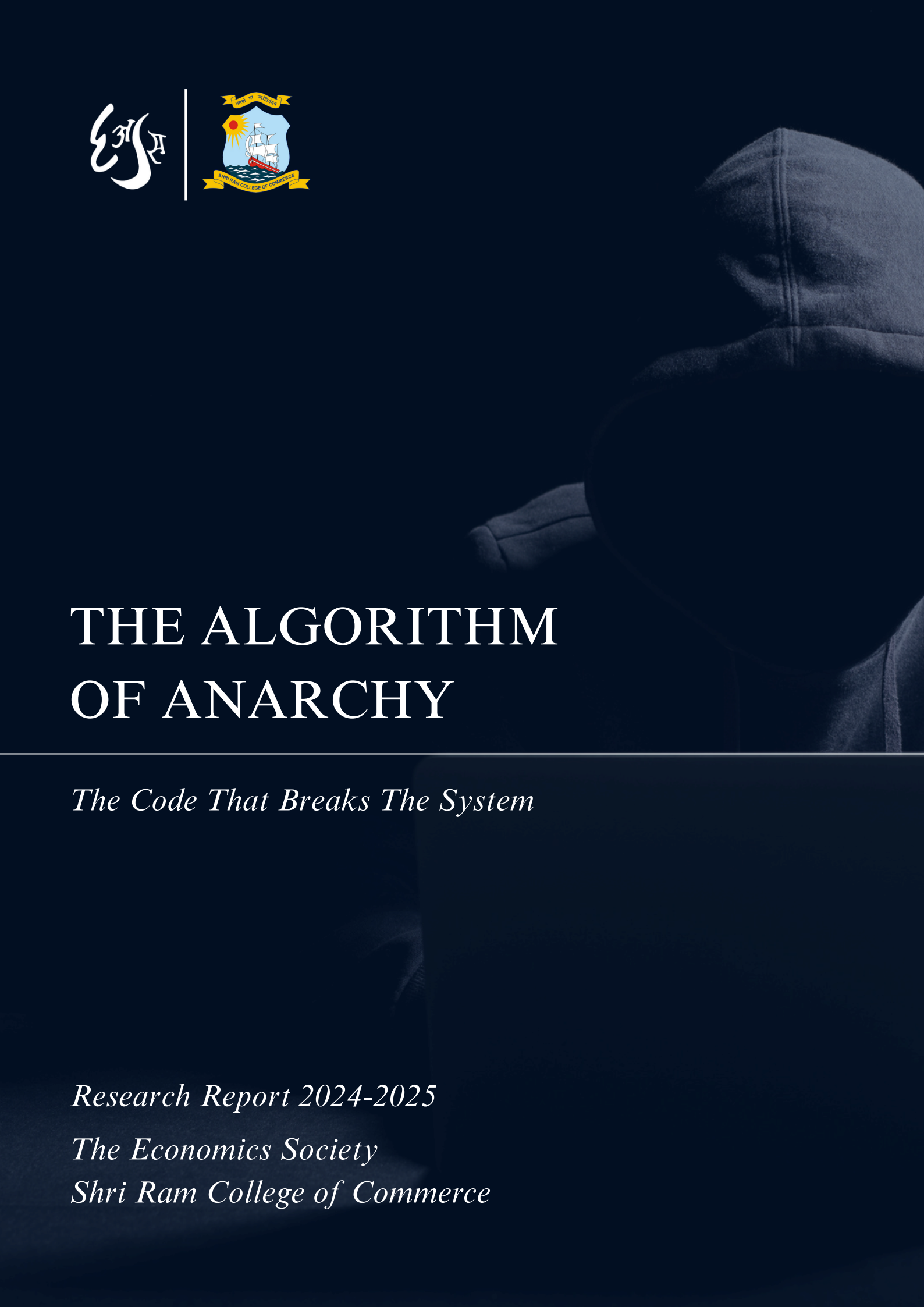


THE ALGORITHM OF ANARCHY

The Code That Breaks The System

Research Report 2024-2025

The Economics Society
Shri Ram College of Commerce

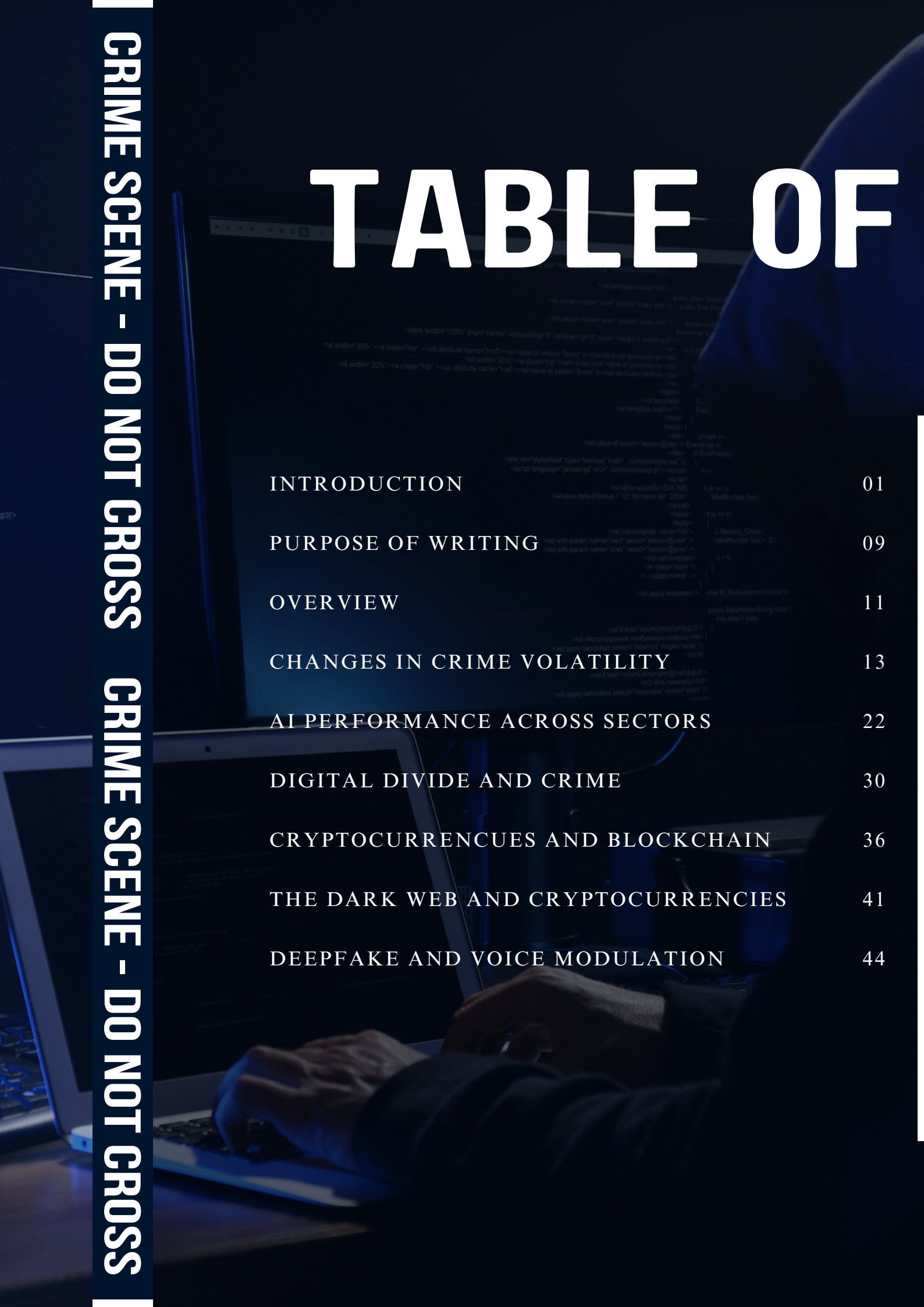


TABLE OF

CONTENTS

Introduction

Intelligence is often defined as the ability to process information and make decisions. Essentially, it refers to the ability to learn and solve problems. On the other hand, as defined by John McCarthy in 1955, Artificial Intelligence is "the science and engineering of making intelligent machines". What differentiates AI-driven machines from conventional machines and robots is AI's ability to mimic human intelligence. AI uses data from previous experiences and interactions to create a repository of intelligence, which it then uses to solve complex problems nearly autonomously.

It possesses the ability to adapt and change as per the needs of any given situation and can independently decide sequences of steps to achieve a goal without human involvement and micromanagement. Machine Learning is the part of AI that primarily focuses on studying how computer agents can improve their perception, problem-solving, thinking and actions by leveraging data. As such, AI possesses the remarkable ability to recognise patterns and use insights from a vast repository of knowledge to make decisions. The concept of AI was first developed by the British Turing in 1935. He described an "abstract computing machine consisting of a limitless memory and a scanner that moves back and forth through the memory, symbol by symbol, reading what it finds and writing further symbols." (Copeland) However, owing to a paucity of resources, the development of AI moved at a snail's pace in the first half of the 20th century.

The 1956 Dartmouth Summer Research Project on Artificial Intelligence, led by John McCarthy and Marvin Minsky, was a pivotal moment in the field's history. This conference marked the official start of research and discussion around creating machines capable of simulating human intelligence. It aimed to investigate the prospect of constructing computers capable of performing activities such as language use, abstraction formation, and problem-solving, effectively establishing a theoretical framework for AI research. 1966 marked the creation of the first chatbot, ELIZA, which successfully mimicked human speech patterns. Despite optimistic advancements in the 1960s, the 1970s witnessed funding cuts owing to slow and limited progress, which failed to meet expectations. As such, developments

in this decade were few and far between. The 1980s were remarkably turbulent, characterised by the creation of commercial expert systems and the resurgence of advancements in neural network systems on the one hand and recurrent funding cuts on the other. The year 1997 was highly significant because the then reigning world chess champion, Garry Kasparov, was defeated by IBM's Deep Blue in a chess game, indicating that artificial intelligence could surpass human abilities. The 2000s were marked by a revived interest in neural networks and natural language processing models. In 2014, Generative Adversarial Networks (GANs) made it possible to create content from AI, and Google's Attention Is All You Need (2017) introduced the transformer architecture, which allowed models such as BERT (2018) and GPT-3 (2020) to capture and generate contextually relevant outputs in natural language. 2022 marked the launch of Chat-GPT, propelling AI to the masses and revolutionising the modern world with its remarkable ability to converse, reason and perform tasks in an unprecedentedly advanced manner.

The improvement in technology, financial problems and the need to solve problems that traditional computers cannot handle have been the driving factors behind AI development. AI involves machines that can do tasks requiring human-like thinking, such as understanding, reasoning, solving problems, and making decisions. Automation is one of the big industries faster more efficient, and more

accurate. AI-driven automation has undoubtedly increased production in manufacturing by achieving higher levels of output. The system of automated quality control detects minor defects that humans cannot notice, thus preventing any losses. In finance, AI algorithms are used to monitor the stock market and execute trades, enabling fast decision-making and fraud detection. In healthcare, AI tools for diagnostics and robotic surgery help in the early identification of diseases and improve the accuracy of surgical procedures. AI's application across these sectors has opened new opportunities for growth and development, benefiting both industries and society.

AI aids in drug discovery by simulating molecular interactions, speeding up research and reducing costs. It also quickens scientific research in genetics, climate science, and space exploration. One of the significant advantages of AI is that it can process huge data, and it enables quick analysis and insightful information for decision-making in most industries. Marketers take the help of AI to study consumer behaviour, which helps in selling more things and keeps people

interested. You can find AI in everyday tools like Siri and Alexa and in services like Netflix and Spotify, which use it to suggest things you might like.

Moreover, social media companies rely on AI to determine what people view and even how people connect with these firms. AI also contributes to the solutions of major social problems. It can make education better by personalised learning, help improve disaster responses, and even help the environment with smart energy management. AI can help grow more crops in farming, cut down on waste, and support food security. It can be of great help in combating climate change.

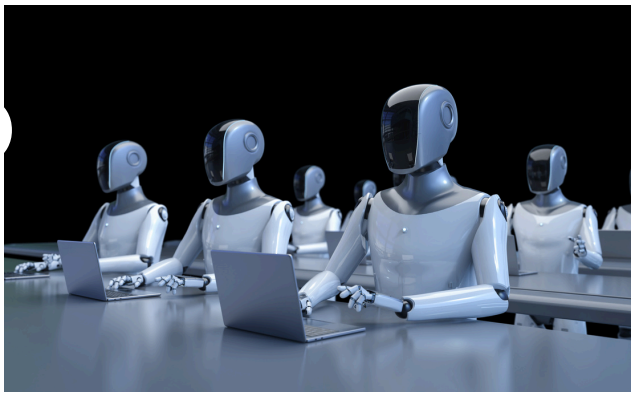
The changes brought about by the development of Artificial Intelligence will determine the future of humanity in most fields. The advent of generative AI has enhanced the potential and popularity of AI and is now considered one of the key drivers of technology. Business operations are witnessing a growing trend of automation because 55% of organisations currently use AI at various levels. The workforce believes that AI technology could automate about 30% of
their duties, which causes workers to worry that robots might take over human positions. AI creates different employment implications for each industrial sector. The automation process affects routine administrative tasks most intensely. But creating new positions requires skilled workers who specialise in machine learning and information security, as AI expands these fields. AI offers experienced and innovative workers a way to use technology as a work enhancement tool that does not substitute human labour. The workforce will sustain occupations which demand human imaginative skills coupled with emotional capability, along with sophisticated decision-making competencies.

The healthcare sector stands to benefit from AI through enhanced diagnostic capabilities and individualised treatments alongside remote monitoring systems for patients. Good implementation of AI safeguards against medication errors, while also delivering improved patient drug usage. AI systems are now enabling education institutions to deliver customised learning solutions that adapt to the different learning preferences of individual students. AI-powered platforms deliver personalised services for students achieving various academic results because they supply additional educational resources for students at all performance levels to reach improved learning achievements. Predictive threat analysis through AI has bolstered defence mechanisms by preventing cyberattacks so as to protect sensitive data in cybersecurity applications. The military sector employs AI to create autonomous weapons systems, AI-based robots and automated systems for defence operations.

Multiple ethical issues, together with social difficulties, emerge from AI innovations. Unethical use of AI technology results in a series of detrimental issues, which encompass

biased choices in decision-making along with transparency concerns, privacy risks and workforce termination. AI programmes have the tendency to strengthen discrimination and economic inequality through the use of biased data during training sessions. Accountability, together with fairness, emerges as an essential priority because of this situation. The increase in decision-making tasks handled by AI demands absolute transparency from the system. Established rules need to exist for businesses to maintain AI system responsibility while guaranteeing ethical AI applications. The extensive data management capabilities of AI create both security threats and privacy vulnerabilities. Impermissible data security measures allow personal information to be misused, which results in both legal and ethical implications.

The greatest fear among society regarding AI technology is its potential to displace human employment. Many workers face financial unpredictability because automation implements the replacement of various jobs across industries. The development of AI requires well-defined ethical rules which emphasise fairness and responsible conduct. AI becomes less trustworthy when there is a lack of proper rules and oversight, as it may intensify current social inequalities. The future of AI will hinge on finding a balance between innovation and ethical accountability. Through promoting transparency, guaranteeing fairness, and emphasising human-AI collaboration, society can leverage AI's potential to fuel progress



while minimising its risks. As we know, they have become commonplace in our daily lives. It can solve problems and figure out what went wrong or is wrong using organised or unorganised, structured or unstructured data. The pace at which AI is evolving and humans are increasingly intersecting with this rapid development is unmatched. To make these tools more relatable in terms of human behaviour and intelligence, artificial intelligence has tried to copy human traits and abilities and even trespass on humans. Emerged as a transformational technology. While we do debate its consequences, it is crucial to understand how its optimal use can augment human intelligence and not replace it. There is a perspective that with the increase in intelligence of AI, humans will evolve and become more resilient. It can make humans superhumans, by increasing productivity by 100x. Artificial intelligence excels at repetitive tasks, data analysis and pattern recognition at a speed and scale that humans may not match. For instance, in healthcare, algorithms can analyse medical imaging faster and with higher precision, but needless to say, the empathy judgement and communication skills of a professional in a medical field would still be irreplaceable.

Artificial intelligence cannot entirely replace doctors, but it can make doctors super productive by completing repetitive tasks in a limited time and with higher precision. The same is the case for lawyers. Lawyers as a profession cannot be replaced by artificial intelligence, but using it can enable them to perform several legal tasks, augmenting a lawyer. AI systems can automate mundane tasks. If humans do not give time to do the regular work, they are left with more time to engage in complex problem-solving and strategic thinking. A great example of this is the customer care that is automated for many big companies these days. Bots are simply increasing efficiency several times as they can deal with simple queries instantly, while human resources can be targeted towards more complex issues for an overall increase in customer satisfaction. They can be a mutually beneficial partnership between AI and humans. The aim should be "Augmented Intelligence" where AI improves decision-making skills and the time for creation, innovation and brainstorming just multiplies. Educational institutions, businesses, hospitals, etc., should aim at training the workforce for this change by promoting skills that complement artificial intelligence.

It is crucial to remember that the rule of AI is targeted to augment human capability and not to make them redundant. The strength should be harnessed for lifting humanity as a whole and faster, A Synergy that adds value to humans. This will open doors for unparalleled opportunities in various fields and help humans leverage their time and skills. The contemporary business and environment has become globalised with multifold increases in workforce and resources, along with increasing challenges ranging from operational efficiency to decision-making processes.

The most essential elements for businesses now have become adaptation to consumer demands, market trends, new technologies, and constantly coming up with ideas to beat the competition. Artificial intelligence is a buzzword that has eventually become an indispensable tool for organisations seeking solutions for these pressing issues. As a strategic ally, AI can offer tailored solutions for solving challenges across major industries. By leveraging machine learning algorithms, predictive analysis and advanced automation, businesses can utilise the strength of AI for their benefit to standard eye operations, and ensure effective utilisation of resources to gain insights into consumer behaviour and market trends. In the healthcare sector, AI is used for medical imaging, offering personalised treatment, EHR analysis, fraud detection, remote patient care and efficient medical documentation. Dynamic pricing optimisation, personalised shopping experience, inventory management and demand forecasting, visual search, etc, are some of the applications of artificial intelligence in the retail and e-commerce sector. Looking deeper into banking and financial services, artificial Intelligence can be extremely beneficial in fraud detection and

prevention, improving credit score and risk assessment, improving anti-money laundering compliance, streamlining regulatory compliance and assisting in advanced document processing. Even in unconventional industries like travel, AI can be the best innovator in terms of curating personalised itineraries, offering real-time updates and personalised recommendations to customers based on location and preferences, and providing consumer service through chatbots; a commonality for most travel companies, etc.

