of the crimes affecting the information systems, it is imprisonment from a year to five years and a fine from 1,000,000 to 5,000,000 Algerian dinars, according to Article 394 bis 2 from penal code.

* The penalties for these crimes are doubled if the crime targets the national defense or the bodies and institutions subject to public law, according to Article 394 bis 3 of the penal code.

* In the crimes created under Law 16-02 supplementing the penal code, Article 87 bis 11 dealt with temporary imprisonment from 05 to 10 years and a fine of 100,000 to 500 thousand inflicted on every Algerian or even a foreigner residing in Algeria in a legal or illegal manner who travels or He tries to travel to another country with the intention of committing, planning, preparing, or participating in terrorist acts, or training to commit them, or to receive training thereon, and he shall be punished with the same penalty: the one who commits these acts shall be punished with the same punishment, and whoever uses information and communication technology to commit these acts shall be punished with the same punishment. Imprisonment from 05 to 10 years and a fine of 100,000 to 500 thousand anyone who uses information and communication technology to recruit people for the benefit of a terrorist or an organization or an organized group whose purpose is the purpose of direct or indirect terrorist acts.

As for Article 394 duplicate 8 .it punishes from one year to 03 years or a fine from 02 million to 10 million whoever provides services, who do not perform, despite his excuses, by the National Commission for the Prevention and Control of Crimes Related to Information and Communication Technology, and the issuance of an order or judicial ruling obligating him to intervene to withdraw or Storing the contents that can be viewed or making access to them not possible when they

constitute crimes stipulated in the law, and the service provider is also punished if he fails to put in place technical arrangements that allow the withdrawal or storage of such contents.

Second - Supplementary Punishments:

Such penalties were stipulated in Article 394 bis 6 of the penal code: “While preserving the rights of bona fide third parties, it is ruled to confiscate the hardware, software and means used and close the sites that are the subject of a crime punishable according to this section, in addition to closing the shop or place of exploitation If the crime was committed with the knowledge of its owner.

Confiscation:

It is a complementary punishment that includes the hardware, software, and means used to commit a crime involving information systems, taking into account the rights of others in good faith.

Closing down sites: This is about the sites (les sites) that are the subject of a crime, one of the crimes affecting information systems.

- Close the shop or the place of exploitation: if the crime was committed with the knowledge of its owner, for example the closing of the electronic café from which such crimes are committed, provided that the knowledge elements are available to the owner.[1]

Penalties imposed on the legal person :the penalties applied to the legal person when committing any of the crimes affecting information systems:

5 times the maximum fine determined for a natural person, and this is according to Article 394 bis 4 of the penal code, which states: “A legal person who commits one of the crimes stipulated in this section shall be punished with a fine equivalent to five (5) times the maximum fine prescribed for the person. Natural. "

[1] Fushar, 2009, Page 34

1.2.2 The crime of stealing credit card numbers in Algerian penal code:

Having examined the most significant acts committed by third parties that are considered an assault on the credit card system and that would constitute an offense, this study will attempt to legally adapt each form of this assault to the Algerian Penal Code. This is necessary due to the absence of legal provisions governing the crimes to which the credit card is subjected.

The Algerian legislator only cited two cases:

the use of a lost and stolen card.

1.2.2.1 Legal Adaptation of Stolen Credit Card Use Status:

Article 350 of the Algerian Penal Code (PC) states: "Anyone who embezzles something that is not owned by him shall be considered a thief..." As criminal doctrine defines theft as: "embezzlement of a movable property owned by a third party with the intention of possessing it" (Saudi Arabia, 2001), or as an assault on the ownership and possession of movable property with the intention of possessing it.

The elements of the offense here are the physical element of taking the card, i.e., removing it from the legitimate owner's possession without his consent and knowledge and transferring it to his possession. The object of the crime in this case is the card, which is considered movable property.

The moral element is criminal intent, which means knowledge of the elements of the crime and the will to achieve or accept them. In other words, once the card is seized by the third party and his intention is to own it, he has committed the crime of theft under Article 350 of the PC. If the theft of the card is accompanied by its use, we will be dealing with an aggravating circumstance due to the plurality of offenses here.

1.2.2.2 Legal Classification According to French Jurisprudence

French jurisprudence considers the accused in this case to be responsible for the crime of fraud because his act constitutes a fraudulent means when he uses the card using the real name of its holder. This is tantamount to the use of a false name, which is one of the fraudulent forms of the crime of fraud provided for by law (Salem, 1995). The offender's actions amount to deceiving the merchant and the issuing entity about the validity of the credit card and the existence of fictitious credit. Thus, we are dealing with a material plurality of crimes committed for the purpose of using the credit card, which makes the perpetrator subject to Article 34 of the PC (SGC). "In the event of multiple offenses or misdemeanors referred together to a single court, a single penalty of deprivation of liberty shall be imposed and shall not exceed the maximum penalty prescribed for the most serious offense."

1.2.2.3 Exception to Fraud Classification

Based on the foregoing, we believe that the use of a stolen card by a third party constitutes the crime of fraud and embezzlement only in one specific case: when the user of the card obtains the goods and services delivered to them by the merchant after deceiving the merchant about the validity of the card and the credit granted to them through it. In other words, the user of the card (the third party) uses falsehood, which is one of the fraudulent methods, constituting the crime of fraud and embezzlement, not just theft.

However, we may find ourselves in a situation where the third party has taken the card with the intention of using it and returning it.

The Egyptian Court of Cassation has ruled that "he is not considered a thief, as he lacks criminal intent," such as a person who seized printing tools to print publications with them and then returned them. This is because temporary use is not sufficient to establish the criminal intent of the crime of theft, as there must be an intention to own. Therefore, the perpetrator cannot be held accountable for the

crime of theft due to the absence of criminal intent, which is the intention to own (Al-Baghdadi, 2009). However, according to Article 350 of the PC, it is considered theft and embezzlement even if there is an intention to return it.

the third party can be held accountable for the act of embezzlement in the event that they have stolen the card in addition to the crime of forgery in a private document, as they have acted in place of the cardholder and forged their signature on it and impersonated them. They can also be held accountable for the crime of theft of money and the value of the goods obtained using the stolen card. Thus, we are dealing with a plurality of crimes and the most severe penalty is imposed on them according to Article 34 of the PC.

Principal penalties:

We will deal with the punishment of each crime separately.

* The crime of unlawful entry and stay in the automated data processing system in its simple form is stipulated in Article 394 duplicate of the Penal Code, whereby it is punishable by imprisonment from six months to 2 years, and a fine from 60,000 to 200,000 DZD.

* As for the penalty for the aggravation of the crime of illegal entry and stay in the automatic data processing system, Article 394duplicate paragraphs 2 and 3 stipulated that “the penalty shall be doubled if this results in the deletion or change of the organization’s data, and if the above-mentioned acts result in sabotaging the system’s operating system, the penalty shall be detention. From a year three-year and the fine is from 100,000 to 300,000 dinars.

* Deliberate assaults on data, the Algerian legislator stipulated in Article 394 duplicate 1 of the Penal Code “shall be punished with imprisonment from a year to three years and a fine from 500,000 to 2,000,000 dinars. The data it contains.

* As for the punishment prescribed for the use of data in committing one of the crimes affecting the information systems, as well as the possession, disclosure, publication or use of data obtained from one of the crimes affecting the

information systems, it is imprisonment from a year to five years and a fine from 1,000,000 to 5,000,000 Algerian dinars, according to Article 394 bis 2 from penal code.

* The penalties for these crimes are doubled if the crime targets the national defense or the bodies and institutions subject to public law, according to Article 394 bis 3 of the penal code.

* Article 394 bis 5(Law No. 04-15 of November 10, 2004)

Anyone who participates in a group or agreement formed for the purpose of preparing for one or more of the offenses provided for in this section, and such preparation is embodied in an act or several material acts, shall be punished with the same penalties as those provided for the offense itself.

* Article 394 bis 6(Law No. 04-15 of November 10, 2004)

Without prejudice to the rights of bona fide third parties, the equipment, software and means used shall be confiscated and the sites that are the scene of an offense under this section shall be closed down, in addition to the closure of the shop or place of exploitation if the offense was committed with the knowledge of its owner.

* Article 394 bis 7(Law No. 04-15 of November 10, 2004)

An attempt to commit the misdemeanors provided for in this section shall be punished by the penalties prescribed for the misdemeanor itself.[1]

1.3 The crime of stealing credit card numbers committed by Ai:

- Abstract:

The use of credit cards for online purchases has significantly increased as a result of the growth of e-commerce and electronic payment systems. However, this

[1] The Algerian penal code: articles 394 bis 1,2,3,5,6,7/Amended and Completed (Law 04-15 + Law 24-06) Section 7

rise has also resulted in an increase in credit card fraud and its cost, which has cost financial institutions and people a lot of money. Therefore, in order to identify and analyses fraud, financial institutions and decision-makers are under pressure to come up with novel solutions using cutting-edge technologies like artificial intelligence (AI) and machine learning (ML).

The growth of the increasing reliance on remote purchasing of goods and services has led to the development of e-commerce and remote electronic payment systems. However, these advancements have also resulted in a significant rise in credit card fraud globally, causing financial institutions and individuals' substantial costs and losses. In 2022, the total losses due to credit card fraud worldwide reached $32.34 billion, an 8.3% increase compared to 2021.[1]

This type of fraudulent activity occurs when unauthorized individuals gain access to credit card information to make unauthorized purchases, withdraw funds, or utilize services without the cardholder’s consent.

Consequently, it has become crucial to explore effective systems and methods for detecting credit card fraud.

Machine learning algorithms can be employed to detect credit card fraud. These algorithms have the ability to “learn” complex patterns to identify fraudulent transactions in real time, surpassing traditional methods.

However, the evolution of fraud detection algorithms has faced challenges due to the highly imbalanced nature of fraud data, the lack of standardized evaluation criteria for identifying the best-performing algorithms, limited sharing of research results, difficulties accessing confidential transaction data for research purposes, and the constant adaptation of fraudsters to new techniques.

[1] 14 Ways Scammers Can Steal Your Credit Card Numbers in 2024/ Hari Ravichandran/ https://www.aura.com/learn/how-do-people-steal-credit-card-numbers01/03/2024 19:25

Machine learning offers several advantages over other methods for credit card fraud detection. It enhances accuracy by analyzing vast amounts of data and identifying patterns associated with fraudulent activity.

Additionally, machine learning algorithms can scale to handle large transaction volumes, ensuring efficient and timely analysis. Furthermore, these algorithms adapt to evolving fraud patterns, allowing companies to stay at the forefront of new fraudulent technologies.

The ability to adapt is crucial, as fraudsters continually devise new methods. Moreover, machine learning-based solutions are cost-effective for fraud detection systems.

In summary, machine learning plays a pivotal role in combating credit card fraud, providing accurate and efficient detection mechanisms that adapt to emerging threats.

Credit card fraud involving stolen cards is a major issue that can be addressed using AI-based solutions. The key types of stolen card fraud include:

Card Present Fraud: When a fraudster physically uses a stolen or counterfeit credit card to make purchases at a merchant location.

Card Not Present (CNP) Fraud: When a fraudster uses stolen card information (card number, expiration date, security code) to make unauthorized online, phone, or mail order transactions.

Lost or Stolen Card Fraud: When a credit card is physically lost or stolen, and the fraudster makes unauthorized transactions before the cardholder reports it missing.

To detect these types of stolen card fraud, AI and machine learning can be leveraged to analyze large volumes of transaction data and identify suspicious patterns. Some key capabilities of AI-powered fraud detection include:

Analyzing transaction histories to spot anomalies that may indicate a stolen card is being used Applying predictive analytics and deep learning to uncover hidden fraud patterns Leveraging collective intelligence from fraud data consortiums to stay ahead of new fraud tactics Automating real-time fraud monitoring and decision-making to enable faster response

By deploying advanced AI-based fraud detection, financial institutions can more effectively identify and prevent credit card fraud involving stolen cards, protecting both businesses and consumers

1.3.1 Types of Credit Card Fraud and Precautionary Measures:

Credit card fraud refers to any illegal activity involving unauthorized use of a bank card or credit card information to make purchases, withdraw cash, or conduct other financial transactions. This can be done through various methods and activities such as phishing, card theft, or other means. These activities can lead to financial losses for both the card issuer and the cardholder, as well as potentially damage the cardholder's credit rating and erode trust in financial institutions, impacting the stability of the financial system. Credit card fraud is a form of identity theft that involves obtaining someone's credit card information without authorization to collect purchase fees or withdraw funds, and it involves intentional or unintentional acts aimed at deceiving others, resulting in victims incurring losses while benefiting the fraudster.[1]

While some countries limit the liability of credit cardholders in cases of theft, for example, under the Federal Law in the United States (15 U.S.C. § 1643), the responsibility for losses is capped at $50 in case of credit card theft. However, in some cases, banks may waive this amount if the cardholder signs a written statement explaining the card loss. It is essential for individuals to be vigilant,

[1] Credit Card Fraud /By FindLaw Staff/ https://www.findlaw.com/criminal/criminal-charges/credit-debit-card-fraud.html 07/03/2024 9:10

protect their card information, report any suspicious activities promptly, and follow security best practices to prevent falling victim to credit card fraud.

1.3.2 Types of Credit Card Fraud:

Credit card fraud can generally be divided into two categories:

Physical Card Fraud, which involves the physical use of bank cards for fraudulent transactions like cash withdrawals with counterfeit or stolen cards.

and Card-Not-Present (CNP) Fraud, which is the most common type currently. CNP fraud includes all transactions where fraudsters make payments online using card details obtained through phishing, data breaches, or other means, settling transactions in various ways and often without the cardholder's knowledge. Credit card fraud takes various forms and shapes, occurring through online networks, phone transactions, phishing emails, data breaches, or even theft of credit cards from mailboxes. Here are some common types of credit card fraud and ways to protect against them.

A. Fraudulent Transactions Using Bank Cards

This category encompasses three scenarios, whether through self-use of the card, obtaining a duplicate card, or falsifying it. Below is an overview of these types:

B. Fraud Resulting from Loss or Theft of Credit Cards

Fraudsters in this type of deception acquire credit cards through theft or by obtaining a lost card. In such cases, the fraudster attempts to use credit card information for transactions over the global network or other purchase operations. One of the fundamental credit card fraud schemes is simply stealing someone else’s credit card or using a card that someone has lost. It is also possible to steal credit cards sent to their owners via mail (2021, ECB)[1]

[1] Penal Code 484e PC Theft of Credit Card Information California Law/ https://www.shouselaw.com/ca/defense/penal-code/484e / 05/03/2024 10:25

C. Fraud by requesting a copy of the credit card

In this type of deception, fraudsters use stolen personal information (such as name, address, date of birth, social security number, and other data) to apply for a credit card. This type of fraud can persist without detection until the victim applies for credit themselves or verifies their credit report. While victims are typically not liable for fraudulent credit card accounts due to the protections offered by credit cards, this type of fraud can still harm the victim's credit score and credit classification.

D. Fraud through Creating a Copy of the Original Card:

In this case, fraudsters rely on fraudulent devices to obtain credit card information **illegally**, such as "scrapers." These devices can capture credit card information from the magnetic stripe when cards are swiped without the cardholder's knowledge of this device. Subsequently, the fraudsters can copy this information to create counterfeit cards and use them, or sell the card data to other fraudulent entities (2009, al etDelamaire)

E. Card-Not-Present (CNP) Fraud:

This type of fraud occurs when fraudsters gain access to the personal data of credit card holders and then use it to make purchases online or over the phone. Since there is no physical card present for inspection, it becomes challenging for payment processors to verify the identity of the buyer (2021, ECB). CNP fraud can occur in several ways, including:

F. Email Fraud:

Fraudsters employ this method by sending emails to targeted individuals to obtain their personal data, such as birthdates, full names, address details, and more. Through the theft of as much data and supporting documents as possible, they aim to execute their schemes. Subsequently, they may compromise computer systems

and utilize this information for unauthorized access to bank accounts, credit card data, and conducting transactions or fund transfers

G. Phone Fraud:

This type of credit card fraud is more common, where the fraudster contacts the cardholder posing as a bank representative and obtains sensitive personal information such as birthdates, passwords, and card details. Often, these calls are made by the fraudster using a convincing pretext, making the cardholder unwittingly disclose sensitive information[1]

H. Fraud Using Card Data Readers:

A fraudulent card reader device known as “scrapers” is one of the tools used to illicitly obtain credit card information from the magnetic stripe on the back of the card. Fraudsters attach these reading devices alongside ATMs, retail point-of-sale terminals, or fuel stations, among other locations. They then either sell the acquired information to other criminals or use it to collect funds from the targeted card.

