From Cyber-crimes to Cyber-Security: Exploring Legal Minefield of Artificial Intelligence in Pakistan

Muhammad Saad Saleem
Advocate, High Court/ LLM, University of Lahore
saadsaleem.lawyer@gmail.com
Faiza Malhooz
Assistant Professor, Govt. Graduate College for Women, Baghbanpura Lahore
faizamalhooz@gmail.com
Tehreem Fatima
Lecturer, University of Home Economics, Lahore
t.fatima1210@gmail.com

Abstract

Artificial intelligence (AI), an imminent power in the control of cyber-criminals, is now recognized as an innovative catalyst in the privacy and information security field, becoming an efficient instrument for protecting sensitive data. This paper explores various legal implications of AI's engagement in the modern world of digital assaults and crimes. Security organizations, government bodies, and legal experts have been forced to adjust and react to new dangers due to the swift growth of artificial intelligence-based cybercrimes. The use of AI in illicit activities, including systematic phishing attempts, data theft, and the development of complex spyware, raises regulatory concerns. This analysis explores the legal ramifications of the detection, legal action, and corresponding fines related to crimes facilitated by artificial intelligence. The present research aims to elucidate the regulatory structures underpinning AI-powered cyber-defence activities using the qualitative research method. Specifically, it explores the intricate aspects of data protection, moral dilemmas, and adherence to applicable laws. These shifts offer innovative prospects and complexities for the regulatory sphere, encompassing concerns regarding partiality, openness, and responsibility in decision-making facilitated by artificial intelligence. The article highlights the complex relationship between artificial intelligence (AI), legislation, and cybersecurity, emphasizing the necessity of an adaptable legal structure capable of handling the increasing impact of AI in the realm of cyber-crime and cyber-security. Collaboration among legislators, legal specialists, and technologists is of utmost importance to establish a legal framework that effectively reconciles the advantages of AI-powered cybersecurity measures with the imperative for comprehensive moral concerns, safeguards for confidentiality, and transparency protocols.

Keywords: Artificial Intelligence, Cyber-crimes, Cyber-Security, Laws

Introduction

Artificial Intelligence has introduced a constantly changing and unpredictable domain that has brought about a paradigm shift in both the arena of cyber-crimes and the discipline of security online. In the context of Pakistan, similar to other regions globally, artificial intelligence (AI) has arisen as a tool with both positive and negative implications. It is utilized not just by individuals and organizations aiming to safeguard digital information but also by people with bad intent who attack weaknesses for their gain.

Law and order situation play an essential role in the economic growth and peaceful living of people. Lawfulness is considered a necessary need for each growing community of the world. It is always challenging for governments to reduce the crime rate in the territory but there are various individuals and gigantic organizations that always become problematic for the governments and the community. Unfortunately, legislative bodies of the states mostly fall behind these criminal individuals and criminal organizations. Due to no laws and even in the presence of ineffective or non-implemented laws, criminal mafias prosper and attract the youth of the nations and the main talent of the nations becomes hostage in the hands of these criminal syndicates. Therefore, the states have to take the matter as soon as possible.

Research Methodology

To conduct an in-depth investigation of the legal regulations surrounding artificial intelligence (AI) in the context of cyber-crimes and cyber-security in Pakistan, the study will utilize a qualitative research approach. Initially, a comprehensive examination of prevailing legislations and regulatory frameworks about cyber-crimes and cyber-security must be undertaken, with particular emphasis on their applicability to actions associated with artificial intelligence (AI).

Research Objective

The objective of this article is to make attempt to learn how these criminal organizations use artificial intelligence and the legislative and executive bodies of the states can use artificial intelligence to counter crime. This research also focuses on the point of how the legal system of Pakistan can be improved by using artificial intelligence.

Significance of Study

The significance of comprehending the legal ramifications associated with artificial intelligence in the context of cyber-crimes and cyber-security cannot be overlooked. The significant potential for the utilization of artificial intelligence (AI) in criminal operations arises as a result of its rapid incorporation into many aspects of everyday existence. Hence, the primary objective of this research is to provide insight into the diverse applications of artificial intelligence (AI) in Pakistan, encompassing both unlawful and lawful activities. Moreover, this highlights the crucial requirement for legal

structures that possess the capability to effectively handle AI-related crimes, while also facilitating the utilization of AI to bolster cyber-security measures.