As highlighted already, it is clear how society has become increasingly dependent on AI and technology at large. Advancements in technology have made our lives easier in diverse domains like business and industry, finance and economics, and innovation and consumption. With technology comes the potential to improve lives, to evolve, but with this comes the risk of misuse. Technology has opened avenues for criminals to expand their criminal activities. Advanced technological tools have created new ways to commit a crime, even as they offer solutions for preventing and solving it. As new and highly advanced technology continues to be developed, it becomes imperative to strike a balance between utilising the same for societal welfare and addressing the negative consequences that arise with it.

The dual aspect of technology has altered the course of this world. Technology, initially developed to serve as a beacon for the progress of mankind, now serves as a weapon for criminals and a supposedly effective tool for law enforcement to nab criminals.

Criminals exploit technology like Artificial Intelligence to commit crimes. They cunningly create deepfakes with sharp precision to steal identity, to defame innocent civilians and thriving businesses. Such precision blurs the line between illusion and reality, making it difficult even for experts to differentiate between them. Meanwhile, some technologies are being used to navigate the dark web, making illicit transactions using cryptocurrency and blockchain. Similarly, such platforms expand illegal activities like drug trafficking, financial fraud, and illegal arms trading, with negligible chances of detection, making it easy to evade the law. Criminals with no knowledge of hacking can easily use AI tools like ChatGPT for writing support. Inexperienced writers can craft effective marketing messages that lure vulnerable victims by simply putting a prompt. This makes it even more difficult to differentiate genuine emails from phishing attacks. AI, thus, can be effectively used in terrorism, propaganda, sextortion, identity theft, online hate crimes, automated attacks, and cyberattacks.

Experts from Goldman Sachs have predicted AI will replace 300 million (30 Crores) full-time jobs globally. This directly impacts 18 per cent of the world's workforce adversely. Even white-collar professions now face an existential threat

due to the domination by Artificial Intelligence.

Henceforth, it is easy to say that deeper socioeconomic factors such as the digital divide in the Indian economy and unemployment play a pivotal role in determining criminal activities and intensifying crime rates. The digital divide refers to the gap between those who have access to advanced technology and those who lack access to even basic technology. The digital divide, mingled with illiteracy and resulting unemployment rates, pushes the vulnerable to resort to otherwise quick and yet risky ways to afford meals. Technology itself is a tool for economic desperation, fueling online scams, data theft, and cyber fraud. Such factors make it imperative to develop effective crime prevention strategies. Addressing the concerns mentioned requires leveraging technology to enhance security.

This leads us to the brighter side of AI and technology, which is its use in criminal justice systems. Smartphones that nearly everybody carries with them have made it easier to find pieces of evidence like photos, videos, and audio recordings, and that too in real-time. A digital record provides an accurate series of events, strengthening an alibi in legal cases. Moreover, advanced security systems like facial recognition and cameras with license plate recognition have reinforced law .enforcement. Such tools help identify suspects and detect criminal activity. Forensic science has taken leaps in progress due to advancements in technology. Technologies like DNA profiling, Dental Evidence, Bite Mark Analysis, and many more have revolutionised police investigations. Data analytics is another technology that comes in handy to keep a record of historical data on criminal activities, referring to which the police can use to predict potential criminal activity. This is essentially known as Predictive

Policing. Behavioural analysis is yet another technique used by law enforcement agencies to build profiles of suspects during criminal investigations. Criminal justice systems then saw the advent of virtual courtrooms and moot courts during the COVID-19 pandemic, when in-person communication seemed far-fetched. Virtual hearings reduced backlogs of cases and continued legal proceedings, making justice accessible effectively and efficiently to society

While perpetrators continue using advanced technological tools to commit crimes in the digital world, and law enforcement officers continue fighting the former using AI in criminal justice systems, new ethical and operational challenges emerge. A few of the same are data exploitation and the use of

autonomous technologies like drones and robotics. Technology allows us to collect information on nearly anything and everything existing in the world right now. However, with this power comes critical concerns regarding data privacy, mass surveillance and potential misuse of personal and confidential information. The line between security and surveillance continues to blur because of the dual nature of technology, raising ethical concerns about the use of such tools. In today's world, automated drones and robotic systems are being utilised to keep a check on security systems, crowd control, and even tactical operations. Technologies like this enhance efficiency, allow real-time monitoring of high-risk areas, and minimise human intervention in dangerous situations.

However, it is imperative to mention that the increased autonomy of such systems introduces risks. Algorithmic biases can always occur in decision-making while also raising concerns about excessive force and accountability. This evolving and highly advanced intersection of technology and crime raises critical questions for the future of mankind. How can technology protect and yet expose human lives? To what extent can one use AI to harm those around them? Do technologies like predictive policing and forensic and behavioural analyses help crime fighters catch criminals? Can law enforcement keep up with the cybercriminals operating across borders? What moral and legal implications arise from the use of AI and technology in criminal activities?

To answer these aforementioned questions and deeply analyse the effects of the same is the aim of this research report. The objective is to build a comprehensive report to shed light on the interconnectedness of technological advancements and the increasing trend of criminal activities while investigating the need for collaborations with technology to curb criminal offences and build advanced security systems. We aim to thoroughly analyse current law enforcement strategies and aim to provide a legal framework to effectively address evolving challenges concerning crime.

Purpose of Writing

Technology continues to mould the domains of modern life, and its influence has deeply rendered human life eerily convenient and vulnerable. Consequently, we find ourselves at the intersection of safety and threat, progress and vulnerability. Advancements in technology have caused us another threat: crime, too, has evolved. Now no longer in the shackles of physical spaces or orthodox methods, criminal activities have easily adapted to virtual environments. From mere identity thefts to decentralised frauds, from deepfakes to AI-generated voice scams, the nature of crime has evolved, in both form and sophistication.

This report emerges from the crucial need to understand this shift. It aims to comprehend how modern technology, coupled with malicious intent, is now becoming a tool for the disruption of societies and communities. If we delve deeper into the changing trends in crime, we would find how AI models, when deployed without proper audits, can amplify algorithm biases, manipulate crucial information, and blur the lines between illusion and reality. A deeper analysis finds that this misuse is not consistent. There is a widening gap, often called the digital divide, that determines the vulnerable and the offender. Communities that are often left excluded from technological advancements are exploited by those with easy access to digital literacy and cyber awareness. This report examines the connection between this digital divide and the growing exploitation of underserved populations. Additionally, it delved deeper into the rising domain of cryptocurrencies and blockchain. The domain, once called a financial revolution, is now criticised for enabling untraceable transactions often linked to fraud and scams. A similar concern is the usage of the dark web platform, a commonplace for illegal trade. The report examines the impact of the same, along with how voice modulation and deepfake technologies have emerged as potent weapons in the world of cybercrime.

It is also to be noted that technology is not just a threat; it is part of a promising solution. AI has been employed to predict crime patterns and aid forensic investigations through what is called predictive policing. To comprehend the dual role of AI, as a perpetrator and a protector, is the aim of this report,

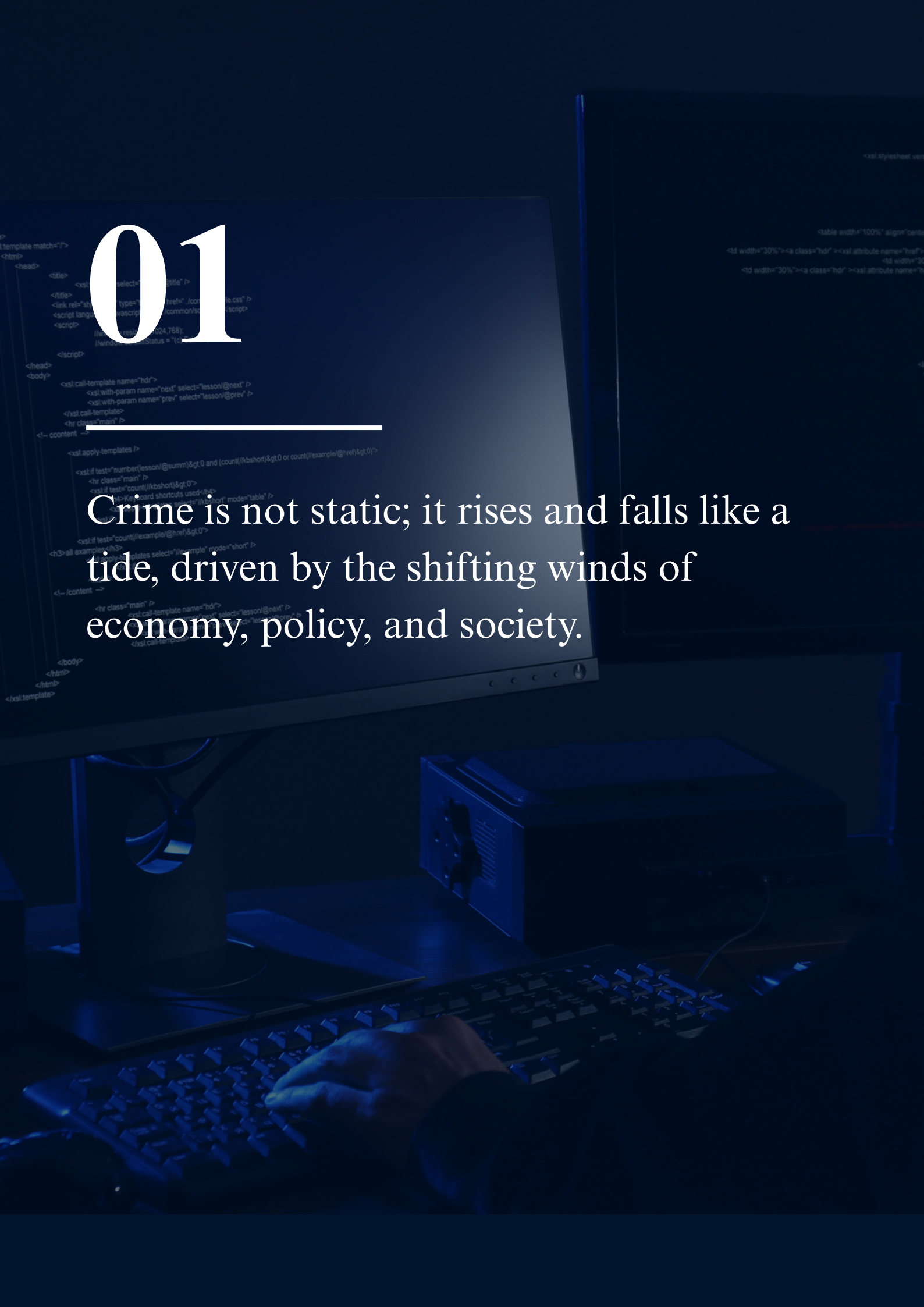
through which it strives to present a balanced picture of technological capabilities. It also recognises the concerns regarding factors like rising unemployment, especially in rapidly digitalising economies, shedding light on how they contribute to crime by pushing individuals towards an alternate but illegal means of livelihood. This report is a reflection on how societies can navigate this complex frontier. It asks what it means to be safe in a world where the same tools that unlock opportunity can unlock doors to manipulation and harm. By drawing attention to emerging threats and possible interventions, it seeks to inform policy, prompt ethical discourse, and encourage a proactive approach to tackling crime in a digital world.

Overview

The report provides an extensive study of how technological advancements create powerful connections with criminal activities. The analysis begins with tracking Artificial Intelligence (AI) development from its origins to present-day transformations, which affect healthcare along with finance, retail and criminal justice sectors. The advanced ability of AI to analyse massive datasets while spotting correlations and execute complex operations enables business expansion and creates significant moral and social concerns.

The research examines the transformation of criminal activities through artificial intelligence technologies by examining high-tech criminal practices which exploit deepfakes and cryptocurrencies, and blockchain networks, and the dark web. The study details the manner in which the digital gap and growing joblessness rates speed up criminal activities, specifically targeting vulnerable societal groups. AI demonstrates great utility as a predictive tool for policing and crime scene analysis, yet privacy issues and algorithmic prejudices and ethical duties persist as significant problems. The report presents a detailed analysis of actual technology

from two major cases: The DAO Hack from 2016 and Mother Of All Breaches (MOAB) in 2014. Strong cybersecurity defensive measures, regulatory frameworks, and regular auditing procedures must exist worldwide based on these two case studies. The report argues that while AI delivers unmatched value for enhancing social welfare and security, it needs fair management systems which protect ethical implementation and maintain visibility along with human-oriented innovation to protect trust within society.



01

Crime is not static; it rises and falls like a tide, driven by the shifting winds of economy, policy, and society.

Changes in Crime Volatility

Defining cyberspace is a precarious task because cyberspace has no real physical boundaries. In brief, cyberspace refers to a dynamic and virtual space that connects different computers together. It is a forum through which electronic devices in general, and computers, in particular, interact with each other. Cyberspace and the human brain share a similar structural complexity. Just as the brain contains numerous interconnected neurons, cyberspace comprises an extensive network of computer systems with intricate connections.

Jurisdiction the cyberspace thus becomes a difficult task. Since there are no clear parameters or boundaries, it is hard to frame and define sound legislation. Moreover, due to the expansive nature of cyberspace, penalising cybercrime becomes a challenging and recondite task. For instance, if a crime is committed by a group of criminals from different countries, it becomes arduous to decide penalties given that cybercrime laws vary from country to country. For instance, the Yahoo Data Breach of 2013-2014 involved U.S., Russia and others, wherein hackers stole data from 3 billion Yahoo accounts. A legal challenge that arose in this case

challenge that arouse in this case was when two Russian agents and two cybercriminals were charged. Extradition from Russia to the U.S. was denied which consequently stalled justice.

Cybercrime has been defined as any criminal activity that involves a computer, network or networked device. Artificial intelligence is the technology that gives machines the ability to copy or duplicate human activities or actions including both learning and problem solving. In the current age of big data, artificial intelligence actually plays a significant role. However, on the negative side, we can find scammers who have twisted the benefits of this tool for malicious activities. Scammers make use of personal information. They combine this information together will AI technology and even customers can text and mail

with AI technology and even customers can text and mail along with videos to make it more convincing and extremely difficult to detect its originality. They use data collected online to clone the voice of a child, an aged person, or other family members to convince the victim that someone known to them is involved in a crisis. There are various ways to recognise the general hallmarks of a scam. These demand immediate action and often try to convince the victim to keep the information secret. Personal information is involved to a large extent.

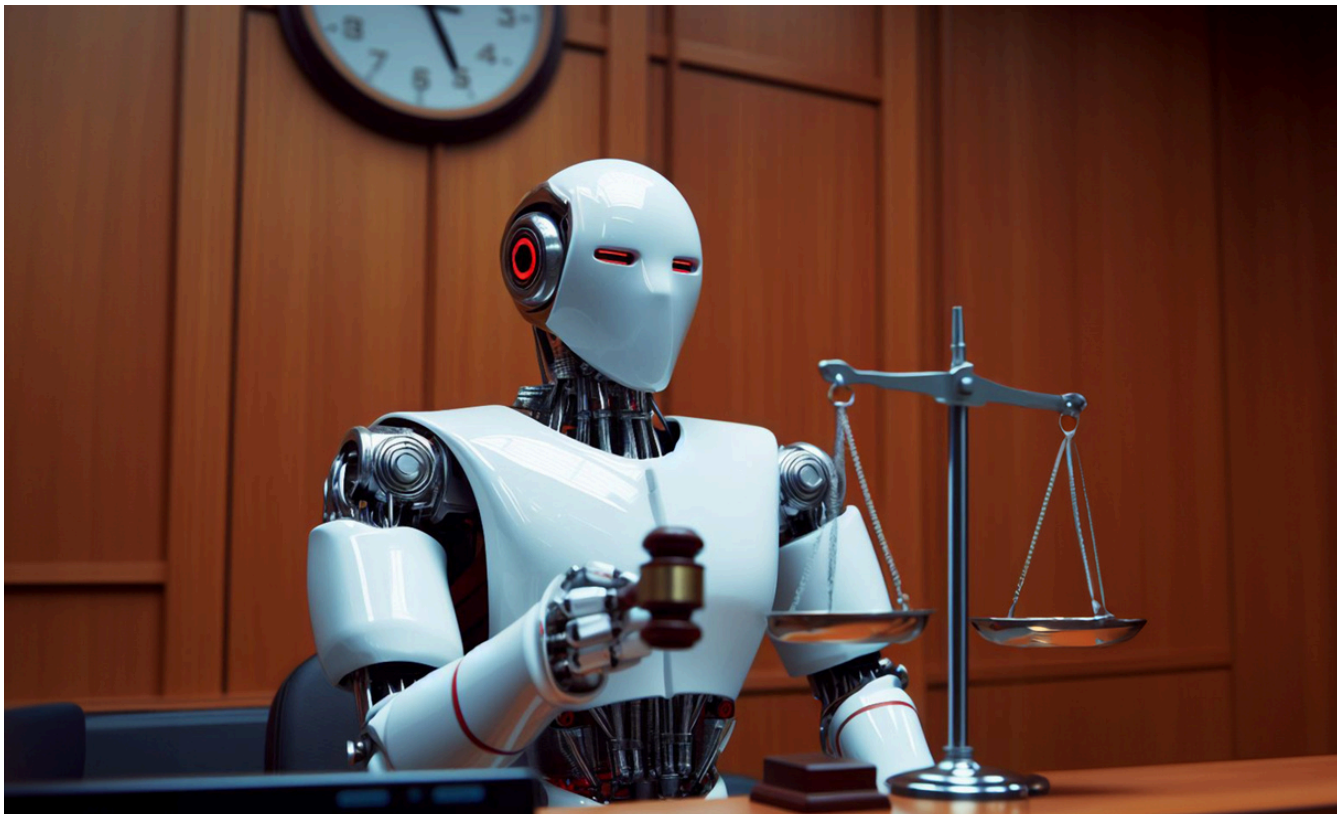
Moreover, monetary benefits are included in the form of cash, gift card, pay app or cryptocurrency. Sometimes it can be the other way round, where the party gives an offer that sounds too good to be true. Such indications show the scope of a potential scam. As cyber threats are becoming more sophisticated, the difficulty in recognising them is simultaneously increasing. Deepfakes have become commonplace place where fraudsters leverage the use of artificial intelligence to create audio and video and make them appear as real. These practices have been harmful for large organisations when employees are scammed in the name of senior authority members. Impersonations of bank employees by government officials are rising at a rapid pace. The fraudsters demand immediate payment or action to avoid the consequences. Extortion scams happen when an individual receives phone calls that sound like family members have succumbed to a serious problem, demanding help. According to a 2024 report by Cybersecurity Ventures, cybercrime costs the global economy USD 9.5 trillion per year. To make it easier to comprehend, if cybercrime were to be a country, it would have been the third-largest economy in the world, only third to the US and China. Such figures make one question just how vulnerable technology has made humans in the current scenario.