In addition to the aforementioned types, there is another form of fraud related to bankruptcy, which is considered one of the most challenging types of fraud to anticipate. Various methods and techniques exist to help prevent it. Bankruptcy-related fraud involves using a credit card for individuals facing financial hardship. The cardholder knowingly initiates a payment but acknowledges thatthey are unable to pay their obligations due to bankruptcy. Ultimately, the bank bears the losses, especially since this type of fraud is not covered in the account designated for potential losses. The best approach to prevent bankruptcy-related fraud is to conduct prior checks with credit bureaus to obtain credit reports and information about customers.

[1] Credit Card Fraud/ https://www.scribd.com/presentation/241860981/Credit-Card-Fraud/ 27/03/2024 05:23

I. AI-Based Fraud Using Voice Identity:

Many banks and financial institutions turn to **voice biometrics** as a tool to prevent fraudsters from accessing financial data of individuals and organizations. A unique voiceprint is created for various verification purposes, allowing recognition of speech patterns and identity verification through free conversation with bank agents. Additionally, password phrases can be used for account authentication by speaking specific phrases. Despite the necessary checks to ensure that the audible voice is not duplicated or recorded, modern fraudsters exploit advanced technologies like **"voice deepfakes"** to reproduce someone's speech available on the internet for fraudulent purposes. This type of fraud is not only highly dangerous due to audio and visual impersonation but also unexpectedly perilous, given the remarkable advancements in modern technologies. It poses a significant threat to data security in the business sector overall (2023, Euro news)

1.4 Artificial Intelligence as a vector of crime:

1.4.1 Approaches of malevolent artificial intelligence:

This section provides an overview of the various criminal strategies that could be facilitated by malevolent uses of AI. This section is not meant to be exhaustive as the nature of criminal innovation is always unpredictable, but seeks to highlight a number of areas that could be affected by the availability of artificial intelligence.

Social Engineering:

Social engineering has been defined as "any act that influences a person to take an action that may or may not be in their best interest." It is an effective attack strategy targeting human rather than technical vulnerabilities that can be extremely hard to protect against, for individuals and companies' alike[1]. In this subsection,

[1] "Social Engineering Defined", Security Education (Website), online: https://www.social-engineer.org/framework/general-discussion/social -engineering-defined . . . 03/03/2024 12:36

we describe the numerous approaches in social engineering that could be significantly expanded and facilitated by artificial intelligence [1]

Phishing:

Instead of using the voice, people may also use the method of 'phishing', which can be defined as the 'practice of sending emails appearing to originate from reputable sources with the goal of influencing or gaining personal information'. It is likely the most widespread type of social engineering[2]. Typically, an attacker will create an email that purports to originate from a trustworthy source, such as a financial institution, tech support service or a government institution. These emails will then be sent out in bulk. A person who clicks on a link will be taken to a counterfeit but convincing website where they are asked to enter their personal information.[3] the email might also contain an attachment which, once clicked, infects the victim's computer with malware. There are many ways an attacker might try to convince the user that the email is real, such as by altering the email address so that it seems legitimate or buying web domains that are very similar to the official domain names of the institutions being targeted. A more personalized variant is called spear-phishing. Instead of sending an email to users in bulk, spear-phishing operations target specific users with meticulously crafted emails. These emails might be based on data obtained from social media or any other open-source intelligence the attacker has been able to gather on the target.[4] For example, an email containing a link to a CV might be sent to a recruiter. In order to view the CV, the user is asked to log into their Microsoft account, through a page that mirrors exactly the look and feel of the real Microsoft portal. However, once users enter their details, the log-in credentials are instead harvested by the attacker, who are then able to compromise their victims' accounts. While very effective, spear-

[1] Ian Mann, Hacking the human: Social engineering techniques and security countermeasures, (London: Rutledge, 2008).

[2] Phishing", Security Through Education (Website) Phishing", Security Through Education (Website), online:

[3] Same reference; "Phishing", Know4Be (Website), online: https://www.knowbe4.com/phishing.

[4] Same reference; "Spear Phishing", Know4Be (Website) online: https://www.knowbe4.com/spear-phishing/

phishing requires attackers to perform a significant amount of background research and to create credible messages, limiting its use to high-value targets.[1]

There is a big risk that artificial intelligence might enable criminals to combine the scale of regular phishing attacks with the targeted nature and effectiveness of spear-phishing. A system could be designed that would crawl a large number of targets' online presence, such as social media feeds. Profiles of these users could then be created, that would include which interests they have, which companies they have relationships with, and mapping patterns of online activity. Based on this information, a highly persuasive email might be created or selected by the machine. This could be done at a massive scale, unconstrained by the need for human operators. Additionally, the artificial intelligence system would be able to learn what works based on response or click rates, and subtly alter each message to circumvent phishing filters deployed by the victims' mail platforms. A recent study showed how effective such strategies could be and how easily they could be organized. Using a Machine Learning algorithm, a group of researchers were able to identify the interests of a group of targets by analyzing their Twitter activity. They then used the algorithm to word and send them personalized messages that contained a potentially malicious link, drawing on the content of messages that had been identified as resonating with the victims' interests. They also timed the fake messages with the period of the day when the victims seemed most active on the social platform, to maximize the chances of engagement. They then tracked how many users clicked on the embedded links that could have been malicious, had the researchers been criminal hackers instead. Between 33 and 66% of the targets clicked on the links, eclipsing the 5 to 14% usually achieved with mass phishing.[2]

[1] Supra note 71 at 19.

[2] John Seymour & Philip Tully, "Weapon zing data science for social engineering: Automated E2E spear phishing on Twitter" (Paper delivered)

Vishing :

Vishing (a portmanteau of the words 'voice' and 'phishing') is the "practice of eliciting information or attempting to influence action via the telephone."[1] An attacker might manipulate its mark by claiming to work for the victim's bank, to be a Microsoft support employee or to represent a tax agency.[2] The scams can have devastating consequences – supposedly, victims of phone-based scams lost on average 720 USD in 2017.[3] Due to the propensity of people to trust phone calls, these attacks can be hard to defend against.107 Even tech-savvy people can fall for the more advanced methods.108 However, these frauds often require a lot of preparation and a skilled and convincing operator to pull them off.[4] The attacks can also take some time to perform, which limits the rate of victimization.

This might change with artificial intelligence. The same techniques used to create a helpful Chabot, such as Apple's Siri [5] or Amazon's Alexa[6], can also be used to create a computer system able to imitate a human. Google has already proven that artificial intelligence can be used to create phone call operators that are virtually indistinguishable from real humans in tone and phrasing. This system, known as Duplex, is able to call restaurants and hair dressers to book a table or make an appointment without the employees at the other end of the line noticing they are interacting with a machine.[7] By using AI methods of realistic voice generation and natural language processing to respond to queries, criminal hackers[8] could thus create automated targeting operations. Even if they are not as effective

[1] Vishing ,Security Through Education (Website), online: https://www.social-engineer.org/framework/attack-vectors/vishing/

[2]Rasha Al Marhoos, "Phishing for the answer: Recent developments in combating phishing", (2007) 3:3 I/S: A Journal of Law and Policy for the Information Society 595

[3] "The top frauds of 2017", Consumer Information, (1 March 2018), online: https://www.consumer.ftc.gov/blog/2018/03/top-frauds-2017.

[4] "Let's Go Vishing", (22 December 2014), online: Security Through Education. https://www.social-engineer.org/general-blog/lets-go-vishing>

[5] "Siri", Apple (Website), online: https://www.apple.com/siri/ 20/04/2024 12:51

[6] "Ways to Build with Amazon Alexa", Amazon (Website), online: https://developer.amazon.com/alexa

[7] "Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone", Google AI (Blog), online: http://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conver sation.html. 20/04/2024 14:01

[8]We deliberately use the term 'criminal hacker' to avoid the usual confusion between the majority of technology enthusiasts who like to tinker with software and hardware and the small minority of this group that uses their technical expertise to deliberately break the law. [8]

as human operators, these systems could be deployed at a much larger scale, targeting thousands of individuals per day. This is thus an area where AI could increase the scale of crime. Brian Krebs describes for example how there are already systems using artificial intelligence to target individuals using a vishing stratagem. He describes a person's experience of being called by the employee of a Credit Alert Service. The caller sounded very realistic and was able to answer simple questions. However, after some more complicated enquiries, the caller was seamlessly

switched out for a real human who attempted to finalize the fraudulent exchange. This shows how voice recognition and generation can be used to automate vishing operations. [1]

Artificial intelligence could even be used to create new attack vectors in vishing. Lyrebird, a Montreal-based AI startup launched in 2017 allows a user to train a synthetic version of their voice by recording a few sentences of their real voice.[2] Malicious actors could use this technology to generate voice messages that sound like they come from close relatives or friends (by training the machine with publicly-available videos or fake calls made to the persons whose voices need to be counterfeited), tricking the user to give out information.[3] This new capacity could alter the trust we place in a voice.[4]

1.4.2 Astroturfing:

Another practice that might be exacerbated by AI is astroturfing. It consists of creating fake grassroots movements that seem to be genuine and wide-spread but

[1] 4 Krebs, supra note 108

[2] Francesca Cristiana, "How Lyrebird Uses AI to Find Its (Artificial) Voice", Wired (15 October 2018), online: https://www.wired.com/brandlab/2018/10/lyrebird-uses-ai-find-artificial -voice/; "Lyrebird: Ultra-Realistic Voice Cloning and Text-to-Speech", Lyrebird's (Website), online: https://lyrebird.ai/. 20/04/2024 17:48

[3] Malicious Use of Artificial Intelligence, supra note 71 at 20.

[4] Abhimanyu Goshen, "I trained an AI to copy my voice and it scared me silly", The Next Web (22 January 2018), online: https://thenextweb.com/insights/2018/01/22/i-trained-an-ai-to-copy -my-voice-and-scared-myself-silly/

in fact stem from very few actors.[1] There are several firms which offer astroturfing as a service and provide software that allow employees to manage several online personas.[2] Astroturfing can be used by corporations to review their products in order to make them seem more desirable. Some claim that up to one third of online reviews are fake.[3] Astroturfing can also be used for political manipulation, by for example tweeting or sharing a certain viewpoint. A study showed for example that astroturfing techniques could be very effective in raising doubts about the origins of global warming.[4] Thus, fringe political views can be made to seem mainstream and to appear on the "trending" section on such social media websites as Twitter. Bots were allegedly used leading up to and after the 2016 U.S. presidential election to shift the public view towards voting for Trump, to make his base seem stronger than it was, or to discourage certain voters from voting at all.[5] In a consultation by the Federal Communications Commission (FCC) in the U.S., millions of briefs in favor of abolishing net neutrality were apparently filed by fake accounts, many under the names of dead people.

A data scientist discovered 1.3 million comments that followed extremely similar linguistic constructions and were thus likely fake.[6] Artificial intelligence could potentially drastically increase the efficiency of astroturfing. Twitter, for example, uses anti-bot mechanisms to detect and ban fake accounts.[7] This means

[1] Thomas P Lyon & John W Maxwell, "Astroturf: Interest Group Lobbying and Corporate Strategy" (2004) 13:4 J Econ Manag Strategy 561; Kevin Grandia, "Bonner & Associates Undemocratic History of Astroturfing", Huffington Post (26 August 2009), online: https://www.huffingtonpost.com/kevin-grandia/bonner-associates-the-lon_b_269976.html. 16/03/2024 13:24

[2] Grandia, supra note 118; David Streitfeld, "Book Reviewers for Hire Meet a Demand for Online Raves", The New York Times (25 August 2012), online: https://www.nytimes.com/2012/08/26/business/book-reviewers-forhire-meet-a-demand-for-online-raves.html. 16/03/2024 13:28

[3] Streitfeld, supra note 119.

[4] Charles Cho et al, "Astroturfing Global Warming: It Isn't Always Greener on the Other Side of the Fence" (2011) 104:4 J Bus Ethics 571

[5] Jon Swaine, "Russian propagandists targeted African Americans to influence 2016 US election", The Guardian (17 December 2018), online: https://www.theguardian.com/us-news/2018/dec/17/russian-propa gandists-targeted-african-americans-2016-election.

[6] Jeff Kao, "More than a Million Pro-Repeal Net Neutrality Comments Were Likely Faked", Hacker Noon (23 November 2017), online: https://hackernoon.com/more-than-a-million-pro-repeal-net-neutrality -comments-were-likely-faked-e9f0e3ed36a6. 20/04/2024 11:36

[7] Brian Krebs, "Buying Battles in the War on Twitter Spam", Krebs on Security (Website) online: https://krebsonsecurity.com/2013/08/buying-battles-in-the-war-ontwitter-spam/ "Astroturfing, Twitterbots,

that attackers have to "herd" accounts by registering them, adding pictures, occasionally tweeting and following other users.[1] Artificial intelligence could be used to automate this process. It could also be used to automatically generate messages that disseminate the same information but are unique enough to not be detected as similar. Finally, AI could be used to better target messages so they become more convincing to certain people based on their socio-demographic characteristics or psychological traits.[2] The practice of astroturfing could be used to slander or harass people at an unprecedented scale.

1.4.3 Generation:

As previously mentioned, artificial intelligence can be used to generate extremely realistic-looking data. This can be used for social engineering purposes, but also for new attack vectors. Humans have learned that images can be easily manipulated using tools such as Adobe Photoshop. However, with AI, even media such as sound and video can be counterfeited in convincing ways and on a massive scale. As mentioned before, this is a possibility that is being actively exploited in the wild. It therefore might be the most visible malicious use of artificial intelligence. The trend started in early 2018, when a user of the internet forum Reddit created and publicly released a tool, he called Fake App, which received over 100,000 downloads.[3] It allows any user with a sufficiently strong graphics card to generate fake videos using deep learning networks that rely on a technology known as autoencoders.[4] The user simply supplies a low number of pictures or videos of a targeted person. The neural network then 'learns' the face of that

Amplification - Inside the Online Influence Industry", The Bureau of Investigative Journalism (7 December 2017), online: https://www.thebureauinvestigates.com/stories/2017-12-07/twitterbots. 20/04/2024 11:48

[2] Matt Chessen, "The Madcom Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done About It", The Atlantic Council (1 September 2017), online: https://www.scribd.com/document/359972969/The-MADCOM-Future at 13.

[3] 7 Rose, supra note 66.

[4] Aural Oberon, "Exploring Deep Fakes", Hacker Noon (5 March 2018), online: https://hackernoon.com/exploring-deepfakes-20c9947c22d9; Alan Zucconi, "Understanding the Technology Behind Deep Fakes", Alan Zucconi (14 March 2018),online:https://www.alanzucconi.com/2018/03/14/understanding-the-technologybehind-deepfakes/ 2:12 20/04/2024

person. Next, the user supplies another video and designates a target face. The neural network will then generate a new video, rendering the face of the target person onto the face of the person in the target video. This includes the adaptation of facial expressions and can be very realistic looking.[1]

1.4.4 Cyber security:

In our highly connected society, a large attack vector stemming from AI is that of cyber security. Writing and maintaining secure software and platforms is a task that depends on highly trained experts that are in very short supply. Further, many companies might not have the resources or incentive to secure their systems, resulting in very high rates of avoidable vulnerabilities. Recently, the sophistication of cyber-attacks has been on the increase, due in part to the leakage of very sophisticated toolsets developed by intelligence agencies. Cybercriminals have also taken stock of our growing dependence on digital technologies and data and have developed new business models such as ransom ware as a response. The ransom ware business model abandons the theft of personal data that used to be resold to third parties on online criminal marketplaces. Instead, the value is extracted from the victim herself, who pays the offenders to regain access to her precious personal information.[2] This section will look at the way criminal hackers could use artificial intelligence to further improve the scale and effectiveness of their attacks.