Artificial Intelligence- Overview

According to Encyclopedia Britannica,

> "Artificial intelligence (AI) is the capacity of machines or robots under computer oversight to carry out operations typically performed by intelligent entities. The term "AI" is commonly used to describe the endeavour of creating artificial intelligence algorithms that include human-like cognitive functions, like reasoning, meaning-finding, generalization, and experience-based learning."[1]

In the contemporary world, Artificial intelligence (AI) can engage in cognitive processes that are typically associated with human intelligence. These processes encompass several activities, including perception, logic, acquiring knowledge, interaction with the surroundings, resolving issues and the manifestation of creative abilities.

> "Artificial intelligence (AI) refers to the emulation of human cognitive activities through the utilization of technology, particularly machine learning. AI encompasses various particular uses such as trained systems, neural networks for the recognition of spoken words, and visual analysis."[2]

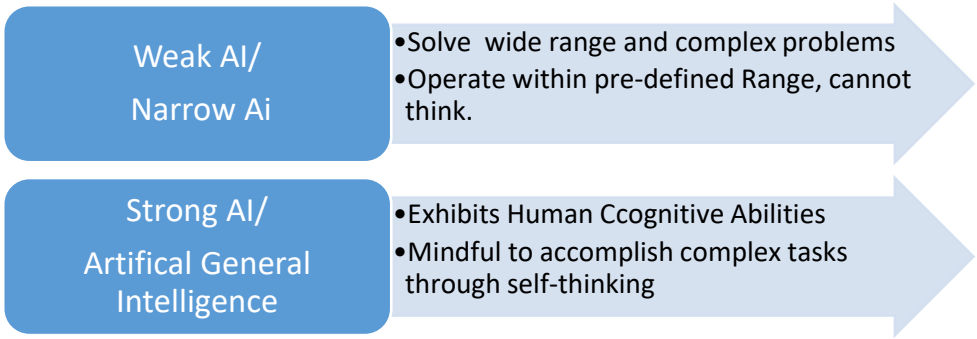
Artificial intelligence is used in businesses for process automation, fraud detection, handling customer complaints and suggestions, for creating firewalls for financial and other critical institutions. It can easily handle detailed and complex data, data patterns, and activity patterns for process automation and detection of crimes. It gives a quicker response than humans and in a more systematic way. Therefore, it is proven as more efficient and less time-consuming than humans. Artificial Intelligence can be sub-categorized into two categories:

a) Weak Artificial Intelligence

Week Artificial Intelligence is also called narrow Artificial Intelligence which is used to perform specific and repetitive tasks regularly week artificial intelligence systems are not in a position to do different and continuously changing tasks which require human judgement and the application of different knowledge and skills in various situations. [3]

b) Strong Artificial Intelligence

Strong artificial intelligence is also called artificial general intelligence which is specifically designed to perform different types of tasks and these systems are mostly able to handle complex data patterns, data analysis, and application of knowledge and skills in diverse and multifaceted situations. Strong artificial intelligence systems are designed to use fussy logic for dissimilar tasks where the application of human judgment is required.[4]



AI Scope and Prospects in Pakistan

Artificial intelligence (AI) is a significant technological advancement within the realm of digital transformation, playing a crucial role in facilitating company expansion. Based on recent research and industry surveys, it is projected that the adoption of AI will see an annual growth rate of 52% by the year 2025. This suggests that enterprises worldwide will rapidly embrace AI technology. Currently, various sectors, including national security, medical services, transportation, and training, are employing artificial intelligence (AI) in their operations. According to the World Economic Forum, the potential impact of robotics in poorer nations may lead to a significant reduction of approximately 66% in employment opportunities.[5] The potential consequences of this event for Pakistan's demographic and political stability are noteworthy. One additional aspect that could potentially exacerbate the adverse consequences of job displacement resulting from automated processes is the limited access to technical skills and educational opportunities in Pakistan. The impact of generated artificial intelligence (AI) on the employment landscape in Pakistan is expected to be intricate and multifaceted, contingent upon various factors such as particular businesses and labour classifications, as well as government rules and standards.

Artificial Intelligence for Crime

Criminals and criminal organizations use artificial intelligence for crime in various and new manners which are becoming very difficult for the state security agencies and the people. Mainly artificial intelligence is used in the following types of crimes:

1. Use of AI for Mimicry of voice for scam, kidnapping, extortion, defamation, security breach
2. Use of Artificial Intelligence in Cybercrimes
3. Use of Artificial Intelligence for Data Theft
4. Use of unmanned vehicles for terrorism
5. Destroying artificial intelligence-controlled systems i.e., traffic signals, public utilities
6. Artificial intelligence is a tool for the generation and publication of fake news.