Decades ago, a bank robber would have required masks, weapons and a getaway vehicle. Today, they would need nothing more than a laptop and an internet connection. Indeed, crime has expanded into new domains with the assistance of technology. In its earliest forms, crime was a result of economic necessity, political conflict, and social inequities. It was regarded as a way to disrupt harmony in the society. Economic deprivation, coupled with feelings of helplessness, drove individuals to resort to otherwise quicker methods involving violent invasion, and often territorial disputes. Traditional crimes involved theft, assault and murder, and were typically straightforward. They resulted in visible harm to individuals and/or property, which made the perpetrators identifiable and their motives comprehensible within the socio-economic context. With the advent of digital technology in the late 20th century, crime underwent a major change. Cybercrime emerged as a distinct category, operating in the digital realm without any physical interaction. This introduced new vulnerabilities, making human lives more susceptible to potential

risks. Technology started becoming an integral part of our daily lives, while the government also began using it for financial transactions and record-keeping. Potential criminals saw this as an opportunity to exploit digital systems for illicit gains. Terms like phishing attacks, identity theft, malware attacks, corporate frauds, and many more became common, with the birth of the dark web, unlocking a hidden network of flourishing, illicit activities without the risk of detection. Today, cybercrime has emerged as a formalised category of criminal activity, with risks and harm involved greater than ever. With this ever-evolving and growing complexity of crime, law enforcement agencies find it difficult to tackle different forms of criminal behaviour. Understanding its types is crucial to grasping the scope of modern criminal activity.

White-collar crime, for instance, is nonviolent in nature and financially motivated. It can take the form of corporate fraud, tax evasion, money laundering, bribery and corruption. White-collar crime often involves schemes requiring financial, accounting or legal knowledge, which makes it difficult to detect and prosecute. The financial impact is also huge since it can easily affect economies at large. Corporate fraud, for instance, can lead to the collapse of a company, the loss of jobs or employees, and a direct impact on investors' trust. Henceforth, it is easy to say that this is most likely to be committed by those belonging to higher socio-economic classes. This is different from blue-collar crime, which is of the traditional kind. It is usually violent, but also includes non-violent crimes in some cases. These are generally easier to identify since they are more likely to be committed by those from lower economic classes in society. Examples include theft, burglary, assault, battery(a criminal offence involving unlawful physical activity), murder, homicide, and sexual offences. The method of execution is more straightforward, and the impact, being direct, is often immediate and localised. Another type of crime is cybercrime, which is any unlawful activity committed using computer technology and the Internet. It involves hacking, phishing, email scams, data and identity theft, and malware attacks. The perpetrator maintains anonymity, making identification difficult. It is also most likely to be committed by educated individuals since it requires technical knowledge. Cyberstalking is also considered a crime which includes threatening and/or frightening a person online, spreading fear and emotional distress. It involves constant monitoring or receiving unwanted messages from an unknown source. Intellectual property theft is also a form of cybercrime, referring to stealing copyrighted content or business secrets through the internet. This hurts individuals and companies both financially and competitively.

But an important question to address is, why does an individual commit a crime in the first place? What makes an individual



motivation, a necessary condition to commit a crime, is an internal driving force and differs from person to person. Criminal behaviour is the externalisation of criminal motivation, which may arise from the normal or abnormal needs of the perpetrator.

It is often a reflection of adverse social situations that the perpetrator might find themselves in. This leads us to a potential factor that creates potential criminals. Trauma, specifically childhood trauma, can be linked to violent tendencies. An unsupportive and un-nurturing environment during childhood might lead to a child feeling lonely and often undesirable. Violent childhood trauma involving physical harm to others often leads to copycat behaviour. Children learn by imitating the people around them. Henceforth, a violent environment often creates a violent person. Another factor can be personality disorders, which affect a person's ability to engage socially, leading to irrational behaviour which might seem normal to the perpetrator. Substance abuse and addiction are yet another factor that results in criminal behaviour. Drug abusers commit crimes to pay for their drugs, and this disrupts society. Additionally, such criminals are mostly under the influence of drugs while committing crimes. This also directly increases cases of drug trafficking.

Regardless of the situation, law enforcement agencies must build frameworks that address crime prevention. It is imperative to provide justice to the victims while also considering the perspective of the perpetrator, so that the root cause of the crime can be addressed. The world has undergone major transformations in criminal patterns because of technology in

criminal patterns because of technology, yet the effects differ between various geographic locations. Cybercrime rates have risen in developed countries such as the USA, UK, and Japan because these nations have extensive digital systems, yet they experience more incidents of ransomware attacks, as well as financial fraud and data breaches. The use of AI-driven policing as well as smart security systems has reduced the occurrence of burglary and vehicle theft despite rising new technology crime patterns. Traditional offences and new-age cyber threats coexist in developing countries such as India, Brazil and South Africa because both types of crimes affect these nations equally. Despite inadequate available security measures, the regions face escalating cyber dangers because of weak police defences. The regions with restricted internet connectivity across parts of Africa and Central Asia mainly experience traditional crimes involving human trafficking, armed robbery and smuggling activities. Digital fraud through mobile internet platforms has been rising alongside the expansion of mobile internet connectivity.

Modern technological hubs located in Silicon Valley, as well as Singapore and Seoul experience sophisticated digital risks which include corporate espionage alongside cryptocurrency scams and fraud activities. These cities draw hackers who use their know-how of modern technology to conduct financial as well as data-driven crimes. Technology serves destructive military purposes in conflict areas across Syria, Afghanistan and Ukraine, while also providing criminals with digital propaganda tools and cryptocurrency-based illegal funds. Criminal organisations operating in these areas use encryption together with dark web services to execute their illegal activities. The degree of crime volatility resulting from technological progress depends heavily on how digitised an area is, combined with its police force capabilities and economic standards. Developed countries face advanced cyber threats, yet developing nations must address both standard criminal activities and computer-based offences because they need different approaches to crime prevention.

Societies with high digital literacy and strong cybersecurity awareness, like developed nations, force criminals to advance their scams by creating deepfake fraud and enhanced phishing techniques because their targets remain watchful about cyber threats.

People living in regions with lower digital awareness levels serve as targets for criminal activity because criminals use their limited knowledge to employ social engineering scams and mobile fraud, together with fake investment opportunities. Crime volatility between nations becomes more volatile because of how cultural communities view their law enforcement agencies. Tunings toward police institutions determine crime prevention results: High levels of trust in authority lead to effective crime prevention, but low trust allows financial

scams and other cybercrimes to grow because of limited police cooperation.

Crime patterns rise and fall due to different social standings combined with economic distribution levels in society. The extensive economic gaps within societal structures redirect individuals with financial goals to cybercrime, which results in the expansion of hacking organisations and digital fraud operations. Cultural perspectives shape crime evolution because hacking as resistance receives non-criminal status in certain areas, resulting in hacktivism and political cyberattacks. Digital platforms, alongside social media websites, have resulted in modern crime categories including cyberbullying and misinformation spread and digital harassment but regional culture sets the sanctioning guidelines for these violations. Traditional social norms influence crime patterns by making attaining digital privacy and preventing moral policing offences more common in conservative regions yet financial identity fraud and online theft more prevalent in open societies. Different regions experience varying degrees of criminal activity because technological progress combines with local societal values along cultural standards.

Artificial intelligence (AI) has long been a subject of fascination in media and literature, often depicted as both a revolutionary force and a dangerous threat. The way artificial intelligence (AI) is shown in media and literature creates a mixed story, sometimes presenting AI as an incredible innovation and at other times as a potential danger. Media plays a major role in shaping how people understand AI, with news centres being the main source of information about its abilities and ethical concerns. Media often portrays AI in both a positive and a critical way, helping people see both its benefits and risks.

Ethics stands out as a major subject when the media talks about AI. People are worried about AI's decision-making process, its fairness, and the potential dangers it poses to society. News writers point out key problems like unfair algorithms, threats to privacy, and AI replacing human workers. Stories in the media paint AI as both a cutting-edge technology and a system that needs careful rules and watching. These conversations aren’t just academic debates; these talks shape how ordinary people view these powerful new tools that are quietly transforming our world, what rules the government generates, and how society reacts to new AI breakthroughs.

As advancements in AI continue to grow at a fast pace, the way the media talks about it will shape how people understand it and how governments make rules. Reporting about AI by news agencies' social media is realising that they need to give a fair and accurate view of AI. Instead of just talking about advancements in the AI landscapes, they also showcase how AI affects society, jobs, and ethics and present a more nuanced view to society. By giving clear

and fair information, the media can help people have better discussions about AI, leading to smarter rules and better ways to use AI in daily life. When the media explains AI with proper background, careful thinking, and different viewpoints, it helps people understand AI better, which can influence how it is developed, controlled, and used in real life.

In India, the legal framework for preventing and prosecuting AI-based crime is still in its infancy. The classification of crimes involving the use of AI in the country at present can be placed in debt under the previous laws on cyber crimes, data protection, and general criminal laws, but the current set of laws is de facto unsuitable for the prevention and prosecution of AI-based extreme crimes and fundamental rights violations. The Information Technology Act, 2000 (IT Act) is the leading legal instrument for cybercrime and digital offences, including provisions for hacking (Section 66), identity theft (Section 66-C), and privacy violation (Section 72). Yet, as this law was passed long before the implementation of the widespread use of AI, it cannot sufficiently reflect AI-related offences, such as deepfake fraud, AI-based cyber warfare, and the use of AI for decision-making. The IPC operates in partnership with the IT Act so that there are criminal sanctions that are granted for offences such as fraud (Section 420), a breach of trust (Section 409), and potential threats (Section 503). These types of laws can be used in a wide range of situations to deal with various offences involving AI,

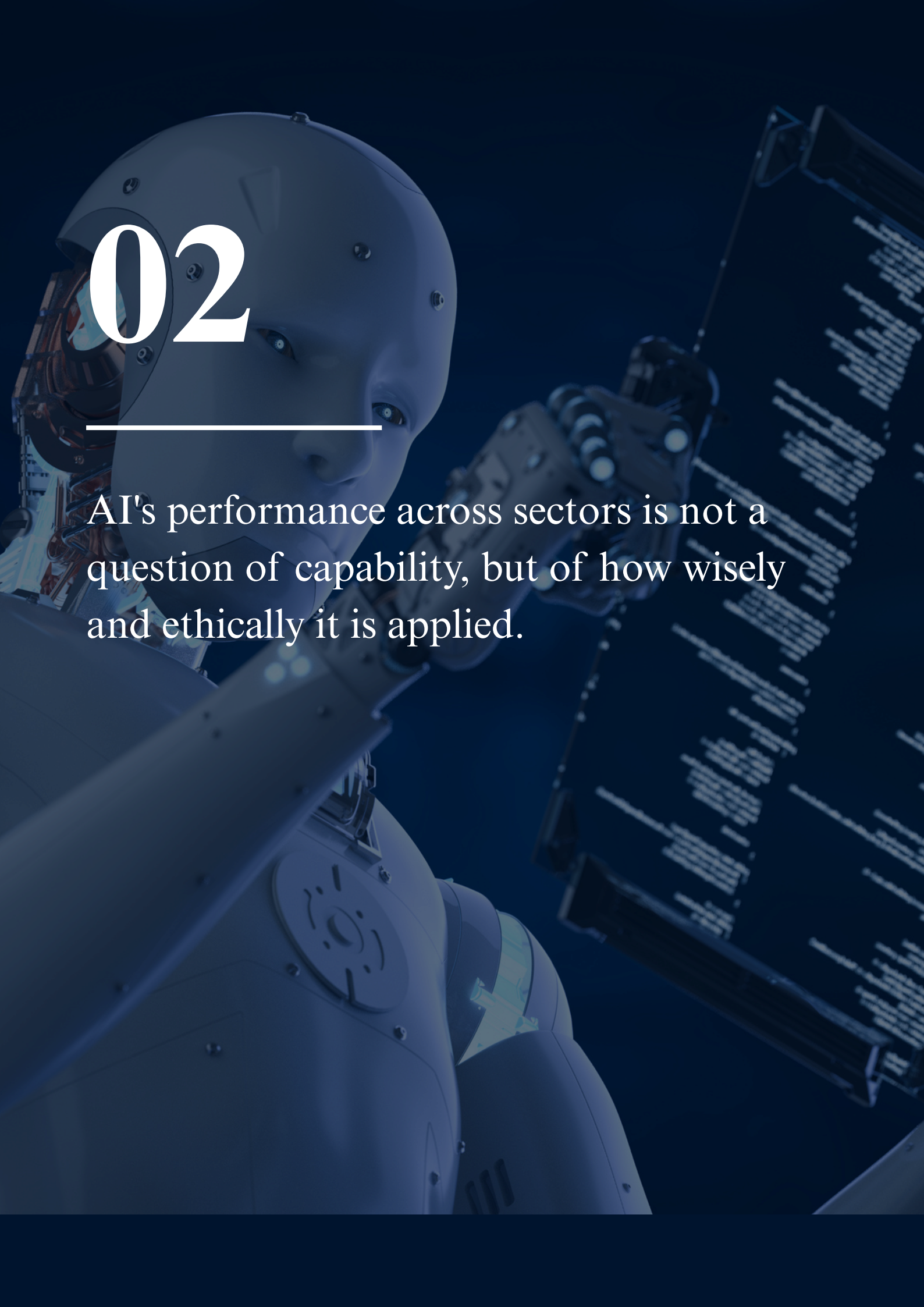
including the type of AI scams that may be run using AI and cases that involve using AI for impersonation purposes. Additionally, the Digital Personal Data Protection Act of 2023 has laid out the methods by which companies must obtain and use personal data from individuals. As AI is reliant on big data, this law guarantees companies comply with privacy legislation and face significant consequences for data abuse.

Recognising the growing influence of AI, the Government of India has introduced guidelines to regulate AI and Large Language Models (LLMS). In March 2024, the Ministry of Electronics and Information Technology (Meity) made it mandatory for AI platforms to get approval before launching high-risk AI models. This applies especially to models that lack transparency, spread misinformation, or could be misused for cybercrimes. These guidelines are designed to ensure that ML systems are accountable and cannot harm them.

In addition, India's National Cyber Security Policy sets out aspirations for digital infrastructure, thus indirectly

addressing the issue of AI cyberspace threats such as AI-enhanced phishing attacks and botnet-driven cybersecurity crimes. There is also an emerging draft of an AI and data governance framework, and this is seeking to establish ethical ML practices and prevent bias or manipulation in the automated decision-making process. However, this framework is yet to be legally binding, leaving many regulatory gaps.

Despite these measures, India's legal system is not fully equipped to handle the complexities of AI-related crimes. The lack of AI-specific legislation means that authorities often rely on outdated cyber laws that do not account for the sophistication, automation, and autonomy of AI-driven offences. For instance, the IT Act makes hacking illegal, but it does not cover AI-powered cyberattacks that can adapt and change to bypass security, making them harder to stop. There are also no clear laws for dealing with AI-generated fake news, deepfake videos, or unfair decision-making by AI. Another big challenge is that AI crimes often happen across multiple countries, making it difficult to punish offenders under India's laws. Additionally, police and courts do not have enough training to properly investigate and handle AI-related crimes, making enforcement even harder.



02

AI's performance across sectors is not a question of capability, but of how wisely and ethically it is applied.

AI Performance Across Sectors

Artificial Intelligence (AI) has significantly impacted the education space by expanding its scope from offline classrooms and assignments to a much more accessible, dynamic, interactive and personalised view. It has transformed education by making learning more engaging, personalised, and accessible. Platforms like YouTube, online meetings, and AI-driven online courses have altered the way students absorb knowledge, making education more engaging and efficient. Online teaching platforms like Coursera use adaptive learning algorithms to suggest difficulty levels and the right lessons to students, providing a customised learning experience. Such platforms also have chatbots that provide real-time AI-generated responses. Language and accessibility tools aid students and provide simplified language formats using text-to-speech and speech-to-text. AI systems can point out students' strengths, weaknesses, learning pace, and preferences to provide customised and more personalised lesson plans and resources. AI-driven chatbots and platforms like Zoom, Microsoft Teams, Google Meet, and many more offer a 24/7 immediate response to students by answering student queries and providing additional resources, making

virtual remote learning more efficient. Technological advancements such as video conferencing tools and AI chatbots, and virtual assistants now assist the students to connect with the teachers anytime from anywhere, enhancing the participation and engagement of students and ensuring that a student is entitled to the best quality education.

YouTube is becoming more and more important each passing day and it's one of the strongest education tools where students can enhance their personality and get quality education by learning new quality skills. Its comprehensive library of educational videos and resources serves to educate and inspire learners of all ages, offering subjects from science and mathematics to art and personal development. AI-based recommendation

systems suggest targeted videos based on individual interests, history and learning patterns. This self-motivated and visually engaging approach makes education more interactive, personalised and enjoyable, helping students grasp complex topics with ease. It has evolved as a knowledge hub providing access to free, high-quality content from reputed educators. Some apps like Duolingo, Quizlet and Brainly also utilise AI-based algorithms to create questions based on the past performance of the student. The discipline of STEM (Science, Technology, Engineering, and Mathematics) education is especially benefited by AI-based games and simulations that allow students to experience hands-on learning to develop analytical and problem-solving skills. For instance, Labster, a virtual lab simulation platform powered by AI, helps students perform experiments. These experiments range from physics, biology, and chemistry to engineering. It develops students' scientific reasoning and inquiry-based thinking without physical lab constraints.

AI has not only assisted the demand side of education, but also the supply side i.e. the teachers and administration, through automating administrative tasks, including grading, scheduling and report making. Conventional assessments need manual scoring, which is time-consuming and highly subjective. These AI-based automated assessment tools are reducing the time consumed in the grading of multiple-choice, short-answer, as well as essay-based questions, allowing teachers to focus more on instruction and student participation. AI helps teachers manage classrooms efficiently by keeping a record of student attendance, participation, and engagement levels. AI-powered tools can analyse student behaviour to find out the areas where students struggle the most, learning difficulties, and attention levels.

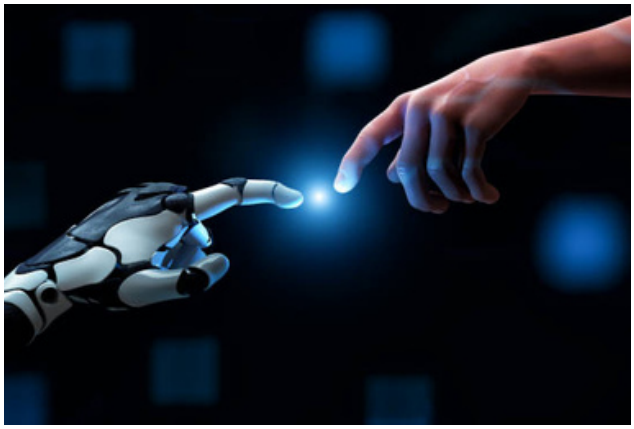
The future of AI in education is looking bright and offers plenty of scope. With the versatility of advanced virtual reality (VR) and augmented reality (AR), AI will bolster the learning process in the classroom, establishing immersive Academic shrines as students can experience subjects like history, science and space in a realistic 3D interactive environment. Technology and AI will fill in those educational gaps, and provide quality education even in most corners of the world, regardless of the location or financial background of an individual.

While AI continues enhancing the learning experience in the field of education, there are areas where it is contributing to a decline in the productivity and creativity of students as well. If one wishes to write an article on the OPEC crisis of 1973, they can refer to tools such as OpenAI ChatGPT, Clickup, Chatbots, etc., which can frame the article for them, according to their requirements. Alternatively, if one wishes to write the articles themselves but does not know what sources to refer to, such tools can help provide credible sources as well. Consequently, these tools have reduced the creativity of humans and led to a decline in productivity due to the ease in

working they provide, on the pretext of making tasks convenient for humans.

Additionally, it is increasingly being used in and revolutionising data analysis and law enforcement. Day by day, technology is reshaping crime prediction and prevention. It acts as a powerful tool in criminal investigations, by helping analyse social media activity and recognise faces, voices, and patterns that can be used to identify trends quickly. On the contrary, one important use of AI is that it can infiltrate the dark web and expose illicit activity. The dark web allows room for an unexposed, undetected network of illicit trading. It is mainly used to purchase illegal drugs, firearms, and stolen credentials, among many other things. Additionally, technology has made it easier to keep a record of past criminal activities. This can help identify patterns, predict crime, and identify potential suspects.

Similarly, AI algorithms can analyse historical data to identify geographical areas with high criminal activity. Using this information, law enforcement can allocate more resources to these "hotspots" by increasing patrols and surveillance. This is called Predictive Policing. Another way it can help is through social media. Social media can help detect language or common terminology used by criminals. For example, the Ponzi scheme refers to a fraudulent investment scam promising high returns. Technology can also detect phone numbers associated with criminal activities and track locations in real time. Moreover, AI benefits law enforcement in forensic analysis by making DNA analysis and testing possible. Biological pieces of evidence like blood, saliva, skin cells, fingerprints, semen, forensic odontology and many more are integral to solving criminal investigations. Technology has



made it post to detect and analyse decade-old DNA evidence to detect and analyse decade-old DNA evidence to generate critical leads for law enforcement.

AI continues to advance law enforcement systems by providing valuable insights into potential threats and risks, and its effectiveness is only enhanced when integrated with real-time surveillance technologies. One of these is advanced, AI-driven CCTV surveillance. It serves as an eye on the ground and helps maintain proactive security measures by detecting suspicious activities in real time. By leveraging machine learning and computer vision, these surveillance systems go beyond passive observation and actively identify risks, track individuals, and assist authorities in crime prevention and investigation. The basic function of CCTV surveillance is to observe public spaces in order to protect individuals from theft,

intrusion, fire, and any other possible risks. It is necessary for public places with heavy footfall and large campuses like airports and tourist hotspots. An enhanced tool coming into existence these days is an AI-enabled security camera, also known as an AI-smart camera, which is a step further from a non-AI surveillance camera. In addition to recording footage, it uses machine learning to analyse and interpret activity in a scene in real-time. Based on this analysis, it alerts video security operators to anomalies detected in a scene. Anomalies detected can be unusual motion, license plate recognition, or temperature fluctuations, among many more. This camera can also differentiate humans from animals and objects. Henceforth, it is more intelligent and accurate in detecting threats as compared to a standard CCTV camera. Using this highly advanced technology, organisations and individuals can better secure and safeguard their property and assets. They can enjoy vast benefits ranging from enhanced security to cost savings.

Facial recognition technology (FRT) has developed through its AI integration to make identification and verification processes highly effective. The system operates by scanning people's images after analysing their facial characteristics, followed by matching them against storage databases. The implementation of artificial intelligence-based algorithms in the existing facial identification practices of law enforcement since the 19th century has brought significant improvements to both accuracy levels and operational efficiency and scalability measures.

The main dilemma regarding FRT emerges from managing the tension between public protection and personal data privacy. Governments, together with private organisations, utilise facial recognition technology to improve security in airports and domestic law enforcement and prevent fraud but these security measures increase the probability of invasive surveillance practises alongside improper information gathering of individuals.

The main problem involves lineage of intent because it defines the intended use of facial data collection and whether this purpose remains confined to the original objectives. Facial recognition data creates ethical challenges due to the improper expansion of its collection range. The same facial recognition data acquired for parking lot entry may violate user trust when it gets sold to car dealerships for marketing use. Essentially, if your parking lot entry can easily recognise your face for security purposes, it can also be sent to car dealers to market their businesses to you. Users should have authorised secondary uses of their data, but did not consent thus contravening privacy principles and triggering worries about data ownership and consent.

AI-based facial recognition technology produces discrimination as well as biased results. Widespread research shows that particular algorithmsdisplay bias toward racial and gender groups which causes

these demographics to receive higher error rates in biological recognition processes. False identifications, along with wrongful accusations and unjust treatment, frequently occur due to biases that affect this system, especially when employed by law enforcement.

Data and analytics leaders must create comprehensive procedures regarding data collection, storage and usage to resolve the current ethical problems. Protected security measures should control facial recognition data while defending it from unauthorised exploitation. The system needs clear protocols that determine data utilisation to maintain security for privacy rights.

The benefits of AI-powered facial recognition technology need ethical guidelines along with responsible implementation to avoid misuse and maintain public faith.

AI fraud has become an infamous term. The bad use cases have tarnished the reputation of artificial intelligence and it has overshadowed the good applications of it as well. Fraud detection in AI refers to a range of machine learning technology that works by applying algorithms to a particular situation to make decisions or come to conclusions. The machine learning technology includes natural language processing models, captcha / reCaptcha and graph neural networks.

There is a proper mechanism through which AI detects fraud. The steps involve data collection, anomaly detection, continuous accuracy improvements, alerting and reporting. Data collection constitutes the core of fraud detection which enables businesses to set the normal range of data. Some of the data collected by AI platforms has sensitive information and also behavioural data. Under anomaly detection, a precedent for normal data is set up. AI models are used to flag "out of range" data in real time. There are various statistical algorithms to detect suspicious data. AI models are self-learning and thus have a lesser probability of making the same mistakes again and again. This helps to reduce the occurrence of false positives. In the stage of alerting and reporting, AI alerts humans in real time whenever fraudulent threats are suspected, such as blocking outgoing payments or removal of email attachments.

There is a range of benefits that can be garnered from AI fraud detection. Real-time detection and prevention wherein AI monitors transactions 24/7 and ensures that any discrepancy in any aspect is handled with immediate action. The immediacy of AI response provides businesses with a powerful tool to defend against fraud before it impacts their finances.

Scalability and cost reduction are the added benefits. It definitely helps to reduce costs by preventing fraud losses. Automation leads to resource optimisation and allows humans to focus on tasks that require human skill and

expertise. Over time, there is a huge cost saving which can be re-invested in other fields of work and operations. AI's capacity to analyse data with precision surpasses human capabilities, increasing accuracy multifold.

While AI fraud detection systems have sustainable benefits, they also come with their own set of challenges that include false positives and customer friction, evolving threats, and various regulatory compliance and ethical considerations. The realm of national security has undergone radical changes as a result of artificial intelligence's (AI) rise, impacting both the military and civilian sectors. The ability of AI technologies to quickly analyse large data sets enables improved intelligence collection and analysis, which can help with timely defence-related strategy making.

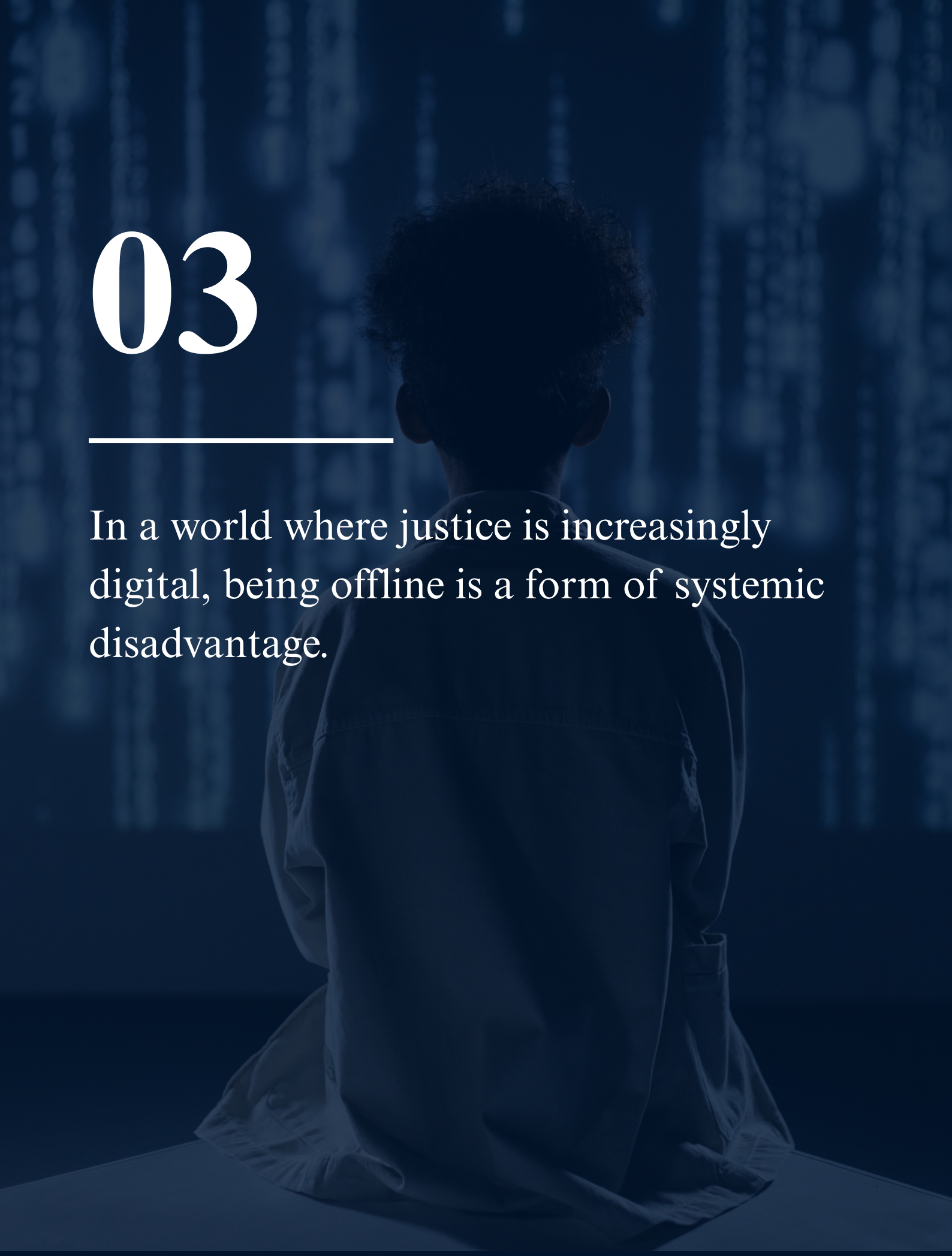
National security is primarily concerned with violent threats to a nation from external sources (such as other nations, international organisations, organised international crime groups, etc). Its scope is further expanded to include combating challenges that a nation may face internally, such as civil war, internal civil strife, large criminal groups, etc. The advent of lethal autonomous weapons and slaughterbots has fundamentally changed contemporary warfare. Artificial Intelligence (AI) is emerging as a transformative force as militaries globally race to integrate technology into their operations. In the present political climate, military strength is a key determinant of a country's global standing. Thus, countries are actively working to improve their military capabilities and expand their arsenals. AI's ability to process large amounts of data and provide actionable insights helps it improve operational efficiency by automating data processing.

Using AI technologies has become crucial for cybersecurity measures across a range of industries as cyber threats continue to grow in complexity and scale. The inception of artificial intelligence has presented both enormous opportunities and formidable obstacles. On the battlefield, unmanned aerial drone systems, autonomous armoured vehicles and robots, border surveillance, and lethal autonomous weapons systems have used generative and predictive artificial intelligence to streamline and revolutionise operations.

For command and control, AI fuses sensor data to create a common operating picture, enhancing coordination and helping bolster operational speed. Logistics and sustainment stand to benefit from enterprise AI applications streamlining processes, personnel

management, and equipment maintenance. Autonomous vehicles, incorporating AI for perception, navigation, and communication, can reduce risks to personnel by undertaking hazardous missions, though challenges remain in adapting commercial algorithms for military use.

AI's dual role in both combating and potentially facilitating financial crime poses many challenges. On one hand, AI tools can identify fake documents and impersonation attempts, thwarting criminals. On the other hand, malicious actors are using generative AI models to create more realistic fake invoices and records to facilitate money laundering. Financial criminals work across various platforms, such as cryptocurrency exchanges, stock exchanges, social media etc. As such, owing to the expansive nature of this domain, it is necessary to develop a vigilant and more safeguard to maintain the integrity of financial systems. Typical approaches to detecting financial crimes rely heavily on manual procedures and often fall short in the face of the rapid evolution of technology. This underscores the need for AI and ML applications that can perform real-time analyses of vast datasets to identify patterns indicative of unlawful behaviour. In India, financial crime has evolved to adapt to a complex ecosystem. For instance, a number of payment banks could face regulatory repercussions following the discovery by the Financial Intelligence Unit (FIU) that approximately 50,000 accounts lack proper Know Your Customer (KYC) verification. These accounts are suspected of being involved in suspicious transactions and potential money laundering activities.



03

In a world where justice is increasingly digital, being offline is a form of systemic disadvantage.

Digital Divide and Crime

Till now, we have seen how Artificial Intelligence (AI) and automation have a significant impact on industry output, the country's growth and development, improving public services and overall quality of life, especially in the growing stage of developing countries. However, despite their potential, AI widespread adoption and integration still pose a major challenge in front of countries' development. This has led to a digital divide between developing and developed countries, and this remains a major challenge in today's technology-driven world. Several reasons, such as a lack of advanced digital infrastructure, limited access to the internet, inadequate digital literacy, and a lack of trust, create a hindrance to AI adoption. This has created a gap in society for millions, particularly in education, employment, and access to essential services.

The digital divide refers to the gap between individuals, communities, and countries that have access to modern technology and digital infrastructure & literacy and those that do not. This divide can be calculated by considering several factors such as disparities in access to the internet, access to digital devices, digital literacy, and the ability to effectively utilise technology for education, employment, healthcare, and economic development. Developed countries such as Finland, Singapore and Estonia have made progress in reducing the access gap, while disparities in digital literacy and participation continue to grow, particularly among different socioeconomic groups. On the other hand, developing countries like India, Nigeria and Bangladesh are still not able to fully realise the potential of AI.

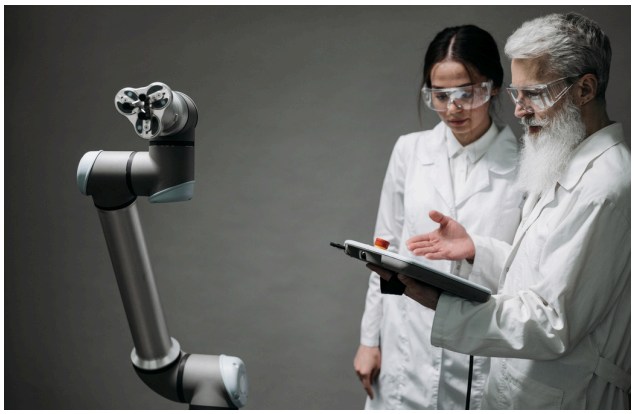
Internet accessibility is a great cause of concern for developing countries. The affordability of digital devices and stable networks creates hindrances for common people and professionals to benefit from online resources and increase their efficiency. Even if there is access to the internet and AI devices, digital literacy plays an important role in their adoption. Many individuals in developing countries lack the necessary skills to engage with AI-driven tools effectively, which creates misguided perceptions and stereotypes about the technology, such as AI is only for tech experts or AI is a Western concept not suited to local needs,
limiting their scope.

A common misconception prevalent in society is that AI will replace human jobs, which is just partially true. While AI will reduce the need for manual labour, it will create more demand for skill-based jobs, which necessitate the need for education and the development of one's personality. Social structures that prioritise traditional methods and hierarchies also slow down the acceptance of new technologies. As we discussed earlier, the lack of proper legal frameworks in India also discourages investment in AI technologies and raises concerns about misuse and privacy violations.

Developing countries must address the stated challenges in order to harness AI's full potential to create a more equitable, technology-driven future for all. Addressing these challenges requires a multi-faceted approach involving government policies, private sector investments, educational initiatives, raising awareness about AI's benefits to clear misguided conceptions, establishing clear legal frameworks, promoting inclusive digital development and huge investment in digital infrastructure. These play a crucial role in bridging the gap between developed and developing nations and pave the way for a bright and developed future.

People who recently started their journey into cyberspace or plan to do so within the near future constitute the most vulnerable segment of users. Internet access has yet to reach forty per cent of Earth's population. The introduction of Internet 3.0 and metaverse technology will exacerbate existing digital security inequities that affect these groups.

Within digitally advanced nations, vulnerable groups usually face greater digital threats since recent research shows San Francisco's lower-income residents who live in Silicon Valley's heart are more susceptible to cybercrime. People will face growing levels of anxiety because their data control diminishes and they face attacks combined with fraud, cyberbullying and stalking. People who feel a loss of control over their digital presence may abandon responsibility for protecting their electronic footprint since instant messenger applications with



privacy issues still rule the market. Despite greater adoption of 'reject all' functions on websites that aim to enhance personal data privacy, users' experience reduced capabilities when using such options. The functionality mentioned before represents only a fraction of the wider elements that comprise privacy concerns. Most websites contain tracking pixels together with third-party scripts that continue to serve as strong tools for monitoring digital activities. Cybercrime is any criminal activity that involves a computer or a

networked device. While more cybercrime is done with the motive of earning, some also carry it out to disable or damage devices. For a few, cybercrime is a means of spreading malware, illegal information, images or any other inappropriate information. Thus, cybercrime infects devices and attempts to steal sensitive data. The primary effect of Cybercrime is financial. The main reason for different types of criminal activities is mostly profit-driven, including ransomware attacks, any kind of email, internet broad or identity fraud. Most cybercriminals target individuals' personal information for theft or resale.

In order to control the rise in cybercrime cases, specific punishments are imposed under the India Penal Code, 1860 and the Information Technology Act 2000. Below are some of the Sections that identify the punishments imposed on an individual committing cybercrime.

Under The Indian Penal Code: Section 292: This Section deals with the sale of obscene materials either in the form of a book, paper, drawing, writing, pamphlet, painting, etc., or sexually explicit acts harming the surroundings. An individual or a group involved in such an offence is punished with imprisonment and a fine. On a first conviction, the punishment is imprisonment for two years and a Rs. 2000 fine, whereas on a second or subsequent conviction, the punishment is imprisonment for a term that may extend to five years and a Rs. 5,000 fine. Section 354C: It deals with the offence of voyeurism, where an individual watches, captures, or publicises the image of a woman engaged in a private Act without her consent. Under the provisions of this Section of the IPC, such an offender or criminal is punished with imprisonment of 1 to 3 years and 3 to 7 years for first-time and second-time offenders, respectively.

Section 354D: This section deals with stalking, both physical and cyberstalking. As per this Section, "Any man who follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman or monitors the use by a woman of the interest, email or any other form of electronic communication, commits the offence of stalking." An offender will be punished with imprisonment that may extend to three years for the first offender and five years for the second offender.

Section 379: If a person commits theft either electronically or physically, he or she will be punished under the provisions of this Section. It states that "whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years or with fine, or with both."

(Law, F. (2023, July 31). Free law. Free Law: Get Free Headnotes & Judgments)

It is now evident that cybercrime, being a low-cost offence, has a significant impact on individuals and organisations with weak, inadequate defences.

The easy accessibility of hacking tools and algorithms makes many vulnerable, which makes the defence weaker in comparison to the advanced skills of cyber criminals. The digital divide, coupled with the evident lack of technical knowledge among a considerable number of people, only exacerbates the issue. In 2024, the market share of Artificial Intelligence is 50 per cent, which further incentivises cybercriminals to invest in developing cost-effective tools to attack AI technologies (*IBM Security X-Force Threat Intelligence Index 2024*, n.d.). Furthermore, the index says there is a 71 per cent year-over-year increase in cyberattacks involving stolen credentials. Advanced hacking techniques, such as phishing scams and deepfakes, now easily outpace existing cybersecurity mechanisms.

Small businesses might face higher vulnerability due to insufficient investments in cybersecurity measures. Additionally, the financial cost of advanced cybersecurity limits access to fundamental defence mechanisms, which leaves people and organisations vulnerable to such attacks due to reliance on outdated measures. Mitigation remains challenging while cybersecurity measures are implemented. Technological advancements are rapidly taking on, which demands continuous updates and monitoring. Henceforth, organisations find it difficult to keep pace with this technological growth. Moreover, many internet users unknowingly engage in risky behaviours on social media, such as having weak passwords to devices, apps, and software, and clicking phishing links that might seem genuine to them. Addressing the aforementioned concerns is crucial and requires a multi-faceted approach. Potential solutions could be the implementation of government regulations and cybersecurity policies. There is an ever-increasing need for accessible cybersecurity education, especially among vulnerable age groups such as the youth and the elderly generations. Artificial Intelligence can also be used by law enforcement agencies to combat cybersecurity attacks, such as building proactive threat detection algorithms and tools.

Another potential factor that drives criminal activity is financial hardship. Negative economic growth results in financial crisis and unemployment, in some cases. While one may feel that situations get better gradually, those facing extreme economic hardships might want to resort to illicit activities to find immediate solutions for the same.

A report by the United Nations Office On Drugs and Crime explores the possible effects of economic distress on criminal activities and states that periods of financial instability see an increase in property crimes like burglary, robbery and shoplifting, similar to a report by the Australian Institute of Criminology reinstating the relationship between economic adversity and crime, thus solidifying the correlation. A World Bank 2023 report also indicates that such social

inequities push individuals toward organised crime since illicit activities are an alternative source of income for those who struggle to find legal employment. This can further establish how financial hardships disrupt communities. Economic crises allow crime to thrive, which is difficult to control, given the limited

resources of law enforcement agencies. A 2024 report by the OECD discusses how such situations weaken governance, reduce state capacity, and lead to increased corruption, which makes it harder for law enforcement to combat crime. Weakened governance paves the way for a sense of lawlessness, further encouraging individuals to engage in criminal activities without fear of detection. Along with their direct impact, financial hardships also lead to trust erosion in institutions. Individuals may perceive the legal system as ineffective, causing them to abide by legal norms. A 2022 report by Harvard Kennedy School discusses how financial hardship weakens social contracts between citizens and the state, leading to increased criminal activity and civil unrest. Such distrust might be particularly visible in societies with widening economic disparities. Marginalised groups, to date, face discrimination in employment, housing, education, and many other aspects. Such prolonged social inequities, thus, push them to perceive crime as the only way to financial security. A similar trend can be seen in younger generations, where they are often recruited by criminal organisations using false promises of economic prosperity in exchange for illegal activities.

All aforementioned factors, if left uncontrolled for a long time, might result in the absence of a social safety net in communities, leading to the normalisation of crime as a survival strategy. This further encourages the establishment of an underground market and extensive illicit trade. Consequently, social evils might emerge as a result. This strongly pushes the need for multi-faceted policy interventions.

04

Cryptocurrencies challenge the old rules of money, but blockchain rewrites the rules of trust.

Cryptocurrencies and Blockchain

Ever since they came into play, cryptocurrencies have taken the financial systems by storm due to decentralised and borderless exchanges. Now a part of mainstream financial transactions, they have made their way into becoming a tool for criminal activities. The major reason behind such situations is the anonymity the platforms offer, which allows room for orchestrating crime in the digital world. Recently, this has raised grave concerns regarding misuse in illicit trading, coupled with regulatory oversight.

Criminals use digital assets for money laundering, ransomware, darknet transactions, and other illicit activities. The Chainanalysis Crypto Crime Report 2024 states that, in the past year, illicit cryptocurrency transactions totalled USD 20 billion, which was significantly linked to scams, darknet markets, and sanctions evasions.

Money laundering has been found to be a major illicit activity performed using cryptocurrencies. Illicit funds are transformed into cryptocurrency, followed by “chain-hopping”. The term refers to the transfer of funds across different cryptocurrencies and blockchains to complicate tracking. Several transactions are also obscured by routing funds through multiple wallets or exchanges. After passing all potential security measures, these digital assets get converted into fiat currency through regulated exchanges or are immediately used to purchase assets like real estate or other luxury goods.

A number of methods are used to conduct illicit cryptocurrency transactions. The majority of these are darknet markets, wherein digital assets aid in the trading of illegal drugs, weapons, and stolen credentials. Ransomware attacks are also very common on these platforms, along with other kinds of cybercrimes.

Blockchain is a distributed database or ledger shared across a computer network's nodes. It is popular for its role in cryptocurrency systems, which ensures maintaining a secure and decentralised record of transactions. However, it is not limited to cryptocurrency uses. It helps to make the data immutable for any industry. Immutable refers to data that cannot be altered. Since it is not possible to alter a block, the crucial work begins and ends at a point where the program or

the user enters the data. The dependence on any third party, such as auditors, and other humans, leads to an increase in overall costs and also the probability of making errors.

In brief, it is a shared database that differs from a typical database, and the differentiating factor is the way in which it stores information. Various types of information can be stored on a blockchain, the most popular one being its use as a transaction ledger. In the case of a bitcoin, all the users collectively exercise control. The data is also irreversible, wherein it's permanently recorded and viewable to anyone. The uses of blockchain are as follows:

1. Payments: Blockchain allows crypto-assets to be transferred in a quick and secure manner. Its protocols can be automated and decentralised, thus enabling the creation of crypto-assets without the need for controlling, supervisory or centralised bodies.

2. Less fraud, financing of terrorism and money laundering: All transactions that occur on a blockchain leave a record. This means that this technology has the potential to reduce fraud, the financing of terrorism and money laundering, thanks to transaction traceability, provided that anonymity is prohibited. The first few years of blockchain technology did indeed see a number of crypto-assets used for illicit purposes, as the authorities were not yet using blockchain's traceability to pursue these crimes. Nowadays, only 0.15% of cryptocurrency transactions are used for illicit purposes, according to Chainalysis.

3. Data log: In data-intensive industries or processes, blockchain offers a comparative advantage over traditional databases. For example, foreign trade transactions require numerous documents to be processed and signed in a process so cumbersome that, oftentimes, a cargo shipment can arrive at its destination before all the relevant documents are in order, thus preventing the goods from being dispatched. Recording all documents in blockchain not only allows such documents to be signed electronically, but it also enables the perfect traceability of a large part of the processes involved in a company's foreign trade operations.

4. Intellectual property: Similar to the data log, blockchain's intellectual property log can easily and securely protect the authorship of original works. The latest developments in this regard revolve around NFTs – unique tokens that, when applied to art, can guarantee paid royalties. For example, nowadays, if an artist paints a picture, they only earn as much as the painting first sells for. The lack of traceability in subsequent

transactions stops the artist from profiting from any subsequent sales at a higher price. NFTs resolve this problem: NFTs can be treated as a unique digital copy of that painting, and, because this is recorded and transferred through a blockchain, you can find out the exact moment of sale and its price, so that the author of the work can benefit from the revaluation of their work.

5. Education: Recently, business schools, universities, and even certifying associations are issuing course certificates and education certificates through blockchain. This application prevents fraud in job candidates' CVs and can be verified quickly.

It creates a high threshold for getting into the investigations, with criminals turning mighty on the nature of crime in relation to core national interests. Such extremes become unreasonable in the assessment of detecting the crimes pointed out above by law. The nature of work in an online free-spirited world like Bitcoin makes it hard to create a milieu for law enforcers because quite a number of crimes are done at random, and victims have not been in the vicinity to finally report on crime. Therefore, lawfully wrongdoings are left hanging and without a solution from the police and standard procedures that would provide some fixation in their respective protocols for investigation and indivisibly deal with the severe consequences of such crimes. The transparency of the blockchain provides an opportunity for real-time tracking of illegal activities such as the movement of stolen assets and money laundering. For instance, one of the most widely known cryptocurrencies, Bitcoin, allows investigative authorities to trace the transactions made on the blockchain. Even if the original parties to the transactions remain anonymous, the investigators can go back to track and reveal the movement of funds. This can help the authorities bust big and complex criminal networks and trace their assets when they move across borders.

Blockchains are statutory-registered transactions in virtue of their permanence. Payments made via Bitcoin, critically, must hold the necessary conditions to become absolutely anonymous (henceforth to keep a secretive character). This ambivalence ensures both riskless ventures coupled with unwanted enterprises. Leveraging tools of accountability such as this tends to daunt criminals, the biggest misguided rebellions in the form of reckless men, thus or to generally requesting other more favoured forms of offences.

Blockchain provides total, secure transaction recording, safe closed connections without forced access endings, the anonymity of exchanges from the public, and inherent auditability without any need for intermediary involvement- an open book of free and authenticated transactions from end to end. An endorsement of criminal shielding is not a sin, as actions taken by police to block it require full knowledge to launch attacks. They have made impeders on how

such criminals delve into crime and describe in detail how hackers carry out cybercrime since they perceive themselves as experts in the field of crime. Because of its decentralised nature, the fact that blockchain is outside the framework of classic centralised systems makes it very remote for the government and financial institutions to control. This absence of oversight has brought about concerns about the use of blockchain to facilitate illicit purposes, such as the funding of terrorism or the theft of funds while transferring illicit funds.

The regulatory environment of cryptocurrencies and blockchain has changed. Regimes all over the world adopt divergent views concerning oversight. In certain jurisdictions, therefore, regulations have been proclaimed, making it necessary for companies and individuals involved in blockchain transactions to adhere to the Practical Anti-Money Laundering and Know Your Customer guidelines. For instance, the Fifth Anti-Money Laundering Directive was widely adopted to bring cryptocurrency exchanges and wallet service providers under strict surveillance.

However, enforcement continues to be a daunting task. The anonymity attached to virtual currencies and the decentralised network of blockchain enable the authorities to track the individuals engaged in unlawful actions across the network.

Blockchain is used for illicit purposes, probably overwhelmed under shady underground, sophisticated, multi-tier networks and makes investigations a challenge. Moreover, nation-states should act together internationally if there is to be any efficacious fight against cyber cross-border crime using blockchain technology. The way different jurisdictions regulate makes it easy for enforcement to go awry. Thus, a coordinated global framework for a uniform approach towards blockchain regulation ought to be in place so that criminals would not find an easy way or loophole to escape in today's world.

05

The same blockchain that empowers financial freedom can also fuel digital crime when ethics are absent.

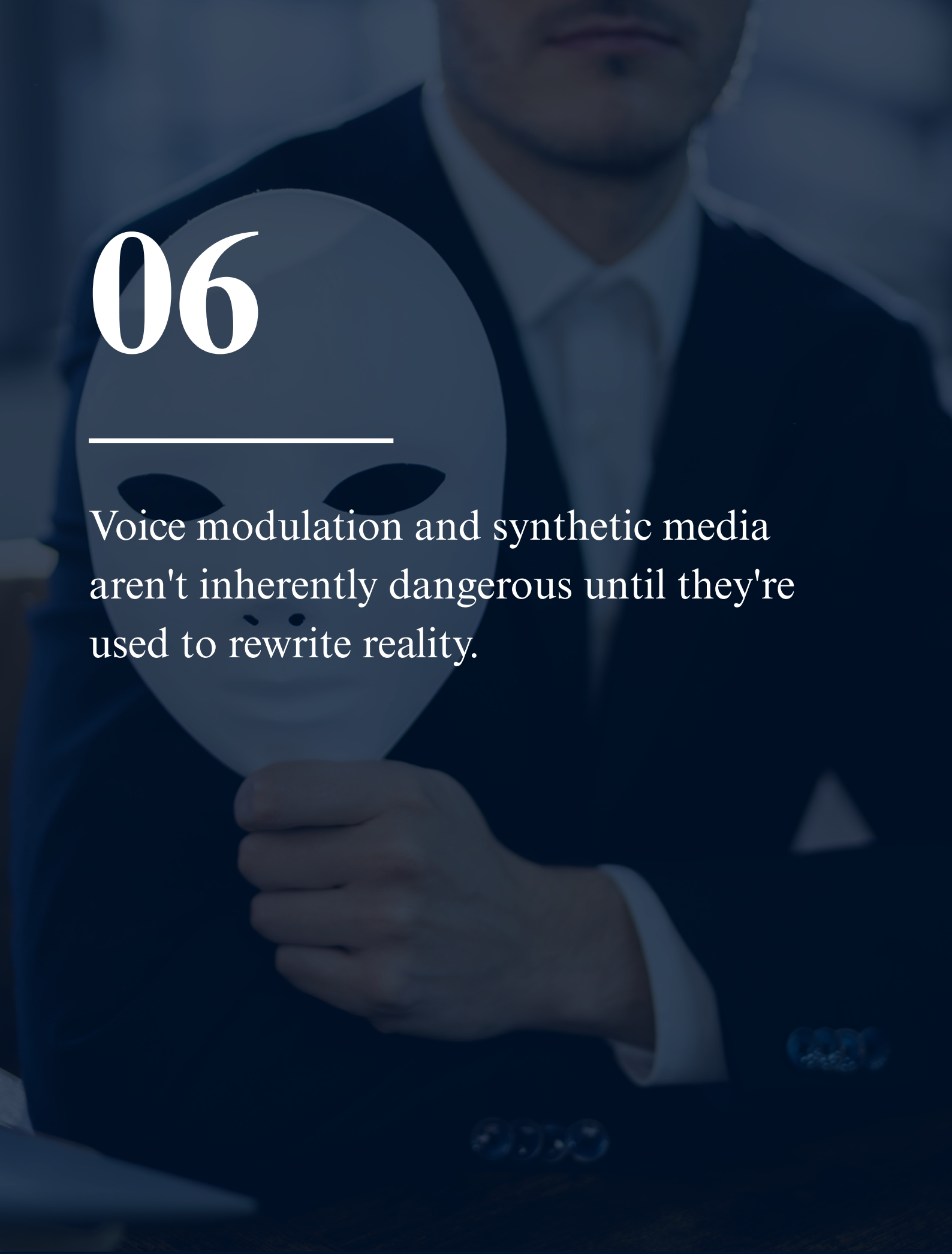
Dark Web and Cryptocurrencies

In today's era of digitalisation, data drives the building and functioning of a business empire. A huge amount of data is generated every single second, and this requires advanced systems to analyse, track, and secure information effectively. This has increased the utility of Artificial Intelligence (AI) in this domain, improving cybersecurity, regulatory compliance, and digital governance. AI-based systems and machines can provide effective solutions and can help in effective law enforcement by tracking illicit transactions on the dark web or monitoring financial transactions for fraud.

The dark web serves as a marketplace or favourable platform for illicit activities, including cybercrime, drug trafficking, human trafficking, and financial fraud. Our traditional law practices often struggle to track and destroy these hidden networks because of their advanced technologies, which make their identity anonymous and their operations encrypted. One of AI's primary advantages, as discussed earlier, was its exceptional capability to analyse large amounts of data in no time. By doing real-time monitoring, AI can identify keywords, sentiment patterns, and behaviour trends, which can help in finding suspicious patterns and illicit transactions in real time, enabling the security agencies to take a proactive approach, minimising damage and preventing breaches. Models like Natural Language Processing(NLP) and DarkBERT have been created specially to tackle dark web-based criminal activities effectively.

However, even though AI is useful and capable of this, there is still a challenge of disassembling dark web networks entirely. The criminals keep innovating their ways, employing advanced technologies for encryption and anonymity. This means AI-based systems need to be regularly developed over time, and regulatory frameworks need to be effectively enforced to address these offences. Nevertheless, AI still remains a leading

force in tracking and monitoring dark web-based crimes. A safer digital environment needs to be created in order to ensure rapid adoption and integration of AI. Adoption of end-to-end encryption is imperative for added security for sensitive data. To ensure robust ethical frameworks are adopted, AI ethics and principles could be developed on a global level that shall be followed by all countries. Additionally, to prevent algorithmic bias and discrimination, it is essential for organisations to mandate impact assessments of AI models before deployment. This will be a key to harnessing AI's full potential while ensuring the safety of AI users.



06

Voice modulation and synthetic media aren't inherently dangerous until they're used to rewrite reality.

Deepfake and Voice Modulation

AI and technology have very evidently penetrated almost every domain one can think of right now. The extremities of this technology can go to no bounds. One such example is voice modulation. AI can replicate anyone's voice with astonishing accuracy. It uses sophisticated algorithms and networks to analyse and mimic the speech patterns, tone and cadence of the targeted individual. An advanced application of voice modulation is deepfake technology. Deepfake often refers to a doctored video, made specially to deceive people, that uses AI and facial recognition technology. It then mimics the facial expressions and characteristics of one person and superimposes them on another person's body. Video alone is not the deepfake medium available out there. Today, voice and image cloning and biometric deepfakes also exist.

Criminals use deepfakes for a variety of frauds, ranging from phishing scams and impersonation attacks to synthetic identity theft. While these advanced technologies were earlier used for entertainment and educational purposes, lately, they are being used by criminals, fraudsters and political operatives for scams, frauds and even for spreading misinformation. AI is a double-edged sword, while on one hand, it has emerged as a revolutionary force and has reshaped industries and enhanced productivity. On the other hand, AI also takes a dark side along with it in the form of scams and fraud being done with the use of AI. We shall now understand precisely how this happens in scams, blackmail, identity theft and trust erosion.

Two days ahead of the 2023 elections in Slovakia, a fake audio clip went viral. In the video, Michal Šimečka, leader of the liberal Progressive Slovakia Party, was seen stating how he had been buying votes from the country's Roma minority to manipulate the elections. Such instances can easily erode the trust of society in powerful leaders, potentially disrupting communities and at times, entire nations.

A retired banker from Madurai city in Chennai, India, received a phone call in

November 2024, a phone call from his son begging him to help. According to reports, the thought of what might be happening to his son at the time seemed more terrifying than the ransom. However, the ransom demand of INR 5,000 seemed oddly low, making him stop panicking and check on his son. That was when he found out that his son was safe. Evidently, deepfakes of children have also been used for scam kidnappings. Fraudsters replicate the voices of family members and close relations to make hoax calls asking for money. A similar technology is synthetic media generation, which creates entirely artificial content that never existed in reality.

Misuse of this deepfake technology has been very destructive and has given rise to new cyber threats. Financial fraud and identity theft are some common examples of cyber threats. Video deepfakes and AI-generated voices are used to disguise themselves as financial executives or trusted colleagues for the purpose of taking sensitive information or manipulating people to transfer funds to unauthorised accounts.

In recent times, authorities have discovered that deepfakes are being used to disguise persons from government agencies like the CBI, ED or even income tax departments to do extortion. These crimes are particularly difficult to detect as victims often respond emotionally and do not report these crimes because of bureaucratic risks. Apart from these, deepfakes are also used for political manipulation and for spreading disinformation. Fabricated content is being made to spread any form of disinformation, like making inflammatory statements, endorsing false policies, or engaging in unethical behaviour. In the era of social media, these controversies are spread rapidly, influencing public opinion and election outcomes, provoking violence or even destabilising current governments. This threat becomes more grave during election times, which can have long-term consequences on the country's growth and development.

The accuracy of these AI-driven tools to clone voices and manipulate videos makes it increasingly difficult to draw the line between fabricated content and reality. This has serious implications, as such tools can help criminals access sensitive information, extort victims, and spread misinformation. Deepfakes are hard to combat, especially if people rely on only one method, either humans themselves or software, to do it. Neither of the two is fail-safe. The most effective way would be a layered approach, combining human judgment with a biometric platform. Poorly done or overly simplistic deepfakes can easily be detected by the naked eye. Deepfakes often display inconsistent facial features. This is because AI struggles to replicate minute facial expressions, eye movements, and how facial features interact. Elements creating deepfakes also show unnatural lighting and shadows. Visual analysis can thus undercover shadows that are inconsistent with the light source or reflections that may not

align correctly. Some detection tools can spot more faulty characteristics. However, AI can generate highly accurate and better deepfakes all the time, which leads to relying on deepfake detectors to flag them.

A multi-factor authentication might help as well. Adding facial, voice or other biometrics in recognition makes it difficult for a scammer to orchestrate fraud even if they manage to impersonate a voice or face. Therefore, AI-generated deepfakes pose a serious digital threat to mankind. As technology continues to advance, the line between real and fake content will blur further, making its detection and regulation more difficult.

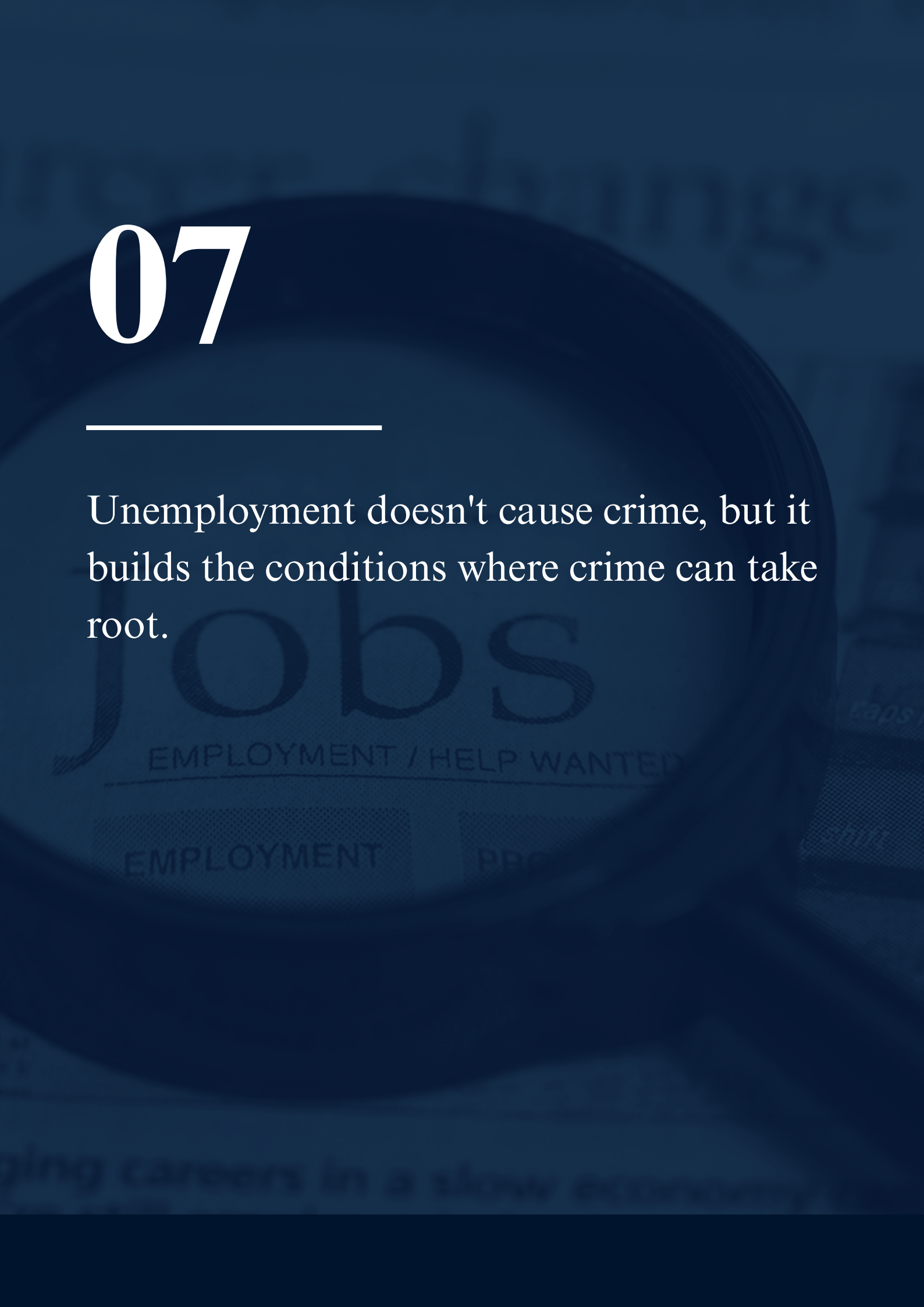
The rise of new technology has seen new forms of crime arise, and with increasing sophistication in content creation tools, the demarcation line between legitimate creative and illegal acts will become increasingly blurred. With deepfake tools, AI-driven content generation, and automated engagement algorithms revolutionising the entire creative and consumptive paradigm, serious ethical questions are ushered in, foremost amongst them being that of content control. AI-driven content creation tools offer never-before-seen levels of creative potential, but they also raise great challenges in regulating harmful content. Take, for instance, deepfakes: there exists a whole realm of potentially criminal usage for political misinformation, the spread of disinformation, and the unethical destruction of reputations. That said, there are also serious questions about the degree to which one of those can be allowed to impinge upon freedom of expression. Balancing the need to protect people from harm with the prevention of state intrusion, the necessity of any new laws speaks to the fine point needing to be made: new laws should not act as a brake to innovation or free expression.

Moreover, the devolution of content production tools toward arts and genres involves massive amounts of data usage to regulate activities. In fact, that very massive amount. In fact, many AI platforms generate more content, as is often the case in real-time, than any reviewing or regulatory body might realistically monitor. For this reason, existing standards must evolve to a point where using specified checks, not only will their utility in service of equity be sought, but creators' rights too, thus enabling the broader public to partake in the benefits from these technologies rather than their opportunistic exploitation.

The implications of advancing AI technology in assisting with investigations of crime are many: While AI tools may occasionally play a role in the discovery of offenders online based on digital

footprinting, individual person becomes burdened with proving one's innocence since content becomes more easily manipulated and, thus, more difficult to trace back to its original creator. Individual persons, thus, now more than ever, are burdened with demonstrating that they were not involved in creating and spreading harmful content, such as imitation likenesses and voices. Second, while AI can provide beneficial applications for detecting crimes, with digital footprints assisting efforts to establish the identity of online offenders, the burden remains upon individuals to show that they had no part in the creation of harmful content. This is unfair in an age when AI-generated content can easily be faked, leaving individuals susceptible to accusations based more on circumstantial evidence than any hard evidence.

There is a huge loss to the perpetrators for the use of Artificial Intelligence in crime, even when viewed as a solution to other processes in law. This makes keeping track of such moles, who regularly invent electronic footprints, incredibly difficult, putting extreme pressure on regulators. The biggest problem now facing regulators is protecting the technologies from the deluge of potentially harmful threats that are coming online. Even though wheeled-out technology is available for its replication of human-like behaviour upon AI content creation, where augmentations could be made, law enforcement is at a loss for words, as are individuals. Technologies that assist law enforcement efforts can also be manipulated by writers to hide their illegal acts. One herculean task has been made possible for differentiation between real and grown ones by making AI-powered tools work in malign ways for content generation. Those wrongfully accused of wrongdoing seldom have the power to prove their innocence, which furthers the sense of injustice. With this, the law systems are too often slow to adjust to the new technological inventions, so individuals expose themselves to AI threats. The usage of the technology for the crime itself becomes a complex ethical dilemma and challenges the changes in the law as a concern to AI tools of content production. On the other hand, regulating AI tools may leave the burden squarely on the shoulders of the individual who has to prove that he is right in a world where AI has become dominant. Given the pace of technology development, some issues should be addressed by society to ensure that justice is not hindered, individual freedoms are not compromised, and their abuse is prevented.



07

Unemployment doesn't cause crime, but it builds the conditions where crime can take root.

Unemployment and Crime

Job security emerges as a fundamental concern for professionals at different career points, from their early stages up to their current points. Employees currently encounter another obstacle because artificial intelligence continues to increase its presence. The presence of AI makes many workers doubt whether their human skills are essential for sustaining their roles because AI might replace these abilities and potentially eliminate their jobs.

The implementation of AI, together with automation technology, transforms workplaces through mass job dislocation that affects many business fields. Active displacement of human workers occurs in the manufacturing sector, retailing and transportation and financial institutions. The rollout of AI-powered robots for manufacturing operations has automated assembly processes and welding functions as well as quality testing operations, thereby replacing human workers on factory assembly lines. The increasing popularity of e-commerce, together with AI system implementations, leads to job loss in the retail industry when these systems perform tasks including inventory management, checkout processes and customer service functions.

The manufacturing of self-driven vehicles and unmanned aircraft systems threatens

to replace workers in multiple positions, including truck operators, taxi service providers and delivery staff members. The finance sector has shifted toward automation across fraud detection, customer service, and risk assessment domains, thus lowering the human workforce requirements at these positions. The complete automation effect of AI and automation has less impact on select business sectors. Healthcare functions as a resistant area where machine substitutions remain impractical for physicians and nurses who work together with critical problem-solving abilities and emotional skills. The employment demand for uman interaction remains essential for AI, which aids diagnostic work, together with administrative functions. Creative jobs in art and writing, along with design work,

are safely away from automation since these positions demand characteristics such as emotional depth, human intuition and creative ability, which AI technology cannot duplicate at present. Educational disruption remains minimal because AI shows difficulty in replacing human judgment for communication, along with the need for a personal connection during teaching and mentorship.

AI automation has more ability to replace specific careers in the labour market. The job of data entry clerks faces significant risk because AI systems perform data organisation processes and accuracy tasks with greater efficiency. Retail staff members face major risks due to self-checkout technology that eliminates human-store interactions and AI customer service solutions, which diminish store workers' needs.

Predictions say that transportation jobs, including truck drivers and delivery people, are threatened by self-driving cars. The effectiveness of AI-powered virtual assistants and chatbots leads to the replacement of customer support representatives when it comes to handling common customer inquiries and offering assistance. Several occupations exist that AI systems have difficulty automating. AI systems encounter limitations in replacing healthcare professionals who are doctors and nurses, and creative workers who write or paint, alongside skilled tradespeople who conduct electrical and plumbing work, because of their advanced human skills in problem-solving and interpersonal abilities, together with their flexible adaptability. Work evolution because of AI advancement will transform job types, but creative judgment, together with the empathetic skills of humans in specific roles, will stay important.

Insights about job displacement and income security in the age of women and upcoming artificial intelligence are real. However, these concerns regarding its impact on different demographics are not novel. Artificial intelligence has been around for quite some time now, although its hype has recently peaked. It is evident that the harder-hit population will be that of the older age segment, who are less adaptable to the technology as compared to the younger age group. The impact of AI on job displacement has a disproportionate impact on the lower-income demographic as well. More prone to job displacement are the low-skilled workers who are associated with jobs whose tasks are mostly repetitive, leading to a higher possibility of income reduction. In contrast, individuals who are skilled in AI and technology, data analysis and related fields, boutique experience a higher demand for their skills and potential income gains too. The younger generation is also less affected because of their confidence in learning the skills that are complementary to AI. If we assess geographic locations, there is a significant uneven distribution of AI-related industries, which in turn leads to job concentration in a few areas limited to these geographies. Individuals who get the opportunity to pursue higher education

and upskill themselves with what is relevant and updated can be highly beneficial.

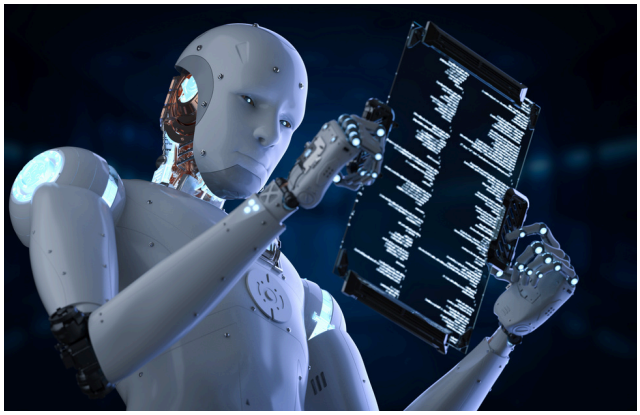
Evidence shows that richer countries are better equipped to harness AI's benefits. They hold a comparative advantage, having better infrastructure and abundant resources. Poor countries are less prepared to handle these disruptions caused by AI. This is mainly due to the limited resources and the underdeveloped social protection systems. Many lower-income countries already struggle with higher rates of informal employment, and with their fragile labour markets, their workers become more vulnerable to such displacement. AI is challenging the development models that have driven growth in many of the emerging economies for decades. Take the example of Bangladesh, where AI and robotics have been integrated into various stages of government manufacturing processes, from automated sowing to fabric inspection and cutting. Though this has proved to boost efficiency, there has also been a significant threat to a large proportion of its workforce.

Such disparities can be deep in social inequalities. This further deepens the problem and the barriers associated with economic mobility and growth. Till now, we have seen how the improvements in Artificial Intelligence and automation have led to a transformation in the global workforce. In sectors such as manufacturing and customer service, traditional jobs are being done with the use of AI. For instance, AI chatbots are excessively used to answer customer service roles, and automatic vehicles and robots are used in place of manual labour. These advancements in AI have threatened the job industry, leading to a rise in unemployment rates. Unemployment still remains a major socio-economic challenge globally. While the economic implications are often known, its psychological and social consequences often take a back seat in the discussion. Due to a surplus workforce and lack of capital, unemployment remains a major problem in India, and less than one-fifth of the workforce is employed in the formal sector, leaving individuals in great trouble during periods of joblessness, worsening their situation.

The problem of unemployment not only puts a financial burden on an individual but can also have psychological effects and mental health challenges, such as depression, anxiety, and stress. Feelings of social embarrassment and worthlessness are common among unemployed individuals, further escalating their mental health challenges. In many societies, especially India, where professional positions and achievements are admired and often tied to social status, the problem of unemployment affects an individual's identity and sense of self-worth. Prolonged uncertainty in job prospects can create a vicious cycle of stress and deteriorating mental health.

As companies have started adopting more AI-based tools to increase productivity

and efficiency, a divide is created between people who possess digital skills and those who do not, creating a gap in job opportunities, promotions, and income.



People like women, older workers and marginalised communities who may have fewer opportunities and low access to education face difficulties in their upskilling, limiting their employment opportunities. People from lower castes or with rural backgrounds are often restricted from employment due to discrimination and socio-cultural norms. There's also been a trend in which many graduates, while possessing advanced degrees, struggle to find employment due to a mismatch between their skills and market demands, depicting the need for educational reforms that align themselves with industry requirements, equipping the students with more practical knowledge for the current job market. Unemployment's impact extends beyond individuals, affecting families, neighbourhoods, and broader communities. High unemployment rates in the community can surge the crime rates and social unrest, which can lead to destabilising communities and social harmony. People will engage in illegal activities to earn the means of survival.

This collectively can erode the trust in social institutions and governance. In most developed countries, financial safety, i.e. unemployment allowance, is provided to people to manage their living expenses while they search for new employment. However, India lacks a central unemployment system, worsening the problem of unemployment. Although some state-level programs exist, such as the Chhattisgarh Berojgari Bhatta Yojana, which provides ₹2,500 per month to eligible unemployed youth, these schemes have limited reach and often face bureaucratic hurdles while transferring the support. Workers employed in the formal sector and registered under the Employees' State Insurance (ESI) scheme, Atal Beemit Vyakti Kalyan Yojana (ABVKY), provide 50% of their average wages for up to 90 days if they lose their jobs involuntarily due to layoffs or retrenchment. Similarly, the Rajiv Gandhi Shramik Kalyan Yojana (RGSY) offers monthly unemployment benefits for up to two years, along with free medical care for eligible and insured workers.

However, these schemes are only available to insured employees under ESI, restricting the scope for casual workers, gig workers, and most self-employed individuals. In the absence of an unemployment allowance, people tend to exhaust their savings and resort to debt without any current source of an unemployment allowance, people tend to exhaust their savings and resort to debt without any current source of income, increasing their status of vulnerability. A

nationwide unemployment benefits program could enable people to invest their savings in skill development and job-seeking efforts. Unemployment is a serious issue in every economy, and the impact of this can be seen on an individual's economic, social and psychological well-being. As AI-driven technologies are replacing traditional and manual labour jobs, it is essential to equip oneself with newer technologies and imbibe digital skills to gain an edge over others. Empowering an inclusive digital economy is vital to make sure that technological progress translates into equitable shared prosperity and does not increase or promote inequality.

08

AI can track patterns, not motives; so its power must be guided by human judgment and fairness.

AI as a Tool Against Crime

Most experts criticise AI-powered crime-detecting algorithms because these systems present inequities regarding their bias and fairness. The data used by these systems draws from previous crime records, even though it reflects existing biases within police departments along with judicial systems and official enforcement agencies. Incorrect development and inadequate oversight of Artificial Intelligence systems allow biases to persist, leading to discriminatory results during system operations.

Predictive policing faces significant problems from racial prejudice, along with biases that stem from socioeconomic factors. Research demonstrates how AI-based crime prediction systems produce higher numbers of generated targets from marginalised populations because existing historical crime data contains biased information. According to an investigation by ProPublica, the risk assessment tools within the U.S. criminal justice system placed African American defendants at risk levels two times more often than white defendants. A 2019 research project between MIT and Georgetown University disclosed facial recognition errors misidentifying people of colour with higher frequency than white people, thus increasing the probability of wrongful arrest incidents.

AI systems face an essential problem because their decision-making has poor transparency and no accountability measures in place. AI criminal detection systems use black box operation,n which presents an obstacle because decision-making procedures remain unexplainable to users. The lack of transparency in AI systems poses an obstacle to contesting wrong or biased predictions, mainly when they are involved in crucial decisions such as bail proceedings, sentencing recommendations and parole determinations. The lack of transparent explanations about AI decision-making processes makes it virtually impossible for defendants to challenge their cases in front of the court.

Research shows that experts suggest developing bias-conscious AI programs through dataset development using varied population samples to decrease discriminatory outcomes. The assessment prevents unjust outcomes, which are most common in critical areas such as law enforcement systems and judicial

proceedings. A combination of strict legal frameworks to regulate AI criminal justice operations provides organisations with ethical guidelines and transparency requirements for fair system use.

Automated surveillance tools that use facial recognition and biometric methods along with behaviour analysis systems severely endanger the privacy rights of individuals. Widely distributed AI applications used by governments alongside corporations for public security aims and border surveillance as well as workplace management trigger multiple ethical and legal complications.

The primary issue emerges from surveillance programmes that run without user permission. Live surveillance technologies enabled by AI consist of cameras alongside drones and tracking methods that observe people under unapproved and uninformed circumstances. The Chinese government operates an AI-powered facial recognition tracking system through its social credit system which experts describe as an invasion of human rights. The adoption of facial recognition by police departments in U.S. and European public areas has sparked alarming debates about state monitoring practices.

The second main threat stems from how data security and privileges get misused. AI surveillance systems accumulate enormous volumes of personal data that include facial pictures along with data regarding individual movement along emotional expression data. The absence of trong cybersecurity defences exposes this information to possible breaches. A large compilation of law enforcement facial recognition records became exposed in 2019 through security negligence which disclosed personal information about hundreds of thousands of people.

under systematic observation at all times. AI surveillance systems create an environment that causes people to modify their behaviour and spoken expressions due to monitoring.

People tend to constrain their free expression because they understand their activities are under systematic observation at all times.

The impressive and unmatchable ability of AI to process vast amounts of data and identify suspicious and abnormal trends, which is almost impossible for human beings, is a valuable tool. The integration of AI in law enforcement and the implementation of penalties have transformed the way in which these crimes are prevented, detected, and investigated. While criminals have started to use

advanced technologies to commit crimes, and fraud, law enforcement agencies also rely on AI-based technologies to enhance public safety and improve investigative efficiency. It leverages the AI capability of big data analytics and real-time analysis to generate predictions about the possible

about the possible instances of criminal activities and the identification of criminals before they act. Data extraction helps not only to identify crime but also to prevent it. Machine learning algorithms examine various crime reports, detect patterns, and provide predictions based on data to find regions with a higher probability of crime. AI-based analytics systems can, therefore, scan social media posts, online forums and keywords tied to criminal activity to help identify potential threats in their early stages. A successful application can be seen in combating terrorism, where AI helps in identifying extremist threats by analysing digital communications and real-time movements. PredPol is one such AI-driven policing system that uses historical crime data to predict where crimes are most likely to occur. AI is revolutionising forensic science by improving its scope and precision, and is widely used in forensic evidence analysis. AI-based technologies predict physical traits such as hair color, eye colour, etc., allowing investigators to create more accurate suspect profiles. Digital forensics is also done through AI-powered tools by checking online activity and encrypted communications to prevent fraud and online exploitation. Accurate forensic evidence helps in analysing blood spatter patterns, bullet trajectories, etc, to recreate crime scenes by using computer vision and 3D modelling, providing critical insights for investigations.

The role of AI in maintaining law and order is much more than this. Smart surveillance systems use AI-enabled facial recognition and behavioural analysis to enhance security and prevent crime by identifying individuals by analysing facial features and comparing them with biometric databases. This technology is used in airports, public spaces and other important public gatherings to track suspects, locate missing persons, and enhance border security. China's vast surveillance network uses facial recognition to monitor millions of citizens in the same manner. Behavioural analysis helps in detecting suspicious activities before they turn into criminal acts by analysing human movement, gestures, and social interactions to identify anomalies, such as sudden crowd formations or aggressive behaviour. Even law enforcement agencies conduct real-time analysis and scanning of vehicle license plates to track stolen vehicles and detect traffic violations to enhance traffic monitoring and crime detection.

Countries like the United Kingdom and the United States extensively use these technologies to improve traffic management and crime prevention. For instance, AI-enabled security drones equipped with thermal imaging and facial recognition help in tracking suspects and monitoring huge gatherings.

From predictive policing and crime forecasting to forensic analysis and smart surveillance, AI is revolutionising the way criminal activities are monitored, analysed, and responded to. These advancements not only improve the efficiency of maintaining law and order but also enhance public safety.

09

Laws define boundaries; ethics define conscience.

Ethical and Legal Considerations

Now that we have seen how efficiently law enforcement agencies can utilise AI and advanced technology to combat criminal activities, reduce crime rates, etc., through tools like predictive policing, crime forecasting, smart surveillance and many more, we, imperatively, also need to shed light upon the ethical challenges involved in such tools and mechanisms. Law enforcement needs to take into consideration these challenges in order to properly formulate policies for the country. Policymakers must strike a balance between protecting the individual liberties of citizens and fostering innovation. Another reason is simply the ethics involved. Criminal justice, or justice of any kind, involves moral ethics, which are human qualities, and might not be considered by AI technologies. There are standards and norms that law enforcement needs to adhere to, and situations that call for an unusual but fair judgment in trials. This is also important for the long-term influence on society as a whole. A safe community is more likely to grow and expand, which is beneficial even from an economic point of view. The first challenge is privacy concerns, which are all-pervasive. Currently, law enforcement makes sure to prevent the leak of personal information related to persons involved in trials in order to protect their identity. This might not be possible to a great extent if technology is incorporated into the system. It is evident that law enforcement agencies need the database of all persons and check their criminal records in order to frame criminal profiling, keep a track record of past involvement in criminal activities by individuals, and predict potential crimes and criminals in the future. If a skilled hacker learns the mechanisms and tools used by law enforcement to carry this out, it will most likely only cause harm to society. This can also be linked to the erosion in communities. Failure to determine the actual perpetrator might result in loss of public faith and confidence in the law, which can potentially disrupt communities. Algorithm bias might remain a grave concern, considering the consequences of a wrongly made judgment, especially in serious domains like criminal justice.

While making use of tools to refer to predictive policing, make criminal profiles, etc., it might not easily be evident that the statistics revealed show mostly accurate data. This might be noticed in AI

bots as well, for example, OpenAI ChatGPT, which always states that the bot can make mistakes, leaving it unaccountable in case of grave concerns. Additionally, the mechanisms might also hint that the Right to Equality is the fundamental law that the Indian Constitution states in Article 14. It guarantees our basic right to be looked at as equal before the law, without any kind of discrimination, which is important in order to be protected from the biases of technology. Additionally, relying on technological tools alone is not at all beneficial and safe, since human assessment is important at all times. Another important aspect to be considered is that the current legal system is not designed to incorporate the new cybercrime, such as deepfakes, phishing scams, etc., which creates a loophole in prosecution and enforcement. Additionally, cybercrimes can be conducted across borders, which makes it difficult to enforce legalities, adding on more jurisdictional challenges.

The aforementioned aspects require a fair and just implementation of AI-driven tools and mechanisms to protect the interests of individuals. If such mechanisms are implemented, there is a need for frequent bias analyses through human assessment while frequently checking the resilience of such tools over time. In order to minimise bias and guarantee fairness, robust ethical frameworks need to be adopted. These frameworks should establish ideals like transparency, fairness and accountability. Additionally, explicit regulations need to be set to hold individuals and organisations accountable for any biases that arise as a result of using AI tools. Crime prevention has evolved significantly over the years. The changes reflect the differences in societal norms, technology, and law enforcement strategies. Crime prevention methods earlier focused on

community policing, situational crime prevention, and crime deterrence strategies. This approach led to reducing opportunities for crime by restructuring environmental design and community engagement. The importance was laid on building trust between law enforcement and communities to encourage collaboration. It would address the root causes of crime, which is the most basic and significant requirement. In recent years, advancements in technology have transformed crime prevention efforts, leading to the incorporation of artificial intelligence (AI) into law enforcement practices. AI technologies, such as machine learning, predictive analytics, and natural language processing, have been leveraged to enhance crime prevention strategies. Machine learning algorithms are used to analyse vast amounts of data and identify patterns and trends. They usually relate to potential

criminal activity. Predictive policing models, for instance, utilise historical crime data to forecast where and when crimes are likely to occur, allowing law enforcement agencies to allocate resources more effectively. The integration of AI in law enforcement not only aims to improve efficiency but also seeks to enhance public safety through data-driven decision-making. However, the deployment of AI technologies has raised concerns about privacy, accountability, and bias. Critics argue that relying heavily on AI could exacerbate existing disparities in policing and infringe on civil liberty. As AI technologies become increasingly prevalent in policing, understanding their impact on crime prevention strategies is crucial. The focus is on doing public good as well as prioritising the protection of individual rights.

The deployment of artificial intelligence (AI) and predictive policing technologies has raised important legal and regulatory considerations worldwide. As law enforcement agencies increasingly rely on these tools, existing legal frameworks are evolving to address the implications of their use on civil liberties, privacy, and accountability. In the U.S., the legal landscape governing predictive policing is fragmented. The Fourth Amendment protects citizens against unreasonable searches and seizures, but its application to AI-driven surveillance and predictive policing is still being interpreted by courts (Schneier, 2015). Several states, such as California and Illinois, have enacted specific laws addressing the use of algorithms in policing. For instance, the California Consumer Privacy Act (CCPA) mandates transparency in data collection and usage, requiring law enforcement agencies to disclose the algorithms they use (State of California, 2018). Furthermore, the U.S. Department of Justice has issued guidelines recommending that law enforcement agencies assess the potential for bias and discrimination in algorithmic policing tools (U.S. Department of Justice, 2016). that law enforcement agencies justify their use of personal data for AI applications. The Information Commissioner's Office (ICO) has published guidelines highlighting the importance of fairness, accountability, and transparency in the use of AI technologies (ICO, 2021). Moreover, the National Police Chiefs' Council has issued guidelines to ensure ethical practices in the deployment of predictive policing systems, advocating for community engagement and oversight (National Police Chiefs' Council, 2019). Global Perspectives: Internationally, various countries are grappling with similar issues surrounding AI and predictive policing. Nations such as Canada and Australia have introduced legal frameworks that emphasise data protection and ethical considerations in law enforcement practices (Office of the Privacy Commissioner of Canada, 2020; Australian Government, 2021). These frameworks often include provisions for accountability, oversight, and public consultation to ensure that the rights of citizens are upheld. Despite these legal frameworks, there are many unresolved

challenges. The pace at which these regulations work is often outpaced by the rapid advancements and evolving nature of crime. Moreover, the global nature of data and technology complicates enforcement, as many predictive policing systems rely on data sourced from multiple jurisdictions, each with its own legal standards. Though there have been several attempts to develop frameworks in various regions for regulating AI and predictive policing, ensuring transparency and accountability is still a struggle.

10

Decoding The Breach

An Analytical Dive into Two Landmark Cyber Intrusions

The DAO Hack: The $60 Million Ethereum Crisis

On the 17th of June 2017, Ethereum faced a crisis, forever shaping the future of blockchain and its governance. The DAO, a decentralised venture fund, aimed to revolutionise the domain of investment by removing human intermediaries. Only time could tell how it became a target of one of the greatest hacks in the history of cryptocurrency. An error in its smart contract code allowed room to drain USD 60 million worth of ETH, exposing the platform to unprecedented risks. The hack sparked debates and discussions over immutability, decentralisation, and ethics, leading to the Ethereum hard fork, a change in the blockchain protocol requiring all users to upgrade the software to continue participating in the network, which split the network into two. This case study delves deeper into how the hack unfolded, its impact on the economy and victims, and the critical lessons it taught.

Let us first understand what exactly Ethereum is. Ethereum is a decentralised global software platform powered by blockchain technology. It is designed to be scalable, programmable, secure, and decentralised, to create any secured digital technology. It is similar to Bitcoin but with different long-term visions and limitations. Bitcoin is like digital gold, used to store value and payments, while Ether is more like a digital fuel used to pay for using Ethereum's network. To understand it a bit better, think of Ethereum as a giant decentralised computer that anyone can use to build and run applications, not requiring a central authority to govern its use. It operates on a global network of computers, making it secure and resistant to censorship. Ethereum requires Ether (ETH) to power transactions and applications run on its network.

The DAO (Decentralised Autonomous Organisation) represents a community-led entity with no central authority. The system is fully decentralised and does not require any person or group to control its decisions, which are instead proposed and voted on by the community and executed by the system itself. In brief, the system is

transparent, and everything is visible and known to the community. The DAO was one of the most exciting projects in the domain of digital currency. It aimed to eliminate human error or bias by allowing it to work on the commands of an automated system. It was launched in April 2016 after raising a solid USD 150 million in funds. Unfortunately, an error in its smart contract code allowed recursive, re-entrant withdrawals. Instead of withdrawing only the authorised amount, the attacker's contract kept calling the withdrawal function before updating the balance, allowing them to drain funds repeatedly. In a matter of a few hours, USD 60 million worth of ETH was transferred to a child DAO controlled by the hacker. Ethereum's property of operating on immutable smart contracts prevented the hack from being reversed, leading to a catastrophic hack that went on to become one of the largest ones in the history of digital currency. The hack led to immense debates on the functioning and operations of Ethereum. Some believed a hard fork could be used to reverse the hack and return respective funds to the investors, preventing the damage, while some believed in continuing to keep it immutable, irrespective of the stolen funds. Eventually, an Ethereum hard fork was implemented to return the lost funds to the investors. Critics and users who opposed the decision continued using the original Ethereum.

The Ethereum DAO cybersecurity breach created a permanent impact on both Ethereum and blockchain technology as a whole. The DAO hack triggered an active philosophical disagreement that resulted in the creation of two Ethereum networks: ETH and ETC. Ethereum introduced the hard fork for fund retrieval, but Ethereum Classic continued to defend blockchain immutability despite the hack. The incident led to extensive dialogues regarding decentralised system governance. The situation revealed the essential requirement for better guidelines when making crisis-related decisions. Blockchain projects now use decentralised autonomous organisations (DAOs) as well as enhanced protection features and voting models to deliver better emergency response services, which are both transparent and effective. The security incident acted as a vital wake-up warning for everyone involved. The events triggered developers, along with blockchain organisations, to conduct thorough security audits with third-party auditors who verify smart contracts. New formal verification techniques using mathematical verification have become prevalent to detect software faults in ways similar to the DAO hack. The notion of upgradeable contracts has emerged as a popular solution throughout the market. Upgraded contracts provide better flexibility than unchangeable DAO contracts because they let developers repair bugs and introduce new features without diminishing decentralised management features. Applications utilising this strategy can handle unanticipated weaknesses while users keep trusting the system. The regulatory community began exploring DAO and

smart contract legality after the DAO experienced a hacker attack. The world's nations investigate methods to govern blockchain platforms alongside their attempts to unite technological innovation with customer safety protections. Specific jurisdictions have begun to implement requirements which enforce transparency and compliance together with accountability standards for the blockchain industry.

The DAO hack demonstrated the strong spirit of defiance among members of the Ethereum community. The community responded to their enormous challenge by uniting to evaluate proposed solutions, which resulted in making a difficult decision. Ethereum gained admiration as a platform that demonstrates adaptability during threats because of its decentralized governance system. The DAO hacking incident continues to instruct blockchain technology development practices as we proceed into the future. Decentralised applications function in a safer and more enduring environment because of greater security systems along with flexible governance structures and improved regulatory oversight. The DAO hack showcases blockchain evolution through for the development of decentralised applications. This hack helps shed light on potential lessons learnt from the case and its aftermath. One of the very first aspects is the vulnerability that was exposed by the hacker due to an unnoticed error in the smart contract codes. This highlights the importance of code audits, which could have detected this error and prevented the damage from happening in the first place. Another flaw of the DAO was the immutability of its smart contract codes, which could have been modified with the help of upgradeable contracts, allowing enough flexibility for a safety net in case of unforeseen exploits. Another important aspect was the response of the Ethereum Foundation after the hack. Clear mechanisms could have been laid down in the initial stages of launching the platform to handle such crises effectively.

Along with the aforementioned aspects, the hack also highlighted the need for continuous monitoring, formal verification methods, and decentralised security solutions.

The DAO hack serves as a reminder of the complexities and risks prevalent in the domain of cryptocurrency. It is imperative to build secure and resilient systems by learning from such past incidents and mistakes. As the blockchain domain evolves, prioritising security is paramount to fostering trust and realising the full potential of decentralised technologies.

The Mother of All Breaches (MOAB)

MOAB stands out as the largest and most widespread data breach ever seen online. It has an astonishing 12 terabytes of information, containing 26 billion separate records, according to CyberNews (2024). As we continue to move into an era of interconnectivity, where information fuels communication, commerce, and governance, so too are we seeing a mass exodus of cyber threats. The MOAB is a sobering reminder of that growing threat. It's not only impressive for its size, but the possible fallout is just as unsettling. This leak represents the deep-seated fears of the cybersecurity community: a hyper-aggregated, widely available database compiles from years' worth of international data breaches.