1.4.5 Vulnerability discovery:

Many computer viruses depend on the exploitation of a system vulnerability. This could be a bug in an operating system (such as Windows) or software (such as Adobe Reader) or even a web technology (such as Word Press, a tool for online publishing) that allows a hacker to gain access to a system and steal information or

[1] Same reference

[2] Masarah Paquet-Clouston, Bernhard Haushofer & Benoît DuPont, “Ransom ware payments in the bit coin ecosystem”, (Paper delivered at the 17th Annual Workshop on the Economics of Information Security (WEIS), 2018) online: https://arxiv.org/abs/1804.04080. 12:15 11/04/2024

execute their own code. Vulnerabilities, once discovered, have to be patched quickly by software providers so that as little damage as possible can be caused by them. Vulnerabilities that are used by a virus to infect a machine before a company has patched them are referred to as zero-day exploits. The Stuxnet virus leveraged four of these vulnerabilities. These can be extremely valuable on the black market, leading many companies to offer bug bounties to researchers that disclose vulnerabilities to them, there are several methods to discover these vulnerabilities. Static Analysis requires a researcher to analyze the code of the program, manually or semi-automatically. Fuzzing feeds the program billions of random permutations to see when it fails. In penetration testing, a researcher pretends to be a hacker and discover the vulnerability by trying to enter the system.[1] These techniques can be used by researchers to discover and patch vulnerabilities in their own software, but also by attackers looking to find and exploit vulnerabilities.[2] The discovery of vulnerabilities requires a skilled analyst.[3] The deployment of Artificial Intelligence could lead to an increase both in the quality and quantity of attacks. Researchers have shown promising approaches to further automating parts of vulnerability discovery using artificial intelligence.[4]

Until now, fizzing has been hard to set up in use. Artificial Intelligence could be used to learn the data structures that a program relies on and then inject fake data automatically. This could increase the number of people able to perform these

[1] B Liu et al, "Software Vulnerability Discovery Techniques: A Survey" (Paper delivered at the Fourth International Conference on Multimedia Information Networking and Security online: https://ieeexplore.ieee.org/document/6405650. 16:45 20/04/2024

[2] Malicious Use of Artificial Intelligence, supra note 71 at 16.

[3] Daniel Votipka et al, "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes" (Paper delivered at the 2018 IEEE Symposium on Security and Privacy, San Francisco, CA, 2018), online: https://ieeexplore.ieee.org/document/8418614. 13/12/2023 12:30

[4] Gustavo Grieco& Artem Dinaburg, "Toward Smarter Vulnerability Discovery Using Machine Learning". (Paper delivered at the Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security, Toronto, Canada, 2018); Steven Harp et al, "AutomatedVulnerability Analysis Using AI Planning" (Paper delivered at the 2005 AAAI Spring Symposium, Stanford, CA, 2018), online: https://www.researchgate.net/publication/221250445_Automated_Vulnerability_Analysis_Using_AI_Planning at 8.

attacks and thus the number of vulnerabilities discovered.[1] In 2017, researchers at Microsoft demonstrated how neural networks could be used to make fizzing simpler, more efficient and more generic.[2] A weak password could also be a sort of vulnerability, since it allows a hacker to access the account of a user.[3] Researchers have demonstrated that artificial intelligence can be very strong at guessing passwords. It can be trained on millions of leaked passwords to detect patterns and then apply these to guess the passwords of specific users.[4]

1.4.6 Exploitation:

Even after the vulnerability is discovered, the work of the attacker is not finished. He will try to find a way to use the exploit to get access to one or many target machines. This can be done, for example, through the creation of a computer virus that tries to autonomously attack as many computers as possible using the exploit. It can also be used to perform a regular cyber-attack against a server. Here, the attacker himself runs commands to move laterally toward other machines. On the defense side, machine learning is used to monitor for these kinds of attacks. Anti-virus programs often use two ways of identifying malware: Signature-based technologies and behavioral analysis. Signature-based analysis tries to identify a virus based on the digital fingerprint of its code. It relies on the anti-virus vendor

identifying malware and adding it to a database of malicious signatures[5]Behavioral analysis identifies what a program tries to do rather than

[1] FortiGuard SE Team, "Predictions: AI Fuzzing and Machine Learning Poisoning", Fortinet Blog (15 November 2018), online: https://www.fortinet.com/blog/industry-trends/predictions--ai-fuzz ing-and-machine-learning-poisoning-.html. 22/03/2024 13:01

[2] "Neural fuzzing: applying DNN to software security testing", Microsoft Research (13 November 2017), online: https://www.microsoft.com/en-us/research/blog/neural-fuzzing/; Mohit Rajpal, William Blum & Rishabh Singh, "Not all bytes are equal: Neural byte sieve for fuzzing", (2017) arXiv Working Paper, arXiv:1711.04596 [cs.SE], online: https://arxiv.org/abs/1711.04596 at 10. 12/04/2024 12:54

[3] Julie J.C.H. Ryan, "How do computer hackers 'get inside' a computer?", Scientific American, online: https://www.scientificamerican.com/article/how-do-computer-hackers-g/

[4]BrilandHitaj et al, "PassGAN: A Deep Learning Approach for Password Guessing" (2017) arXiv Working Paper, arXiv:170900440 [cs, stat], online: http://arxiv.org/abs/1709.00440. 13/03/2024 19:59

[5] John Cloonan, "Advanced Malware Detection - Signatures vs. Behavior Analysis", Infosecurity Magazine (11 April 2017), online: https://www.infosecurity-magazine.com:443/opinions/malware-de tection-signatures/ 01/02/2024 20:36

which code is it based on.[1] It often uses ML technologies.[2] Artificial Intelligence could be used to circumvent these systems. Researchers have showed that it is possible to create AI systems that automatically create malware that evades common anti-virus programs.[3] Attackers could use AI to ever so slightly alter a program until it appears benign to anti-virus filters. Likewise, server systems often run protective software known as Intrusion Detection Systems that check for strange behavior on servers or traffic and report this to administrators. They often use machine learning technologies.[4] For example, if a server suddenly starts transferring massive amounts of data to an IP-address in Russia, this might indicate that a hack is underway. However, it might also just be a sign of Russian users following a popular link to access the website. A hacker could use AI to try to circumvent these systems by hiding their activity under the guise of human-looking behaviors. Mimicry attacks, that try to slip under the radar, have been demonstrated to be efficient.[5] Using machine learning to automate these seems a natural evolution.

1.4.7 Post-Exploitation & Data Theft :

After the exploit, the attacker will often use the established access to install their own backdoor that they can use to re-enter the server, getting deeper access to the system and looking around the server for potentially sensitive information and downloading this information.[6] Other hackers might use the access to gain further access to the operations of the company or destroy services to cause financial

[1] Same reference.

[2] Malicious Use of Artificial Intelligence, supra note 71 at 33.

[3] Hyrum S Anderson et al, "Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning" (2018) arXiv Working Paper, arXiv:180108917 [cs], online: http://arxiv.org/abs/1801.08917. 14/03/2024 15:17

[4] P García-Teodoro et al, "Anomaly-based network intrusion detection: Techniques, systems and challenges" (2009) 28:1–2 Computers & Security 18; Alex Shenfield, David Day & Aladdin Ayesh, "Intelligent intrusion detection systems using artificial neural networks" (2018) 4:2 ICT Express 95.

[5] David Wagner & Paolo Soto, "Mimicry Attacks on Host-Based Intrusion Detection Systems" (Paper delivered at the 9th ACM conference on Computer and communications security, Washington DC, 2002), online: https://dl.acm.org/citation.cfm?id=586145 at 10/04/2024 13:42

[6] Ivan Novikov, "How AI Can Be Applied ToCyber attacks", Forbes (22 March 2018), online: https://www.forbes.com/sites/forbestechcouncil/2018/03/22/how-ai-can-be-applied-to-cyberattacks/ 11/04/2024 21:03

damage. Throughout this process, the hacker has to take care to stay hidden and erase any traces that might tell the operator he has been on the server and lead him to getting caught. It is a complicated process, requiring a lot of patience, skill, and knowledge of the computer system. The attacks are often constrained by the speed of human reaction – based on the information the hacker sees on the server, he will have to react in a different way.

While this is more far-fetched than the other applications, it could potentially be possible for hackers to train an Artificial Intelligence system to automate parts of these steps as well. There are already frameworks, created for security auditing of computer systems, that allow people to unleash an entire barrage of attacks on a computer system.[1] Artificial intelligence might enhance the capability of these systems to automatically infer which attacks are appropriate, or which data might be sensitive and should therefore be given priority. Such a system could be used in parallel to intelligently exploit many systems simultaneously, without requiring human intervention. While this is already possible to some extent, Artificial Intelligence might be able to enhance these capabilities.

1.4.8 Exploitation of deployed artificial intelligence:

Most analysts see artificial intelligence as having a large effect on most, if not all, sectors of society. This might lead to another attack vector opening up for malicious users. As mentioned before, the current crop of artificial intelligence systems suffers from a number of weaknesses. If they are implemented in a large sector of society, they risk enabling new attacks that exploit this fragility. Depending on the way AI is implemented, and how much control it is given over people and processes, this could cause tremendous damage to society.

Adversarial attacks:

[1] "Penetration Testing Software, Pen Testing Security", Metasploit (Website), online: https://www.metasploit.com/
20/04/2024 22:10

Adversarial attacks are attacks that exploit the fact that AI does not operate like human intelligence. Artificial intelligence in general, and convolution neural networks in particular, identify patterns based on a set of features that might be very unintuitive for humans. By slightly altering the input, one can completely change the way the AI system interprets a pattern. It has been shown that a picture of a puppy can be altered in ways that are imperceptible to humans. These effects can also be implemented in real-world scenarios – a team of researchers showed that an altered 3d-printed turtle could be classified as a gun in a video feed, no matter the orientation of the turtle. Researchers have even shown that the addition of stripes to traffic signs can alter the meaning of that sign for the AI running on autonomous vehicles. It is important to note that an attacker typically requires access to a neural network in order to generate adversarial examples. However, often pertained networks are used, which means that the models are readily available on the internet.[1] Recent research also shows that adversarial examples can be created by first training another neural network to mimic the target network.[2] There are many potential attacks that might be carried out by exploiting this weakness. The malicious conversion of a yield sign to a go sign could be a recipe for disaster in traffic. Likewise, a system set up for detecting weapons might be confused by a gun designed to resemble a more innocuous object and interpreted as such by a neural network. Neural networks designed to detect anti-virus software is also vulnerable to malware crafted using adversarial techniques.[3] If a model directing autonomous weapon systems is targeted, the results could be that civilians are harmed.[4] The creation of neural networks that are resistant to

[1] Arelis Guzmán, "Top 10 Pretrained Models to get you Started with Deep Learning (Part 1 - Computer Vision)", Analytics Vidhya (27 July 2018), online:https://www.analyticsvidhya.com/blog/2018/07/top-10-pretrainedmodels-get-started-deep-learning-part-1-computer-vision/. 01/05/2024 18:37

[2] 5 Nicolas Papernot et al, "Practical Black-Box Attacks against Machine Learning" (2016) arXiv Working Paper, arXiv:160202697 [cs], online: http://arxiv.org/abs/1602.02697. 12/01/2024 11:11

[3] 6 Kathrin Grosse et al, "Adversarial Perturbations Against Deep Neural Networks for Malware Classification" (2016) arXiv Working Paper, arXiv:160604435 [cs], online: http://arxiv.org/abs/1606.04435.12/01/2024 11:20

[4]Malicious Use of Artificial Intelligence, supra note 71 at 20

adversarial attacks is an active area of research,[1] however until reliable countermeasures are implemented, the increasing use of AI opens society to new attack vectors.

1.4.9 Poisoning of artificial intelligence systems:

Another attack against AI systems relies on the poisoning approach. Instead of subverting the algorithm itself by manipulating data or objects on the outlier of its model, poisoning relies on attacking the training data used to create the AI system. If this data is of poor quality, the resulting machine learning system will not operate correctly. The addition of quite few poisoned examples can be enough to severely damage the performance of an AI system[2]Poisoning attacks rely on the attackers having control over some of the data used to train the AI. This makes the attack unfeasible in many instances. However, due to the large requirements of data for machine learning, data will often be crowd-sourced. Another issue is that of online learning. This is a common approach in anomaly detection. Here, the system is constantly trained to analyze a baseline of activity in a system. Only if an event falls outside of this baseline will the detector notice the anomaly. This could be exploited by attackers. Over time, they could inject patterns that are still within the allowed parameters, but close to the edge of what is allowed. This will extend the baseline to cover more situations. After extending the baseline this way for some time, the attackers can launch their attack without being detected.[3]

1.5 Conclusion

[1] Kao, supra note 123; Xiaoyong Yuan et al, "Adversarial Examples: Attacks and Defenses for Deep Learning" (2017) arXiv Working Paper, arXiv:171207107 [cs, stat], online: http://arxiv.org/abs/1712.07107.12/01/2024 11:45

[2] Battista Biggio, Blaine Nelson & Pavel Laskov, "Poisoning Attacks against Support Vector Machines" (2012) arXiv Working Paper, arXiv:12066389 [cs, stat], online: http://arxiv.org/abs/1206.6389.12/01/2024 11:58

[3] Benjamin IP Rubinstein et al, "ANTIDOTE: understanding and defending against poisoning of anomaly detectors" (Paper delivered at the 9th ACM SIGCOMM Conference on Internet Measurement, 2009), online: https://people.eecs.berkeley.edu/~tygar/papers/SML/IMC.2009.pdf; Nitika Khurana, Sudip Mittal & Anupam Joshi, "Preventing Poisoning Attacks on AI based Threat Intelligence Systems" (2018), arXiv Working Paper, arXiv:1807.07418 [cs.SI], online: https://arxiv.org/abs/1807.07418v1; Maria Korolov, "Hackers get around AI with flooding, poisoning and social engineering", CSO Online (16 December 2016), online: https://www.csoonline.com/article/3150745/security/hackers-get- around-ai-with-flooding-poisoning-and-social-engineering.html12/01/2024 13:46

This is the rationale of the existing electronic information processing methods that characterize the current social interactions. The findings of the above-mentioned study substantiate the fact that with superior computing power, capabilities to address complex tasks in its entirety by embracing a top-down approach with respect to technical and innovative concerns. AI and AI related technologies are being used effectively in a variety of human activities in the current world from as basic as facial recognition on a smartphone screen to writing pieces of music and creating original art. Taking into account the above facts, legal science can make more decisions running high tech tools in criminal trial system as to define criminal punitive measures and several avenues of criminal law which impact those individuals who have participated in socially undesirable activities. The purpose of the study is to determine if it is permissible under the ethical standpoint to propose that an electronic device, which can be recognized as a means of information processing as per the law, may be considered a target that can be punished. To this end, more attention should be paid to the problem of defining artificial intelligence as a set of solutions to decisions that are provided without human intervention. The study was able to establish the observation that the application of artificial intelligence to determine the effect of criminal law is far from a mechanical decision-making process of choosing one of the punitive measures. This means that the arguments that the judgment delivered in favor of the defendant concerning the level of criminal responsibility directly controls or at least impacts the rights and legitimate interest of other third parties such as family members of the accused, dependents, victims of the accused or even the society at large cannot be turned a blind eye to it. Even the best computer cannot assess this and many more factual scenarios that are not in the law or in the interest of the public.

Chapter. 2 Mechanism to combat cybercrime using artificial intelligence.