7. Cyber attacks on financial institutions using artificial intelligence
8. Use of artificial intelligence for scam sales and frivolous reviews

Nowadays crime by use of voice mimicry is very common. In Arizona, a mother was called by a criminal who used the voice of her daughter using artificial intelligence and said "Mom, these bad men have me, help me, help me!". This sentence was in the voice of her daughter. Her mother verified and found her daughter safe in her house and it was just a scam call to extort ransom money amounting to $1 Million from the mother of a daughter who was 15 years of age by using artificial intelligence. [6]

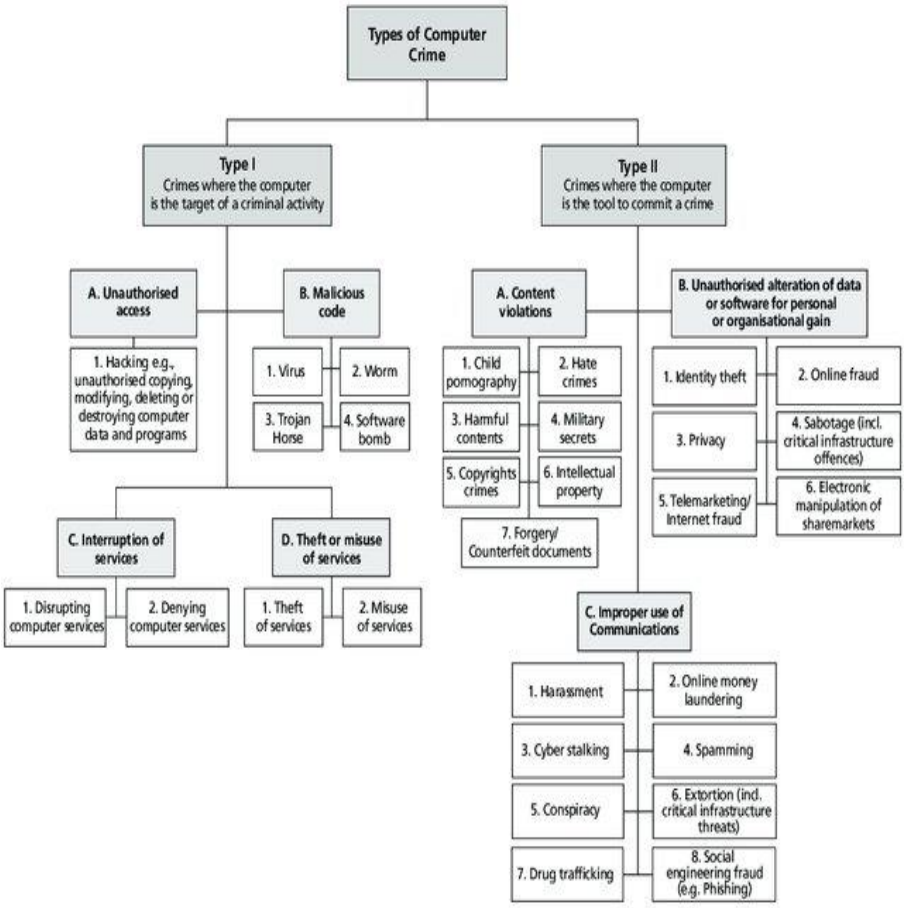
The advancement of AI has resulted in an increased level of sophistication and credence in telephone fraud. In contemporary times, fraudulent individuals are employing advanced technology to replicate and imitate sounds, encompassing those belonging to acquaintances and relatives. The concerning pattern is contributing to an increasing number of financial losses attributed to fraudulent activities. According to the Federal Trade Commission, the financial losses incurred by Americans due to fraudulent activities reached around $9 billion in the previous year, representing a significant surge of more than 150% within two years.[7]

Nowadays criminals also use voice impersonation for data extraction with illegal means and illegal use. They make calls to financial institution's accounts holders with the showing the same number of financial institutions and by having the same voice (Using artificial intelligence) to extract confidential data of the client i.e., atm details and then the amount in the account gets transfered to another fake account. Criminals also create fake calls by using the same voice of the person on any matter to defame him or her. Sometimes these types of crimes are committed by high-profile politicians to defame their opposite parties[8] and sometimes it is committed by professional criminal organizations to blackmail or to get some monetary benefits in some other ways. [9]

Some people also create fake news and use media especially social media for the proliferation of those news with their ulterior motives. Sometimes criminals try to use the voice of the high executives in calls to their juniors to transfer amounts to a specific bank account and sometimes they are successful in their attempt. Artificial intelligence is also used for security breaches in high-profile security areas where voice recognition or face scanning is used as a password for entry. This method is commonly used where unauthorized physical access is required for criminals to commit any illegal task. Chat GPT is another artificial intelligence tool which is most commonly used in intellectual dishonesty. It is used for article and thesis drafting, gathering information and techniques for committing various forms of crimes.