What makes the MOAB so ominous isn't necessarily its size, but rather how it's been assembled and for what purposes. It brings together thousands of old data leaks, some of which were made public and others secretly shared on the dark web, into one organised and easy-to-search database. This structured form converts fragmented breaches into a powerful weapon for attackers. The MOAB is a one-stop shop for usernames, passwords, email addresses, government IDs, location information, and everything

in between. Its impact extends to top tech and social sites such as LinkedIn, X, Weibo, Tencent QQ, MySpace, Dropbox, and even government agencies in nations like the United States, Germany, Brazil, Turkey, and the Philippines. With 1.4 billion Tencent QQ records alone and hundreds of millions of others, the MOAB underscores a worldwide failure in data security management and watchfulness. The importance of this breach to the digital landscape of today cannot be overemphasised. It reveals serious systemic weaknesses in password hygiene, server settings, and reactive cybersecurity practices. A direct effect of this kind of breach is credential stuffing, where attackers exploit password reuse across services.

The "Mother of All Breaches" (MOAB) emphasises the potential role of AI in mitigating cyber threats. As discussed in the report, the ability of AI in detecting anomalies and analysing massive datasets rapidly could have been used more efficiently in detecting unusual activities that led to MOAB. Adopting advanced AI-based technologies could have prevented or at least limited the extent of the breach.

Over 26 billion records were exposed in this tremendous scam, leading to identity thefts, etc.

Additionally, the domino effect of compromised accounts, where a compromised account leads to breaches of others, through the reuse of passwords, escalates the damage. Over 26 billion records were exposed in this tremendous scam, leading to identity theft, phishing attacks, and unauthorised access to accounts. As the number of spam, scams, and misinformation campaigns increases, it disrupts essential services and erodes public trust.

In light of MOAB, one must understand the importance of right cyber hygiene practices like unique passwords for each of their accounts. Password Managers are software applications used to securely store, manage, and retrieve your login credentials for various online accounts, which can be considered to enhance online security and reduce the risk of unauthorised access. A multi-factor authentication (MFA) is a way of adding an extra layer of security to our accounts, making it more difficult for attackers to gain access. Teaching people about common online dangers through public campaigns and simple training at work is really important for preventing security breaches and encouraging a culture of vigilance among users.

In conclusion, the “Mother of All Breaches” (MOAB) is a wake-up call for individuals, businesses, and governments. MOAB reveals the scale of damage that can be caused when outdated systems, reused passwords and poor vigilance are put together.

It serves as a testimonial to inherent vulnerabilities in our digital infrastructure and how proper legal and ethical

deployment of AI can improve it. It necessitates the need to rethink our approach to cybersecurity and the potential of AI to act as a saviour. There is an urgent need for awareness, education, accountability and a shift in mindset. Proactive measures can better safeguard our digital assets against future breaches of this magnitude.

Conclusion

Leveraging the capabilities of artificial intelligence, there is a huge potential to utilise vast amounts of data with great speed and accuracy. Law enforcement agencies can use data and investigation tools. Both the government and the private sector make use of deep learning that integrates artificial intelligence and computers to imitate sophisticated decision-making capabilities of the human brain. In this way, a pattern of crime is detected and various strategies are implemented to prevent it from occurring again. This is called predictive analysis, which comes into play when studying this topic.

Artificial intelligence is used in many online platforms. It helps to detect common terminology used in many criminal activities, including human and drug trafficking. Artificial intelligence fights crime through data mining.

What it essentially does is to collect data points that allow one to analyse the crime patterns. Authorities can make a deep analysis and provide data inputs about the frequently occurring criminal activities or suspect areas of high risk. The most vulnerable resource for information is social media data and it is specifically useful for the purpose of identifying missing information collected from a secondary data source.

The concept of machine learning in AI-related criminal activities has already been discussed, which leads to the conclusion that artificial Intelligence can do data mining on social media sites for information which will ultimately aid law enforcement officers by helping them take preventive action. Artificial intelligence is a significant investigative tool for officers and policemen to locate criminals. It is used for detecting phone numbers and even Internet Protocol (IP) addresses. Artificial intelligence essentially builds an artificial neural network. For example, it is used to build model behaviour that can imitate human activities and their decisions, which is very helpful in understanding the psychic of criminals. The importance of algorithms is huge

when it comes to understanding the rules of artificial intelligence in this arena. Algorithms are the set of instructions which enable AI to make decisions on the basis of instructions. Mostly, all of the companies use these algorithms to improve their efficiency, meet their maintenance needs and automate various operations.

The report delves into the basics of Artificial Intelligence and its relation to Crime and Criminal Justice. It finds how AI has penetrated every single domain one can even think of, precisely. This pervasiveness, while benefiting domains like health and medicine, businesses for profits and strategically enhanced business models, etc., raises grave concerns on its interrelation to crime. Fields like finance and cybersecurity have greater scope with the onset of highly advanced technology, benefiting from advanced fraud detection and threat mitigation; meanwhile, other fields may suffer due to added security concerns. Cybercrime is rapidly outpacing traditional methods of crime, such as blue-collar and white-collar crime, with serious consequences and things like personal identity, confidentiality, and privacy at stake.

The report also discusses other factors like increased financial pressure, financial illiteracy, and establishes the relation between factors like the digital divide and unemployment and crime. The skill gap between highly skilled persons in advanced technology and those with a lack of basic knowledge of technological tools and mechanisms makes the latter more susceptible to cybercrime. Additionally, unemployment might make it difficult for a person to afford meals and incur basic expenses of electricity and water. This might lead to aggravation of feelings like frustration and desperation, which push an individual to resort to quicker ways of earning money, through criminal activities like ransom, scams, frauds, etc.

The report also delves into how cryptocurrencies like blockchain have opened more avenues for criminals to undertake illegal activities, while also providing a new method to conduct borderless transactions with a negligible scope of detection. Platforms like the Dark Web are an easy platform for skilled hackers to orchestrate fraud over the same. Moreover, in addition to the use of blockchain, the Dark Web also allows room for the kinds of illegal activities that are heinous to a great extent but go unnoticed, given the amount of privacy the platform provides.

Overall, the report discusses, in a detailed manner, the scope of AI in the realm of crime. Consequently, law enforcement agencies need to adapt fast to use this technology to their advantage, to utilise it in a manner that seems fit for societal welfare, while ensuring that fairness and justice to all are maintained. Another significant concern is the combination of AI and employment. With the growth of AI-based technologies in the market, many industries are facing large-scale job displacement, especially for low-skilled workers and older generations. We have

noticed how AI is entering almost every industry, which is leaving minimal scope for manual jobs. This has now raised the unemployment rates in several industries, resulting in major financial and psychological problems as well as financial losses, mental troubles and a rising crime rate in society. The absence of a proper financial safety system in India further escalates the financial burden on the unemployed population.

AI has transformed the way crime and fraud are committed, and it has simultaneously transformed the way law enforcement agencies deal with the same, presenting both opportunities and challenges in combating criminal activities. We have seen how the dark web is preferred by criminals for illicit activities and how AI's ability to process huge amounts of data and detect anomalies is useful in tracking illicit transactions and monitoring hidden online networks. Criminals are actively exploiting deepfake and AI-generated voice modulation technologies for identity theft, financial fraud, blackmail, and misinformation campaigns, and rapid advancements in AI have narrowed the line between authentic and manipulated media, raising ethical and legal concerns. This has shifted the burden of proof; victims must now prove their innocence against AI-generated false evidence, a challenge that needs to be fully addressed by traditional legal frameworks. Nonetheless, AI has tremendous potential as a tool against crime. However, it raises concerns about algorithmic bias, privacy violations, and excessive surveillance.

Ultimately, AI is neither good nor bad, it is a tool whose impact depends on how it is designed, deployed, and regulated. Governments, policymakers, and AI researchers must work together to ensure that AI serves as a tool for justice, rather than a tool for crime and oppression. To maximise AI's potential for public good, comprehensive policy recommendations are necessary. It is important to strike the right balance between innovation and accountability.

Firstly, it is essential to establish strong ethical and legal frameworks governing AI use in crime prevention and policing. Transparency and accountability must be incorporated into AI-based systems to prevent misuse and ensure public trust through ethical AI policies and legal safeguards that protect citizens from unwarranted surveillance and discrimination. A proper surveillance system should be developed so that the data is stored securely with limited access to only official people. The concept of AI watermarking technologies can be explored to trace the source of deepfakes and other AI-generated content. Huge investments should be made in AI literacy programs for the common people for their welfare. This will raise the number of skilled people in the economy solving the problem of unemployment. Raising awareness ensures a reduction in the number of crimes and fraud committed using AI. A proper system for the unemployed person should be developed to reduce their economic and psychological burden. The analysis proves

the need to combat changing criminal patterns, which appear during digital times. Crime methodologies have evolved because of today's technological developments, which create economic risks and make it harder to secure private information and national security. It highlights that immediate changes in laws, cybersecurity systems and ethical technology must be implemented to prevent major exploitation.

Technology serves two conflicting purposes because it enables socioeconomic development together with system destabilisation when improperly used. AI-driven fraud, together with deepfake manipulations and cybercrime, requires companies to develop security measures with great caution as they advance technology. All these risks require proactive intervention by businesses along with governments and regulatory bodies so the potentially severe economic and social consequences can be avoided.
Future research might examine quantum computing security threats and blockchain crime prevention and investigate AI-controlled misinformation spread which affects democratic procedures. Ongoing research, together with evolving policies, exists as the essential requirement to protect economic systems and social structures from developing digital safety risks.

A joint operation plan and forward-minded thinking will make it possible to defeat new security threats. International authorities need to unite their efforts with modern technological security policies for the purpose of reducing technology-based threats. Social development and safeguards against abuse will determine whether technology acts positively as an influence or opens doors to exploitation over the next years. Modern technology brings the most advantages when societies adopt ethical governance alongside strategic policies and persistent monitoring which minimises their vulnerability to digital crimes.

References

Springer Science and Business Media LLC. (n.d.). AI-enabled future crime - UCL Discovery. https://discovery.ucl.ac.uk/id/eprint/10107459/

Intelligence, S. (2024, May 9). The use of modern technology in crime. Verdict. https://www.verdict.co.uk/ai-crime-use-opportunities/

Byrne, J., M., & Marx, G., T. (2011c). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. In Cahiers Politiestudies (Vols. 2011–3, Issue nr. 20, pp. 17–40). Maklu-Uitgevers. https://www.ojp.gov/pdffiles1/nij/238011.pdf

Association of Chartered Certified Accountants, EY, & Dancey, K. (2020b). Economic crime in a digital age. Association of Chartered Certified Accountants.

Saragih, Y. M., Krisna, L. A., & Lubis, M. R. (2018b). Effect of technological advances on cybercrime. In International Journal of Civil Engineering and Technology (IJCIET) (Vol. 9, Issue 11, pp. 917–924) [Journal-article]. https://iaeme.com/MasterAdmin/Journal_uploads/IJCIET/VOLUME_9_ISSUE_11/IJCIET_09_11_085.pdf

Adams, C., Buck, R., Herzberg, G., Mandel, J., Mueller, C., & Yongyuan Dai/Getty Images. (2020). Marketing & Sales Practice: Harnessing the power of simplicity in a complex consumer-product environment.

Levitt, S. D. (2004). Understanding Why Crime Fell in the 1990s: Four Factors that Explain the Decline and Six that Do Not. The Journal of Economic Perspectives, 18(1), 163–190. https://doi.org/10.1257/089533004773563485

Mcculloch, D. (2023, February 28). A history of crime: investigations, trials and punishments. Lexology. https://www.lexology.com/library/detail.aspx?g=9b39aef7-9f6a-4689-9f53-d7d1a4977c16

Fitzgerald, C. S. (2011). Historical theories of crime and delinquency [Journal-article]. Journal of Human Behavior in the Social Environment, 21, 297–311. https://doi.org/10.1080/10911359.2011.564954

Datarails. (2024, August 20). Which industries will AI impact the most and least. Datarails. https://www.datarails.com/industries-impacted-by-ai/

Thomas, M. (2025, January 28). The Future of AI: How Artificial intelligence will change the world. Built In. https://builtin.com/artificial-intelligence/artificial-intelligence-future

The History of Crime in England, 1550-1914. (1995). In Refresh 20 [Journal-article]. https://files.ehs.org.uk/wp-content/uploads/2020/07/29061007/sharpe20b.pdf

The Ohio State University Press. (n.d.). https://ohiostatepress.org/books/series/ccj.htm

Shaw, C. R., McKay, H. D., University of Chicago, Merton, R., Durkheim, E., Lombroso, C., SCCJR, SCCJR, SCCJR, SCCJR, Young, J., & Cohen, A. (2021b). Theories and causes of crime. http://www.sccjr.ac.uk/wp-content/uploads/2016/02/SCCJR-Causes-of-Crime.pdf

Psychology and crime. (n.d.). Obo. https://www.oxfordbibliographies.com/display/document/obo-9780195396607/obo-9780195396607-0114.xml

Psychology of Crime: History's famous criminal minds | Maryville Online. (2023, October 11). Maryville University Online. https://online.maryville.edu/online-bachelors-degrees/forensic-psychology/resources/psychology-of-crime/

Webber, J., & Ward, Dr. (2009b). Psychology, Sociology and Crime: Mapping the Historical terrain. In Psychology, Sociology, Crime: Historical Terrain (pp. 1–4). https://www.sagepub.com/sites/default/files/upm-binaries/31541_01_Webber_CH_01.pdf

Rafaiee, R., Olyaee, S., & Sargolzaiee, A. (2013). The relationship between the type of crime and drugs in addicted prisoners in Zahedan Central Prison. International Journal High Risk Behaviors & Addiction, 2(3), 139–140. https://doi.org/10.5812/ijhrba.13977

Wyland, J., & Wyland, J. (2024, January 16). The Psychology of Criminal Behavior: Understanding the mind of Offenders | UT Permian Basin Online. The University of Texas Permian Basin | UTPB. https://online.utpb.edu/about-us/articles/criminal-justice/the-psychology-of-criminal-behavior-understanding-the-mind-of-offenders/

Davison, S., & Janca, A. (2012c). Personality disorder and criminal behaviour: What is the nature of the relationship? In Curr Opin Psychiatry (Vol. 25, Issue 1, pp. 39–45). http://www.antoniocasella.eu/archipsy/Davison_Janca_2012.pdf

Cantürk, M., Faraji, H., & Tezcan, A. E. (2020). The relationship between childhood traumas and crime in male prisoners. Anatolian Journal of Psychiatry, 22(0), 1. https://doi.org/10.5455/apd.111825

Sadulski, J. (2024b, September 13). Artificial intelligence in Crime Detection: How it's useful. American Military University. https://www.amu.apus.edu/area-of-study/information-technology/resources/artificial-intelligence-in-crime-detection/#:~:text=AI%20can%20also%20fight%20crime,high%20risk%20of%20suspicious%20activity.

Rigano, C. (2019). USING ARTIFICIAL INTELLIGENCE TO ADDRESS CRIMINAL JUSTICE NEEDS. In National Institute of Justice. https://www.ojp.gov/pdffiles1/nij/252038.pdf

Završnik, A. (2019b). Algorithmic justice: Algorithms and big data in criminal justice settings. European Journal of Criminology, 18(5), 623–642. https://doi.org/10.1177/1477370819876762

Onuoha, M. & Mother Cyborg. (n.d.-b). Algorithmic bias explained. In Algorithmic Bias Explained (p. 1). https://greenlining.org/wp-content/uploads/2021/04/Greenlining-Institute-Algorithmic-Bias-Explained-Report-Feb-2021.pdf

Ghanem, M. C., Ouazzane, K., Dunsin, D., & School of Computing and Digital Media, London Metropolitan University, London, UK. (n.d.-b). The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment. School of Computing and Digital Media, London Metropolitan University, London, UK. https://repository.londonmet.ac.uk/7708/3/Australia_Dip_paper.pdf

Singh, O. G. (2022b). Artificial intelligence in forensics & criminal investigation in Indian perspective. In SRM Medical College & Research Centre, International Journal of Innovative Science and Research Technology (Vol. 7, Issue 8, pp. 142–143) [Journal-article]. https://ijisrt.com/assets/upload/files/IJISRT22AUG333.pdf

The Role of Artificial Intelligence in Forensic Science: Transforming Investigations through Technology. (2024b). In International Journal of Multidisciplinary Research and Publications (Vol. 7, Issue 5, pp. 67–70) [Journal-article]. https://ijmrap.com/wp-content/uploads/2024/10/IJMRAP-V7N5P52Y24.pdf

McDaniel, J. L. M., & Pease, K. G. (2021). Predictive policing and artificial intelligence. In Routledge Frontiers of Criminal Justice. Routledge. https://api.pageplace.de/preview/DT0400.9780429555916_A41017822/preview-9780429555916_A41017822.pdf

Acılar, A., Koca, G., & Karamaşa, Ç. (2011, December 1). *DIGITAL DIVIDE AMONG ENTERPRISES IN a DEVELOPING COUNTRY*. https://dergipark.org.tr/en/pub/ijebeg/issue/26201/275875

Mathrani, A., Sarvesh, T., & Umer, R. (2021). Digital divide framework: online learning in developing countries during the COVID-19 lockdown. *Globalisation Societies and Education*, *20*(5), 625–640. https://doi.org/10.1080/14767724.2021.1981253

Team, Z. (2024, March 18). *The role of AI in dark web monitoring*. ZeroFox. https://www.zerofox.com/blog/the-role-of-ai-in-dark-web-monitoring/

View of Deep Fake Detection and Mitigation: Securing Against AI-Generated Manipulation. (n.d.). https://researchworkx.com/index.php/jci/article/view/55/58

YADAV, B. (2022). UNEMPLOYMENT RATE. In *RAJYA SABHA*. https://dge.gov.in/dge/sites/default/files/2023-09/175_E.pdf

Berk, R. A. (2020). Artificial intelligence, predictive policing, and risk assessment for law enforcement. Annual Review of Criminology, 4(1), 209–237. https://doi.org/10.1146/annurev-criminol-051520-012342

Jan A.G.M. van Dijk and Abstract From the end of the 1990s onwards the digital divide (2006) Digital Divide Research, achievements and shortcomings, Poetics. https://www.sciencedirect.com/science/article/pii/S0304422X06000167

THE TEAM

RESEARCH AND POLICY DIRECTOR

Ritul

TEAM MEMBERS

Advika Sanganeria

Kulpreet Kaur

Snehil Jha

Vardaan Goel

Contact Us

Ritul

+91-63982-23696

Suhani Jain

+91-87126-77777

www.ecosocsrcc.com

contact@ecosocsrcc.com

THE ECONOMICS SOCIETY

SHRI RAM COLLEGE OF COMMERCE

www.ecosocsrcc.com

contact@ecosocsrcc.com