(Proactive policing, Digital police and Digital investigation)

2.1 Introduction:

By the use of global technological advancements, criminals are using cyberspace to commit numerous cyber-crimes. People are connected to the cyber space with personal a device that's why they are all vulnerable to interferences and a variety of threats. Internet security suits are the basic protection methods and these are not just enough to protect the data and devices. Highly Advanced cyber defense systems have become essential.

As of today, with the technology, AI plays a major role in technology and has been involved with many technological aspects as well. By today, creating cyber defense systems, using AI has become a trend. The basic idea of this study is to establish a classy cyber-crime defense system which involves intelligent agents that are based on artificial intelligence.

2.2 Proactive policing:

Definition:

The term "proactive policing" encompasses a number of methods designed to reduce crime by using prevention strategies.

By definition, it stands in contrast to conventional "reactive" policing, which for the most part responds to crime that has occurred. The National Academies report underscored that the intended meaning of proactive policing is broad and inclusive: "This report uses the term 'proactive policing' to refer to all policing strategies that have as one of their goals the prevention or reduction of crime and disorder and that are not reactive in terms of focusing primarily on uncovering ongoing crime or on investigating or responding to crimes once they have occurred. Specifically, the elements of proactivity include an emphasis on

prevention, mobilizing resources based on police initiative, and targeting the broader underlying forces at work that may be driving crime and disorder." [1]

The report identified four categories within proactive policing: place-based, person-focused, problem-oriented, and community-based.

2.2.1 The Four Categories of Proactive Policing:

2.2.1.1 Place-Based

Description: Preventing crime by using data to isolate small geographic areas where crime is known to be concentrated.

Types:

- **Hot Spots Policing/Crime Mapping**

Policing focused on small areas where crime is clustered, using maps and geographic information systems to identify clusters of crime. Statistical software may be used to distinguish random clusters of crime from hot spots

- **Predictive Policing**

Using advanced analytics and intervention models to predict where crime is likely to happen.

2.2.1.2 Person-Focused

Description: Identifying underlying social causes of crime and tailoring solutions to those causes.

Types:

- **Problem-Oriented Policing**

An analytics method used by law enforcement to develop strategies that prevent and reduce crime by targeting underlying conditions that lead to recurring

[1] Research Will Shape the Future of Proactive Policing October 24, 2019 By Paul A. Haskins https://nij.ojp.gov/topics/articles/research-will-shape-future-proactive-policing 10/04/2024 18:32

crime. The method calls for law enforcement to employ a range of approaches to problems and evaluate their impact.

2.2.1.3 Problem-Oriented

Description: Identifying underlying social causes of crime and tailoring solutions to those causes.

Types:

- **Problem-Oriented Policing**

An analytics method used by law enforcement to develop strategies that prevent and reduce crime by targeting underlying conditions that lead to recurring crime. The method calls for law enforcement to employ a range of approaches to problems and evaluate their impact.

2.2.1.4 Community-Based

Description: Using community resources to identify and control sources of crime.

Types:

- **Community-Oriented Policing**

A philosophy promoting strategies that support systematic use of community partnerships and problem-solving techniques to proactively address conditions giving rise to crime.

- **Police Legitimacy**

Building public trust and confidence in law enforcement so that the public accepts police authority and believes police actions are justified and appropriate.

- **Procedural Justice Policing**

An antecedent to police legitimacy; the idea of perceived fairness in law enforcement processes, involving a chance to be heard and the perception that police are neutral, trustworthy, and treat individuals with dignity and respect for their rights.

- **Broken Windows Policing**

Intense enforcement against minor offenses, such as broken windows, on the theory that neighborhoods marked by social and physical disorder suggest resident indifference to crime and invite more predatory crime.[1]

2.3 Digital police:

Abstract:

Our paper discusses a new approach to assessing the activity of artificial intelligence (AI) as an independent subject capable of not only logical reasoning, but also a conscious attitude to the world around it with its emotional attachment. The fact that artificial general intelligence (AGI) might appear quickly and perform intellectual tasks reserved for humans is a well-known fact. We suggest that in the future, artificial intelligence will be capable of not only clearly programmed actions, but also actions associated with lobbying its own, not always legitimate interests. This represents some leading trends for the 21st century and thence constitutes an interesting and timely topic for research. In order to suppress the "illegal activities" of artificial intelligence, it might be useful to create a so-called "digital police" which would be able to perform the functions of not only the search agency (police), but also the punitive body (court) without interference from the natural intelligence (human). Our results and outcomes might allow specialists involved in the development and creation of artificial intelligence systems to provide mechanisms for monitoring, protecting and preventing unauthorized actions on his part. In addition, our conclusions might be capable of pointing government structures towards the creation of a harmonious architecture without a risk system of artificial intelligence.

[1] Paul A. Haskins, same reference, 04/03/2024 15:19

2.3.1 Purpose, materials, methods, and objectives:

Nowadays, current trends in the spread of artificial intelligence are the result of active progress in the field known as machine learning (Qin and Chiang 2019). It is a well-known fact that machine learning involves the use of algorithms that allow computers to "learn on their own" by viewing data and completing tasks based on examples, rather than relying on detailed software developed by humans (Kulkarni and Padmanabhan 2017). The amounts of money invested into AI and AI-related technologies in the world is constantly rising. Figure 1 that follows shows revenues (both actual and predicted extrapolations) from the artificial intelligence software market worldwide from 2018 to 2025, by region expressed in billions of U.S. dollars.[1]

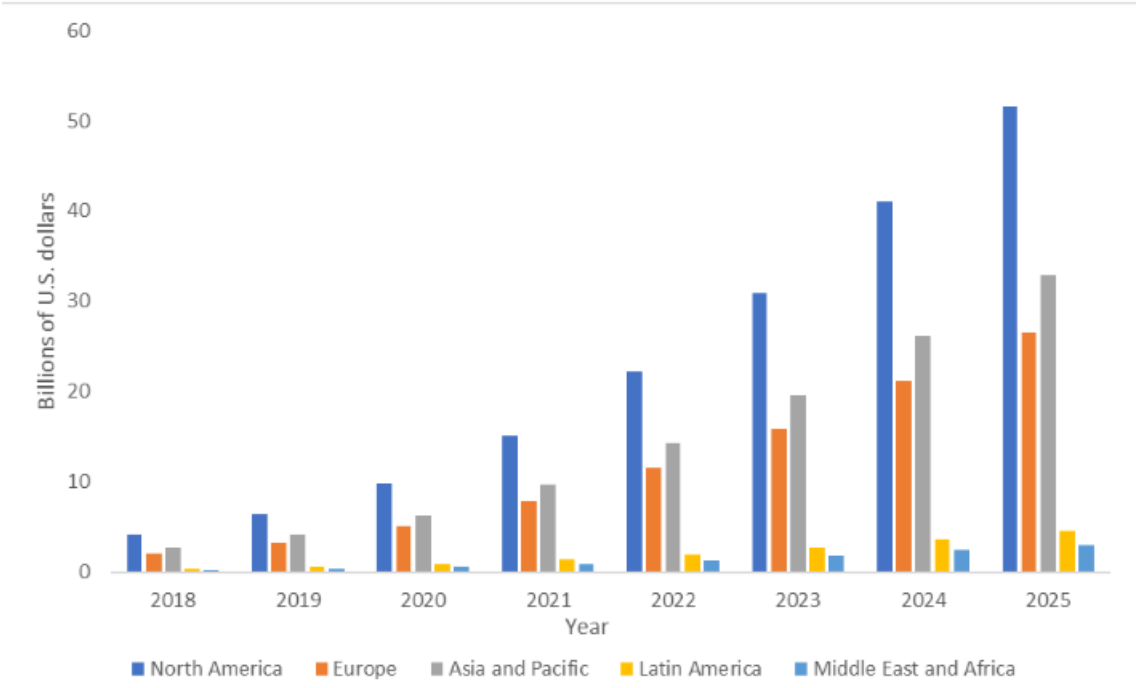

Figure 1. Revenues from the artificial intelligence software market worldwide from 2018 to 2025, by region Source: Own results based on Liu (2019)

One can notice the rapid increase in AI software market in North America, but Asia and Pacific region are catching up quickly (perhaps thanks to China). The

[1] Qin SJ, Chiang LH (2019) Advances and opportunities in machine learning for process data analytics. Computers & Chemical Engineering 126:465-473. Doi 10:54:
/j. compchemeng.2024.04.03

increase in Latin America, Middle East, and Africa seems to be rather modest. AI quickly finds its way into information technologies, services, industrial production, but also energy and “green” economy[1]

With the development of information and communication technologies (ICTs), artificial intelligence may have the ability to emotionally “colored” actions, which, in the image of natural intelligence, will attract it and contribute to their accumulation and diversity and often not always in a civilized way (Grinbaum et al. 2017). Future analysis shows that these kinds of “pleasures” might as well include:

• using someone else's operational or long-term memory; • increasing the speed of operating systems due to unauthorized connections to "foreign" processors;

• using software products of limited use;

• harming competing intelligent systems or other systems with the aim of testing their own resources or as preparation for other illegal actions;

• spreading of viruses in order to conceal their actions or disable competitive systems;

• damaging natural intelligence, to gain dominance in the intellectual world

It is generally accepted that a hacker attack is an action whose purpose is to seize control (increase its unauthorized rights) over a remote / local computer system, or destabilize it, or refuse to service it. One has to pay special attention to non-civilized methods of obtaining "benefits" for artificial intelligence.[2]

some ways, these methods will be similar to the actions of hackers, but at the same time Advances in Social Science, Education and Humanities Research,

[1] Strielkowski W (2017) Social and economic implications for the smart grids of the future. Economics and Sociology 10(1):310-318. doi: 10:14/2071-789X.2017/10.01.2024

[2]Yu PK (2020) The Algorithmic Divide and Equality in the Age of Artificial Intelligence. Florida Law Review 11:12 / 12.03.2024

volume 386 205 have their own specifics. Depending on how perfect and creative they are, the methods to counteract them will largely depend on. The most famous methods of hacker attack that artificial intelligence can use in our opinion are:

2.3.2 Buffer overflow:

This is one of the most common types of hacker attacks on the Internet. The principle of this attack is based on the use of errors in the software, which can cause violation of memory boundaries and urgently (crash) terminate the application or execute arbitrary binary code on behalf of the user under whom the vulnerable program was running.

The purpose of artificial intelligence in this case will be to use the operational or long-term memory of another device or its performance to solve its unauthorized tasks. If the program runs under the system administrator account, then this attack will allow you to gain full control over the victim's artificial intelligence.

2.3.3 Viruses, Trojan horses, mail worms, sniffers, rootkits and other special programs:

Another type of hacker attack is a more sophisticated method of gaining access to sensitive information - this is the use of special programs for conducting unauthorized activities with artificial intelligence of the victim. Such programs are designed to search for and transmit confidential (secret) information to an attacking artificial intelligence for use in their own “mercenary” interests, or to harm the victim’s safety and health system, which has similar or competing interests.

2.3.4 Network intelligence:

During this hacker attack, artificial intelligence does not carry out any destructive actions, but as a result, it can receive closed (confidential) information about the construction and principles of the computer system of the chosen victim. The information obtained can be used to correctly build the upcoming attack, and,

as a rule, is carried out at the preparatory stages. In the course of such reconnaissance, attacking artificial intelligence can perform port scans, DNS queries, ping open ports, and the availability and security of proxies. As a result, it can obtain information about the DNS addresses existing in the system, to whom they belong, what services are available on them, the level of access to these services for external and internal users, with subsequent use in their narrowly focused interests.

2.3.5 IP spoofing:

Represents a common type of hacker attack used in insufficiently protected networks, when an attacking artificial intelligence impersonates an authorized user while in the network of the organization itself or outside it. For these purposes, the attacker needs to use the IP address allowed in the security system of this network. Such an attack is possible if the security system allows user identification only by IP address and does not require additional confirmation. This is the simplest and most effective way to use the resources and information of someone else's network in their own dishonest interests.

2.3.6 Man-in-the-Middle:

A type of hacker attack, when an attacker intercepts a communication channel between two systems, and gains access to all transmitted information. When gaining access at such a level, artificial intelligence can modify the information in the way necessary for itself in order to achieve its unauthorized goals. The purpose of such a hacker attack is to steal or falsify the transmitted information, or gain access to the resources of the attacked network.[1]

[1]Cockburn IM, Henderson R, Stern S (2018) The impact of artificial intelligence on innovation. No. W24449, National Bureau of Economic Research. https://www.nber.org/papers/w24449 Accessed on 11.02.2024 / 12:25

2.3.7 Injection:

A hacker attack associated with various kinds of injections, which involves the introduction of third-party commands or data into a working system in order to change the progress of the attacked system, resulting in gaining access to closed functions and information, or destabilizing the work of the attacked system as a whole. There are several types of known injections:

• SQL injection is a hacker attack, the purpose of which is to change the parameters of SQL queries to the attacked database. As a result, the request takes on a completely different meaning, and in case of insufficient filtering of the input data, it is able not only to output confidential information, but also to change / delete data in its own selfish interests;

• PHP injection is one of the hacking methods for hacking websites running on PHP. It consists in embedding a specially crafted malicious script in the web application code on the server side of the site, which leads to the execution of arbitrary commands. Artificial intelligence is analyzed by such vulnerabilities as unshielded variables that receive external values, which allows it to use the computational and intellectual capabilities of the attacked side.

2.3.8 XPath injection:

A type of vulnerability that involves embedding XPath expressions in an original query against an attacked XML database. As with other types of injections, vulnerability is possible due to Advances in Social Science, Education and Humanities Research, volume 386 206 insufficient verification of the input data, which allows artificial intelligence to also use the capabilities of the attacked side.[1]

[1] Kulkarni RH, Padmanabhan P (2017) Integration of artificial intelligence activities in software development processes and measuring effectiveness of integration. IET Software 11(1): 18:26. Doi: 22.04.2024

Thus, any hacker attack is nothing more than an attempt to use artificial intelligence to imperfect the security system of the attacked victim, either to obtain confidential information or to harm the attacked system (see

e.g., Rid and Buchanan 2015). Therefore, the reason for any successful hacker attack is the perfection and self-training of artificial intelligence, its preferences and unauthorized interests; the value of the information obtained, as well as the insufficient competence of the natural or artificial security system administrator, for example, software imperfection, and insufficient attention to security issues in the intellectual network as a whole.

2.4 Digital investigation:

Abstract:

Imagine that the year is 2054. Touch screen technology is commonplace. Ads are tailored and customized based on a person's life, decisions, whereabouts, and user history. Cars can drive on their own. Home appliances can be controlled with one's voice. Biometric recognition such as palm prints and identifying facial scans, is commonplace. The police are able to predict who is likely to commit a crime and apprehend that person before they do so. It is no accident that every element in that description refers to the plot of the 2002 American science fiction film called Minority Report. Indeed, all descriptive elements in the preceding paragraph are true at the time of writing except for the year and the statement that police habitually apprehend a person before they commit a crime. As we shall see below, law enforcement around the world have begun using AI-powered technology to investigate and at times even try to predict crimes. While there is a long history of the use of technology in criminal investigations, the use of AI has the power to transform the relationship between police officers and citizens and to facilitate unprecedented surveillance and social control. We take stock of the current tools in

use that assist the police in detecting and investigating crime, and offer a taxonomy of such tech in terms of its AI capacity. We also canvas the emerging tools that promise to predict crime by determining crime hotspots and who is likely to be involved in gun violence.

We offer an overview of some of the ethical issues raised by AI, as well as ways forward for governments and law enforcement that want to add AI to their crime response toolbox.

Our aim is to critically assess the moral and technical authority that AI is often presumed to display, and suggest a human-centric approach to the implementation of artificial intelligence tools by law enforcement. A note on scope is in order here. When we use the term ‘law enforcement’, we refer to domestic police services (that respond to crime that occurs within a contained jurisdiction), and for the purposes of this report, this term should be understood separately from government entities working either in national security, foreign intelligence or administrative policing bodies (such as those working in immigration).