Using artificial intelligence, potential criminals create software which is circulated on social media with a single click on the link, they get the location and some other information of the potential victim and then a

survey-type form appears that collects much confidential information and then they call the same individual after the gap of some days. They use that same data in a call and ask for some further data in a tricky manner and then use it for their ulterior motives. Artificial intelligence also becomes helpful for hackers who breach the security walls of financial institutions to transfer funds from one account to another account. Unmanned vehicles are also a part of artificial intelligence and these are also used as a weapon for terrorism and spy activities. Some people also use artificial intelligence to disrupt traffic signal control systems just to disturb the flow of traffic. Some people do it for fun and do it as a part of a complete crime strategy. [10]



Use of Artificial Intelligence for Crime Control and Cyber-Security

Although artificial intelligence is new to crime investigating agencies in most of the world somehow it is being used in some areas of the world for crime surveillance, crime prevention and culprit identification. Artificial intelligence tools are considered very helpful in establishing, identifying and evaluating crime patterns and activities which otherwise go overlooked by

human surveillance. These tools are different and are used in different practical situations. Some tools have strong artificial intelligence but others have weak artificial intelligence. Tools which are used to detect and investigate social media crimes are different from the cyber-attacks on financial institutions. The main areas where artificial intelligence is being used for cyber security are as follows:

White-collar Crimes

The government agencies can establish an integrated and self-supported artificially intelligent system where this artificially intelligent system can have access to all records of the state departments, and financial institutions. This system can automatically identify abnormal patterns to identify the crime. For example, if an abnormally huge amount is deposited in any bank account, then the artificially intelligent system can, on its own, get its information and then a systematic process should be started automatically. That system should get the personal information of the account holder and then relate it to the record of NADRA to get information about the address and family chart of that specific person. Then the system must get the ID card number of that person and collect the data regarding his other properties. At the next step, the system should match these properties with the records of the federal Board of Revenue to identify whether he has declared his properties or not. Furthermore, the system should also evaluate whether the person has the proper source of income to justify that amount. All of these steps should be made by the artificially intelligent system at its motion and if any abnormality arises then the system should report this abnormality to the relevant persons in authority systematically.

CCTVs for facial recognition and identification of crime scene

Identification of missing persons is a main problem of this age. There are a huge number of incidents regarding this crime in any society. Identification of criminals and absconders. Artificially intelligent systems are more accurate and speedier than humans. Strong artificially intelligent systems are also capable of identifying a specific individual in crowded areas. Closed Circuit Cameras (CCTV) with facial recognition capacity can be installed in public areas for the identification of missing persons, criminals and absconders. These CCTV Cameras can be connected with artificially intelligent software which can be further connected with the record of NADRA. With the help of this, the full details of the culprit can be collected. If the government establishes an integrated system which connects the record of NADRA with the Board of Revenue and telecommunication companies then the police can easily use these CCTV cameras to identify the criminal, their family background, their home address, their list of properties with their locations and sims beings used under the names of criminals and their family members which can also be helpful to identify the

exact physical location of the criminal. Although, these types of cameras are normally used in security-sensitive areas but now this technology is not very expensive so its use has also increased in businesses and other public areas. The use of CCTVs can play a vital role in crime prevention and crime control. This can also help the crime investigating agencies in identifying the culprits and solving difficult cases.

These cameras can also be used to regulate the traffic flow. These cameras can also self-identify the accidents, nature of accidents, number of accidents in a particular time, and average speed of vehicles which can help the state agencies to identify the speed limits, and road repair requirements, and systematically identify the requirement of new roads or expansion of existing roads. These cameras can also be installed in drones as well. These CCTVs can be helpful in search and rescue operations.

Footages of these cameras can be used as images of crime scenes (maps) for courts to establish the guilt of wrongdoers.

Robots

Robots having strong software of artificial intelligence can be used in a very innovative manner. Robots can be used at places where human entry could be dangerous. Entering a place where culprits have hidden or the place where bombs have been installed and they need to be defused. These can help in providing safety to the officials of law enforcement agencies.

Social Media Analysis and Reporting

Nowadays, social media scams are increasing with speed. Defamation through social media using fake calls, fake information, fake pictures and videos is also very common. Incidents of business Scams are also increasing day by day. Artificial intelligence can be used to monitor and control an individual's behaviour. Artificial intelligence can also be used to monitor public behaviour to check the emotional temperature on any specific national issue to avoid any incident which may disturb the tranquillity of society.

Interconnection of different artificially intelligent systems

The state can ensure a system of artificial intelligence in which the sharing of different artificially intelligent systems is possible. The commercial sector should also be encouraged to install strong artificially intelligent systems to detect and prevent crimes in society. For example, departmental stores can use artificially intelligent systems to identify professional thieves. Artificially intelligent systems in the pharmaceutical sector can identify abnormal chemical buying which can help in identifying drug cartels, drug addicts, and chemical or medicine smugglers. artificially intelligent systems installed in shipping companies can also give a hit to the state about human trafficking.

Schools may install systems of license plate recognition to identify the suspicious movement of vehicles. They can also install a system of fascial

recognition to avoid any unauthorized movement to avoid any crime incident.

Therefore, the sharing of artificially intelligent systems installed by the state should coordinate with the privately owned artificially intelligent systems.

Predictive policing

Predictive policing is statistically evaluating the available data and then establishing patterns according to the data. This helps the police in identifying the major crimes which are going to be committed. It also helps to identify the key risky areas where these crimes are more likely to happen and against whom. This critical data analysis can also help identify the persons and organizations which are potential criminals. In this way, the resources can be allocated based on need and more appropriate allocation of resources could be made. This can be beneficial in maintaining a low or zero crime rate.[11]

PredPol- An Artificially Intelligent System in the US

There is a crime prevention software which is being used in New York named as PredPol.[12] This software is used to analyze crime data and patterns to determine when and where the crime is going to happen. It is used to determine who can be the possible victim and who can be the potential criminal. Based on the findings of this software, police department places their resources in various places. This total phenomenon is also called predictive policing. On the other hand, certain checks are been placed on these systems to ensure privacy and civil rights of the citizens.

"PredPol utilizes a limited set of three data indications, namely crime category, crime setting, and incident date/time, to generate its predictive models. The utilization of sensitive data is strictly avoided. Demographic, ethnic, economic and social data are strictly avoided throughout the utilization process. The implementation of this approach effectively mitigates the potential occurrence of privacy infringements or violations of civil rights that have been observed in alternative intelligence-driven law enforcement frameworks. The web interface on Google Maps presents predictions in the form of red boxes. Each square represents an area measuring 150 meters by 150 meters. The boxes depicted in the visual representation symbolize the regions with the utmost vulgarity, as well as during the associated work shifts, namely during the daytime sway, and evening shifts. Law enforcement personnel are directed to allocate approximately 10% of their shift duration to conducting patrols in the vicinity of PredPol boxes."[13]

A Proposed AI-driven Judicial System for Pakistan

The adoption of artificial intelligence in the judicial system of Pakistan can revolutionize the justice-providing capacity of Pakistan. As per international reports judicial system of Pakistan falls much behind, but it is now getting influenced by Artificial Intelligence.[14] It takes years and years to decide even

the simple cases. The credibility of decisions passed by the courts mostly comes under clouds at the political level and the individual level. Minor procedural changes in the laws cannot update this system. This system needs a major shift and artificial intelligence is the only option available for Pakistan. Pakistan has to establish a new judicial system starting from scratch in which artificial intelligence can play a vital role. The proposed judicial system for Pakistan using artificial intelligence is described below:

1. A portal should be established under the control and command of the honourable Supreme Court or High Court in which every citizen/person of Pakistan should have a right to create his account and log into it to file his or her case.
2. When a person creates an account on the portal then there should be a link where the petitioner can upload his petition.
3. After uploading the petition, the petitioner should have a link available on the portal to pay the court fees. The portal should allow the petitioner to submit his/her court fees online or he/she may have the option to upload the receipt of the court fee (deposited in the bank) on the portal.
4. After uploading of petition and paying of court fee, the staff available at the head office level (High Court or Supreme Court) should send the notices to the addresses of the respondents available in the petition. It should not be the duty of the petitioner.
5. The notices should show the details of the portal link on which the respondents or the advocates of respondents can upload their written replies.
6. The time to upload a written reply should be mentioned on the notices.
7. The Respondents should upload their written reply within time on the portal. After the passing of that time, the link to upload a written reply should be removed automatically.
8. After uploading of written reply, the charge sheet or issue framing should be framed by the artificially intelligent system in which all of the prevailing laws of Pakistan had already been programmed. This should not be framed by the judicial staff. This step will hardly take a few seconds or a maximum of minutes.
9. These issues or charges should be uploaded on the portal without any delay. So that the parties to the case may prepare themselves for the documentary and oral evidence.
10. After framing charges or issues, the parties should upload their documentary evidence on the portal without any delay.
11. After that, the stage of oral evidence comes. The honourable High Court or the honourable Supreme Court may allow the union councils or the police stations to arrange a room for the evidence recording and the parties to the case should go to the nearest police

station or union council office for online recording of evidence and the oral evidence should be recording using artificial intelligence and no human involvement should be made.