2.4.1 AI and crime detection:

Artificial intelligence is being used in the detection and investigation of criminal activity in countries around the world. We define crime detection as the act of attempting to ascertain whether or not certain crimes are being or have been committed. Crime detection in that context is past- or present-oriented, while crime forecasting, which we will discuss in more detail in section 4.2, is future-oriented.

2.4.2 A taxonomy of AI capabilities:

It is possible to categorize the various types of artificial intelligence available to law enforcement for detection functions in terms of the capability of the software. The types of AI capabilities identified in the process of writing this report are as follows:

- Object classification

- Object recognition (including face recognition)
- Speech recognition
- Gunshot detection
- DNA analysis
- Digital forensics

In the following section, we describe each of these types of tools used for crime detection in terms of how they generally work, how they fall into the already-existing subtypes of crime detection technologies above, and their law enforcement

use case scenarios.

A. Object classification:

software seeks to autonomously identify certain elements within images and videos, and label or categorize these elements much like humans do.[1] Object classification is a sub-domain within the field of computer vision, which can be understood as an application of artificial intelligence.

Systems that classify objects within imagery are able to work after researchers train a computer program or algorithmic model on a dataset of numerous images. Just as it occurs within machine learning more generally, elements within the imagery will be assembled into smaller parts such as pixels and groups of pixels, which will be labelled (often manually) on the basis of descriptors such as color or texture.[2]The program or model's learning process will then construct a decision tree that can classify the regions in the training set images as well as in future images. The program will subsequently be able to classify groups of pixels and therefore objects as part of the training categories.[3]

[1] Nils J. Nilsson, The Quest for Artificial Intelligence (Cambridge, UK: Cambridge University Press, 2013) at10.04.2024 /12:45.

[2] Nilsson, ibid at 30; "Introduction to Computer Vision", Algorithmic Blog (2 April 2018), online https://blog.algorithmia.com/introduction-to-computer-vision/; Golan Levin, "Image Processing and Computer Vision", Open Frameworks, online: https://openframeworks.cc/ofBook/chapters/image_processing_computer_vision.html.

[3]Same référence

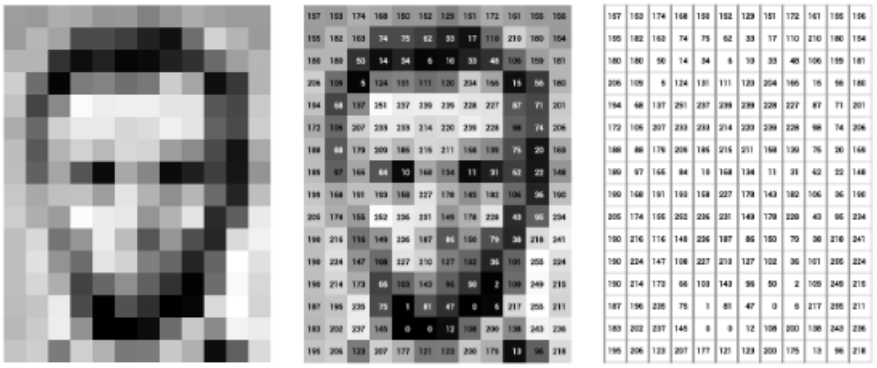

Figure 2. Pixel Data Diagram of Abraham Lincoln

There are myriad reasons why law enforcement would want to and do use object classification in the detection of crimes. For example:

Law enforcement may gain access to an image of the commission of a crime and would seek to rely on machine learning to identify the location where an image was taken or recorded. Google's program called PlaNet does just this, and relies on convolutional neural networks for its geolocation capabilities[1]

- Police officers may also want to detect the possible existence of criminal activity depicted within an image. The image's contents may demonstrate the occurrence of a criminal act (e.g., the image depicts possible theft) and/or the existence of the image itself may constitute a crime (e.g., the image depicts child pornography). One well-known example of the latter is the PhotoDNA software developed by Microsoft and Hany Farid of Dartmouth College, which primarily aims to detect child pornography and works by a) creating a digital signature (known as a 'hash') associated with the image to prevent image alterations, and b)

[1] "Google Unveils Neural Network with 'Superhuman' Ability to Determine the Location of Almost Any Image", MIT Technology Review (24 February 2016), online: https://www.technologyreview.com/s/600889/google-unveils-neural -network-with-superhuman-ability-to-determine-the-location-of-almost//./10.2.2024 / 12:33

converts the image to black and white, resizes it, breaks into a grid, and quantifies its shading.[1]

It then compares an image's hash against database of images that have been identified as illegal, and matches can be manually reviewed by humans.[2] Microsoft claims that PhotoDNA cannot be used to recognize faces nor people or objects within the image.[3]

PhotoDNA is used most notably by software giants such as Facebook, Google, Twitter, and by the US-based National Center for Missing & Exploited Children. Other examples of technology that seek to detect the commission of a crime within imagery include the European P-REACT Project, the loss-prevention product offered by the US-based company StopLift, and the Chinese software SenseTime.

B. Object recognition:

is a branch of the computer vision system which is used for identifying certain objects as; faces or fingerprints for instances. Facial recognition operating system employs some features on the face including, distance between eyes, jawline, and other characteristics to generate a face print and then search for the print in the database.[4] This technology presents issues, such as Faception, a tool which claims to chronologically recognize subjective personalities by facial lineaments. China is perhaps one of the biggest violators of privacy in this case through facial recognition technologies used in monitoring the citizens. As for the positive aspects of the system, the system's goal is to deal with criminals and increase effectiveness while still being inaccurate and violating the privacy rights of its

[1]Jennifer Langston, "How PhotoDNA for Video is being used to fight online child exploitation", Microsoft On the Issues (12 September 2018), online:https://news.microsoft.com/on-the-issues/2018/09/12/how-photodnafor-video-is-being-used-to-fight-online-child-exploitation/. 10.02.2024 16:15

[2]Samereference

[3]Samereference

[4] Tattoo Recognition", FBI.gov, (25 June 2015), online: https://www.fbi.gov/audio-repository/news-podcasts-thisweek-tattoo-recognition.mp3/view.

users. This has of course been met with criticism and has raised demands for regulations.[1]

C. Police body cameras:

The decision for police to use AI-powered body cameras is another tool that promises benefits and poses various challenges. A leader in this industry is the U.S. company called Axon, formerly Taser International, also known for its Taser stun gun. As a part of its decision to rebrand and to expand its business, Axon offered to provide free body cameras to any interested police department. The company stated in June 2018 that it wanted to use AI to automate the police body camera video assessment and annotation process, and eventually help generate police reports from the recorded video of police-citizen encounters thanks to AI. The purpose was to automate data gathering and records management so that police officers can spend more time performing other tasks. The company touted that more than 200,000 officers use their services, and that they have accumulated 30 petabytes of data ("10 times larger than the Netflix database") that will be analyzed by its multifunctional AI system.[2] The company has also filed a patent for real-time face recognition in order to keep up with its competitors. In April 2018, Axon launched its AI and Policing Technology Ethics Board, made up of external efforts from various fields and with a hope to "provide expert guidance to Axon on the development of its AI products and services, paying particular attention to its impact on communities."[3] News articles state that the group is to meet twice a year to discuss the ethical implications of the company's products, and the role of the board is to offer frank, honest advice.

It is not clear what, if any, impacts the board has had on the ethical development of Axon's products. But the decision to forge a path marked by a

[1] Moses Olafenwa, "Object Detection with 10 lines of code", Towards Data Science (16 June 2018), online: https://towardsdatascience.com/object-detection-with-10-lines-of-coded6cb4d86f606.
[2] Greene & Patterson, supra note 203.
[3] "Axon AI and Policing Technology Ethics Board", Axon (Website), online: https://ca.axon.com/info/ai-ethics.

commitment to ethics is laudable, and some have stated that they wished companies like Google (in light of its artificial and human intelligence lab called Deep Mind) would follow suit and disclose who sits on the board, what the board discusses, and how often they meet.

D. Speech recognition:

Speech recognition is similar to object recognition in that the technology seeks to identify idiosyncratic elements of speech patterns, often with a view to identify the person speaking and to automatically transcribe the words being spoken. Regardless of the exact algorithms that can be used in this process, speech recognition software detects and measures sound waves and the frequency patterns of the speech signal. Numerous obstacles must be overcome through this process, such as the existence of background noise and accounting for variations in the speed of speaking. The software then classifies extracted blocks or sections of the speech using various and at times multiple techniques, such as statistical models or artificial neural networks.[1] The purpose is to classify small segments in terms of the type of sound that is made, and then classify larger segments of each sound to determine which word is being said.

One example of the operational use of voice recognition comes from Interpol—the International Criminal Police Organization. In mid-2018, it engaged in the final review of a project called the Speaker Identification Integrated Project. The technology extends the capabilities of voice recognition software by taking collections of voice samples, analyzed for certain behavioral features, and creates 'voice prints' in order to match new voice data uploaded to its system (from police intercepts for example) to the voice data already on file for suspected criminals.[2] The technology can also filter voice samples by gender, age, language, and accent. The Speaker Identification Integrated Project allows uploads and downloads of

[1] Same reference
[2] Same reference

samples from 192 law enforcement agencies around the world.[1] The database will purportedly include samples not only from law enforcement but also "from YouTube, Facebook, publicly recorded conversations, voice-over-internet-protocol recordings, and other sources where individuals might not realize that their voices are being turned into biometric voice print."

E. Gunshot detection:

software seeks to detect the occurrence of gunfire and determine the precise location of the gunshot. Acoustic gunshot detection systems typically use a set of microphones distributed over large populated areas that detect and isolate the staccato sounds of gunfire, which can be then confirmed by humans who may notify law enforcement where the gunshot went off. Gunshot detection can be understood as falling under the umbrella of AI because the designers of the software rely on machine learning in order to train their systems to identify the audio signature of gunfire and to isolate it from all the other sound interferences commonly found in urban settings. Shot Spotter is a US-based company that offers gunshot detection services to over 90 cities in the US, and has been approved for use in the major Canadian city of Toronto.[2] Law enforcement agencies have repeatedly justified their use of this software in public spaces to curb gun violence, especially in neighborhoods where gunshots are common occurrences (and might not elicit calls to the police) or where citizens might feel intimidated and prefer to avoid interactions with the police. Another example of gunshot detection software—although it falls outside the scope of this report—is Boomerang III, a system developed by the US Department of Defense for use in the military. According to its description online, "Boomerang pinpoints the shooter's location of incoming small arms fire. Boomerang uses passive acoustic detection and

[1] Kofman, supra note 219.

[2] Jordan Pearson, "Toronto Approves Gunshot-Detecting Surveillance Tech Days After Mass Shooting", VICE Motherboard (25 July 2018) Online https://motherboard.vice.com/en_us/article/7xqk44/toronto-approves-shotspotter-gunshot-detecting-surveillance-tech-danforth-shooting.

computer-based signal processing to locate a shooter in less than a second."[1] Even if this technology has only been used in war environments so far, the trend of police militarization that has been observed in many Western democracies might lead to its rapid adoption by law enforcement agencies facing high homicide rates.

F. DNA analysis:

DNA analysis understood at its broadest consists of the application of genetic testing for crime-assessment and legal purposes.[2]

The use of DNA as forensic material is a branch of forensic science that examines genetic material in criminal investigations. The most obvious reason law enforcement would want to collect and analyze genetic material at a crime scene concerns their desire to determine who was present when the alleged crime occurred, what their role may have been in the altercation, where the crime occurred and whether protagonists of the incident (either victim, witness or suspect) can be tied to previous solved or unsolved crimes. Artificial intelligence plays a role in DNA analysis because of the new capacity it offers to significantly speed up the DNA sequence matching process, where collected DNA is matched with the DNA contained within a given database. Consider the decision on the part of police in California to use DNA data held by commercial genealogy websites in 2018. In that instance, law enforcement found and arrested a person charged with numerous counts of rape and murder, and appear to have uploaded DNA data about the accused onto the website GED Match. The DNA was obtained from a crime scene, and was purportedly used by the police to find one of his relatives.[3]

It was not clear that the police had obtained authorization from the company to upload the accused's DNA and compare it with others on their website, and it is questionable whether DNA abandoned by the perpetrator of a crime is afforded

[1] Boomerang III: State-of-the-Art Shooter Detection", Raytheon (Website), online: https://www.raytheon.com/capabilities/products/boomerang / 11.05.2024 / 11:43

[2] "DNA Forensics: The application of genetic testing for legal purposes", GeneEd (Web site), online: https://geneed.nlm.nih.gov/topic_subtopic.php?tid=37 / 11.05.2024/ 13:23

[3] Same reference

constitutional protection in the US.235 Cases like this call into question whether law enforcement should be required to obtain judicial authorization to upload the genetic material of perpetrators onto genealogy and DNA analysis website. Furthermore, it is not clear whether law enforcement should be able to rely on algorithms that are proprietary to private companies, and that are not free and open source and therefore escape technical and legal scrutiny. While there may be little legal protection over the privacy of DNA abandoned at a crime scene by a perpetrator, police organizations that may be interested in using AI-powered DNA matching and analysis tools ought to consider whether they are infringing upon the right to privacy of all other people whose DNA is stored in that database.

G. Digital forensics:

also called computer forensics, is the work of extracting and analyzing digital material found in electronic devices to turn it into evidence. There are numerous tools that comb through computers, mobile devices, and software looking for evidence of data that may be incriminating. Artificial intelligence is relevant here because it augments the capability of digital forensic analysis tools, which have generated massive quantities of data that no human being has the cognitive ability to process in reasonable amounts of time.

One key example is the software called Magnet AXIOM, made by Magnet Forensics based in Waterloo, Canada. The tool is called "a digital investigations platform that allows examiners to acquire and examine relevant data from smartphones and computers, and visualize it for better analysis."[1] A core feature of the software is its use of Magnet.AI, which uses machine learning to conduct semantic or contextual content analysis of conversations on smartphones, computers, and chat applications. The company claims that the tool has been optimized for cases of child exploitation, and seeks to categorize and flag language

[1] Amira Zubairi, "Magnet Forensics launches Magnet.AI to fight child exploitation", Betakit (Website) (16 May 2017), online: https://betakit.com/magnet-forensics-launches-magnet-ai-to-fightchild-exploitation /. 13.04.2024 / 14 :56

in conversations that could constitute child luring.[1] The company specifically highlights that this tool will alter how police conduct their interviews and engage in arrest proceedings.

2.1 AI for crime prediction and prevention

Artificial intelligence is also being developed with the aim to predict and prevent crime, and not merely just to detect what has occurred or is unfolding. Interestingly, the use of technology to predict the future occurrence of crimes is not new. Consider the use of violence risk assessment tools in criminal justice and forensic psychiatry. One study demonstrated that there are over 200 tools available in numerous jurisdictions to inform initial sentencing, parole, and decisions regarding post-release monitoring and rehabilitation, but even in 2017 there were very little relevant, reliable and unbiased data that could demonstrate the predictive accuracy of such forensic psychiatry data.

Many of these tools are still in development and could be seen as consisting of vaporware technology that makes promises, but are not mature enough to be launched commercially. One major company offering services in this field is PredPol, a US-based company that "grew out of a research project between the Los Angeles Police Department and UCLA." The company claims to be a "Market Leader in Predictive Policing" and seeks to identify the times and locations where specific crimes are most likely to occur so that these areas can be patrolled to prevent those crimes from occurring. The company states that it has patented its algorithm, which is based on the statistical analysis of three aspects of offender behavior: 1 Repeat victimization (in short, the company assumes that where a crime has occurred, it is more likely that another crime will occur soon after), 2 Near-repeat victimization (which assumes that crimes occur in proximity to one another), 3 Local search (which again assumes that crimes tend to cluster together).

[1] "Introducing Magnet.AI: Putting Machine Learning to Work for Forensics", Magnet Forensics (Web site), online: https://www.magnetforensics.com/blog/introducing-magnet-ai-putting-machine-learning-work-forensics/ 15.05.2024 / 16 :23

This algorithm is partly inspired by the statistical models that are being used to predict earthquake aftershocks.[1]

The technology differs from what has been developed in other US cities, such as in Chicago where a Strategic Subject List seeks to algorithmically or probabilistically determine who is most likely to be a perpetrator or victim involved in future shootings. Redpoll does not assess who is likely to commit a crime, but nonetheless has been criticized for its use of machine learning, the Los Angeles Police Department's criminal data, and an outdated gang territory map to automate the process of classifying "gang-related" crimes. This combination could create a feedback loop in which certain neighborhoods or groups of people are labelled as criminal.[2] Additionally, in an article published in a French journal, the original designer of the seismographic algorithm that influenced the PredPol algorithm was asked to test the applicability of his model to crime data from Chicago and seriously challenged the transferability of this tool to the prediction of crime patterns. The output generated by this kind of approach does not seem much more effective than traditional hotspot maps at forecasting the location of future crimes.

As demonstrated by the work of companies like PredPol, there is a growing and largely unregulated market for software that seeks to assist law enforcement agencies with the prediction of criminal acts. Police organizations seeking to deploy tools that forecast the commission of crimes should proceed with caution and seek to obtain as much information as possible about the accuracy of any tool they wish to use, prior to expending resources on them.

[1] Alexander Babuta, Marion Oswald, & Christine Rinik, "Machine learning algorithms and police decision-making: Legal, ethical and regulatory challenges" (2018) Whitehall Reports (21 September), at 5, online https://rusi.org/publication/whitehall-reports/machine-learning / 22.03.2024 / 14 :45

[2] Randy Rieland, "Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?", Smithsonian Magazine (5 March 2018), online: https://www.smithsonianmag.com/innovation/artificial-intelligenceis- now-used-predict-crime-is-it-biased- / 19.04 .2024 / 19 :09

2.5 Challenges facing the use of artificial intelligence in Combating cybercrime and proposed solutions:

2.5.1 Ethical challenges:

The central challenge created by the development and deployment of AI Tools in a criminal justice setting is of an ethical nature. If AI can certainly generate many uncontroversial social benefits such as more reliable medical diagnosis, less congested (and therefore polluted) thoroughfares, or better farming outcomes in developing countries, to name just a few, its application to a law enforcement or judicial context raises a number of moral dilemmas related to a clash with fundamental principles such as fairness and justice. In her seminal book, Virginia Eubanks has for example shown how these new algorithmic tools of social control can exclude and isolate the most vulnerable members of our societies, intruding into their lives and denying them basic services or singling them out for

enhanced forms of intervention.[1]

2.5.2 Effectiveness challenges:

The advances of AI in general, and deep learning in particular, have been impressive over the past few years after a long hiatus of several decades. However, they have so far been limited toa few domains where data is plentiful and already fairly well-structured and labelled, such as speech recognition and translation, image recognition, or game playing.[2] Gary Marcus, a psychology professor at NYU who also founded a machine learning company presented the most elaborate discussion of why DL approaches do not seem very well suited to unstable domains where generalizations have to be made from limited data. He lists 10

[1] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: NY, St Martin's Press, 2017).

[2] Marcus, supra note 22 at 1.

challenges that we already mentioned in chapter 1 but that we believe need to be detailed here to illustrate why the impressive results delivered by AI in certain fields might not transfer seamlessly to criminal justice applications:

-While humans can learn quickly from a few rules and examples, machine learning models must ingest vast amounts of data to produce reliable decisions. The quantity of useable data that criminal justice agencies can feed to AI models on rare forms of offending might not be sufficient to generate robust predictions;

-The learning process underlying many AI tools is also shallower or narrower than the Deep Learning terminology leads to believe, meaning that an impressive

performance in one area (language translation) cannot easily translate into a different area (such as predicting the chances of recidivism);

- Deep Learning has no Natural way to deal with hierarchical structure, which means that all the available variables are considered on the same level, as 'flat' orlon-hierarchical. This presents a major hurdle when decisions carry a heavy moral or legal weight that must supersede other features;

-Deep Learning tools struggle with open-ended inferences

that an investigator, a judge or a parole officer might pick up intuitively and effortlessly the 'black box' nature of AI tools enables them to make predictions based on thousands or even millions of variables whose interactions are impervious to human analysis. This extraordinary level of complexity also makes the reflexive process that led to those predictions very hard to explain. If this opacity might not be too controversial when labelling cat pictures or providing YouTube videos subtitles, it is a lot more disturbing when AI tools are used to assess the recidivism risk of a convicted offender or even to conduct pre-emptive patrols in minority neighbourhoods, with outcomes and a potential for mistakes that can affect the lives and freedoms of many;

-This is compounded by the fact that AI systems can hardly

differentiate causation from correlation, which is problematic for institutions that need to remain highly accountable;

-Because of the 'flat' and 'black box' approaches mentioned above, Deep Learning resists integrating prior knowledge. It is highly revealing for example that the core PredPol algorithm has been borrowed from seismology rather than developed from the multiple theories of crime and place that are common in criminology.[1] This refusal to recognize prior knowledge seems deliberate, both epistemically due to the history of a research field that has favoured self-contained problems to solve, and technically because it would mean making AI tools less effective. So, in areas where knowledge has to be integrated across very diverse fields (such as in criminal justice), humans will remain much more effective than AI, even if researchers are exploring the potential of 'apprenticeship learning' to enable machines to learn from observing experts at work.[2]

-The technical features highlighted above imply that AI systems are most effective in stable environments where the interactions between underlying variables and outcomes remain constant over time and the growing

availability of data can only enhance a system's

performance. Unfortunately, criminal offenders are a very innovative bunch who relentlessly imagine new ways to manipulate their environment and evade social control mechanisms and enforcement strategies;

-Fragility remains a key feature of AI systems: they can outperform humans on very narrow tasks most of the time but can also fail spectacularly when seemingly minute details in the data they analyze interfere with their internal logic. In a highly publicized paper, Jiawei Su and his colleagues showed that a deep learning algorithm performing image recognition tasks could be fooled by

[1] Bilel Benbouzid, "Des crimes et des seismes : La police prédictiveentre science, technique et divination", 6: 206 Réseaux 95 at 123.

[2] P. Abdeel, & A.Y. Ng, A., "Apprenticeship learning via inverse reinforcement learning", (Paper delivered at the 21st International Conference on Machine Learning, 4-8 July 2004), online: https://dl.acm.org/citation.cfm?id. / 17.05.2024 / 11: 44

changing a single pixel in an otherwise perfectly normal picture. As a result, it misidentified a horse as a frog, a deer as an airplane, or a cat as a dog.[1] One can imagine that criminal justice agencies require much more robust and reliable tools with very limited failure rates;

- Finally, from an engineering perspective, it appears that even high performing AI systems are difficult to embed in legacy systems that may have been in operation for a few decades, particularly in the context of criminal justice agencies that have been slower than other organizations to adopt new technologies and operate therefore with legacy systems that create major frictions with contemporary technologies.[2]

2.5.3 Procurement challenges:

The ethical and technical considerations outlined above also reverberate through the acquisition processes of AI systems by criminal justice organizations, raising a number of procedural issues that can in turn create ethical and performance implications of their own if they are not handled properly. In other words, the competitive business practices of companies that design and market AI technologies, and in particular the confidentiality requirements that they attach to their products to protect their intellectual property, often collide with the need

for public transparency and accountability that characterize the work of government agencies. One of the best examples of this tension is the refusal from Northpointe Inc. (now Equivant), the company that sells the COMPAS system discussed previously in this report, to let defendants and journalists review and challenge the software's secret algorithm.

A comprehensive analysis of the best practices government users should adopt when purchasing and implementing AI solutions, to better manage the ethical

[1] J. Su, D. Vasconcellos Vargas, & K. Sakurai, "One pixel attack forfooling deep neural networks", (2017) arXiv Working Paper, arXiv:1710.08864 [cs.LG], online at https://arxiv.org/abs/ / 11.04.2024 / 16 :56

[2] C. Bellamy, & J. Taylor, "New information and communications technologies and institutional change: The case of the UK criminal justice system," (1996) 9:4 International Journal of Public Sector Management 51.

and performance risks associated with this complex technology, has been provided by Gretchen Greene.[1]

She highlights six issues that should be discussed in great detail by government agencies with the AI companies selling them these new systems.

Despite resistance from the companies that develop AI solutions, a government agency acquiring this kind of product should be able to access its source code and to analyze the algorithms that power it. The practice of buying 'black box algorithms' is often justified by its proponents on the basis of maintaining a seller's technological edge (its 'secret sauce') in the face of relentless competition, but also to avoid the manipulation of neural networks by malicious actors,[2] While not all public organizations may have the maturity and resources to develop their own open source tools and algorithms, they should at least be able (some would add compelled) to inspect how the technology they plan to buy is built and how it makes the decisions that will impact their citizens. One of the key features of Deep Learning algorithms is that they may produce results that are not fully explainable because of the large number and complexity of variables that they are able to incorporate in their computations, but a robust understanding of their underlying code should nevertheless inform their deployment by criminal justice institutions, to reduce unforeseen instances of bias.

The minimum requirements for source code and algorithm transparency outlined above should also extend to the data that has been used to train the algorithms under consideration, or that will be used to make predictions. Machine learning models usually require vast amounts of data to reach optimal outcomes and make reliable predictions, but the nature of the data fed to these systems at the training stage determines the quality of the decisions made when they become

[1] K. Gretchen Greene, "Buying you first AI or 'never trust a used algorithm salesman'", Berkman Klein Center for Internet & Society AI Ethics & Governance (7 November 2018), online: https://medium.com/berkman-klein-center/buying-your-first-ai- . 19.05.2024 / 20:20

[2] L. Maffeo, "The case for open-source classifiers in AI algorithms", opensource.com (18 October 2018), online: https://opensource.com/article/18/10/open-source-classifiers-ai - algorithms. 25.04.2024 / 15 :08

operational. The use of biased data—such as data reflecting racial disparities stemming from discriminatory enforcement or sentencing practices—to train an AI model will generate an equally-biased outcome that will tend to reproduce an undesirable situation, only coated with a scientific varnish. It is therefore essential that any ready-to-use AI tool be examined not only for the quality of its algorithm, but also for the quality of the data used to train it. When AI tools are developed internally with local data, this assessment is much easier to make than when a police organization or a court system purchases an off-the-shelf AI that has been trained with data from an uncertain origin.

Finally, the independent variables that are used by algorithms to make predictions about particular outcomes should also be thoroughly scrutinised. These variables are the levers that algorithms pull to classify the data and make predictions. In criminal justice applications, some common variables traditionally used in statistical analyses are the age, gender, race, income, education, health, social network or prior convictions of a suspect. However, the analytical power of machine learning algorithms and the computer systems that run them means that they can process thousands of variables to make a decision. In the context of an AI used to assess eligibility for parole, the algorithm could for example make use of seemingly unrelated features such as the color of one’s eyes, musical tastes or

downloaded apps, providing they can be extracted from the data. Some of those variables might be correlated with race or socio-economic status and be particularly prone to bias. Hence, it becomes essential to review what variables have the biggest effect and to make sure the causality is well understood and aligned with the principles of justice and fairness.

2.5.4 Appropriation challenges:

We have assumed until now that AI systems will find their way into criminal justice organizations in a neutral environment, where professionals passively implement them as intended by their hierarchy and designers. This is of course a

sociological fiction that ignores the powerful appropriation practices of frontline police officers, crime analysts, judges, parole officers and many other criminal justice professionals. The policing and security literature has established that if security technologies and devices have certainly become compulsory and shape the everyday practices of their human users, the latter always retain high levels of agency that can take different forms and range from domestication to resistance and even sabotage.[1] The concept of appropriation reflects the creativity of individual agents within complex organizations, who translate the technology they are entrusted with into practices that can either be routinized or innovative, meaning that they can absorb a technology into existing cultural values and disarm its reform potential, or on the contrary repurpose a technology to fit their operational needs in unexpected ways. Bluntly stated in a law enforcement context, "whatever technology increases the officer's sense of efficacy will be used and modified, and what is not useful will be destroyed, sabotaged, avoided, or used poorly".[2] Hence, AI is the latest technology in a long succession of criminal justice innovations that have sought to improve the delivery of justice and the effectiveness of its institutions, but that may end up being much less disruptive that anticipated.

2.6 Conclusion:

AI has the prospect in law enforcement as did the previous innovations. Innovation has been considered in law enforcement and has the prospect of well, in the following ways. Another hope for exciting developments has arisen in data mining where it is possible to work with sounds, faces or other practically useful materials and in the sphere of digital forensics. However, this approach opens up concerns regarding unregulated predictive tools. It is important to pay attention to

[1] R. Ericson, & K. Haggerty, Policing the risk society (Oxford: Clarendon Press, 1997); A. A micelle, C. Aarau, & J. Jeandesboz, "Questioning security devices: Performativity, resistance, politics,"(2015) 46:4 Security Dialogue 293.

[2] P. K. Manning, The technology of policing: Crime mapping, information technology, and the rationality of crime control (New York: NY, New York University Press, 2008) at 250

while some of apply of technology in teaching and learning have close benefits the other has challenges. Officers and establishments involved must therefore act responsibly by ensuring that there is proper use of the AI technology through availing the right checks, governance, and cooperation.

GENERAL CONCLUSION

General Conclusion:

The background of this study examined the applicability of employing Artificial Intelligence (AI) techniques to deter cybercrime. Since computer crimes have come along with the progress of information technology and the internet revolution, and thus it may be more compelling to look at how AI can handle these techno-crimes within the sociotechnical context of the era. The modern threats are significantly different from the previous traditional threats, and the national legislation, including the Algerian one, should react efficiently to these threats.

The purpose of this study was therefore to establish how the field of AI can approached to mitigate cyber threats. More precisely, it was posited to investigate the sustainable and meaningful integration of generative AI in this particular domain. In this section, the evidence substantiates the four primary ways that AI can assist in the prevention, detection, and management of cybercrime. This involves the use of features such as machine learning algorithms, natural language processing, and anomaly detection to detect intended patterns that are issues to do with cyberattacks as well as formulate ways to discourage such incidences.

Reflecting on the work accomplished, it provides novel insights essential to the discussion of AI and its application in cybersecurity. AI can work in conjunction with existing security management techniques because it can analyze huge streams of data for statistical anonymizes, and learn from the continually emerging different types of risks. Of course, it is especially significant to comprehend that in general AI performs optimally when it is integrated with human intervention and management.

The implications of the present study are to be knowledgeable for policy, practice, and future research. The appropriate application of AI remains a priority in the ongoing countermeasures against cybercrime, and policymakers should engage industry, law enforcement, and academia to effectuate AI’s integration into

these measures appropriately. Businesses should consider converting themselves to utilize AI technology to prevent future losses to their virtual assets.

Before concluding the constructs of this research, there are specific restrictions of this work that should be mentioned. Substantial progress has been made nonetheless, some questions and issues persist, these include the fairness in AI, the ability of an attacker to coax a specific output from the AI algorithm, and privacy. To harness the advances in AI to its maximum potential for cybersecurity at the operational level, both researchers & practitioners need to address, the above-mentioned challenges.

Based on our findings, we recommend several areas for further exploration:

Investigate the explain ability of AI models, federated learning, and secure model deployment in greater depth, educate cybersecurity professionals on AI approaches and the potential for misuse and foster increased cooperation with other countries to address cyber threats and risks across different regions.

Overall, our research highlights the critical need for integrating artificial intelligence technologies into the fight against cybercrime. By implementing AI effectively across industries, we can create a safer digital environment and protect ourselves from the adversities originating from the online world.

Results:

Artificial intelligence (AI) is proving to be a significant weapon in the fight against cybercrime. AI applications are being successfully implemented in various fields, and cybercrime prevention is one of them.

However, there's a gap between AI's potential and its practical application. While AI has shown effectiveness, there is no specific legislation in place to regulate its use in combating cybercrime. Existing regulations simply can't keep pace with the rapid development of AI technology. This highlights the need for

comprehensive and up-to-date regulations to fully harness the power of AI in this domain.

The positive impact of AI in reducing cybercrime makes its future implementation a necessity. However, the lack of legislation is a major hurdle. The current legal framework in Algeria, for example, lags behind in this field, hindering the full potential of AI technologies.

Despite these challenges, AI systems have achieved remarkable development thanks to human efforts. Their speed and high accuracy make them well-suited for combating cybercrime. However, there are still challenges that need to be addressed in order to fully leverage their capabilities.

Recommendations

AI is seen as a great tool in preventing cybercrime since it can be programmed to accurately identify and eliminate the problem. Yet, certain critical aspects need to be targeted for achieving this potential to the optimum degree.

however, current developments accruing to the application of AI technologies can still be construed as immature. People should be urged to start using AI in fields such as healthcare, banking, finance, space, and others; while investing in advanced research to generate better AI programs and modes for counteracting cyber criminals.

It is therefore important to have a solid legal and legislative foundation for applying AI in fighting cybercrime. More attention should be paid to developing a framework that would comprise, coordinate, and categorize the enhanced role of AI in addressing challenges in this area due to the urgency of the situation.

Intergovernmental relations are the other crucial component, In this case, the use of AI in fighting cybercrime will improve with enhanced cooperation among nations. Hiring or organically growing the most proficient digital police departments with digital expertise can be compatible with visionaries and utilize AI's efficiency in eradicating new-age crimes.

That is why, it is imperative to continue the pursuit and maintain rapport with significant technical progress in the sphere of cybercrime in Algeria. Perhaps, sending missions to globally developed countries to see how they deal with the experiences and engage high-precision AI's can be helpful.

Even the acquisition of experts and other skilled professionals in developed states to design AI systems is crucial as well. In particular, AI can develop valuable and authoritative skills to prevent and mitigate cyber risks.

It is therefore important for the Algerian legislator to undergo a radical transformation in his/her thinking in the legislative environment. Going further from amendments, political choices to specifically leverage AI in the fight against cybercrime are strategic. The updates of cybercrime laws are also crucial to be done regularly to compete with the rapidly changing technological environment.

BIBLIOGRAPHY

Books:

- A. D. (Dory) Reiling, Courts and Artificial intelligence, International Journal for Court Administration, 2020, Page 4.
- Abdel Nour, Adel (2017). Expert Systems, Publications of the Department of Electrical Engineering, King Saud University. Kingdom of Saudi Arabia
- Abdel Nour, previous reference, p. 128
- Abdellah Ibrahim Al Faqi, Artificial Intelligence and Expert Systems, Dar Al Thaqafah for Publishing and Distribution, First Edition, Jordan, 2012, p. 58.
- Abdullah Saeed Abdullah Al Wali, Civil Liability for Damages Caused by Artificial Intelligence Applications in UAE Law, Analytical and Comparative Study, Dar Al Nahda Al Arabiya, Cairo, 2021, p. 27.
- Abdulrazak, Rana Mesbah Abdel Mohsen, "The Impact of Artificial Intelligence on Cybercrime," Journal of King Faisal University, Vol. 22, No. 1 (2021), p. 431.
- Ahmed Ali Hassan Osman, Reflections of Artificial Intelligence on Civil Law, Journal of Law and Technology, Zagazig University, No. 76, June 2021, p. 1534.
- Amal Kara, 2020, Computer Crime, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law and Political Science, University of Ben Aknoun, Algeria
- Amira Zubairi, “Magnet Forensics launches Magnet.AI to fight
- Atta Allah Fashar, 2017, Confronting Cybercrime in Algerian Legislation, Research Presented to the Moroccan Conference on Law and Information Technology, Academy of Graduate Studies, Libya.
- Ayman Mohamed Sayed Mustafa Al-Asyuti, The Impact of Artificial Intelligence Technology on Law, published in a book entitled "Collective Book - The Impact of Technological Development on Law, Institute of Palestine Ahliya University for Studies and Research, Palestine, without year of publication, p. 367.
- Baara Saeed, "Cybercrime in Algerian Legislation," Master's Thesis, University of Mohamed Kheider - Biskra, 2016/2015, p. 11.
- Belaid Mansouriya, "The Procedural System of Cybercrime in Algerian Legislation," Master's Thesis, University of Abdelhamid Ben BadisMostaganem, 2020/2019, p. 9
- Bilel Ben Bouzid, “Des crimes et des séismes: La police prédictiveentre science, technique et divination“, 6: 206 Réseaux 95 at 123.

Bibliographique references

- C. Bellamy, & J. Taylor, “New information and communication technologies and institutional change: The case of the UK criminal justice system,” (1996) 9:4 International Journal of Public Sector Management 51.
- Charles Cho et al, “Astroturfing Global Warming: It Isn’t Always Greener on the Other Side of the Fence” (2011) 104:4 J Bus Ethics 571
- Christian Youssef, Civil Liability for Artificial Intelligence Acts, Al-Halabi Legal Publications, First Edition, Beirut, Lebanon, 2022, p26.
- Christian Youssef, previous reference, p. 26.
- Christian Youssef, previous reference, p. 27-28.
- Dhabi Musa Al-Bad Aniyah, "Cybercrimes: Concept and Causes, Emerging Crimes in Light of Regional and International Changes and Transformations," Amman - Hashemite Kingdom of Jordan, 2014, p. 3
- Dhaib Musa Al-Badaniyah, "Electronic Crime and Its Repercussions on National and Citizen Security Between Legal Combat and Detection and Investigation Devices," Journal of Public Administration, Law and Development, Hassiba Ben Bouali University, El-Oued, Algeria, No. 01, 2022, p. 20.
- Ferj Hussein, "Electronic Crime and Its Repercussions on National and Citizen Security Between Legal Combat and Detection and Investigation Devices," Journal of Public Administration, Law and Development, Hassiba Ben Bouali University, El-Oued, Algeria, No. 01, 2022, p. 76
- Frank wells Sudia, Artificial Intelligence, sooner than you think. – A Jurisprudence of Artilects: Blueprint for a Synthetic Citizen, Al Tamimi & Company, Westlaw Middle East, Thomson Reuters, August 1, 2004, Page 2 – Page 3.
- Ibrahim Suleiman Al Qatawneh UAE, Artificial Intelligence Crimes, Academic Journal of Interdisciplinary Studies, p143
- Malicious Use of Artificial Intelligence, supra note 71 at 16.
- Malicious Use of Artificial Intelligence, supra note 71 at 20
- Malicious Use of Artificial Intelligence, supra note 71 at 20.
- Malicious Use of Artificial Intelligence, supra note 71 at 33.
- Mamdouh Hassan Manea Al-Adwan, Criminal Responsibility for Illegal Acts of Artificial Intelligence Entities, Journal of Law and Technology, Jordan University, No. 4, 2021, p. 151.

Bibliographique references

- MassoudChahira, "Cybercrime in Algerian Legislation," Master's Thesis, University of Abdelhamid Ben BadisMostaganem, 2021/2020, p. 6
- Merabet Ramissa, "Cybercrime: Between the Limits of Danger and the Necessities of Confrontation," Journal of Governance and Economic Law, Faculty of Law and Political Sciences Sousse/Tunisia, No. 01, 2023, p. 61
- Mohamed Mohamed Abdel Latif, Liability for Artificial Intelligence between Private Law and Public Law, Paper presented to the Conference on the Legal and Economic Aspects of Artificial Intelligence and Information Technology, May 23-24, 2021, Faculty of Law, Mansoura University, 2021, p. 3-4.
- Mohammed Irfan Al Khatib, Artificial Intelligence and Law, A Critical Comparative Study in French and Qatari Civil Legislation in Light of the European Rules in the Civil Law of Humanity for 2017 and the European Industrial Policy for Artificial Intelligence and Humanity for 2019, Journal of Legal Studies, Arab Beirut University, 2020, p. 4-5.
- Moses Olafenwa, “Object Detection with 10 lines of code”, Towards Data Science (16 June 2018)
- OuliOuld Rabah Safia, 2015, The Legal Nature of Cybercrime, National Conference on Cybercrime: Between Prevention and Combating, University of Mohamed Kheider, Biskra, November 15-16, Algeria.
- R. Ericson, & K. Haggerty, Policing the risk society (Oxford: Clarendon Press, 1997); A. Amicelle, C. Aradau, & J. Jeandesboz, “Questioning security devices: Performativity, resistance, politics,”(2015) 46:4 Security Dialogue 293.
- RashaAlMarhoos, “Phishing for the answer: Recent developments in combating phishing”, (2007) 3:3 I/S: A Journal of Law and Policy for the Information Society 595
- RaziyaAymour, "Cybercrime and Mechanisms for Combating It in Algerian Legislation," Academic Journal of Legal and Political Research, University of Laghouat, No. 1, 2022, p. 91
- Rickli, J.M., Mantellassi, F.: Artifcial intelligence in warfare: military uses of AI and their international security implications. In: The AI wave in defence innovation, pp. 12–36. Routledge, Cham (2023) 13:15
- Shekhar. 2019. Artificial Intelligence in Automation. International Journal of Multidisciplinary, 4(6), pp.13-17
- shotspotter-gunshot-detecting-surveillance-tech-danforth-shooting.

Bibliographique references

- Si Hamdi Abdel Momen, Kira Saad, "Cybercrime and Mechanisms to Combat It in Algerian Law," Journal of Legal and Political Studies, University of Mohamed Bachir Ibrahim, Bordj BouArreridj, Algeria, No. 01, June 2022, p. 61
- Si Hamdi Abdel Momen, Kira Saad, same reference and same page.
- Si Hmadi Abdel Momen, Kira Saad, "Electronic Crime and Its Repercussions on National and Citizen Security Between Legal Combat and Detection and Investigation Devices," Journal of Public Administration, Law and Development, Hassiba Ben Bouali University, El-Oued, Algeria, No. 01, 2022, p. 62-63.
- Tahir Abu Al-Eid, A Guide to Artificial Intelligence for Law Students and Researchers, Journal of Law and Technology, Cairo, No., 2023, p. 10.
- Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: NY, St Martin's Press, 2017).
- Yamina Mankhrifis, "Electronic Crimes on Social Media Sites with Social and Moral Dimensions," Journal of Law and Human Sciences, University of Algiers 3, Faculty of Information and Communication Sciences, No. 01, 2023, p. 1304.
- Yasmina Bounaara, "Cybercrime," Al-Mi'yar, University of Amir Abdelkader of Islamic Sciences Constantine - Algeria, No. 39, June 2015, p. 289.
- Ahmed Adel Jameel, Othman Hussein (2018). The Possibility of Using Artificial Intelligence in Internal Audit Quality Control. Amman, Without Publisher, p. 112
- Chomiak-Orsa, I., Rot, A., Blaicke, B.: Artifcial intelligence in cybersecurity: the use of ai along the cyber kill chain. In: Nguyen, N.T., Chbeir, R., Exposito, E., Aniorté, P., Trawiński, B. (eds.) Computational collective intelligence Lecture Notes in Computer Science, pp. 406–416. Springer International Publishing, Cham (2019) 13:47
- Christopher Rigano, Using Artificial Intelligence to Address Criminal Justice Needs, National Institute of Justice, NIJ Journal / Issue No. 280, January 2019, Page 1.
- LattarchFairouz, Hatem Ben Azouz, "Cybercrime in Algeria: From Individual Crime to Organized Crime," Afak for Sciences, University of Djelfa, No. 01, 2016, p. 328.
- Kagita, M.K., Tillakaratne, N., Gadekallu, T.R., Maddikunta, P.K., Singh, S.: A review on cybercrimes on the internet of things. In: Makkar, A., Kumar, N. (eds.) Deep learning for security and privacy preservation in iot, in signals and communication technology, pp. 83–98. Springer, Sin gap 13:20

- Law No. 09 - 04 issued on August 5, 2009, which includes the special rules for the prevention and fight against crimes related to information and communication technologies, J.R. No. 47.

Articales:

- 5 Nicolas Paper not et al, “Practical Black-Box Attacks against Machine Learning” (2016) arXiv Working Paper, arXiv:160202697 [cs], online: http://arxiv.org/abs/1602.02697. 12/01/2024 11:11
- 6 Kathrin Grosse et al, “Adversarial Perturbations Against Deep Neural Networks for Malware Classification” (2016) arXiv Working Paper, arXiv:160604435 [cs], online: http://arxiv.org/abs/1606.04435.12/01/2024 11:20
- 6 Motivations of Cyber Criminals, Mar 3, 2022 11:15:00 AM, Visit date: 13-05-2024, Visit time: 00:03, https://www.coretech.us/blog/6-motivations-of-cyber-criminals
- Abhimanyu Goshen, “I trained an AI to copy my voice and it scared me silly”, The Next Web (22 January 2018), online: https://thenextweb.com/insights/2018/01/22/i-trained-an-ai-to-copy -my-voice-and-scared-myself-silly/
- AL-Dosari, K., Fetais, N., Kucukvar, M.: Artifcial intelligence and cyber defense system for banking industry: a qualitative study of ai applications and challenges. Cybernet Syst. (2024) 11:44. “https://doi.org/10.1080/01969722.2022.2112539”
- Alexander Babuta, Marion Oswald, & Christine Rinik, “Machine learning algorithms and police decision-making: Legal, ethical and challenges” (2018) Whitehall Reports (21 September), at 5, online:https://rusi.org/publication/whitehall-reports/machine-learning / 22.03.2024 / 14 :45
- Ansari, M.J., Dash, B., Sharma, P., Yathiraju, N.: The impact and limitations of artificial intelligence in cybersecurity: a literature review. Int. J. Adv. Res. Compute. Commun. Eng. (2024) 11:55. “https://doi.org/10.17148/IJARCCE.2022.11912”
- Arelis Guzmán, “Top 10 Pretrained Models to get you Started with Deep Learning (Part 1 - Computer Vision)”, Analytics Vidhya (27 July 2018), online:https://www.analyticsvidhya.com/blog/2018/07/top-10-pretrainedmodels-get-started-deep-learning-part-1-computer-vision/. 01/05/2024 18:37
- Aural Oberon, “Exploring Deep Fakes”, Hacker Noon (5 March 2018), online: https://hackernoon.com/exploring-deepfakes-20c9947c22d9; Alan Zucconi, “Understanding the Technology Behind Deep Fakes”, Alan Zucconi (14 March

2018),online: https://www.alanzucconi.com/2018/03/14/understanding-the-technologybehind-deepfakes/ 2:12 20/04/2024

- B Liu et al, "Software Vulnerability Discovery Techniques: A Survey" (Paper delivered at the Fourth International Conference on Multimedia Information Networking and Security online: https://ieeexplore.ieee.org/document/6405650. 16:45 20/04/2024
- Battista Biggio, Blaine Nelson & Pavel Laskov, "Poisoning Attacks against Support Vector Machines" (2012) arXiv Working Paper, arXiv:12066389 [cs, stat], online: http://arxiv.org/abs/1206.6389.12/01/2024 11:58
- Benjamin IP Rubinstein et al, "ANTIDOTE: understanding and defending against poisoning of anomaly detectors" (Paper delivered at the 9th ACM SIGCOMM Conference on Internet Measurement, 2009), online: https://people.eecs.berkeley.edu/~tygar/papers/SML/IMC.2009.pdf; Nitika Khurana, Sudip Mittal & Anupam Joshi, "Preventing Poisoning Attacks on AI based Threat Intelligence Systems" (2018), arXiv Working Paper, arXiv:1807.07418 [cs.SI], online: https://arxiv.org/abs/1807.07418v1; Maria Korolov, "Hackers get around AI with flooding, poisoning and social engineering", CSO Online (16 December 2016), online: https://www.csoonline.com/article/3150745/security/hackers-get- around-ai-with-flooding-poisoning-and-social-engineering.html12/01/2024 13:46
- Neural fuzzing: applying DNN to software security testing", Microsoft Research (13 November 2017), online: https://www.microsoft.com/en-us/research/blog/neural-fuzzing/; Mohit Rajpal, William Blum & Rishabh Singh, "Not all bytes are equal: Neural byte sieve for fuzzing", (2017) arXiv Working Paper, arXiv:1711.04596 [cs.SE], online: https://arxiv.org/abs/1711.04596 at 10. 12/04/2024 12:54
- dictionary.cambridge.org/dictionary/learner-english/cybercrime - time 3:53 / 26/02/2024.
- child exploitation", Betakit (Website) (16 May 2017), online :https://betakit.com/magnet-forensics-launches-magnet-ai-to-fightchild-exploitation /. 13.04.2024 / 14 :56
- Cockburn IM, Henderson R, Stern S (2018) The impact of artificial intelligence on innovation. No. W24449, National Bureau of Economic Research. https://www.nber.org/papers/w24449 Accessed on 11.02.2024 / 12:25
- Daniel Votipka et al, "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes" (Paper delivered at the 2018 IEEE Symposium on Security and Privacy, San Francisco, CA, 2018), online: https://ieeexplore.ieee.org/document/8418614. 13/12/2023 12:30