12. After the recording of evidence, the examination should be done online using artificial intelligence and should be ensured that no one can cheat during the cross-examination. This assurance could be made while using artificial intelligence not by involving any human being.
13. There should be a specified time for evidence recording.
14. Once the evidence stage of the case completes then the specific time should be given to the parties to upload their written arguments on the portal.
15. Just after the completion of the written arguments stage, the artificially intelligent system may draft the final judgement of the case using the prevailing statutory and case laws which could have already been programmed in the artificially intelligent system.
16. After the passing of judgment, the small causes cases should be finalized and in the case in which a huge amount is involved, the appeal should be directly referred to the High Court.

In this way, the artificial intelligent courts can be established which can decide the cases within the maximum time of one month and there will be no chances of human errors. This court system shall cater for the issues of lawyer's strikes, judicial officer's leaves, and travel problems for the parties. In this way, the whole lower cadre judicial system (Up to District and Session Court) can be converted to artificial intelligence. This can help in providing in time justice. This step can also cater the integrity and competency issues. This system shall be free from human errors and the ratio of superseding of the decision shall be reduced. These will be courts without human beings. These courts will not have any premises or staff. This method will also reduce the financial burden on the state because the salary and electricity budgets will be reduced and the less expensive but more effective judicial system will be introduced to the public.

Cyber Security Regulations in Pakistan

After 5G and 6G, the world has changed dramatically. Criminals and criminal organizations are using these technologies along with other artificial intelligence techniques to manage their criminal activities. By keeping in view, the Government of Pakistan is continuously trying to update the laws regarding cyber security but unfortunately, the state agencies are far behind as compared to the professional criminal syndicates. The Government of Pakistan has chronologically passed the following legislation.

1. Electronic Transactions Ordinance (ETO) 2002
2. Prevention of electronic crimes or cybercrimes ordinance 2007

3. Prevention of Electronic Crimes Act 2016
4. National Cyber–Security Policy 2021

1. Electronic Transactions Ordinance (ETO) 2002

This ordinance was passed in 2002 to ensure the security of electronic transactions. The area of operation of this ordinance is the whole of Pakistan. Certain acts have been declared as offences under this ordinance which are as follows:

1. Provision of false information, etc. by the subscriber.
2. Issue of false certificate, etc.
3. Violation of privacy of information
4. Damage to information system, etc.[15]

All of these offences were made non-bailable, compoundable and cognizable.

2. Prevention of Electronic Crimes or Cybercrimes Ordinance 2007

The area of operation of this ordinance is the whole of Pakistan. This ordinance was promulgated in 2007 for the prevention of electronic crimes and cybercrimes. The following acts were declared as offences under this ordinance:

1. **Criminal access**
   Individuals who deliberately obtain illicit access to an entire computer network or any portion thereof, regardless of whether safety precautions are violated, shall be subject to penalties including incarceration for a maximum period of two years, a monetary punishment of not more than three hundred million rupees, or each of them.
2. **Criminal data Access**
   Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.
3. **Data Damage**
   Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.
4. **System Damage**
   Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.
5. **Electronic Fraud**
   Whoever falls under this category of offence shall be punished with imprisonment of 7 years or with a fine or both.
6. **Electronic Forgery**
   Whoever falls under this category of offence shall be punished with imprisonment of 7 years or with a fine or both.
7. **Misuse of Electronic system or electronic device**

Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.

8. **Unauthorized access to codes**
   Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.
9. **Misuse of encryption**
   Whoever falls under this category of offence shall be punished with imprisonment of 5 years or with a fine or both.
10. **Malicious code**
    Whoever falls under this category of offence shall be punished with imprisonment of 5 years or with a fine or both.
11. **Cyberstalking**
    Whoever falls under this category of offence shall be punished with imprisonment of 7 years or with a fine not exceeding one hundred thousand Rupees or both.
12. **Spamming**
    Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.
13. **Spoofing**
    Whoever falls under this category of offence shall be punished with imprisonment of 3 years or with a fine or both.
14. **Unauthorized interception**
    Whoever falls under this category of offence shall be punished with imprisonment of 5 years or with a fine not exceeding five hundred thousand or both.
15. **Cyber Terrorism**
    Whoever falls under this category of offence shall be punished with imprisonment of 10 years or with a fine not less than ten million or both.
16. **Enhanced punishment for offences involving sensitive electronic systems**
    Whoever falls under this category of offence shall be punished with imprisonment of 10 years or with a fine not exceeding one million or both.[16]

3. Prevention of Electronic Crimes Act 2016

This Act was passed in 2016 and is applicable in the whole of Pakistan. The following activities are considered as offences under this law:

- Unauthorized access -the act of illicitly infiltrating computer systems or data without proper authorization.
- The act of duplicating or disseminating data without proper authorization.
- The act of affecting or inflicting damage to computer systems or data.

- Engaging in unauthorized activities to obtain access to critical computer systems or data.
- Engaging in unauthorized replication or dissemination of sensitive information.
- The act of disrupting or causing damage to critical computer systems or data.
- The act of endorsing or commemorating an illegal act.
- The utilization of digital methods for engaging in acts of terrorism.
- The proliferation of communications that propagate animosity or prejudice.
- Engagement in facilitating, financing, or orchestrating acts of terrorism.
- The fabrication of counterfeit digital files.
- Participating in internet scams or engaging in fraudulent activity.
- The act of producing, acquiring, or disseminating instruments intended for illicit purposes.
- Engaging in the unauthorized utilization of an individual's personal information.
- Unauthorized distribution of mobile-related items.
- The act of making unauthorized alterations to communication devices.
- Engaging in the unauthorized interception or surveillance of information.
- Engaging in behaviours that transgress an individual's dignity or esteem.
- Behaviours that infringe upon the dignity and privacy of individuals, particularly those who are underage.
- Engaging in the unauthorized possession or dissemination of pornographic photos involving underage individuals.
- The development and distribution of malicious software.
- Participating in continuous acts of harassment on the internet.
- The act of transmitting uninvited and frequently inappropriate information.
- Online impersonation - the act of assuming the identity of another individual on digital platforms, often to deceive others.[17]

4. National Cyber Security Policy 2021

The National Cyber Security Policy was finalized in 2021. In which it was discussed that there are already certain laws in Pakistan which are trying to regulate and control cybercrimes but they are not fulfilling the purpose properly as its enforcement is not up to the mark. Therefore, there is a need for new updated policies and enactments to ensure cyber security.

As it is stated in the policy, "The National Cyber Security Policy 2021 is subject to inclusive review every three years and as when required, depending on the emerging global cyber trends and technological advancements by the relevant organization in consultation with all stakeholders."[18]

Recommendation

- Ongoing Legal Education (CLE) is vital for guaranteeing that legal practitioners are equipped with the necessary knowledge and skills to effectively navigate the evolving landscape of artificial intelligence (AI) and its multifaceted ramifications for cybercrime and cyber defence.
- To provide adaptable legal structures capable of accommodating the swift advancements based on artificial intelligence cyber dangers and possibilities.
- Facilitate cooperative efforts among governmental entities, security agencies, and commercial technology corporations to exchange data and cultivate preemptive cybersecurity plans.
- It is imperative to consistently undertake comprehensive evaluations of prevailing laws and rules about cybercrime and cyber to ascertain their continued pertinence and efficacy.
- The significance of privacy safeguards in AI-driven cybersecurity solutions should be underscored, with careful consideration of striking a balance between ensuring safety and safeguarding human rights.
- Implementing Security Measures for Addressing Prejudice in Artificial Intelligence Algorithms Employed in Legal Proceedings, Including Risk Analysis and Making Choices.
- The establishment of transparency about artificial intelligence (AI) applications inside the legal system. The objective is to guarantee that the operations of algorithms are comprehensible and capable of being verified.
- To advocate for the ethical and responsible utilization of artificial intelligence (AI) within the realm of cybersecurity, while concurrently condemning any deployment of AI for illicit or detrimental intentions.
- To disseminate knowledge to the public at large on best practices for cybersecurity, their legal entitlements, and the potential hazards linked to AI-driven cyber assaults.
- Promote multilateral collaboration is crucial in effectively combating cross-border cybercrimes and achieving convergence of cyber rules on a worldwide scale