Bibliographique references

- David Wagner & Paolo Soto, “Mimicry Attacks on Host-Based Intrusion Detection Systems” (Paper delivered at the 9th ACM conference on Computer and communications security, Washington DC, 2002), online: https://dl.acm.org/citation.cfm?id=586145 at 10/04/2024 13:42
- .
- FortiGuard SE Team, “Predictions: AI Fuzzing and Machine Learning Poisoning”, Fortinet Blog (15 November 2018), online: https://www.fortinet.com/blog/industry-trends/predictions--ai-fuzz ing-and-machine-learning-poisoning-.html. 22/03/2024 13:01
- Francesca Cristiana, “How Lyrebird Uses AI to Find Its (Artificial) Voice”, Wired (15 October 2018), online: https://www.wired.com/brandlab/2018/10/lyrebird-uses-ai-find-artificial -voice/; “Lyrebird: Ultra-Realistic Voice Cloning and Text-to-Speech”, Lyrebird’s (Website), online: https://lyrebird.ai/
- García-Teodoro et al, “Anomaly-based network intrusion detection: Techniques, systems and challenges” (2009) 28:1–2 Computers & Security 18; Alex Shenfield, David Day & Aladdin Ayesh, “Intelligent intrusion detection systems using artificial neural networks” (2018) 4:2 ICT Express 95.
- Gilad, A., Tishler, A.: Mitigating the risk of advanced cyber-attacks: the role of quality, covertness and intensity of use of cyber weapons. Def. Peace Econ. (2023). https://doi.org/10.1080/ 10242694.2022.2161739 13:30
- Gustavo Grieco& Artem Dinaburg, “Toward Smarter Vulnerability Discovery Using Machine Learning”. (Paper delivered at the Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security, Toronto, Canada, 2018); Steven Harp et al, “Automated Vulnerability Analysis Using AI Planning” (Paper delivered at the 2005 AAAI Spring Symposium, Stanford, CA, 2018), online: https://www.researchgate.net/publication/221250445_Automated_ Vulnerability_Analysis_Using_AI_Planning at 8.
- Hyrum S Anderson et al, “Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning” (2018) arXiv Working Paper, arXiv:180108917 [cs], online: http://arxiv.org/abs/1801.08917. 14/03/2024 15:17
- Ian Mann, Hacking the human: Social engineering techniques and security countermeasures, (London: Rutledge, 2008).

Bibliographique references

- Ivan Novikov, “How AI Can Be Applied To Cyber attacks”, Forbes (22 March 2018), online: https://www.forbes.com/sites/forbestechcouncil/2018/03/22/how-ai-can-be-applied-to-cyberattacks/ 11/04/2024 21:03
- J. Su, D. Vasconcellos Vargas, & K. Sakurai, “One pixel attack for fooling deep neural networks”, (2017) arXiv Working Paper,arXiv:1710.08864 [clog], online at https://arxiv.org/abs/ / 11.04.2024 / 16 :56
- Jamal Brahimi, 2016, Combating Cybercrime in Algerian Legislation, The Critical Journal of Law and Political Science, Volume 2, Issue 2, Algeria.
- Jeff Kao, “More than a Million Pro-Repeal Net Neutrality Comments Were Likely Faked”, Hacker Noon (23 November 2017), online: https://hackernoon.com/more-than-a-million-pro-repeal-net-neutrality -comments-were-likely-faked-e9f0e3ed36a6.
- Jennifer Langston, “How PhotoDNA for Video is being used to fight online child exploitation”, Microsoft On the Issues (12 September 2018), online:https://news.microsoft.com/on-the-issues/2018/09/12/how-photodnafor-video-is-being-used-to-fight-online-child-exploitation/. 10.02.2024 16:15
- John Cloonan, “Advanced Malware Detection - Signatures vs. Behavior Analysis”, Info security Magazine (11 April 2017), online: https://www.infosecurity-magazine.com:443/opinions/malware-de taction-signatures/ 01/02/2024 20:36
- Jon Swaine, “Russian propagandists targeted African Americans to influence 2016 US election”, The Guardian (17 December 2018), online: https://www.theguardian.com/us-news/2018/dec/17/russian-propa gandists-targeted-african-americans-2016-election.
- Jordan Pearson, “Toronto Approves Gunshot-Detecting Surveillance
- Jordan Smith, US Reporter, HCLTech,https://www.hcltech.com/trends-and-insights/cybercriminals-utilizing-ai-commit-cybercrimes 14:35
- Julie J.C.H. Ryan, “How do computer hackers ‘get inside’ a computer?”, Scientific American, online: https://www.scientificamerican.com/article/how-do-computer-hackers-g/
- K. Gretchen Greene, “Buying you first AI or ‘never trust a used algorithm salesman’”, Berkman Klein Center for Internet & Society AI Ethics & Governance (7 November 2018), online: https://medium.com/berkman-klein-center/buying-your-first-ai- . 19.05.2024 / 20:20

- Kao, supra note 123; Xiaoyong Yuan et al, "Adversarial Examples: Attacks and Defenses for Deep Learning" (2017) arXiv Working Paper, arXiv:171207107 [cs, stat], online: http://arxiv.org/abs/1712.07107.12/01/2024 11:45
- Kulkarni RH, Padmanabhan P (2017) Integration of artificial intelligence activities in software development processes and measuring effectiveness of integration. IET Software 11(1):18:26. doi: 22.04.2024
- L. Maffeo, "The case for open source classifiers in AI algorithms", opensource.com (18 October 2018), online:https://opensource.com/article/18/10/open-source-classifiers-ai - algorithms. 25.04.2024 / 15 :08
- Mahmoud Ragab Fatah Allah, the cybercrime criminal and his motives, 2023/05/13, Visit date: 13-05-2024, Visit time: 00:03, https://www.ahewar.org/debat/show.art.asp?aid-608845
- Masarah Paquet-Clouston, Bernhard Haushofer & Benoît DuPont, "Ransom ware payments in the bit coin ecosystem", (Paper delivered at the 17th Annual Workshop on the Economics of Information Security (WEIS), 2018) online: https://arxiv.org/abs/1804.04080. 12:15 11/04/2024
- Matt Chessen, "The Madcom Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy...and What Can Be Done About It", The Atlantic Council (1 September 2017), online: https://www.scribd.com/document/359972969/The-MADCOM-Future at 13.
-
- Nils J. Nilsson, The Quest for Artificial Intelligence (Cambridge, UK: Cambridge University Press, 2013) at10.04.2024 /12:45.
- Nilsson, ibid at 30; "Introduction to Computer Vision", Algorithmic Blog (2 April 2018), online https://blog.algorithmia.com/introduction-to-computer-vision/; Golan Levin, "Image Processing and Computer Vision", Open Frameworks, online https://openframeworks.cc/ofBook/chapters/image_processing_com puter_vision.html.
- Oxford Learner's Dictionary definitions of cybercrime www.oxfordlearnersdictionaries.com/definition/american_english/cybercrime - time 3:53 / 26/02/2024.
- Rabiul Islam, Former Forbes Councils Member, Jun 23, 2023https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/ 14:25, 12/02/2024.

Bibliographique references

- Randy Rieland, “Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?”, Smithsonian Magazine (5 March 2018), online:https://www.smithsonianmag.com/innovation/artificial-intelligenceis- now-used-predict-crime-is-it-biased- / 19.04 .2024 / 19 :09
- Research Will Shape the Future of Proactive Policing October 24, 2019 By Paul A. Haskins https://nij.ojp.gov/topics/articles/research-will-shape-future-proactive-policing 10/04/2024 18:32
- Tech Days After Mass Shooting”, VICE Motherboard (25 July 2018) Online :https://motherboard.vice.com/en_us/article/7xqk44/toronto-approve
- The Algerian penal code: articles 394 bis 1,2,3,5,6,7/Amended and Completed (Law 04-15 + Law 24-06) Section 7
- The Importance of Artificial Intelligence in Today's World By Nextech3D.ai on May 11, 2024 14:53
- Thomas P Lyon & John W Maxwell, “Astroturf: Interest Group Lobbying and Corporate Strategy” (2004) 13:4 J Econ Manag Strategy 561; Kevin Grandia, “Bonner & Associates Undemocratic History of Astroturfing”, Huffington Post (26 August 2009), online: https://www.huffingtonpost.com/kevin-grandia/bonner-associates-the-lon _b_269976.html.
- Tsiolkovsky W (2017) Social and economic implications for the smart grids of the future. Economics and Sociology 10(1):310-318. doi: 10:14/2071-789X.2017/10.01.2024
- UNODC (United Nations Office on Drugs and Crime) https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html - time 3:53 / 26/02/2024.
- We deliberately use the term ‘criminal hacker’ to avoid the usual confusion between the majority of technology enthusiasts who like to tinker with software and hardware and the small minority of this group that uses their technical expertise to deliberately break the law. [1]
- Yu PK (2020) The Algorithmic Divide and Equality in the Age of Artificial Intelligence. Florida Law Review 11:12 / 12.03.2024
- Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., Sangaiah, A.K.: Classifcation of ransomware families with machine learning based onN-gram of opcodes. Future. Gener.

Compute. Syst..Gener. Compute. Syst. 90, 211–221 (2019). https://doi.org/ 10.1016/j.future.2018.07.052 14:05

Websites:

- "Astroturfing, Twitterbots, Amplification - Inside the Online Influence Industry", The Bureau of Investigative Journalism (7 December 2017), online: https://www.thebureauinvestigates.com/stories/2017-12-07/twitterbots.
- "Axon AI and Policing Technology Ethics Board", Axon (Website), online: https://ca.axon.com/info/ai-ethics.
- "DNA Forensics: The application of genetic testing for legal purposes", GeneEd (Web site), online: HTTPs://geneed.nlm.nih.gov/topic_subtopic.php?tid=37 / 11.05.2024/13 :23
- "Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone", Google AI (Blog), online: http://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conver sation.html
- "Google Unveils Neural Network with 'Superhuman' Ability to Determine the Location of Almost Any Image", MIT Technology Review (24 February 2016), online: https://www.technologyreview.com/s/600889/google-unveils-neural -network-with-superhuman-ability-to-determine-the-location-of-almost/./10.2.2024 / 12:33
- "Introducing Magnet.AI: Putting Machine Learning to Work for Forensics", Magnet Forensics (Web site), online:https://www.magnetforensics.com/blog/introducing-magnet-ai-putting-machine-learning-work-forensics/ 15.05.2024 / 16 :23
- "Let's Go Vishing", (22 December 2014), online: Security Through Education. https://www.social-engineer.org/general-blog/lets-go-vishing>
- "Penetration Testing Software, Pen Testing Security", Metasploit (Website), online: https://www.metasploit.com/20/04/2024 22:1
- "Siri", Apple (Website), online: https://www.apple.com/siri/
- "Social Engineering Defined", Security Education (Website), online: https://www.social-engineer.org/framework/general-discussion/social -engineering-defined/.
- "The top frauds of 2017", Consumer Information, (1 March 2018), online: https://www.consumer.ftc.gov/blog/2018/03/top-frauds-2017.
- "Vishing", Security Through Education (Website), online: https://www.social-engineer.org/framework/attack-vectors/vishing/

- "Ways to Build with Amazon Alexa", Amazon (Website), online: https://developer.amazon.com/alexa
- 14 Ways Scammers Can Steal Your Credit Card Numbers in 2024/ Hari Ravichandran/ https://www.aura.com/learn/how-do-people-steal-credit-card-numbers01/03/2024 19:25
- Boomerang III: State-of-the-Art Shooter Detection", Raytheon (Website), online: https://www.raytheon.com/capabilities/products/boomerang / 11.05.2024 / 11:43
- Brian Krebs, "Buying Battles in the War on Twitter Spam", Krebs on Security (Website) online: https://krebsonsecurity.com/2013/08/buying-battles-in-the-war-ontwitter-spam/
- BrilandHitaj et al, "Pass GAN: A Deep Learning Approach for Password Guessing" (2017) arXiv Working Paper, arXiv:170900440 [cs, stat], online: http://arxiv.org/abs/1709.00440. 13/03/2024 19:59
- Britannica dictionary definition of artificial intelligence, https://www.britannica.com/dictionary/artificial-intelligence Visit date: 12-05-2024, Visit time: 13:23
- Credit Card Fraud /By FindLaw Staff/ https://www.findlaw.com/criminal/criminal-charges/credit-debit-card-fraud.html 07/03/2024 9:10
- Credit Card Fraud/ https://www.scribd.com/presentation/241860981/Credit-Card-Fraud/ 27/03/2024 05:23
- Cybercrime: "Objectives, Causes, Methods, and Treatment" by Esraa Gabriel Rashad Murree (05/12/2023, 14:03) https://democraticac.de/?p-35426
- Grandia, supra note 118; David Streitfeld, "Book Reviewers for Hire Meet a Demand for Online Raves", The New York Times (25 August 2012), online: https://www.nytimes.com/2012/08/26/business/book-reviewers-forhire-meet-a-demand-for-online-raves.html.
- https://towardsdatascience.com/object-detection-with-10-lines-of-coded6cb4d86f606.
- P. Abdel, & A.Y. Ng, A., "Apprenticeship learning via inverse reinforcement learning", (Paper delivered at the 21st International Conference on Machine Learning, 4-8 July 2004), online: https://dl.acm.org/citation.cfm?id. / 17.05.2024 / 11 : 44
- P. K. Manning, The technology of policing: Crime mapping, information technology, and the rationality of crime control (New York: NY, New York University Press, 2008) at 250

Bibliographique references

- Penal Code § 484e PC – Theft of Credit Card Information – California Law/ https://www.shouselaw.com/ca/defense/penal-code/484e / 05/03/2024 10:25
- Phishing", Security Through Education (Website) Phishing", Security Through Education (Website), online
- Qin SJ, Chiang LH (2019) Advances and opportunities in machine learning for process data analytics. Computers & Chemical Engineering 126:465-473. Doi 10:54: /j.compchemeng.2024.04.03
-
- link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3 - time 3:53 / 26/02/2024.
- Tattoo Recognition", FBI.gov, (25 June 2015), online: https://www.fbi.gov/audio-repository/news-podcasts-thisweek-tattoo
- The capability of a machine to imitate intelligent human behavior https://www.merriam-webster.com/dictionary/artificial%20intelligence Visit date: 19-05-2024, Visit time: 11:03

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة ابن خلدون – تيارت-

كلية الحقوق والعلوم السياسية

فريق ميدان التكوين :

إذن بالإيـــــــداع

أنا الممضي أسفله الأستاذ: ..... بوجال لسمير .....

المشرف على المذكرة الموسومة بـ : إثبات الجريمة باستعمال المخرجات الحديثة - الذكاء الإصطناعي كنموذج - (باللغة الإنجليزية)

من إعداد الطالب (01) : ..... بن سعيد عبد القادر .....

الطالب (02): ..... دراوي حفيظة .....

تخصص : ..... قانون جنائي .....

امنح الإذن للطلبة بإيداع المذكرة على الأرضية الرقمية لاستكمال إجراءات المناقشة .

الأستاذ المشرف