Conclusion

Nowadays, we are living in the age of artificial intelligence. These artificial intelligence tools are easily accessible to all individuals and organizations. Unfortunately, organizations are using these instruments to promote and glamourize their criminal activities but the state agencies are far behind as compared to the criminals and that is why security concerns have been increasing the recent past and this risk keeps on increasing at an astonishing rate. Some countries have started working on it and getting better results in crime control but still, they are not up to the mark. As far as Pakistan is concerned, we are far behind in this sector. Police departments working in Pakistan are not aware of artificial intelligence. Only a few individuals have a basic level of understanding. They are still using old and obsolete techniques in crime investigation. Our judicial system is not aware of artificial intelligence and this is one of the major reasons due to which our judicial system is not delivering justice to the general public. Laws are also not in line with the requirements. They need to be updated especially in the area of artificial intelligence. Therefore, the state has to increase awareness in society regarding artificial intelligence. Furthermore, the government should conduct training programs for police officials and officials of the judiciary. Legislation should also be updated by the legislative bodies to ensure that the crime rates in the country can be lowered. To optimize the utilization of artificial intelligence (AI) while mitigating the risk of its illicit application, legislators must confront moral issues and navigate the complexities of legal hurdles. The capacity of artificial intelligence (AI) to bring about great social results is substantial. However, it is imperative to ensure ethical growth, oversight, and continuous surveillanceto mitigate any possible adverse effects that may arise, particularly about humanity's monetary stability and sovereignty.

References

[1] Encyclopedia Britannica," November 8, 2023, https://www.britannica.com/technology/artificial-intelligence.

[2] "What Is Artificial Intelligence and How Does AI Work? TechTarget," accessed November 10, 2023, https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.

[3] "Strong AI and Weak AI - A Comprehensive Comparison - Tars Blog," accessed November 10, 2023, https://www.hellotars.com/blog/strong-ai-and-weak-ai-a-comprehensive-comparison/.

[4] "What Is Strong AI? | IBM," accessed November 10, 2023, https://www.ibm.com/topics/strong-ai.

[5] "Pakistan and Artificial Intelligence (AI)," The Nation, September 6, 2023, https://www.nation.com.pk/06-Sep-2023/pakistan-and-artificial-intelligence-ai.

[6] "Arizona Mom Who Fell Victim to Deepfake Kidnapping Scam Gives Gripping Testimony | Daily Mail Online," accessed November 10, 2023, https://www.dailymail.co.uk/news/article-12192741/Arizona-mom-fell-victim-deepfake-kidnapping-scam-gives-gripping-testimony.html.

[7] "Scammers Use AI to Mimic Voices of Loved Ones in Distress - CBS News," accessed November 10, 2023, https://www.cbsnews.com/news/scammers-ai-mimic-voices-loved-ones-in-distress/.
[8]"AI-Generated Image to Mislead People: Minister," DAWN.COM, 07:04:41+05:00, https://www.dawn.com/news/1754709.
[9] Aqdas Afzal, "Shackling Artificial Intelligence," DAWN.COM, 05:19:47+05:00, https://www.dawn.com/news/1777440.
[10] "Scams Are Ruining Pakistan's Digital Economy | WIRED UK," accessed November 10, 2023, https://www.wired.co.uk/article/pakistan-scams-digital-economy-gaming.
[11] Jibran Rasheed Khan et al., *PREDICTIVE POLICING: A Machine Learning Approach to Predict and Control Crimes in Metropolitan Cities*, 2019.
[12] "PredPol Mission | About Us | Aiming to Reduce Victimization Keep Communities Safer," *PredPol* (blog), accessed November 10, 2023, https://www.predpol.com/about/.
[13] "How PredPol Works | Predictive Policing," accessed November 10, 2023, https://www.predpol.com/how-predictive-policing-works/.
[14] "Pakistan Technology's Growing Influence On the Legal System," accessed November 10, 2023, https://www.scholarshipsads.com/buzz/technologys-growing-influence-in-pakistans-legal-system/.
[15] Electronic Transactions Ordinance (ETO) 2002, https://pakistancode.gov.pk/pdffiles/administratordbc98dd49f2df3b1d07bb986dcceb9a3.pdf
[16] Prevention of Electronic Crimes Ordinance, 2007, https://pklegal.org/pdf/Prevention-of-Electronic-Crimes-Ordinance-2007-(PECO2007).pdf
[17] Prevention of Electronic Crimes Act, 2016, https://na.gov.pk/uploads/documents/1470910659_707.pdf
[18] "National Cyber Security Policy" (Ministry of Information Technology and Telecommunication, Pakistan, 2021),https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf.