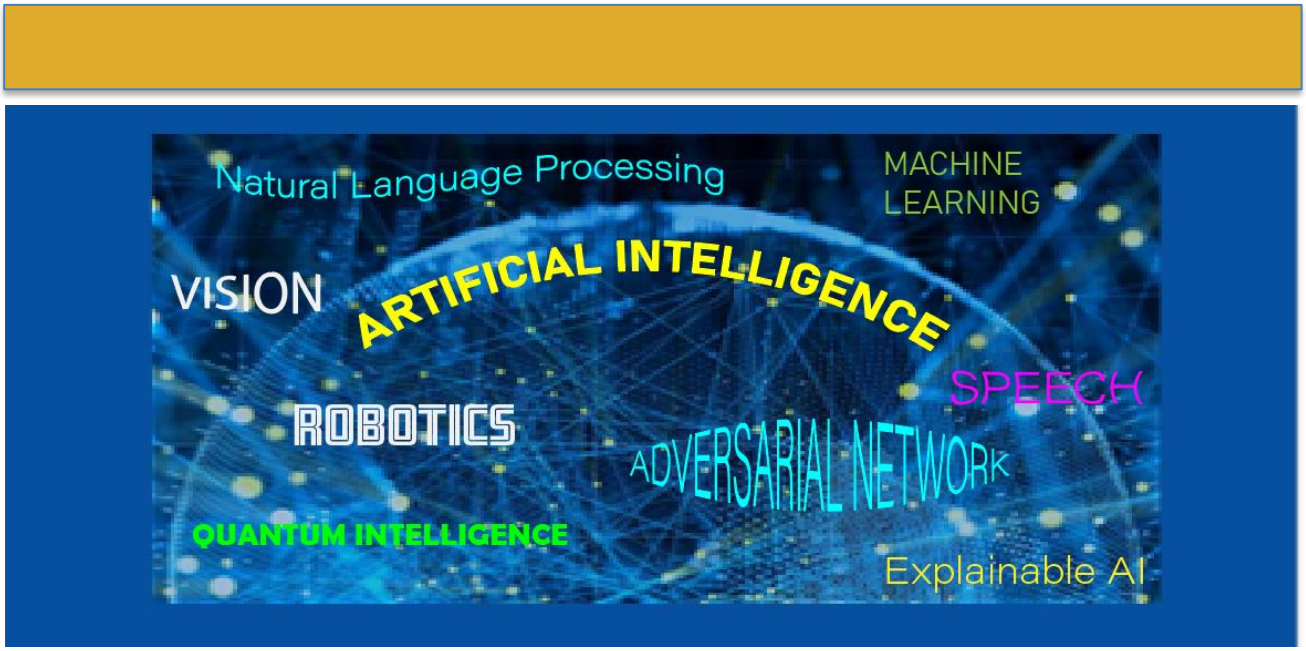
EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

Impact of Technology Deep Dive Report I

STUDY ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE INFRINGEMENT AND ENFORCEMENT OF COPYRIGHT AND DESIGNS



March 2022

Impact of Technology Deep Dive Report I

STUDY ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE INFRINGEMENT AND ENFORCEMENT OF COPYRIGHT AND DESIGNS

ISBN 978-92-9156-312-8 doi: 10.2814/062663 TB-01-22-114-EN-N

Contents

Foreword

Over the past 50 years, the world has witnessed landmark innovations and revolutionary changes that have transformed economies, jobs, and even society itself, fundamentally altering the way we live, work and relate to one another. Artificial intelligence (AI) and related technologies are among the most important drivers of change, and have an impact on every area of intellectual property rights (IPR). This study has been drawn up as a tool for practitioners, shedding light on how these technologies are used both to safeguard copyright and designs and infringe them.

Understanding the implications of these transformations is vital at a time when the Fourth Industrial Revolution (4IR) is transforming virtually every area of the economy and society. We are seeing inventions and breakthroughs in the fields of autonomous transport, biotechnology, the Internet of Things (IoT), smart devices, AI, 3D printing, robotics, and quantum computing. These inventions affect healthcare, transport, agriculture and law enforcement, among other fields, and the pace of global innovation has accelerated greatly during the last decade. According to some estimates, by 2023 there will be some 29 billion connected devices on the planet that use AI technologies, and the underlying algorithms are becoming ever more central.

Infringements of IPR through the malicious use of various new technologies, including AI, are on the rise, as reported by Europol's European Cybercrime Centre (EC3), the EU Agency for Cybersecurity (ENISA) and the United Nations. In May 2021, the EU's Council of Ministers named IP crime as one of the top 10 priorities in the fight against organised crime for 2022-2025. This issue will be tackled through the European multi-disciplinary platform against criminal threats (EMPACT). The European Union Intellectual Property Office (EUIPO), via the European Observatory on Infringements of Intellectual Property Rights, will be actively involved in supporting the implementation of this priority under the EMPACT.

In this new era, it is critical that we adopt ‘smart’ intellectual property strategies, and the EUIPO, working with its network of partners and IP stakeholders, has been developing tools and promoting best practices. This study represents another step on the journey to creating an IP excellence hub in which new technologies and AI work to protect legitimate businesses and citizens.

Christian Archambeau
Executive Director
EUIPO

Acronyms

AAAI	American Association for the Advancement of Artificial Intelligence
ACR	Automatic content recognition
AGI	Artificial general intelligence
AI	Artificial intelligence
A.L.I.C.E	Artificial Linguistic Internet Computer Entity
ANI	Artificial narrow intelligence
ASI	Artificial superintelligence
ASIMO	Advanced Step in Innovative Mobility
APT	Advanced Persistent Threat
BEC	Business email compromise
CaaS	Cybercrime-as-a-Service
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CoE	Council of Europe
CJEU	Court of Justice of the European Union
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed denial of service
EC	European Commission
EG	Impact of Technology Expert Group
EIPPN	European Intellectual Property Prosecutors Network
ETL	ENISA Threat Landscape
ENISA	European Union Agency for Cybersecurity
EU	European Union
FGCS	Fifth-generation computer systems
FORTRAN	Formula Translator
HNN	Hopfield neural network
IoE	Internet of Everything
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Intellectual property
IPR	Intellectual property right
IPTV	Internet protocol television

ISP	Internet service provider
LEA	Law enforcement agency
LSTM	Long Short-Term Memory
MANIAC I	Mathematical Analyzer, Numerical Integrator, and Computer
MASP	General Multi-Annual Strategic Plan
MITI	Ministry of International Trade and Industry of Japan
MS	Member State(s) (of the European Union)
NLP	Natural language processing
OCR	Optical character recognition
OAP	Operational Action Plan
PSP	Payment service provider
SIENA	Secure Information Exchange Network Application
SP2025	EUIPO Strategic Plan 2025
TLD	Top-level domain
UBA	User behaviour analytics
UNICRI	United Nations Interregional Crime and Justice Research Institute
WIPO	World Intellectual Property Organization

Definitions

The following terminology and definitions will be used in this study.

3D printing: the field of printing 3D objects. The cycle begins with a digital file in which the item to be printed is digitally arranged using either 3D printing software or a 3D scanner. This digital file is then exported to a 3D printer, which uses dedicated software to assemble the digital model into a physical object by building liquid material up in layers that then harden until the finished object emerges.

Artificial intelligence: a subfield of computer science focused on developing computer systems that can perform tasks that would normally require human intelligence. These systems are designed by humans, and when given a complex goal can act in the physical or digital dimension. In the context of this study, AI is understood as computer code (implemented in software and hardware) that dynamically adapts according to algorithmic rules as large datasets are processed, with the aim of predicting phenomena and assisting decision-making.

Artificial neural networks (ANN): computer systems intended to mimic the way the human nervous system analyses and processes information. They are based on the functioning of the human brain, with interconnected neurons that process information by transmitting it towards (inputs) and away from (outputs) the brain. ANNs are a subset of machine learning (ML) systems and are at the centre of deep learning algorithms.

Algorithm: a series of instructions and rules that a computer must follow to complete an assignment, which can be used to handle and process data and perform calculations or various other actions.

Cloud computing: the process of storing and accessing data and other programs on the internet rather than on a computer hard drive.

Computer speech: the capability of a machine to apply speech recognition and synthesis to create human-like speech. AI can be used in speech recognition, natural language processing (NLP), and translation. Several speech recognition applications are generated by automatic speech recognition, conversion of audio to text, and processing the text to determine its meaning.

Convolutional neural network (CNN): a type of neural network that has one or more convolutional layers (in which a filter is applied to an input that results in an activation). CNNs are mainly used for image processing, classification, and segmentation, as well as for other auto-correlated data. They are deep learning neural networks designed for processing structured arrays of data such as images.

Copyright: is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, plays, music, paintings, photographs, sculpture, films and choreography, to computer programs, databases, advertisements, maps, technical drawings and architecture. For the purposes of this study, references to copyright include the 'related rights' set forth in copyright-related treaties administered by WIPO and relevant EU directives.

Cryptography: the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Deep learning (DL): a subset of machine learning that uses a special type of algorithm known as a neural network and that is able to process a wider range of data resources. In some cases, it may require less human data pre-processing to achieve more accurate results than other machine learning approaches. DL must have more than three layers of neurons (including input and output).

Design: the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation (Article 3 of Regulation (EC) 6/2002 on Community designs). At international level, design rights are understood somewhat differently; that is, non-EU countries may not recognise a design as a stand-alone right. Instead, these countries may protect designs through a combination of other intellectual property laws, such as patent, trade mark and copyright laws.

Expert system (ES): a subfield of AI concerning the use of a computer program designed to solve complex issues and imitate a human expert's decision-making ability through extracting knowledge from its knowledge base and using reasoning and inference rules in accordance with user queries.

Explainable AI (XAI): a set of processes and methods that enables users to understand and trust the results generated by machine learning algorithms. XAI can be defined as AI that produces details or reasoning to make its functioning clear or easy to understand.

Generative adversarial networks (GANs): generative models used in machine learning frameworks that can create new data instances that resemble the training data. GANs are algorithmic architectures that use two neural networks, pitting one against the other to generate new, synthetic items of data that can pass for real data.

Generative design: a design exploration process in which designers or engineers select specific goals to add to the generative design software, along with selected parameters including performance or spatial requirements, materials, manufacturing methods, and cost constraints.

Infringement: a term that covers directly IP-infringing acts as well as contributory and preparatory acts and other closely related illegal acts or criminal offences (e.g. cybercrime offences, money laundering, etc.)

Intellectual property (IP): creations of the mind, such as: inventions; literary and artistic works; designs; and symbols, names and images used in commerce. IP is protected in law by patents, design, copyright, trade mark and trade secret law, which enable people to earn recognition or financial benefit from their inventions or creations.([1])

Intellectual property infringement: the unauthorised use, translation, adaptation, reproduction, or sale of materials or products that are legally regarded as protected intellectual property (IP), as defined in the relevant legislation.

Internet of Things (IoT): a network of physical objects – 'things' – that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools.

Machine learning (ML): a subfield of AI focused on creating applications that learn from data and can progressively improve their accuracy. This process allows the system to develop beyond the data and algorithms with which it was originally provided, with a view to achieving independent development and learning based on previous experience gained in the same manner.

([1]) WIPO, "What is Intellectual Property?" https://www.wipo.int/about-ip/en/

Malicious software (malware): software designed to carry out an unauthorised process that will have an adverse impact on the privacy, integrity, or accessibility of an information system. This term commonly includes viruses, worms, Trojan horses, and other code-based processes that infect a host, as well as spyware, and some forms of adware.

Natural language processing (NLP): a subfield of AI focused on providing machines with the ability to read, understand and derive meaning from human languages. NLP adopts a cognitive approach by enabling the extraction of data to create relations, making it possible to identify figures of speech and perform sentiment analysis.

Quantum computing: an area of computing focused on developing computer technology based on the principles of quantum mechanics, a mathematical machine used to predict the behaviours of microscopic particles or to measure instruments created to explore those behaviours.

Recurrent neural network (RNN): a type of artificial neural network that uses sequential or time series data. While traditional deep neural networks assume that inputs and outputs are independent of each other, the output of recurrent neural networks depends on the prior elements within the sequence.

Reinforced learning: a behavioural model similar to supervised learning, but one in which the algorithm is not trained using sample data; rather, the model learns through trial and error. The system must iteratively test solutions independently to discard or further develop them. This process is driven by ‘rewards’ for appropriate solutions and ‘punishments’ for unsuccessful approaches.

Robotics: a branch of engineering encompassing the conception, design, manufacture, and operation of robots. This field frequently overlaps with other related fields such as electronics, computer science, artificial intelligence, mechatronics, nanotechnology and bioengineering.

Supervised learning: a category of machine learning in which the AI system starts by knowing the right answers by receiving an input-output pair; it must then adjust the algorithms so that the answers are as accurate as possible from the existing dataset, meaning that supervised learning can calculate an output when given a certain input.

Trade secrets: a form of intellectual property that protects confidential information that may be sold or licensed. To be considered a trade secret, the information must be commercially valuable because it is secret, be known only to a limited group of persons, and be subject to reasonable steps taken by the rightful holder of the information to keep it secret, including the use of confidentiality agreements for business partners and employees. In the EU, civil protection of trade secrets is regulated by Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Law enforcement varies depending on the criminal laws of each Member State.

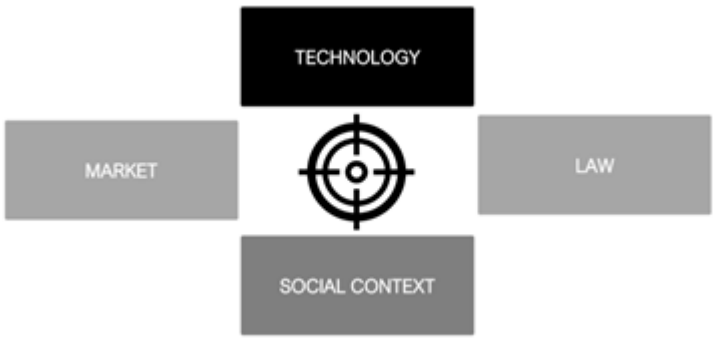
Unsupervised learning: a category of machine learning that processes a large amount of unlabelled data without an input-output configuration and uses algorithms to extract meaningful features needed to label, sort, and classify data in real time, without human intervention.

Executive Summary

Background

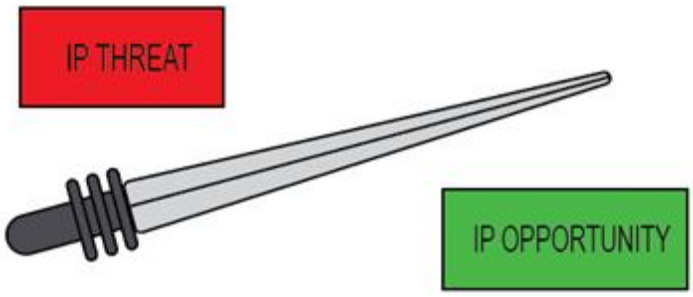
In early 2019, the European Union Intellectual Property Office (EUIPO) established an Impact of Technology Expert Group (EG). The group is composed of experts with knowledge of and practical experience in monitoring the impact of new and emerging technologies on the infringement and enforcement of intellectual property rights. The EG follows a specific approach based on an adaptation of Lawrence Lessig's 'Code and Other Laws of Cyberspace' theory (the Code Theory), which describes how human online activity is regulated by law, social norms, and the market, taking into consideration the internet's technical infrastructure (referred to as 'code'). The Code Theory has been adapted by the EG in the sense that it believes all technological impact on intellectual property should be considered from four angles: the market; the law; the social context; and the technology itself.

Expert Group's adaptation of Lessig's Code Theory



The approach followed in analysing the impact of new technologies on IP can be described using the 'double-edged sword' metaphor shown in the figure below. The starting point is the consideration that the use of a particular technology either to infringe IP or to protect and enforce them presents, to some extent, the same features in each case. This metaphor also suggests that there may be weaknesses in the application of technologies on each side that can be exploited by the other.

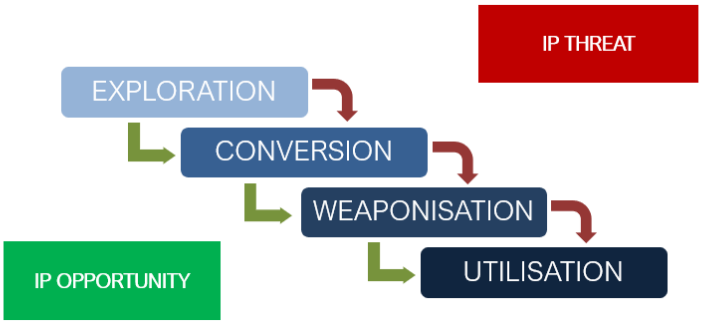
The 'double-edged sword' metaphor



The EG developed a unique methodology called the 'Intellectual Property Tech Chain', which is described in detail in its first report, published in September 2020, entitled 'Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020'. According to this methodology, the development of any application follows four steps:

- **exploration**, i.e. assessing the technology to ascertain whether it could be used to infringe or protect/enforce IP;
- **conversion** of the technology to enable the achievement of the identified goal;
- **weaponisation**, i.e. finalising the application's development;
- **utilisation**, i.e. actual monetisation or use of the application to infringe or protect/enforce IP.

The 'Intellectual Property Tech Chain'



In 2021, the EUIPO commissioned the United Nations Interregional Crime and Justice Research Institute (UNICRI) to carry out the first deep-dive research project applying this methodology in cooperation with the Impact of Technology Expert Group.

The current crime landscape was considered when drafting this study. The yearly strategic Internet Organised Crime Threat Assessment (IOCTA) report, produced by Europol's European Cybercrime Centre (EC3), provides an overview of the emerging threats and developments in the cybercrime landscape. In 2020, the highest-priority threats included social engineering, ransomware, and other forms of malware. It is essential to consider the impact of the 'cyber-' element of cybercrime when analysing criminal activity, since it frequently has a bearing on nearly every aspect of this activity. In the recent IOCTA 2021 report, Europol listed the ransomware affiliate programs using supply-chain attacks to compromise the networks of large corporations and public institutions and deploy new multi-layered extortion methods, overlayered mobile malware attacks, and distributed denial of service (DDoS) for ransom. Chapter 5 of this study will explain how these threats are also relevant in the context of copyright and designs.

The development and evolution of cybercrime must also be considered in conjunction with the misuse of AI, including in AI-facilitated IP crime. The emerging malicious use of AI can enhance the impact of cybercrime since it is able to perfect social engineering attacks at scale and, among others, it can be used:

- for document-scraping malware to make attacks more efficient;
- to evade image recognition and voice biometrics;

- to create ransomware attacks through intelligent targeting, evasion, and data pollution by identifying blind spots in detection rules;
- to improve blockchain capabilities in online crime.

The relevance of addressing IP crime has also been raised as a priority in the current context. In May 2021, the EU's Council of Ministers included IP crime among the top 10 priorities in the fight against organised crime to be addressed in 2022-2025. On 26 May 2021, the Council adopted the conclusions setting the 2022-2025 EU priorities for the fight against serious and organised crime through the European multi-disciplinary platform against criminal threats (EMPACT).

In this context, this study aims to provide an assessment of the impact of AI technologies on both the infringement and enforcement of copyright and designs.

Methodology

The purpose of this study is to analyse the impact of AI technologies on both the infringement and enforcement of copyright and designs. These have much in common with the infringement and enforcement of other IPs (e.g. trade secrets, trade marks, and patents) through the application of AI, but this study will not take these other types of IP specifically into consideration.

This study is meant as a practical, practitioner-oriented tool to help understand the impact of AI and put this impact into a broader perspective. To this end, 20 scenarios have been developed to demonstrate existing or potential misuse of AI technologies to infringe copyright (and related rights) and designs, as well as the use of AI to enforce these same rights. The focus of enforcement of the selected IP is the application of AI in the field of law enforcement. However, there are, and will be in the future, many relevant applications of AI that overlap or have many commonalities with voluntary enforcement measures, civil enforcement, and certain aspects of administrative enforcement.

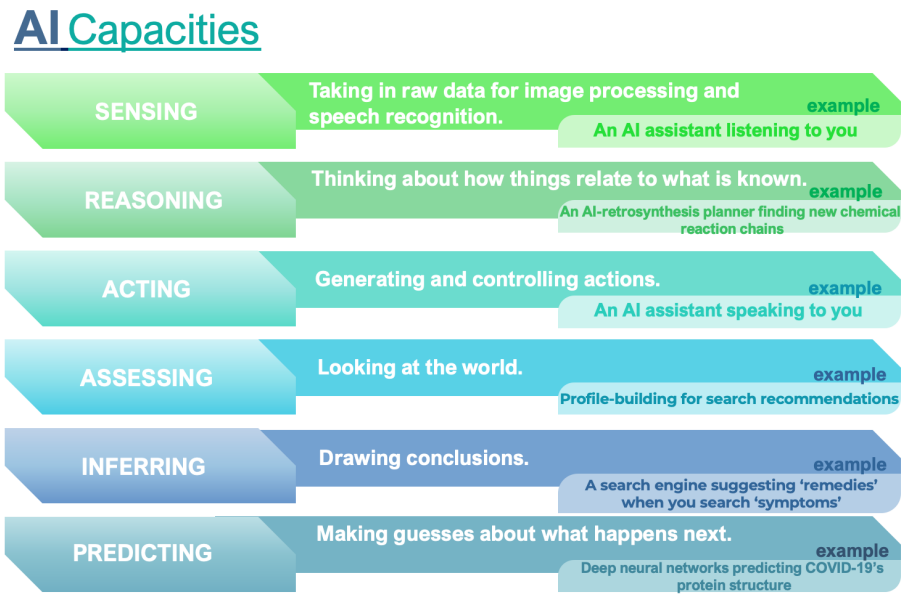
The data collection encompassed a variety of elements: a desk review study; interviews and focus group discussions; and case analysis. At the start of the project, the EUIPO facilitated contact with a broad group of experts (including the Impact of Technology Expert Group), who were invited to contribute to and support the research. The researchers then contacted other experts to supplement the information thus obtained.

Generally, experts were identified based on their knowledge of and experience with AI technologies themselves, the copyright and design infringement and enforcement landscape, and (in particular) issues surrounding the application of AI in the infringement and enforcement of copyright and designs. Many of the experts reviewed and commented on the methodology of the study, and all of them actively supported the research, including through participation in group discussions and online interviews and, whenever possible, providing case studies.

Key findings

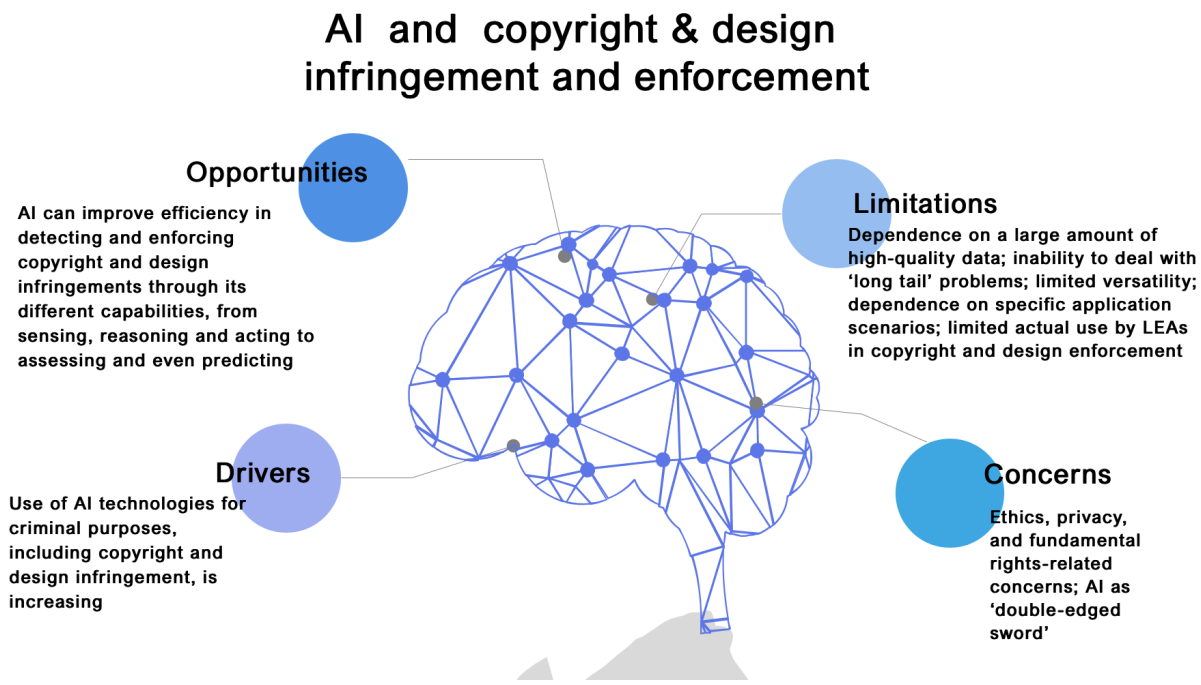
AI technologies have passed through different phases since their initial development, dating back to the late 1940s and early 1950s, but there is still no widely agreed-upon and precise definition of what AI is. It is commonly understood as a subfield of computer science focusing on developing computer systems that can perform tasks that would normally require human intelligence.

AI has various capabilities, from sensing, reasoning, and acting to assessing and even predicting.



AI has various subfields, each of which has its own specific aspects in addition to certain shared elements. These subfields pursue a number of operational objectives, including machine learning, natural language processing, computer vision, computer speech and expert systems. Quantum computing, although it is not necessarily linked to AI, could be used to enhance the capacity of AI applications, while explainable AI, encompassing a set of processes and methods, enables users to understand and trust the results generated by ML algorithms.

Against this background, the study found that there are multiple **opportunities**, **drivers**, **limitations** and **concerns** regarding the use of AI in infringement and enforcement of copyright and designs.



There are several **opportunities** for AI to improve efficiency in detecting copyright and design infringements and in enforcing copyright and design rights, since it can be used to perform a number of different functions ranging from sensing, reasoning and acting to assessing and even predicting. Currently, the main areas of AI development are machine learning, natural language processing, computer vision, expert systems, and explainable AI. Explainable AI is currently receiving increased attention by experts and policy makers. Other technologies enhanced by AI, such as quantum computing, blockchain, 3D printing, generative design, cloud services, and robotics also have great potential. AI can identify and prioritise risks, instantly spot malware on a network, guide incident

response, and detect intrusions before they occur. For example, machine learning stands out as a key AI subfield that can be used to develop law enforcement tools such as the analysis of large amounts of information to detect threats and identify social engineering bots, scanning of images to detect false pages or illicit content, improving automatic content recognition (ACR) tools, and providing insights to find infringement patterns.

Natural language processing can be used to analyse and block cyberattacks like phishing, identify the behaviour of fraudsters, and create a correlation analysis aimed at promptly identifying infringements. Computer speech and computer vision are also successfully employed in this field. Some of their uses include pattern recognition to predict future infringements, detection of marketing of infringing goods, and the detection and analysis of fraudulent logos or other images. Quantum computing could be adopted to improve AI tools, enabling them to process larger amounts of data. For example, AI and quantum computing can be used by customs and law enforcement authorities to recognise patterns within large datasets and identify similarities. Expert systems, on the other hand, can be used by law enforcement to decide which strategy is more adequate to protect a system from specific vulnerabilities, including those linked to copyright and design infringements.

As for the **drivers**, the various capabilities of AI make it attractive for malicious actors. AI can emulate many acts performed by humans and in some instances can exceed human performance in terms of efficiency and scalability. Moreover, certain crimes – with the support of AI technologies – can be performed on a much larger scale, targeting thousands of victims simultaneously. As depicted by the double-edged sword metaphor, the same technologies can be used both by malicious actors and for enforcement purposes, including in the field of copyright and designs. Fraudsters and criminal groups employ or may employ the same AI techniques used by enforcement agencies to overcome cybersecurity measures and evade detection. This is known as the ‘AI/cybersecurity conundrum’: as AI matures and is increasingly used in the field of cybersecurity, the potential downsides of this technological advance increase as well. In this regard, adversarial machine learning could help to spot and to overcome cybersecurity measures, including breaking through defences and developing dynamic malware to evade detection. AI technologies can be used to make such attacks more efficient, as in the case of AI-supported password guessing and CAPTCHA breaking. Furthermore, natural language processing tools can be employed to produce deepfake music videos, and generative design-based tools can be used in the manufacture of infringing copies.

Finally, it is worth keeping in mind that there is always a human being behind any AI algorithm and its practical application vectors. Explainable AI, though it does not solve all possible issues, could be used by law enforcement authorities as part of an increased use of innovative tools – including AI – in analysis and prediction, while at the same time better achieving the prerequisites of fairness, accountability and transparency. The use of AI in law enforcement and the judiciary should in any case always be subject to strong safeguards and human oversight through built-in human control.

The current **limitations** of AI include, in particular: its dependence on a large amount of high-quality training data; its inability to deal with long-tail problems (i.e. the difficulty and cost required for AI to achieve strong performance at the 'long tail' of data distribution); its limited versatility; its dependence on specific application scenarios; and the inherent biases of the AI's developer. More powerful machine learning algorithms can learn complex non-linear relationships between input and output data, but to do so they require a large amount of quality data. Machines still need to understand the world through perceptual and cognitive learning in a more accurate manner, enabling them to simulate real-world scenarios through reinforcement learning to perceive information and then transform that perceived information into abstract knowledge through attention, memory, and understanding. This might be achieved through the intersection, integration, and optimisation of algorithms and the continuous improvement of academic study. In addition, notwithstanding the expanded use of innovation technologies in law enforcement, according to the interviews undertaken in the context of this study the actual use of these technologies by public authorities to enforce copyright and designs is still generally limited. Furthermore, law enforcement and customs authorities will need to continuously monitor the new technology landscape to ensure they are properly prepared and trained.

Finally, the development and application of AI has raised some **concerns** related to ethics, privacy and fundamental rights. As AI and related technologies are used to make determinations and predictions in areas of great importance such as combating criminality, including copyright and design-related crime, AI has the potential to impact fundamental human rights in profound ways. AI algorithms are powered by data collected and processed by technologies that increasingly surround us at every minute of our lives.

Many experts argue that AI algorithms must be built to align with overarching human goals. The EU Parliament, in its recent Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), has clearly stated that 'AI should not be seen as an end in itself, but as a tool, with the ultimate aim of increasing human well-

being, human capabilities and safety'. As a result, the fundamental human right to privacy must be duly considered when data is collected by law enforcement authorities. Algorithms and AI should be 'ethical by design', with no built-in bias, in a way that guarantees maximum protection of fundamental rights. The EU Parliament in the same resolution invites 'European stakeholders, including the Member States and the Commission, to ensure, through international cooperation, the engagement of partners outside the EU in order to raise standards at international level and to find a common and complementary legal and ethical framework for the use of AI'. Policy makers are invited to be actively involved and to draw the legal boundaries within which these technologies are allowed to operate. Retroactive deconstruction of an algorithm may be required to assess the factors that influence a model's predictions.

1 Structure, background, and context of the study

As an introduction to this study on the impact of artificial intelligence technologies on the infringement and enforcement of copyright and designs, this chapter presents the study's structure, as well as the background and overall context within which it was developed.

1.1 Structure and content of the study

The study comprises five chapters, two annexes and the bibliography. The present chapter describes the study's background and context, starting from the current criminal landscape, which involves cybercrime and organised criminal involvement in IP crime. Chapter 1 also presents the 'Intellectual Property Tech Chain' methodology developed by the EUIPO's Impact of Technology Expert Group, which is applied in the study, and the main elements of the EUIPO's Strategic Plan 2025 (SP2025) related to AI and its work in support of the European multi-disciplinary platform against criminal threats (EMPACT).

Chapter 2 outlines the study's goals and target audience and presents its data acquisition and analysis methodology, including 20 fictional scenarios linked to two storylines concerning copyright and designs of physical products and digital content; these scenarios illustrate the infringement and enforcement possibilities of AI.

Chapter 3 introduces the background information relevant to understanding the main technological concepts used in the study. In addition, this chapter describes the main 'streams' and techniques of the technology that will be referred to in the fictional scenarios presented in Chapter 5 as possible infringement and enforcement tools. Finally, this chapter addresses the societal impact of AI technologies to help the reader understand the context in which these technologies operate or could operate in the future.

Chapter 4 offers a bird's-eye view of AI as applied in the infringement and enforcement of copyright and designs, focusing on various relevant AI technologies. The description of each technology aims to clarify its meaning and scope of application, in order to facilitate comprehension of the scenarios in

Chapter 5. Alongside the ‘streams’ and techniques presented in Chapter 3, these applications of AI illustrate its various elements and uses in combination with other tools.

Chapter 5 presents 20 fictional scenarios related to the possible use of AI technologies and tools in the infringement and enforcement of copyright and designs. These scenarios are based on two storylines, one centring on physical products and another on digital content. Technological tools were analysed for each scenario to provide examples of the adoption of AI in both infringement and enforcement.

The conclusion presents the key findings in terms of opportunities, drivers, limitations and concerns related to the use of AI in copyright and designs. Annex 1 contains the list of experts who agreed to be interviewed and mentioned in the study, while Annex 2 provides more in-depth information on the different aspects of AI technologies covered in the core text.

1.2 Current internet crime and artificial intelligence-supported crime threat landscape

The current cybercrime landscape, and the role of artificial intelligence and new technologies in illegal activities on the internet, must be considered in assessing these technologies’ impact on the infringement and enforcement of copyright and designs.

AI and other new technologies represent opportunities for malicious actors, who can use them to facilitate and enhance their attacks, exploit new victims, and create more innovative criminal business models while reducing the chances of being caught ([2]). The following chapters of this study will describe in detail AI’s relevance to the field of IP and design infringement.

Every year, Europol's European Cybercrime Centre (EC3) produces the Internet Organised Crime Threat Assessment (IOCTA), focusing on emerging threats and developments in the cybercrime landscape. It is essential to consider the impact of the 'cyber-' element of cybercrime in analysing criminal activity, since it frequently has a bearing on nearly every aspect of this activity.

([2]) Trend Micro, UNICRI & Europol. (2020). Malicious uses and abuses of artificial intelligence. https://www.europol.europa.eu/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-–-and-it’s-not-just-deep-fakes.

In 2020, the highest-priority threats included social engineering, ransomware, and other forms of malware; Chapter 5 of this Study will show how these threats are also relevant to copyright and designs. According to the IOCTA, cybercriminals have refined their methods, making their work available to others, for instance, through so-called Cybercrime-as-a-Service (CaaS) ([3]). Criminal activity has in fact evolved significantly due to the supply of readily available data (including personal and other sensitive information) and the existence of a CaaS community helping criminals to carry out highly targeted attacks. In this context, data compromise is a central aspect of several threats. This is also true of copyright and design infringement.

The development and evolution of cybercrime can also be considered in conjunction with the misuse of artificial intelligence, including in the AI-facilitated IP crime. In particular, the emerging malicious use of AI can enhance the impact of cybercrime. AI can undertake social engineering attacks at a larger scale; it can be used to make attacks by document-scraping malware more efficient; and it can be used to evade image recognition and voice biometrics. AI-based ransomware attacks can perform intelligent targeting and evasion or data pollution by identifying blind spots in detection rules. Finally, AI can also improve blockchain capabilities in online crime.

Law enforcement authorities, including those involved in the enforcement of IP and designs, face several challenges. The ability of AI to upscale criminality without physical proximity, blurring jurisdiction and providing stronger tools for obfuscation and anonymisation in the new criminal structures and methods, and the evolution of CaaS to offer more elaborate AI-supported services, in combination with decentralised blockchain solutions, are threats that need to be effectively addressed.

In the recent IOCTA 2021 report, Europol emphasised that the current global pandemic has accelerated ongoing changes cybercrime, including innovation among cybercriminals, who have sought to capitalise on new opportunities. Among its key findings, Europol listed ransomware affiliate programs that use supply-chain attacks to compromise the networks of large corporations and public institutions and employ new multi-layered extortion methods, overlayered mobile malware attacks, and DDoS (Distributed Denial of Service) for ransom. Criminals also use the names of well-known Advanced Persistent Threat (APT) groups to scare their targets into complying with ransom demands.

([3]) Europol. (2021). Internet organised crime threat assessment (IOCTA) 2021.https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021.

Furthermore, IOCTA 2021 recognised that the pandemic continues to have a significant impact on the European online fraud landscape, where phishing and social engineering are still the principal vectors for payment fraud and investment fraud. However, business email compromise (BEC) and CEO fraud also remain key threats. In addition, dark web users are increasingly adopting anonymous cryptocurrencies. All these elements will be further analysed in the context of copyright and designs.

The European Union Agency for Cybersecurity (ENISA), in its 2021 ENISA Threat Landscape (ETL) annual report, confirmed EUROPOL's findings. The ELT identified the following primary threats: 1) ransomware; 2) malware; 3) cryptojacking ([4]); 4) email-related threats; 5) threats against data; 6) threats against availability and integrity; 7) disinformation/misinformation; 8) non-malicious threats; and 9) supply chain attacks ([5]). Cybercriminals are increasingly motivated by monetisation, including the monetisation of stolen information through data auctions on the dark web and the increased use of ransomware. Cryptocurrency continues to be the most common payout method for threat actors.

Threats against data, frequently referred to as data breaches or data leaks, involve the release of sensitive, confidential, or protected data into an untrusted environment. One of the consequences of relevant threats against data that can be observed is the fact that approximately 58 % of supply chain attacks were aimed at gaining access to data (predominantly customer data, including personal data and intellectual property). Compromise through phishing emails, and brute-forcing of remote desktop services (RDP) remain, according to ENISA, the two most common ransomware infection vectors ([6]).

In 2021, traditional DDoS campaigns have become more targeted, more persistent, and increasingly multi-vector, and have been amplified by the COVID-19 pandemic. The IoT is also used as a threat vector for DDoS. Attackers can build massive botnets to launch DDoS attacks or distribute malware ([7]).

While the threat of the criminal use and abuse of AI can be seen as overwhelming and far-reaching, it important to stress that this technology also provides law enforcement authorities with potentially powerful tools, since it can enhance the currently available tools by providing better data management for, inter alia, risk analysis, open-source intelligence (OSINT) techniques, and image and text

([4]) Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.
([5])European Union Agency for Cybersecurity (ENISA). (2021). ENISA Threat Landscape 2021. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
([6]) European Union Agency for Cybersecurity (ENISA). (2021). Op. cit., p. 9.
([7]) European Union Agency for Cybersecurity (ENISA). (2021). Op. cit., p. 69.

detection. The current study will therefore also present possible uses of AI technologies for the enforcement of copyright and designs.

1.3 IP crime among the top 10 priorities in the fight against organised crime

In Europe, the fight against IP crime is also of great importance due to the involvement of criminal networks. In May 2021, the EU's Council of Ministers included IP crime among its top 10 priorities in the fight against organised crime ([8]) for 2022-2025 ([9]), which will be addressed through the European multi-disciplinary platform against criminal threats (EMPACT).

The 10 priorities that have been identified for 2022-2025 are the following:

1) high-risk criminal networks;
2) cyberattacks;
3) trafficking in human beings;
4) child sexual exploitation;
5) migrant smuggling;
6) drug trafficking;
7) fraud, economic and financial crimes;
8) organised property crime;
9) environmental crime;
10) firearms trafficking.

EMPACT Priority 7 targets fraud, economic and financial crimes. It proposes, inter alia, 'to combat and disrupt criminal networks and criminal individual entrepreneurs involved in IP crime and in the production, sale or distribution (physical and online) of counterfeit goods or currencies, with a specific

([8]) The United Nations Convention against Transnational Organized Crime (2000) provides an internationally agreed upon definition of an organised criminal group as 'a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit.' This definition was also adopted in the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime.
([9]) https://www.consilium.europa.eu/en/press/press-releases/2021/05/26/fight-against-organised-crime-council-sets-out-10-priorities-for-the-next-4-years/.

focus on goods harmful to consumers' health and safety, to the environment and to the EU economy' ([10]).

Through EMPACT, the EU has adopted an integrated approach to its internal security, involving measures that range from external border controls, police, customs and judicial cooperation to information management, innovation, training, prevention, and the external dimension of internal security. It began in 2010, setting the EU's law enforcement priorities, with a focus on serious and organised crime. It is an intelligence-led and EU Member State-driven cooperation instrument that allows Member States, agencies, and other actors to work closely to address key criminal threats, using tools such as law enforcement training and joint operations to dismantle criminal networks and their structures and business models.

EMPACT works with General Multi-Annual Strategic Plans (MASPs) across Common Horizontal Strategic Goals for all the Operational Action Plans (OAPs) that will be implemented within each plan. This approach aims to strengthen consistency and coherence among OAPs as well as the multi-disciplinary and multi-agency approach.

EMPACT continuously considers the role and impact of emerging technologies in its priority assessment. In this context, the EUIPO will be actively involved in supporting the implementation of this priority within the EMPACT framework ([11]).

1.4 The EUIPO's Impact of Technology Expert Group

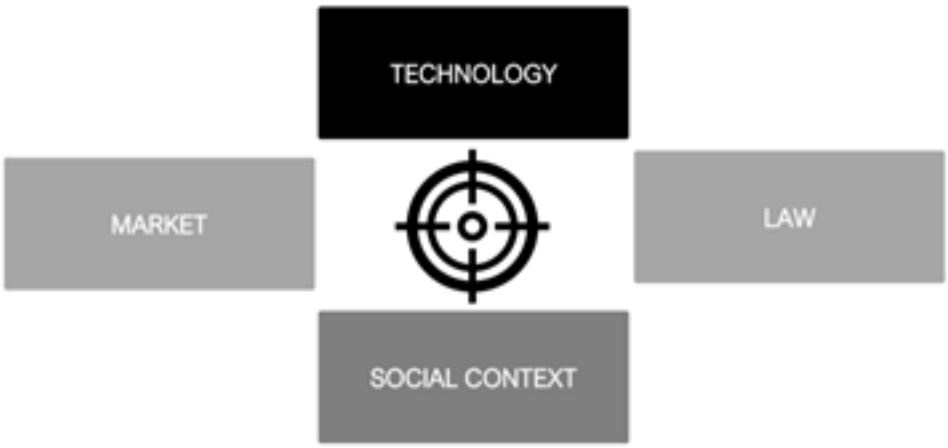
In 2019, the EUIPO established an **Impact of Technology Expert Group** to discuss and monitor the influence of emerging technologies on the protection, infringement, and enforcement of intellectual property rights.

The Expert Group (EG) follows a specific approach based on an adaptation of Lawrence Lessig's 'Code and Other Laws of Cyberspace' theory ([12]), which describes how human online activity is

([10]) EUROPOL (2021). EU Policy Cycle EMPACT. EMPACT 2022+ Fighting crime together. https://www.europol.europa.eu/empact.
([11])EUIPO (2021). IP crime among the 10 priorities in the fight against organised crime. https://euipo.europa.eu/ohimportal/en/web/guest/news/-/action/view/8720583.
([12]) Lessig, L. (1999). Code and Other Laws of Cyberspace. Basic Books.

regulated by law, social norms, and the market, taking into consideration the internet's technical infrastructure (named 'code'). Lessig's Code Theory is applied by the EG in the sense that it believes all technological impact on IP should be considered from four angles: the market; the law; the social context; and the technology itself (see Figure 1).

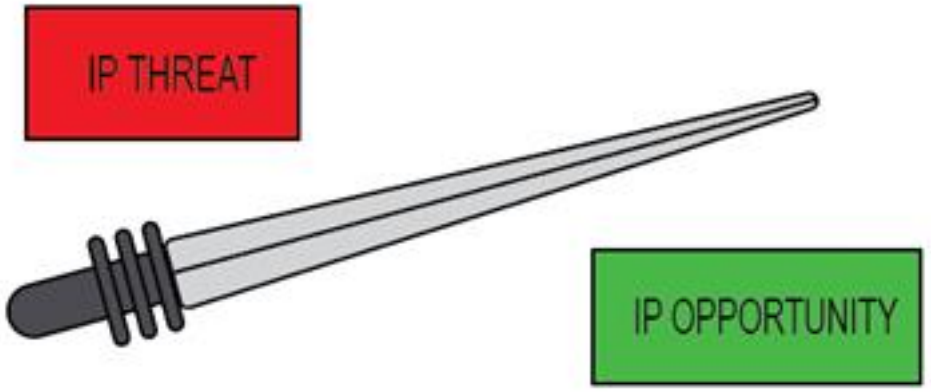
Figure 1 – The EG's adaptation of Lessig's Code Theory



The EG's approach in analysing the impact of new technologies on IP can be described using the 'double-edged sword' metaphor shown in the figure below. The starting point is the consideration that the use of a particular technology either to infringe IP or to protect and enforce them presents to some extent the same features in each case. This metaphor also suggests that there may be weaknesses in the application of technologies on each side that can be exploited by the other ([13]).

([13]) EUIPO (2020). Intellectual Property Infringement and Enforcement. Tech Watch Discussion Paper 2020. p. 21. https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2020_Tech_Watch_paper/2020_IP_Infringement_and_Enforcement_Tech_Watch_Discussion_Paper_Full_EN.pdf.

Figure 2 –The 'double-edged sword' metaphor



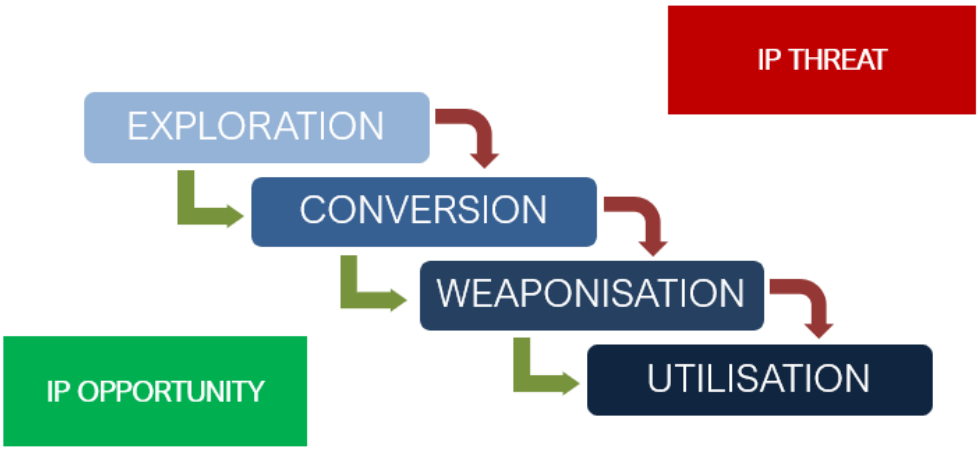
Source: 'Intellectual property infringement and enforcement' (EUIPO, Tech Watch discussion paper, 2020)

The first tangible result of the Impact of Technology Expert Group's work has been the development of a unique methodology to be applied in each Tech Watch activity called the 'Intellectual Property Tech Chain', as described in the 'Intellectual property infringement and enforcement' discussion paper ([14]). According to this methodology, the development of any application of a technology follows four steps (see Figure 3 below):

- **exploration**, or assessment of the technology to ascertain whether it could be used to infringe or protect/enforce IP;
- **conversion** of the technology to enable the achievement of the identified goal;
- **weaponisation**, or finalisation of the application's development;
- **utilisation**, or actual monetisation or use of the application to infringe or protect/enforce IP.

([14]) EUIPO, op. cit.

Figure 3 – The 'Intellectual Property Tech Chain' methodology



Source: 'Intellectual property infringement and enforcement' (EUIPO, Tech Watch discussion paper, 2020, p. 8)

For each application of a technology, the methodology distinguishes between proactive and reactive approaches. The proactive approach refers to applications developed to achieve a specific goal without responding to a specific threat. The reactive approach, on the other hand, refers to applications developed in response to a specific threat.

In 2021, the EUIPO commissioned the United Nations Interregional Crime and Justice Research Institute (UNICRI) ([15]) to carry out the first deep-dive research project applying this methodology in cooperation with the Impact of Technology Expert Group.

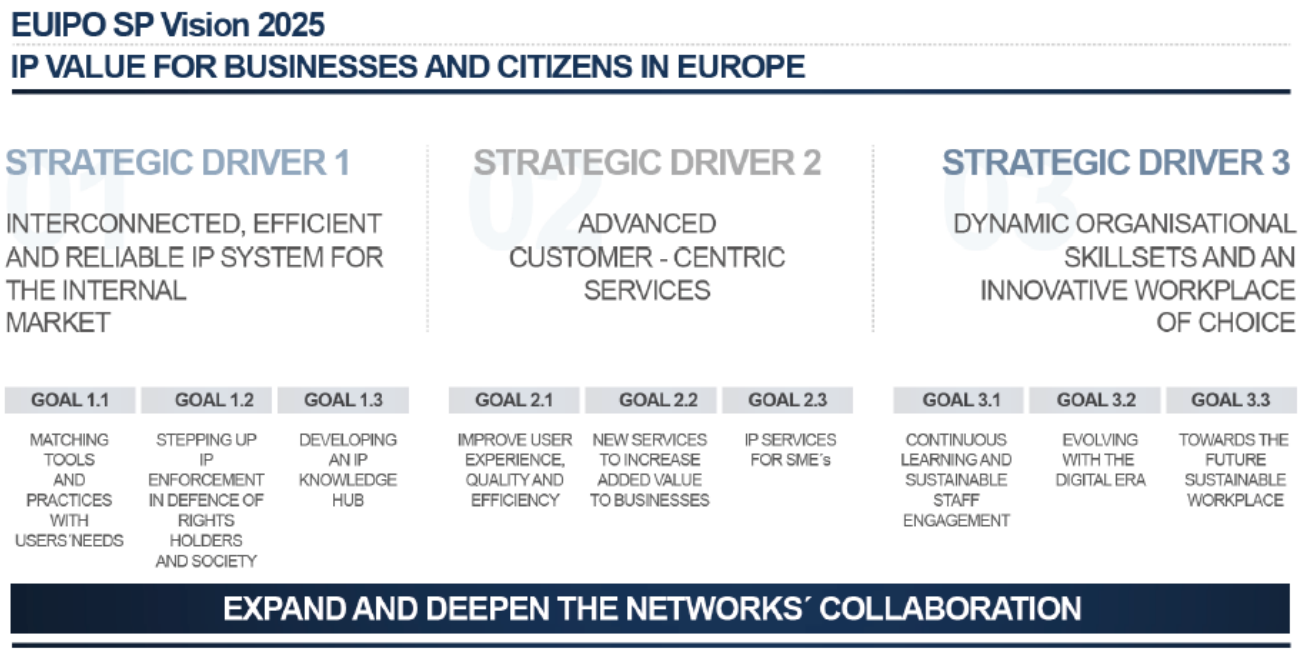
([15]) The UNICRI team comprises Marco Musumeci, UNICRI Programme Manager, and three international consultants: Vittoria Luda di Cortemiglia, John Zacharia and Mariana Diaz Garcia. This team authored the study, with valuable contributions by the EUIPO's Erling Verstergaard.

1.5 Artificial intelligence in the EUIPO's Strategic Plan 2025

Innovation, new technologies and artificial intelligence are important areas of the EUIPO's work. The EUIPO's Strategic Plan 2025 (SP2025) ([16]) aims to provide customer-centric services and contribute to a stronger IP system, efficient enforcement, and better understanding of IP rights in a global and increasingly digital environment by building and promoting sustainable networks, thereby supporting competitiveness, innovation, and creativity in the EU.

The SP2025 foresees three 'strategic drivers'. The first focuses on an 'interconnected, efficient and reliable IP system for the internal market' and the second is dedicated to 'advanced customer-centric services'. The third, entitled 'dynamic organisational skill sets and an innovative workplace of choice', includes a specific objective (Goal 3.2 – Evolving with the Digital Era) dedicated to innovation and artificial intelligence, representing a great opportunity for businesses.

Figure 4 – EUIPO Strategic Plan 2025



Source: EUIPO (2020). Strategic Plan 2025, p.15.

([16]) European Union Intellectual Property Office (EUIPO) (2020). Strategic Plan 2025. https://euipo.europa.eu/ohimportal/strategic-drivers.

Goal 3.2 seeks further opportunities for the EUIPO to harness its current AI-based solutions in a wide variety of business cases, including formalities, classification, image search, goods and services comparison, and chatbots. To this end, machine learning, natural language processing and deep learning techniques will be employed. All these solutions will be described further in Chapter 3. Quality control will be performed to avoid the most common pitfalls of machine learning implementation, namely discrimination, vulnerability to misuse, violation of privacy, failure to perform and lack of explainability ([17]).

1.6 AI in criminal law and its use by the police and judicial authorities in criminal matters

To conclude this introductory chapter, it is important to emphasise that the use of AI by police and judicial authorities is currently the subject of much debate in Europe. In October 2021, the European Parliament issued a resolution on AI in criminal law and its use by the police and judicial authorities in criminal matters ([18]). The resolution recognises AI's strategic position and potential to generate substantial benefits in terms of efficiency, accuracy, and convenience, and to increase human well-being, capabilities, and safety. However, it also emphasises the significant possible risks that it poses to fundamental rights and democracies based on the rule of law.

One of the resolution's central considerations is the guarantee of fundamental rights and freedoms throughout the life cycle of AI and related technologies, especially during their design, development, deployment, and use. This should apply to the enforcement of the law under all circumstances. This perspective puts people at the centre, demanding an AI worthy of public trust that always works in the service of humans. The EU Parliament resolution also emphasises that AI systems should be designed so that they can always be shut down by a human operator. This needs to be accompanied by a clear model for assigning criminal responsibility for the potential harmful effects of AI systems, since regulatory provisions in this field must always maintain human accountability.

The resolution emphasises that the use of AI in law enforcement may entail several significant risks to the fundamental rights of individuals, including: opaque decision-making; various types of

([17]) EUIPO (2020). IP Innovation. Strategic Driver 03. Goal 3.2 Evolving with the Digital Era. https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/contentPdfs/Strategic_Plan_2025/project_cards/SD3_Artificial_Intelligence_implementation_PC_en.pdf.

([18]) European Parliament (2021). Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). 6 October. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html.

discrimination and errors inherent in the underlying algorithm, which can be reinforced by feedback loops; and risks to privacy and personal data, freedom of expression and information, the presumption of innocence, the right to an effective remedy and a fair trial, and individual freedom and security. In addition, AI systems used by law enforcement and the judiciary can be vulnerable to AI-powered attacks against information systems or data poisoning. For these reasons, the European Parliament highlights the importance of having AI systems that are safe, robust, secure, and fit for purpose, and that respect the principles of fairness, data minimisation, accountability, transparency, non-discrimination and explainability.

The issue of how to properly collect and present evidence of the use of AI is outside the scope of this study, as criminal law and procedure vary (sometimes significantly) among the different EU Member States in prescribing how investigators and prosecutors must collect and present electronic evidence.

It is nonetheless important for investigators and prosecutors to keep in mind the issue of proper electronic evidence collection and presentation when AI is involved in a criminal copyright or design infringement case. Like other forms of electronic evidence, investigators must consider how best to identify and preserve digital evidence establishing how a criminal has used AI to infringe copyright and design rights, and prosecutors must think strategically about how best to present this evidence properly and effectively in court to prove that a defendant has committed criminal copyright or design infringement. This process of identifying, preserving, and presenting electronic evidence can certainly be more challenging than it is with more traditional non-electronic evidence. Nevertheless, the challenges remain largely the same whether the electronic evidence relates to the use of AI or any other form of electronic evidence. For example, investigators and prosecutors will often have to work with digital-forensic experts regardless of the type of electronic evidence in question.

At the same time, investigators and prosecutors may have to identify and work with experts in the type of electronic evidence in question (such as AI-related evidence) as they build and prove their criminal copyright and design infringement cases. Therefore, investigators and prosecutors should keep abreast of the ways in which the emergence of new types of technology, such as AI, may impact how they collect electronic evidence of the use of this technology in a criminal investigation and present it in court during a criminal prosecution.

2. Scope and methodology

The purpose of this study is to assess the impact of artificial intelligence technologies and applications on both the infringement and enforcement of copyright and designs. The study targets law enforcement officers, prosecutors, and judges, as well as policymakers, rights holders, and civil society, and is meant as a practical, user-friendly, and problem-oriented tool. It aims to be easily accessible to an audience familiar with IP issues but without prior in-depth knowledge of AI technologies. For this reason, 20 different scenarios have been developed to illustrate possible copyright and design infringements using AI technologies, as well as the use of AI in the enforcement of copyright and designs. The scenarios have been devised to be well-suited for workshop discussions, seminars and other means of capacity-building and networking.

AI is an emerging and disruptive technology. It has a growing number of practical implications that will profoundly affect the protection, management, infringement, and enforcement of all types of IP. For the purposes of this study, the term 'infringement' covers directly IP-infringing acts targeting copyright and design rights as well as similarly directed contributory and preparatory acts and other closely related illegal acts or criminal offences (e.g. cybercriminal offences and money laundering).

The following types of IP are the main focus of the study:

- copyright – digital content;
- copyright – applied art;
- copyright – other copyright-protected physical products;
- rights related to copyright – digital content;
- *sui generis* protection of databases – digital content;
- registered Community designs – products;
- registered Community designs – digital items;
- unregistered Community designs – products;
- unregistered Community designs – digital items;
- registered design rights in the European Union Member States (EUMS) – products;
- registered design rights in the EUMS – digital items.

The study deliberately uses examples of works that are undisputedly protected by either copyright or design rights to ensure that it focuses on the use of AI to facilitate infringement or enforcement of copyright and design rights.

The following issues are outside the scope of the study:

- substantive issues related to the protection of copyright and designs;
- questions about the examination of design applications;
- questions about documentation systems for unregistered rights;
- management of the rights in question (e.g. individual and collective management of copyright and related rights).

Nor does the study cover the topics dealt with in the study on copyright and new technologies by the Directorate-General for Communications Networks, Content and Technology (DG CNNCT) ([19]), such as ownership of works created with AI, or AI data used in AI mining.

Significant effort has been made to ensure that the study does not overlap with other research projects and initiatives. This ensures that its results provide an original perspective and will provide many readers with an eye-opening survey of a technology that is growing quickly in importance for businesses, consumers, and society as a whole.

The study covers the following technologies:

- existing AI technologies and related applications;
- AI technologies and applications that are likely to be developed in the foreseeable future;
- quantum computing-related AI;
- combinations of AI and other emerging technologies (e.g. blockchain and robotics)

([19]) EC (2020). Call for tender for a study on copyright and new technologies: copyright data management and artificial intelligence. https://ec.europa.eu/digital-single-market/en/news/call-tender-study-copyright-and-new-technologies-copyright-data-management-and-artificial.

2.1 Data acquisition methodology

The study relies on data and information collected both through desk research and experts' interviews. The UNICRI team carried out a preliminary thorough examination of existing reports and literature related to AI and IP infringement- and enforcement-related issues, as a basis for the study.

Two storylines and 20 scenarios in which AI is used for the infringement and enforcement of copyright and design

For the assessment of the possible use of AI technologies and tools in copyright and design infringement and enforcement, the research team has developed twenty practical fictional scenarios related to two main storylines, one related to physical products and the other to digital content, which are thoroughly presented in Chapter 5. The two storylines developed by UNICRI are imaginary but have been developed based on actual cases or on situations that may become possible in the near future in light of current technological developments.

- **Storyline α** concerns copyright and designs of **physical products** developed by a famous fashion company and their infringement and enforcement by a criminal group using AI to make their criminal activities more effective;

- **Storyline b** concerns copyright and designs of **digital content** developed by a famous digital media conglomerate, and their infringement and enforcement by a criminal group working online using AI technologies.

The two storylines and the twenty fictional scenarios were used as basis for the interviews with experts.

The infringements described in the current study are of such a scale and nature that in one or more EU Member States they would constitute serious offences and would most often be carried out by

organised criminal groups ([20]). In addition, in the context of the storylines and scenarios, enforcement specifically refers to law enforcement authorities' efforts against serious and organised crime.

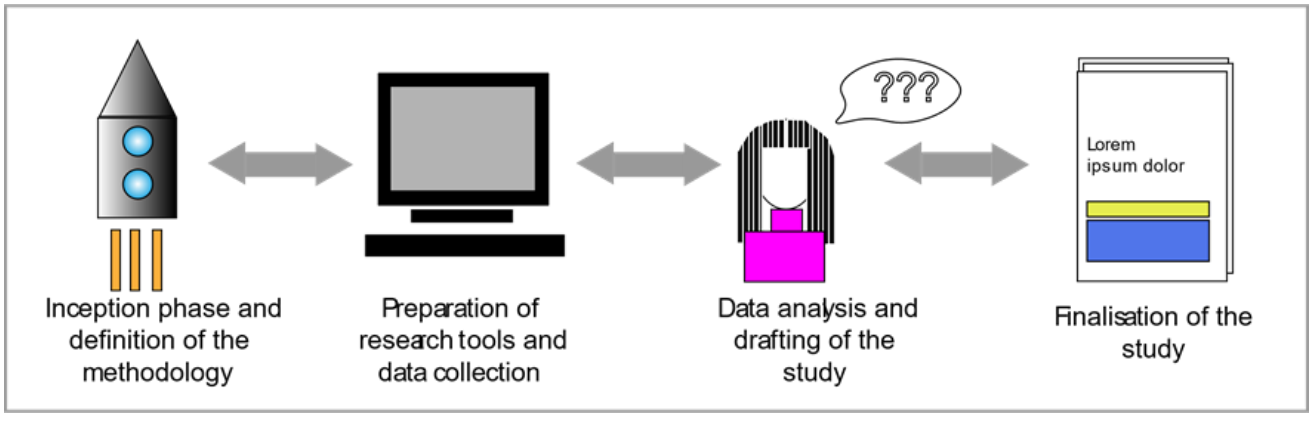
Discussions and interviews with experts

The EUIPO Observatory's Impact of Technology Expert Group and other experts have been actively involved in defining the scenarios and in the different phases of the research. Representatives from other departments of the EUIPO also supported the research.

UNICRI and the EUIPO organised interviews and group discussions with the selected experts via video conference calls. Experts involved in the research who agreed to be acknowledged in the study are listed in Annex 1.

The activities shown in Figure 5 below were undertaken across four phases between March and November 2021.

Figure 5 – Research phases



([20]) See fn 14 – 'organised criminal group' as defined by Article 5 of the United Nations Transnational Organised Crime Convention. https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf and the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0841&from=EN.

3. Introduction to artificial intelligence

This chapter presents the main concepts and capacities of AI and an overview of its subfields. More in-depth information on the evolution of the technology, AI streams and layers, and capacities can be found in Annex 2 'Additional information on AI'. This section explores the technology, describing several concepts relevant to AI which will be used in the following chapters when describing its applications in protecting, infringing, or enforcing IP.

3.1 What is artificial intelligence?

3.1.1 The concept of AI

Over the course of its evolution ([21]), artificial intelligence has been defined in different ways ([22]), but there is still no widely agreed-upon and precise single definition of the concept.

AI is commonly understood as a subfield of computer science that focuses on the development of computer systems that can perform tasks that would normally require human intelligence ([23]). These systems are designed by humans and, when given a complex goal, act in the physical or digital dimension by:

1. **perceiving** their environment through data acquisition,
2. **interpreting** the collected structured or unstructured data,
3. **reasoning** on the knowledge, or **processing** the information, derived from this data and
4. **deciding** the best action(s) to take to achieve the given goal ([24]).

([21]) See Annex 2, section 1, '1 Phases in the history of artificial intelligence'.
([22]) See Annex Definitions'.
([23]) Trend Micro, the United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-—-and-it's-not-just-deep-fakes.
([24]) Trend Micro, the United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol. (2020). Op. cit.

AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions ([25]). In the context of this study, AI is understood as follows ([26]):

Definition of AI used in the study

Computer code (software and hardware) that, according to algorithmic rules, dynamically adapts as large datasets are processed with the aim of predicting phenomena and assisting decision-making.

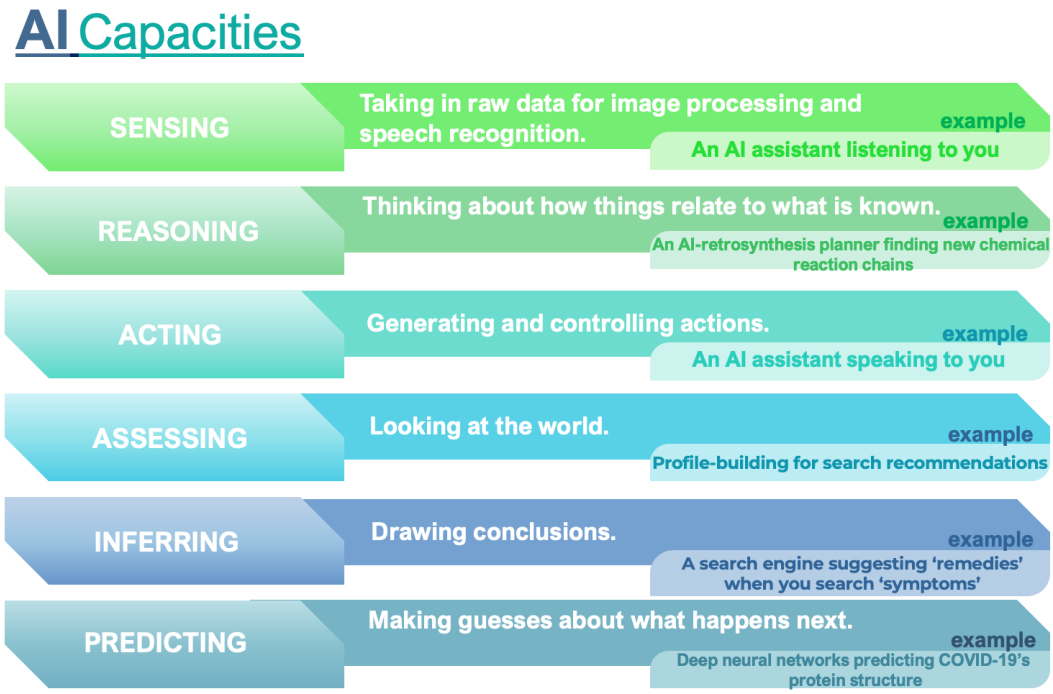
3.1.2. AI capacities

AI can be seen as an attempt to simulate certain human intelligence processes in computer systems, particularly learning, reasoning, planning, self-correction, problem-solving, knowledge representation, perception, motion, manipulation, and creativity ([27]). In this regard, AI systems are primarily advanced learning systems. With the application of AI, a machine can learn to perform a task previously performed by a human with little or no human intervention. Some of the techniques encompassed by AI include: advanced statistics-based machine learning algorithms and multi-task learning algorithms; deep learning executed in a multiple layer neural network (a computer framework imitating the human brain); and prediction models to support decision-making and other kinds of probabilistic reasoning that combine deductive logic with probability theory ([28]).

([25]) Trend Micro, the United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol. (2020). Op. cit.
([26]) This does not aim to provide a fully comprehensible technical or legal definition but only an understanding of the technology in the context of the topic covered by this study.
([27]) Dinesh G. Harkut and Kashmira Kasat (2019). Introductory Chapter: Artificial Intelligence - Challenges and Applications, Artificial Intelligence - Scope and Limitations, Dinesh G. Harkut, IntechOpen, DOI: 10.5772/intechopen.84624.
([28]) European Observatory on Infringements of Intellectual Property Rights (EUIPO), Impact of Technology Expert Group. (2020). Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020 (Rep.). doi:10.2814/15483 TB-001-20-448-EN-N.

AI can therefore employ several different capacities, ranging from sensing, reasoning, and acting to assessing and even predicting, as shown in Figure 6.

Figure 6 – AI capacities



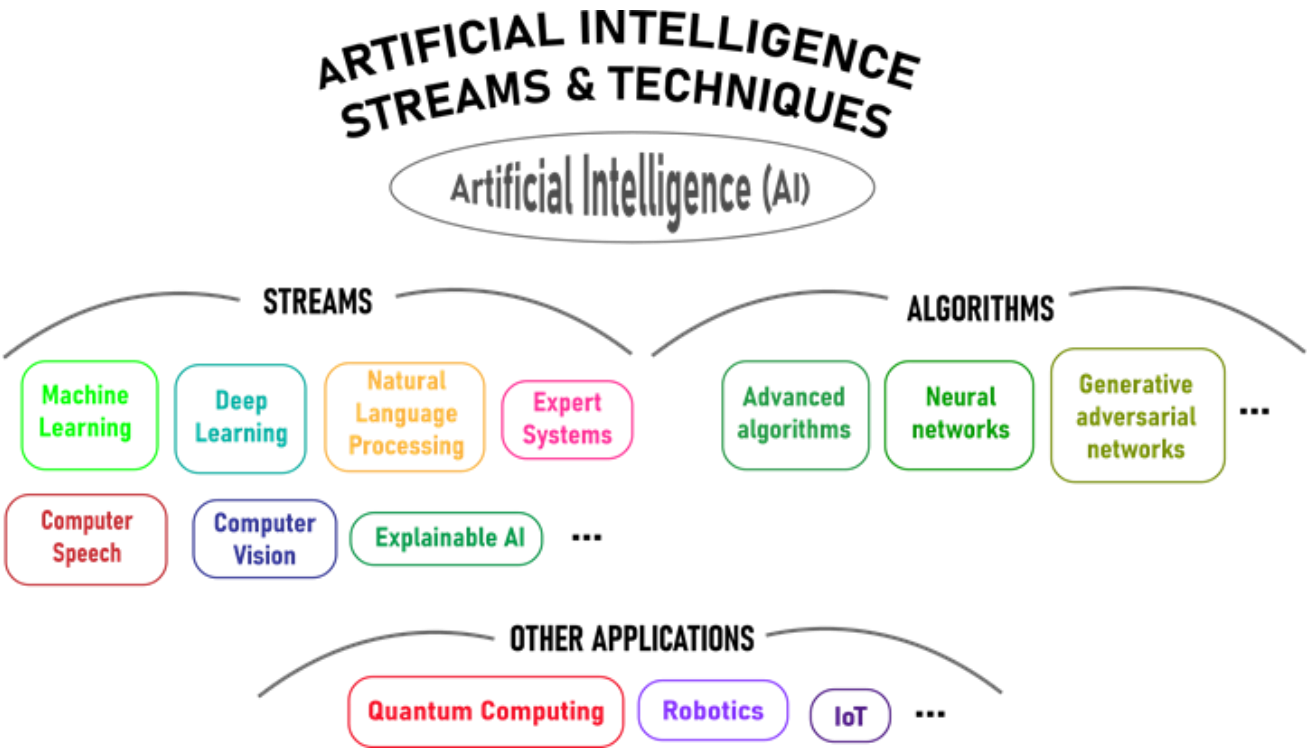
3.1.3 AI streams

AI has been used in different areas, and can be divided into several streams depending on the respective system's functioning. The various elements of AI can be combined to add numerous features to an application, or they can be used solely to perform specific tasks. Robotics and quantum computing are related technologies that are considered relevant in the context of this study when used in combination with AI streams. At the foot of the pages in this section is a legend introducing a colour code for the different AI streams in question.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

Figure 7 – AI streams and techniques



3.1.4 The basis of AI technologies: advanced algorithms

Algorithms are the basis of AI technologies. They can be defined as a series of instructions and rules that a computer must follow to complete an assignment. They can be used to handle and process data and perform calculations or act in various ways ([29]). Algorithms are used in AI technologies to calculate and process data and to automate reasoning; in the latter case they do not only follow explicitly programmed instructions but are designed to allow computers to learn on their own from

([29]) ThinkAutomation. (n.d.). What is an algorithm? An 'in a nutshell' explanation. https://www.thinkautomation.com/eli5/what-is-an-algorithm-an-in-a-nutshell-explanation/.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

data examples that reflect human knowledge ([30]). Algorithms used in AI can be broadly divided into classification algorithms and those suited to other applications such as regression, ranking, and labelling, which separate subject variables into various classes and then predict the class for a given input ([31]).

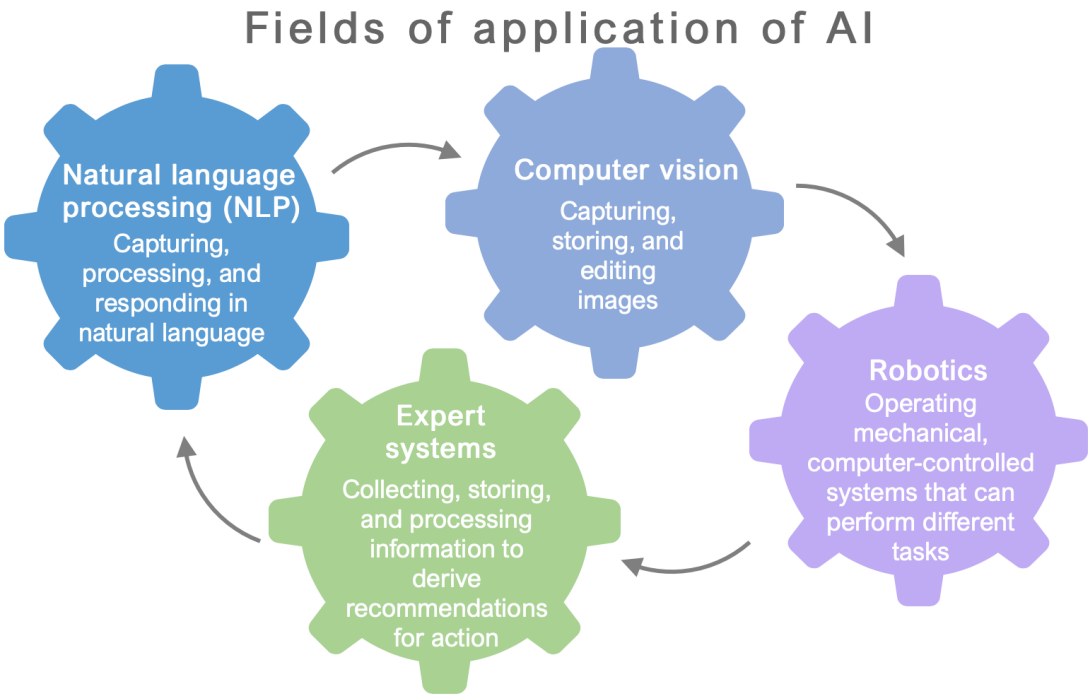
Algorithms enable the development of different AI tools that can be used to protect designs and other IP, as well as for enforcement purposes. Algorithms can enhance the capabilities of existing tools and expand their use to other areas.

3.2 AI subfields

Artificial intelligence is divided into various subfields, each of which has its own specific aspects in addition to certain shared elements and pursues different operational objectives. The major relevant subfields are summarised below to facilitate understanding of the scenarios presented in Chapter 5.

([30]) DeAngelis, S. F. (2015). Artificial intelligence: How algorithms make systems smart. https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/.
([31]) DeAngelis, S. F. (2015). Op. cit.

Figure 8 – AI subfields



3.2.1 Machine learning (ML)

Machine learning is a subfield of AI that focuses on the creation of applications that learn from data and are able to progressively improve their accuracy ([32]). This process allows the system to increasingly develop beyond the data and algorithms originally supplied to achieve independent development and learning based on previous experience gained in the same manner ([33]). The initial algorithms used in the process of programming ML are the starting point for the development of new algorithms, and if the new algorithms prove more meaningful and efficient during the learning process,

([32]) IBM Cloud Education. (2020). What is machine learning? https://www.ibm.com/cloud/learn/machine-learning.
([33]) Kreutzer, R. (2020). Understanding artificial intelligence: Fundamentals, use cases and methods for a corporate AI journey. Cham, Switzerland: Springer.

LEGEND
ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

the system will continue to work with them independently ([34]). ML has become one of the main elements used in AI to develop possible copyright and design protection tools for law enforcement, as explained in more detail in the scenarios presented in Chapter 5. Some of the uses of ML for enforcement include analysis of large amounts of information to detect threats, identification of social engineering bots, scanning of images to detect fraudulent pages or illicit content, improving automatic content recognition tools, and providing insights to find infringement patterns. On the other hand, as will be mentioned in the same scenarios, ML can also be used for infringement. The technology can be used to learn from social media and create fraudulent profiles or imitate real ones, scan websites to identify price changes and popular products, develop smart phishing attacks, automatically eliminate watermarks, and identify patterns to exploit personal information. It can also be combined with computer vision to create fraudulent registration pages and invoices.

The operation of ML follows four main steps:

1. Firstly, **the training data** is prepared. This is a dataset representative of the data the ML model will process to solve the issue it is designed to address ([35]).
2. Secondly, an **advanced training algorithm** is chosen to create the model.
3. Thirdly, the model is **trained** to learn a specific task. Training the model means running data inputs through the algorithm to compare the output with the results it should have produced, adjusting it so it yields a more accurate result, and repeating the process until the algorithm regularly returns the correct result ([36]).
4. Finally, the model is used with **new data** to test its accuracy and effectiveness over time ([37]).

Several different types of ML and ML models can be distinguished.

- *Artificial neural networks (ANNs)*

([34]) Kreutzer, R. (2020). Op. cit.
([35]) IBM Cloud Education. (2020). Op. cit.
([36]) IBM Cloud Education. (2020). Op. cit.
([37]) IBM Cloud Education. (2020). Op. cit.

Artificial neural networks are ML models that mimic the way the human nervous system analyses and processes information ([38]). ANNs are the foundation of AI; they address issues that would prove almost unsolvable by human or statistical methods, and have self-learning capabilities that allow them to generate better results as more data becomes available ([39]). ANNs are **based on the functioning of the human brain**, with interconnected 'neuron' nodes responsible for processing information by transmitting it towards (inputs) and away (outputs) from the brain ([40]). Processing units act as the base that is fed with inputs and outputs, while inputs are the source from which the ANN learns to produce the desired output ([41]). Moreover, ANNs adopt a set of learning rules called 'backpropagation', or backward propagation of error, to improve their output ([42]).

- *Generative adversarial networks (GANs)*

  GANs are generative models used in ML frameworks that can create new data instances that resemble the training data ([43]). They are algorithmic architectures that use two neural networks, pitting one against the other to generate new, synthetic items of data that can pass for real data ([44]). GANs are widely used to **generate images, videos, and voices** ([45]). They can create images that resemble real photographs of human faces even though they do not portray any real individual ([46]). GANs are also known for their role in the generation of fake media content, including the creation of '**deepfakes**' ([47]). A deepfake is a specific type of synthetic media in which an individual in an image or video is replaced with another's likeness ([48]) ([49]).

([38]) Andreu Perez, J., Deligianni, F., Ravi, D., & Yang, G. (2017). Artificial Intelligence and Robotics. https://www.researchgate.net/publication/318858866_Artificial_Intelligence_and_Robotics.
([39]) Frankenfield, J. (2020). Artificial neural Network (ANN). https://www.investopedia.com/terms/a/artificial-neural-networks-ann.asp.
([40]) Frankenfield, J. (2020). Op. cit.
([41]) Frankenfield, J. (2020). Op. cit.
([42]) Frankenfield, J. (2020). Op. cit.
([43]) Google Developers. (n.d.). Generative Adversarial Networks. https://developers.google.com/machine-learning/gan
([44]) Pathmind. (n.d.). A beginner's guide to Generative adversarial Networks (GANs). https://wiki.pathmind.com/generative-adversarial-network-gan.
([45]) Pathmind. (n.d.). Op. cit.
([46]) Google Developers. (n.d.). Op. cit.
([47]) Pathmind. (n.d.). Op. cit.
([48]) Somers, M. (2020). Deepfakes, explained. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.
([49]) Sample I. (2020). What are deepfakes – and how can you spot them? *The Guardian*, 13 January. https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

- *Supervised learning*

  In the supervised learning process, the AI system starts by knowing the right answers, and must then adjust the algorithms so that the answers are as accurate as possible given the existing dataset ([50]). In this case, the algorithm's objective algorithm is already known, and humans must identify each element of the input data and the output variables ([51]). Therefore, the algorithm is trained on the entered data to identity the connection between the input and output data points ([52]). This type of learning requires a small amount of training data and facilitates training because the results of the model can be compared to real labelled results. **Text and image classification** are common applications of this process ([53]).

- *Unsupervised learning*

  Unsupervised machine learning processes a large amount of unlabelled data and uses algorithms to extract meaningful features needed to label, sort, and classify the data in real time without human intervention ([54]). Unsupervised learning focuses less on the automation of decisions and predictions (although in some cases it still makes predictions, e.g. to predict the next word in a sentence) and more on **recognising patterns and relationships** in data that humans would be unlikely to identify ([55]). In unsupervised learning, the system does not have predefined target values. Therefore, it must independently recognise similarities and patterns in the data ([56]). To achieve this, the algorithm receives unlabelled data in which it independently recognises a structure, enabling the identification of data groups that exhibit similar behaviour or similar characteristics ([57]).

- *Reinforced learning*

([50]) Kreutzer, R. (2020). Understanding artificial intelligence: Fundamentals, use cases and methods for a corporate AI journey. Cham, Switzerland: Springer.
([51]) Kreutzer, R. (2020). Op. cit.
([52]) Kreutzer, R. (2020). Op. cit.
([53]) IBM Cloud Education. (2020). Op. cit.
([54]) IBM Cloud Education. (2020). Op. cit.
([55]) IBM Cloud Education. (2020). Op. cit.
([56]) Kreutzer, R. (2020). Op. cit.
([57]) Kreutzer, R. (2020). Op. cit.

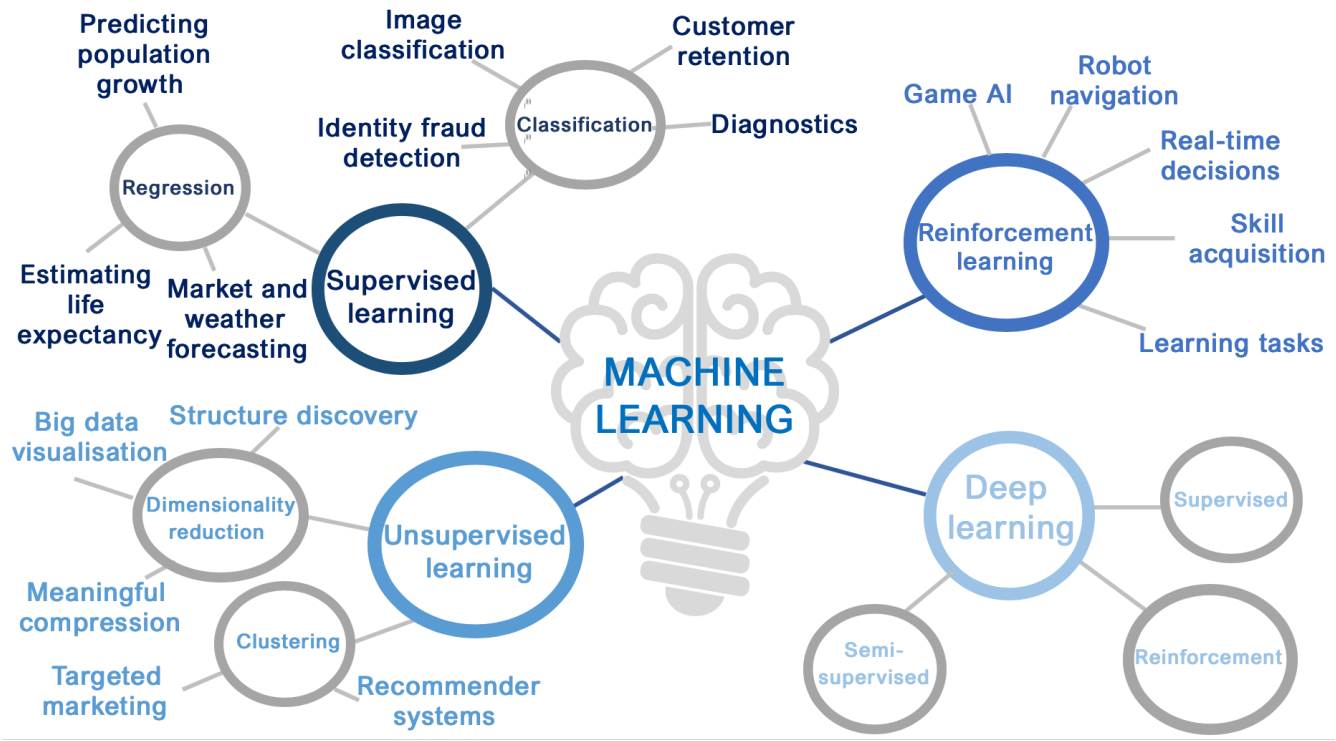
Reinforced learning is similar to supervised learning, except that the algorithm is not trained using sample data; rather, it learns through **trial and error** ([58]). The system must iteratively test solutions independently to discard and/or further develop them; at the same time, this process is driven by 'rewards' for appropriate solutions and 'punishments' for unsuccessful approaches ([59]). This approach is often adopted when **only a small amount of training data is available**, when the **ideal outcome cannot be clearly defined**, or when something can **only be learned from interaction with the environment** ([60]). During the reinforced learning process, the algorithm automatically optimises its actions by constantly correcting itself ([61]).

- *Deep learning (DL)*

  Deep learning uses specially designed neural networks able to process a wider range of data resources. These networks require less human pre-processing of the data but frequently provide more accurate results than other ML approaches ([62]). 'Deep' refers to the large number of layers in the neural network ([63]). The algorithms used in DL are ANNs (see below) requiring large amounts of data that go through multiple layers of calculations; they apply different weights and biases at each successive layer to repeatedly adjust and improve the results ([64]). DL models are usually unsupervised or semi-supervised, and reinforcement learning models can also be DL models ([65]).

([58]) IBM Cloud Education. (2020). Op. cit.
([59]) Kreutzer, R. (2020). Op. cit.
([60]) Kreutzer, R. (2020). Op. cit.
([61]) Kreutzer, R. (2020). Op. cit.
([62]) Kreutzer, R. (2020). Op. cit.
([63]) Kreutzer, R. (2020). Op. cit.
([64]) Kreutzer, R. (2020). Op. cit.
([65]) Kreutzer, R. (2020). Op. cit.

Figure 9 – Types of machine learning algorithms and applications



3.2.2 Natural language processing (NLP)

Natural language processing is a subfield of AI that enables the extraction of data to create relations, making it possible to identify figures of speech and perform sentiment analysis ([66]). Rather than interpreting a text or speech based on its keywords, which was the previously used mechanical method, NLP adopts a cognitive approach by analysing the meaning behind those words ([67]). It is therefore the branch of AI that allows computers to understand, interpret, and manipulate human

([66]) Lopez Yse, D. (2019). Your Guide to Natural Language Processing (NLP). https://towardsdatascience.com/your-guide-to-natural-language-processing-nlp-48ea2511f6e1.
([67]) Lopez Yse, D. (2019). Op. cit.

language ([68]). NLP is a tool for **content extraction**, **classification**, **machine translation**, **question answering**, and **text generation**. Subsets of NLP include natural language understanding (NLU), concerning machine reading comprehension, and natural language generation (NLG), used to transform data into words understood by humans ([69]). In addition, NLP may use ML and DL methods to effectively absorb and process unstructured speech and text datasets ([70]).

As will be explained in Chapter 5, NLP is also relevant for law enforcement, since it can analyse and block cyberattacks like phishing, identify the behaviour of fraudsters, and create a correlation analysis. NLP is also mentioned in Chapter 5 as a tool for infringement in certain situations, such as the creation of text in fraudulent emails and communications and the replication of text to create fraudulent registration pages for goods or other official documents.

There are several different applications of NLP.

- *Text-to-speech (TTS)*
  Text-to-speech is a type of speech synthesis application that generates a spoken audio version of the text in a computer document with the goal of rendering natural-sounding speech signals for downstream applications, including assistant devices such as Google's Assistant, Amazon's Echo, and Apple's Siri ([71]).

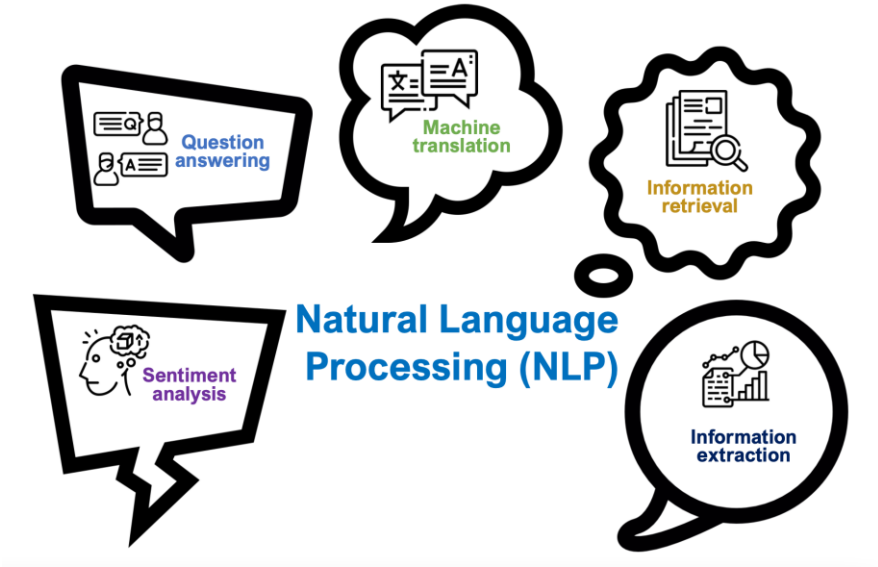
- *Speech-to-speech (STS)*
  Speech-to-speech processes a speech input to generate another speech output, for example in translation applications or in digital personal assistants' question and answer sequences ([72]).

- *Text-to-text (TTT)*

([68]) Overby, S. (2020). Artificial intelligence (AI) vs. natural language processing (NLP): What are the differences? https://enterprisersproject.com/article/2020/2/artificial-intelligence-ai-vs-natural-language-processing-nlp-differences
([69]) Overby, S. (2020). Op. cit.
([70]) Overby, S. (2020). Op. cit.
([71]) Ma, E. (2019). How does your Assistant device work based-on Text-to-Speech technology? https://becominghuman.ai/how-does-your-assistant-device-work-based-on-text-to-speech-technology-5f31e56eae7e
([72]) Kreutzer, R. (2020). Op. cit.

Text-to-text translates digital text into another language using a translation program like DeepL or Google Translate ([73]).

Figure 10 – Natural language processing (NLP)



3.2.3 Computer speech

Computer speech refers to a machine's application of speech recognition and synthesis to create human-like speech ([74]). In speech recognition, the computer takes sound vibrations as inputs and uses an analogue-to-digital converter to translate the sound waves into a digital format ([75]). Advanced speech recognition in AI also includes voice recognition, in which the computer can distinguish a

([73]) Kreutzer, R. (2020). Op. cit.
([74]) National Academy of Sciences (1994) Voice Communication Between Humans and Machines. Washington, DC: The National Academies Press. https://doi.org/10.17226/2308.
([75]) Horowitz, J. H. (2020). Speech Recognition in AI. https://itchronicles.com/speech-to-text/speech-recognition-in-ai/.

particular speaker's voice ([76]). AI is used in different areas related to the **imitation of human speech**, for example, speech recognition and translation; furthermore, several speech recognition applications are powered by **automatic speech recognition** and NLP ([77]). Automatic speech recognition is the conversion of audio to text, while NLP refers to the processing of text to determine its meaning ([78]). In Chapter 5, the use of computer speech for infringement can be observed in the imitation of existing voices and designs. However, it can also be used for enforcement, for instance in identifying online marketing of infringing products.

3.2.4 Computer vision

Computer vision refers to the processing of signals that represent images, training computers to interpret and understand the visual world ([79]). It follows three main steps:

1. the system acquires an image for analysis in real time through video, photos or 3D technology;
2. it processes the image through a previously trained model ([80]);
3. it understands the image through an interpretative process (i.e. it implements the model to perform a specific task) in which an object is identified or classified ([81]).

Computer vision can be used in the segmentation of images for separate examination, advanced **object detection**, **facial recognition**, detection of the outside edge of an object or landscape for better identification of the content, **pattern detection**, **image classification**, and feature matching ([82]). Computer vision can provide various support tools for enforcement, as will be shown in the scenarios in Chapter 5. Some of its uses include pattern recognition to predict future infringement, detection of

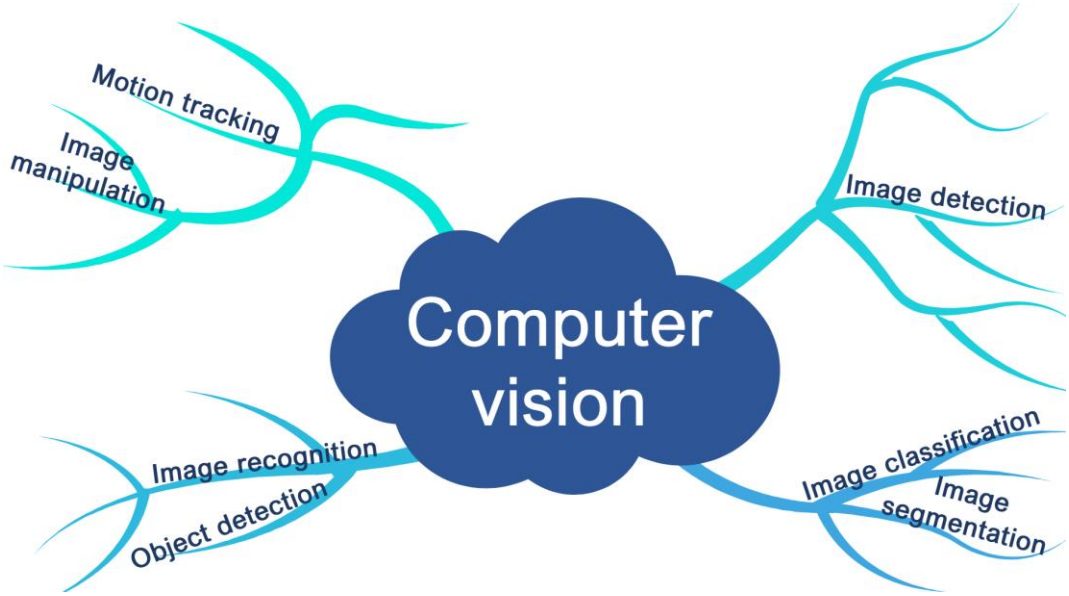
([76]) Horowitz, J. H. (2020). Op. cit.
([77]) Horowitz, J. H. (2020). Op. cit.
([78]) Horowitz, J. H. (2020). Op. cit.
([79]) Kreutzer, R. (2020). Op. cit.
([80]) SAS. (n.d.). Computer vision: What it is and why it matters. https://www.sas.com/en_us/insights/analytics/computer-vision.html#technical.
([81]) SAS. (n.d.). Op. cit.
([82]) SAS. (n.d.). Op. cit.

marketing of infringing goods, and detection and analysis of logos or other relevant images. The use of computer vision for infringement is also described in the scenarios, as it can enable the copying of popular product designs, colours and shapes, and detect and replicate patterns in visual anti-counterfeiting technology. In addition, it can be combined with other technologies to create fraudulent registrations or invoices.

Computer vision not only enables systems to derive meaningful information from visual inputs, but also allows them to take action or make recommendations based on that information ([83]). Convolutional neural networks (CNNs) and DL are used for this purpose ([84]). DL uses algorithmic models to allow the computer to teach itself about the context of visual data, while CNNs help the DL model to 'see' by dividing the images into labelled pixels ([85]). The neural network iteratively assesses the accuracy of the predictions until the predictions start to come true, allowing the computer to recognise images in a way similar to humans ([86]).

([83]) IBM. (n.d.). What is computer vision? https://www.ibm.com/topics/computer-vision.
([84]) IBM. (n.d.). Op. cit.
([85]) IBM. (n.d.). Op. cit.
([86]) IBM. (n.d.). Op. cit.

Figure 11 – Computer vision concepts



3.2.5 AI quantum computing

Quantum computing focuses on developing computer technology based on the principles of quantum mechanics, which is a mathematical machine used to predict the behaviours of microscopic particles, or to measure instruments adopted to explore those behaviours. Quantum computing is not necessarily linked to AI, but could be used to enhance the capacity of AI applications. Every computer application is composed of 'bits' in some combination of ones and zeroes ([87]). An ordinary computer uses microchips on which transistors act as switches that can either be in the 'off' position (represented by a zero) or the 'on' position (represented by a one) ([88]). Quantum computers use

([87]) Katwala, A. (2020). Quantum computing and quantum supremacy, explained. https://www.wired.co.uk/article/quantum-computing-explained.
([88]) Katwala, A. (2020). Op. cit.

LEGEND
ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

'qubits' instead of bits: as well as being on or off, qubits can be both on and off at the same time, in what is known as 'superposition' ([89]).

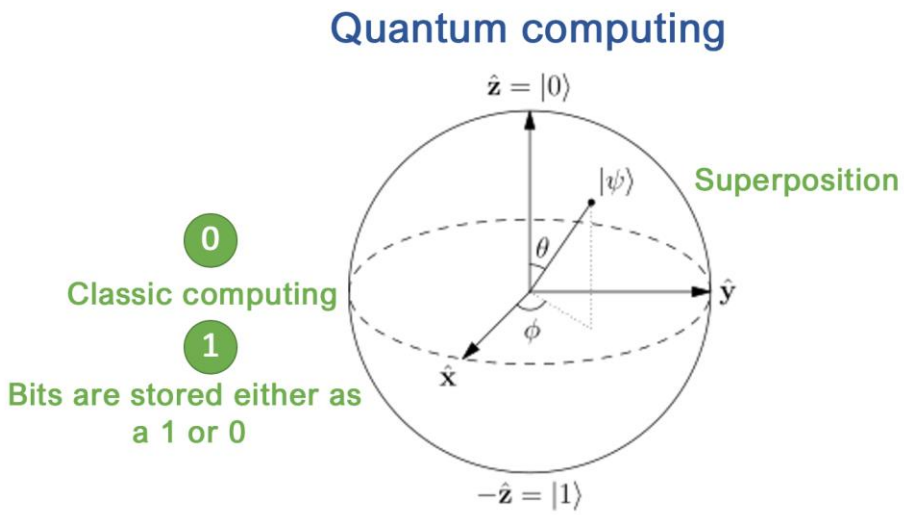
Datasets are becoming larger and more complex, placing considerable strain on current computer systems. A number of issues related to problem-solving and capability restrictions are expected to be solved in seconds through the use of quantum computing. Certain technologies, such as AI, and in particular ML, can benefit from progress in quantum computing ([90]).

At present, nearly all the industrial applications of AI are based on supervised learning, and are used for image recognition or consumption forecasting. In the area of finance, AI and quantum computing can help improve fraud detection. Moreover, quantum computing-trained models could be used to **detect patterns** that would be almost undetectable with conventional equipment. Finally, the acceleration of algorithms could allow machines to handle **high volumes of data** ([91]).

In the scenarios in Chapter 5, quantum computing is mentioned as a technology that could improve AI tools, enabling them to process larger amounts of data. For example, AI and quantum computing can be used by customs and law enforcement authorities to recognise patterns in large datasets and identify similarities. On the other hand, the same capabilities can be used to improve tools used for infringement.

([89]) Katwala, A. (2020). Op. cit.
([90]) Marr B. (undated). How Quantum Computers Will Revolutionise Artificial Intelligence, Machine Learning and Big Data. https://www.bernardmarr.com/default.asp?contentID=1178.
([91]) BBVA (2020). How may quantum computing affect Artificial Intelligence? https://www.bbva.com/en/how-may-quantum-computing-affect-artificial-intelligence/.

Figure 12 – Quantum computing



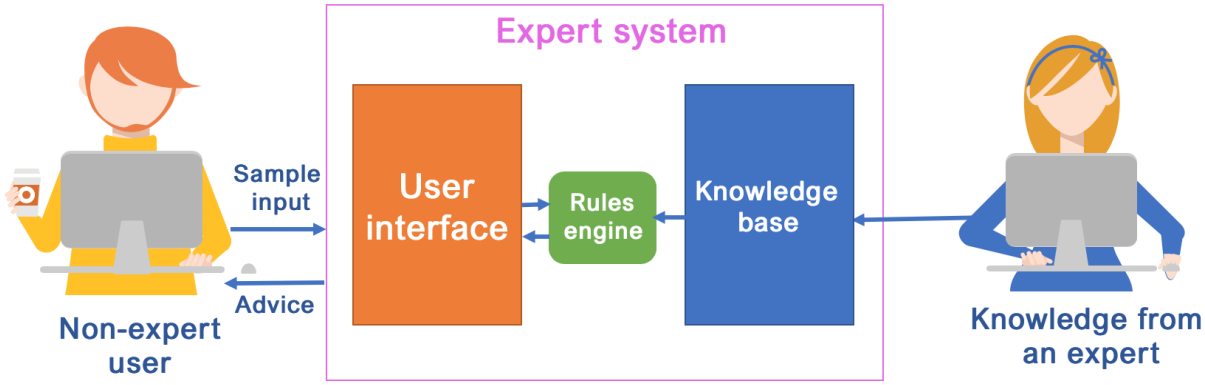
3.2.6 Expert systems (ESs)

Expert systems are computer programs designed to solve complex issues and imitate the decision-making ability of human experts by extracting knowledge from their knowledge base using reasoning and inference rules in response to user queries ([92]). An ES uses specific knowledge about its domain of application and adopts an inferential procedure to solve issues that would normally require human expertise ([93]).

([92]) Javapoint. (n.d.). Expert systems in artificial intelligence. https://www.javatpoint.com/expert-systems-in-artificial-intelligence.
([93]) University of Missouri-St. Louis. (n.d.). Expert systems and applied artificial intelligence. https://www.umsl.edu/~joshik/msis480/chapt11.htm.

The relevance of ESs derives from the specific knowledge about a narrow domain stored in the system's knowledge base ([94]). ESs are based on '**knowledge engineering**', in which knowledge about the specific domain is acquired from human experts and other sources ([95]). The main feature of an ES is the accumulation of knowledge in its databases, from which conclusions are generated by the inference engine ([96]). Areas of application include classification, diagnosis, monitoring, process control, design, scheduling and planning, and option generation ([97]). Expert systems also provide valuable tools to minimise the risks presented in the scenarios in Chapter 5, as they can help law enforcement authorities to decide which strategy is most adequate to protect a system from specific vulnerabilities.

Figure 13 – Expert systems



([94]) University of Missouri-St. Louis. (n.d.). Op. cit.
([95]) University of Missouri-St. Louis. (n.d.). Op. cit.
([96]) University of Missouri-St. Louis. (n.d.). Op. cit.
([97]) University of Missouri-St. Louis. (n.d.). Op. cit.

3.2.7 Explainable artificial intelligence (XAI)

Explainable artificial intelligence is not a subfield of AI; rather, it is a set of processes and methods enabling users to understand and trust the results generated by ML algorithms ([98]). XAI can be defined as AI that produces details or reasoning to make its functioning clear or easy to understand ([99]). It describes an AI model, in addition to its expected impact and potential biases ([100]). Furthermore, XAI helps to determine a model's precision, fairness, transparency, and results in AI-based decision making ([101]).

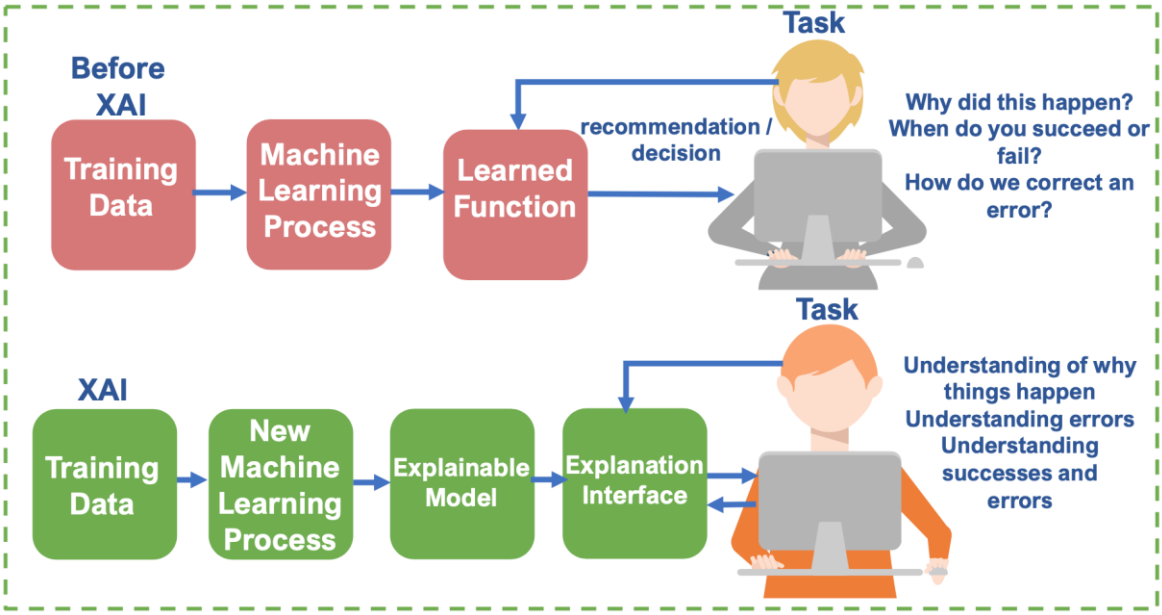
One of the challenges in the development and implementation of AI is that humans need to comprehend and retrace how the algorithm arrives at an output, a calculation known as a 'black box', which is almost impossible to interpret ([102]). Black box models are derived directly from the data, and not even the algorithm's creators can fully comprehend or explain what exactly the algorithm does or how it obtains a specific result ([103]).

Full understanding of how an AI-enabled system has arrived at a specific output is extremely useful, since it can help developers to ensure that the system operates as expected, which may be required if the system is to meet regulatory standards. Explainability may also be essential in allowing those affected by a decision to challenge or change the outcome ([104]).

XAI can be used in the scenarios in Chapter 5 to better understand the ML processes used in different tools and consequently to improve those tools. However, XAI can also be used by infringers to understand and improve their own tools.

([98]) IBM. (n.d.). Explainable AI. https://www.ibm.com/watson/explainable-ai.
([99]) Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., et al.. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82-[115] doi:10.1016/j.inffus.2019.12.012.
([100]) IBM. (n.d.). Explainable AI. Op. cit.
([101]) IBM. (n.d.). Explainable AI. Op. cit.
([102]) IBM. (n.d.). Explainable AI. Op. cit.
([103]) IBM. (n.d.). Explainable AI. Op. cit.
([104]) IBM. (n.d.). Explainable AI. Op. cit.

Figure 14 – Explainable artificial intelligence (XAI)



3.3 Social impacts of AI technologies

Having introduced the main aspects of AI and its subfields, this chapter will address, albeit briefly, the potential major social impacts of AI technologies, and raising a number of important ethical and fundamental rights-related concerns; a thorough analysis of this complex issue is clearly beyond the scope of this study.

The world is now witnessing the so-called 'Fourth Industrial Revolution' ([105]), characterised by new and advanced technologies that allow increasing interaction between the digital and physical worlds, capable of innovations advancing with a speed and on a scale unprecedented in human history. This

([105])World Economic Forum (WEF) (2016). The Fourth Industrial Revolution: what it means, how to respond https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

metamorphosis is radically changing the ways in which individuals, companies, and institutions relate to one other ([106]). The impact of AI on our society has had, and will in the near future have, far-reaching economic, legal, political and regulatory implications ([107]). These new technologies will transform societies in areas such as safe transport, mobility, security, health, media content recognition, service quality, and employment ([108]). The social impacts of AI will clearly affect the economy and the labour force. The present study will focus on AI technologies' impact on crime, law enforcement and criminal justice, taking into account the relevant ethical and fundamental rights-related issues (including data protection and privacy concerns). Further observations on these issues are provided in Annex .

In the European Union, the discussion around AI and its various implications is very lively and has resulted in a number of EU Parliament resolutions. At the global level, the United Nations has put in place a number of important initiatives related to AI's role in sustainable development. While AI technologies may support breakthroughs in achieving the UN's Sustainable Development Goals (SDGs), they may also have unanticipated consequences that will exacerbate inequalities and negatively affect individuals, societies, economies and the environment ([109]).

3.4 The EC's proposal for AI regulation

Finally, this chapter will conclude with an overview of current legal initiatives around AI in the EU. The European Commission is in the process of taking important regulatory steps in this field. The EU overall approach to AI aims to ensure that any AI improvements are based on rules that safeguard the functioning of markets and the public sector, and people's safety and fundamental rights, as

([106]) DBI (n.d). Globalization 4.0 – The role and impact on the economy of emerging technologies in the paradigm of Globalization 4.0. Economistas #165. https://www.dbi.srl/the-role-and-impact-on-the-economy-of-emerging-technologies-in-the-paradigm-of-globalization-4-0/.

([107]) Marr B. (n.d). What Is The Impact Of Artificial Intelligence (AI) On Society? https://bernardmarr.com/default.asp?contentID=1828.

([108])EUIPO (2020). Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020. https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2020_Tech_Watch_paper/2020_IP_Infringement_and_Enforcement_Tech_Watch_Discussion_Paper_Full_EN.pdf.

([109])United Nations (2021). Resource Guide on Artificial Intelligence (AI) Strategies. DESA. New York. June. https://sdgs.un.org/sites/default/files/2021-06/Resource%20Guide%20on%20AI%20Strategies_June%202021.pdf.

indicated by the European initiative on AI launched in 2018 ([110]). In 2020, the EC's white paper on 'AI – A European approach to excellence and trust' set out policy options on promoting AI while addressing the risks associated with certain uses ([111]). In 2021, the EC published a proposal for a regulation laying down harmonised rules on AI. The proposal aims to develop an ecosystem of trust by proposing a legal framework for reliable AI, based on the EU's values and fundamental rights, to give people the confidence to embrace AI and encourage its development by businesses ([112]).

The proposed legal framework, which is still under discussion, addresses the risks posed by the various uses of AI systems while at the same time promoting innovation, recognising the need to preserve individual safety and fundamental rights without overly inhibiting AI innovation. To this end, a risk-based approach is suggested ([113]). The gradation of risks is represented as a four-level pyramid: unacceptable risks, high risks, limited risks, and minimal risks; further information is available in Annex .

In 2021, the Coordinated Plan on Artificial Intelligence 2021 Review puts forward a concrete set of joint actions for the European Commission and Member States on how to create EU global leadership on trustworthy AI ([114]).

([110]) European Commission (2018). Communication From The Commission Artificial Intelligence for Europe (COM(2018) 237 final). Brussels, 25 April. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN
([111]) European Commission (2021). White Paper on Artificial Intelligence - A European approach to excellence and trust https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
([112]) European Commission. (2021). Op. cit.
([113]) Gaumond E. (2021). Artificial Intelligence Act: What Is the European Approach for AI? 4 June. https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai.
([114]) European Commission (2021). Coordinated Plan on Artificial Intelligence 2021 Review. https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe

Additional efforts worth mentioning include several initiatives in the fields of external border management and possible applications of emerging technologies, including AI ([115]).

1. Regulation (EU) 2016/1624 on the European Border and Coast Guard (EBCG) proposes general principles for integrated European border management, and Regulation (EU) 2019/1896 strengthens the mandate of the European Border and Coast Guard Agency (Frontex).
2. The European Commission's 2018 European Strategy and Coordinated Plan on AI offers a European perspective on the diverse technological, ethical, legal, and socio-economic implications of AI and principles for its uses in the public and private sectors.
3. The EU Security Union Strategy 2020 outlines the main priorities for improving internal security. These include strengthening the provision of data services in the areas of border surveillance and maritime security.

All these policy and regulatory measures will affect the development and use of AI and related technologies by private-sector actors as well as law enforcement and customs agencies, including in the areas of copyright and design enforcement. On the other hand, they will have little or no impact on malicious actors, as these by definition operate 'outside the law'.

([114]) European Border and Coast Guard Agency (FRONTEX). (2021). Artificial Intelligence-Based Capabilities for the European Border and Coast Guard. Frontex. https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf.

4. A bird's-eye view of AI applied in infringement and enforcement of copyright and design

This chapter will provide a birds-eye view of the various AI technologies that have been found relevant to this study. They are presented briefly, without technical explanations of precisely how they are built or how they function; rather, the purpose is to clarify their meaning and scope of application and allow a proper understanding of the fictional scenarios in Chapter 5.

The weaponisation and monetisation of AI also feature in the following sections, since the development of AI tools and their use both to protect and infringe IP can be observed in the subsequent examples and scenarios. It is must be emphasised that AI and related technologies are tools. They are neither good nor bad in themselves. Rather, it is the use of these technologies that determines whether they are beneficial or harmful. 'Technology is neither good nor bad; nor is it neutral' ([116]). The legend at the foot of the page links the different technologies presented in this chapter with the AI streams introduced in Chapter 3.

The listing of technologies below is not meant to suggest any ranking in terms of frequency or seriousness.

4.1 AI-supported malware

Malicious software, or 'malware' is software designed to carry out an unauthorised process that will adversely affect the privacy, integrity, or accessibility of an information

([116]) Kranzberg M. (1986). "Technology and Culture", Vol. 27, No 3, July, pp. 544-560. The Johns Hopkins University Press.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

system. This software commonly includes viruses, worms, Trojan horses, and other code-based entities that infect a host, as well as spyware and some forms of adware ([117]) ([118]).

The use of AI to improve the effectiveness of malware is still in an experimental phase, but its monetisation and weaponization are expected to increase in the near future: AI-supported and AI-enhanced cyberattacks that have been studied are proof that criminals are already taking steps to broaden their use of AI ([119]). Artificial Intelligence can be used maliciously to control malware in order to create more convincing spam, evade detection, and better adapt itself to each target ([120]). Cybercriminals might be able to determine how AI-powered security software identifies malware, enabling them to adapt their own software and easily evade detection. In some cases, the samples can be modified to trick the AI into flagging legitimate files as malware, triggering false positives ([121]).

AI-supported malware could be integrated into a variety of techniques to enhance their negative impact: changing the malware's behaviour and characteristics based on context, eliminating itself when it suspects it is being analysed, and performing malicious activities only on specified systems ([122]). Furthermore, malware programmers could train security solutions that use ML to preserve certain malicious files or to produce false positives. Specifically, AI malware might be used to ([123]):

1. solve the CAPTCHA authentication method (Completely Automated Public Turing test to tell Computers and Humans Apart) using ML ([124]);

([117]) For more information see CERN. (n.d.). Recommendations about Viruses What is a virus? Why virus are bad? How not to get a virus? How to get rid of a virus? https://espace.cern.ch/winservices-help/NICESecurityAndAntivirus/VirusHoaxesAndSpyware/AboutViruses/Pages/default.aspx.
([118]) Computer Security Resource Center (CSRC). (n.d.). Malware. https://csrc.nist.gov/glossary/term/malware.
([119]) Trend Micro, UNICRI, EUROPOL (2020). Malicious Uses and Abuses of Artificial Intelligence. p.6.
([120]) Malwarebytes Labs. (2019). When artificial intelligence goes awry: Separating science fiction from fact. https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf.
([121]) Malwarebytes Labs. (2019). Op. cit.
([122]) Malwarebytes Labs. (2019). Op. cit.
([123]) Malwarebytes Labs. (2019). Op. cit.
([124]) Zhao N., Liu Y., Jiang Y., (2017). CAPTCHA Breaking with Deep Learning. CS 229 Final Project. http://cs229.stanford.edu/proj2017/final-reports/5239112.pdf.

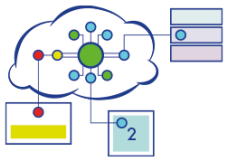
2. carry out 'spear phishing' via a service ([125]) or scanning social media using AI to identify people connected to particular organisations, gathering information to make spear phishing campaigns more effective;
3. improve spam to make it more convincing by training it to adapt to the receiver; this could include use of the target's language, line of business, and other personal details that increase the likelihood of their opening the attachment.

This last approach is known as 'deep targeting', which usually refers to techniques used in marketing to learn the behaviours, habits, and values of a person or group in order to create successful advertising campaigns ([126]). As illustrated in the previous examples, cybercriminals can use this end-user behavioural analysis (UBA) to learn user conduct and blend into their targets' environment ([127]). UBA technology searches for patterns of usage indicating unusual or anomalous behaviours ([128]). However, anti-malware security measures can also be improved by adopting AI tools such as ML. Beyond adding malware samples to security software, AI can also detect future versions and similar variants of the same malware, as it enables the evaluation, organisation, and condensation of threat variants ([129]). In this case, AI must be continuously supervised and adjusted by humans, since if the 'weave' of the neural net is too wide, malware may evade detection, and if it is too fine, the security solution may trigger false positives ([130]).

AI-supported malware is one of the infringement-related issues mentioned in the scenarios in Chapter 5, due to its role in the use of fake identities in phishing attacks and the creation of false documents. The complexity of the attacks performed with AI-supported malware can itself be targeted by specialised law enforcement units using AI tools such as ML, as described in the scenarios.

([125]) CrowdStrike. (n.d.). Spear-Phishing definition. https://www.crowdstrike.com/cybersecurity101/phishing/spearphishing/?utm_campaign=dsa&utm_content=dach&utm_medium=sem&utm_source=goog&utm_term=&gclid=Cj0KCQjwseDBhC7ARIsAI8YcWL2yDufFJRZP1_8_4nKXYDWyL3HYHeTHMnJFh4ED1_8PT2Eelw1HM0aAlj8EALw_wcB.
([126]) Kraus, P. (2021). Will AI malware change the game? https://www.securitymagazine.com/articles/94757-will-ai-malware-change-the-game.
([127]) For more information, see Green, A. (2020). What is User Behavior Analytics? https://www.varonis.com/blog/what-is-user-behavior-analytics/.
([128]) Green A. (2020). Op. cit.
([129]) Malwarebytes Labs. (2019). When artificial intelligence goes awry: Separating science fiction from fact. https://www.malwarebytes.com/resources/files/2019/06/labs-report-ai-gone-awry.pdf.
([130]) Malwarebytes Labs. (2019). Op cit.

4.2 AI cloud services



Cloud computing refers to the process of storing and accessing data and other programs over the internet instead of the computer's local hard drive ([131]). Cloud computing services have increasingly become the target of attacks, as they store large amounts of company and user data, and some companies also use them to operate consumer services such as email and photo libraries ([132]).

Existing types of cloud application services include Infrastructure-as-a-Service (IaaS), which allows the user to pay for services based on usage, and frequently covers the rental of storage, networks, operating systems, servers, and virtual machines (VMs) ([133]) ([134]). Another type is Platform-as-a-Service (PaaS), which was created to facilitate web creation and mobile app design by providing an inbuilt infrastructure of servers, networks, databases, and storage that is automatically updated and managed ([135]). Finally, Software-as-a-Service (SaaS) is a type of cloud application service in which the cloud provider performs management and maintenance tasks ([136]).

The role of cloud services in AI can be seen in t certain machine learning tasks such as batch processing, serverless computing, predictive analytics, and orchestration of containers ([137]). Other AI services in this category include text analytics, speech, vision, and translation. Furthermore, the use

([131]) Griffith, E. (2020). What is cloud computing? https://uk.pcmag.com/networking-communications-software/16824/what-is-cloud-computing.
([132]) Giles, M. (2018). Six cyber threats to really worry about in 2018. https://www.technologyreview.com/2018/01/02/146501/six-cyber-threats-to-really-worry-about-in-2018/.
([133]) For more information see: Microsoft. (n.d.). What is a virtual machine (VM)? An intro to virtualization and the benefits of VMs. https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/.
([134]) Bhatia, V. (2020). The Role of Artificial Intelligence in Cloud Computing. https://www.goodfirms.co/blog/role-of-ai-in-cloud-computing.
([135]) Bhatia, V. (2020). Op. cit.
([136]) Bhatia, V. (2020). Op. cit.
([137]) Bhatia, V. (2020). Op. cit.

of cognitive computing models ([138]) would allow users to share their personalised data, which can be trained to provide well-defined services ([139]). This way, issues such as the need to find the appropriate algorithm or the correct training model are eliminated ([140]).

The use of cloud services in AI can provide an additional mechanism to improve and facilitate use of the tools described in the scenarios in Chapter 5, due to their role in the automation of various tasks. Conversely, however, the adoption of cloud services can also improve infringement tools that might be developed.

4.3 AI in generative design

Generative design is a design exploration process in which designers or engineers select specific goals to add to the generative design software, along with selected parameters including performance or spatial requirements, materials, manufacturing methods, and cost constraints ([141]). After receiving these inputs, the software analyses all the possible permutations of a solution to develop and suggest design alternatives. During this process, the software also tries and learns from each iteration to identify which strategies and combinations work, and which ones do not ([142]).

In this way, AI in generative design can quickly produce a large number of concepts that are adapted to the project's requirements. In traditional design, the process usually starts with a model based on an engineer's or designer's knowledge. However, in generative design, design parameters are

([138]) For more information see: Botelho, B. (2018). What is cognitive computing? https://searchenterpriseai.techtarget.com/definition/cognitive-computing.
([139]) Bhatia, V. (2020). Op. cit.
([140]) Bhatia, V. (2020). Op. cit.
([141]) Autodesk. (n.d.). What is generative design? https://www.autodesk.com/solutions/generative-design.
([142]) Autodesk. (n.d.). Op. cit..

established, and the AI then generates a model based on them ([143]). Generative design allows the creation of precisely optimised and customised design solutions and can solve various engineering challenges, such as how to make product components lighter, stronger, or more cost-effective ([144]). Generative design has great potential in the development of tools that improve and facilitate the design process; however, as described in Chapter 5, it can also be used for infringement when adopted by criminals.

4.4 AI in robotics

An industrial robot is an automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be either fixed in place or mobile for use in industrial automation ([145]). In general, a robot is any machine that can be used to perform complex actions and tasks automatically; specifically, robotics relates to the automation of physical tasks ([146]).

Robotics can integrate some sub-fields of AI: for example, 'smart robots' adopt ML to improve their performance progressively ([147]). Robots that incorporate AI are usually able to automate far more tasks than purely robotics-based technologies ([148]). The autonomy of a robot in its surroundings can be classified into different subdivisions such as perceiving, planning, and executing (i.e. manipulating, navigating, and collaborating) ([149]). One of the main objectives of using AI in robotics is to optimise the

([143]) Formlabs. (n.d.). Generative design 101. https://formlabs.com/blog/generative-design/#What%20Is%20Generative%20Design%3F.
([144]) Formlabs. (n.d.). Op. cit.
([145]) International Federation of Robots (IFR). (n.d.). International robot standardization within ISO. https://ifr.org/standardisation.
([146]) Raj, M., Seamans, R. (2019). Primer on artificial intelligence and robotics. https://jorgdesign.springeropen.com/articles/10.1186/s41469-019-0050-0.
([147]) Raj, M., Seamans, R. (2019). Op. cit.
([148]) Raj, M., Seamans, R. (2019). Op. cit.
([149]) Andreu Perez, J., Deligianni, F., Ravi, D., & Yang, G. (2017). Artificial Intelligence and Robotics. https://www.researchgate.net/publication/318858866_Artificial_Intelligence_and_Robotics.

robot's degree of autonomy through learning, evaluating the robot's level of intelligence in predicting the future, specifically in planning a task and in interacting with its environment, either through manipulating it or navigating through it ([150]). In the scenarios in Chapter 5, AI in robotics is mentioned as a means of optimising the mass production of infringing products and the processes in their supply chain. The benefits of adopting AI in robotics could also be used by infringers to develop tools to automate certain tasks. However, it is also a valuable tool for future improvements in the general security of the manufacturing process, including the creation of unique visual identities for products to identify original goods.

4.5 Smart devices and AI

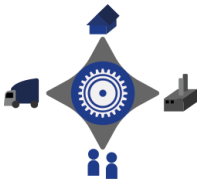
A 'smart device' is a context-aware electronic device capable of performing autonomous computing and connecting to other devices through a wire or wirelessly to exchange data ([151]). Therefore, smart device technology may be applied to various objects such as simple sensor nodes, home appliances and smartphones ([152]). Smart devices are essential for the development of other technological advances such as the Internet of Things (IoT) and smart cities.

The key characteristics of AI as used in smart devices are context-awareness, device connectivity and autonomy ([153]). 'Context-awareness' is the ability of a system or one of its components to obtain data about its environment at any moment and adapt its behaviour accordingly. 'Autonomous computing' refers to a device or devices that carry out tasks autonomously without the direct control of the user, while 'device connectivity' refers to a device that can connect to a data network ([154]). In other cases, such as the integration of AI in the IoT, applications include components like smart

([150]) Andreu Perez, J., Deligianni, F., Ravi, D., & Yang, G. (2017). Op. cit.
([151]) Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device? - a conceptualisation within the paradigm of the internet of things. Visualization in Engineering, 6(1). doi:10.1186/s40327-018-0063-8.
([152]) Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). Op. cit.
([153]) Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). Op. cit.
([154]) Silverio-Fernández, M. (2019). What is a smart device? - the key concept of the internet of things. https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-the-internet-of-things-52da69f6f91b.

devices, intelligent 'systems of systems' and end-to-end analytics ([155]). The combination of AI and the IoT also allows systems to be predictive, prescriptive, and autonomous. The continuous evolution of emerging applications will enable IoT sensors to collect a vast amount of data, while AI can aid in deriving intelligence to devise smarter applications for a smarter world ([156]). Smart devices may in the future be part of the infrastructure used in the technology presented in the scenarios in Chapter 5, since it equips regular devices with additional capabilities, increasing the technology's potential. However, smart devices could also be employed by infringers.

4.6 AI-enhanced supply chain



Artificial intelligence is also increasingly being used to improve supply chain operations and make them more cost-effective through its integration into supply chain management solutions and related management information systems to enhance automation and provide better visibility into static, real-time data ([157]). In addition to implementing fully automated decision-making, AI systems can adapt diverse types of cognitive computing to improve cooperation between artificial and human intelligence ([158]). Furthermore, AI-based tools can help to automate other stages in the supply chain, such as demand forecasting, production planning, and predictive maintenance ([159]).

AI-driven tools can be adapted to diverse aspects of the supply chain, including inventory management, to analyse and interpret datasets; warehouse administration; worker and material

([151])Liaqat, S., Ullah, S., Dashtipour, K., Zahid, A., Arshad, K., Assaleh, K., & Ramzan, N. (2021). AI-powered IoT for Intelligent Systems and Smart Applications. https://www.frontiersin.org/research-topics/15144/ai-powered-iot-for-intelligent-systems-and-smart-applications.
([152]) Liaqat, S., Ullah, S., Dashtipour, K., Zahid, A., Arshad, K., Assaleh, K., & Ramzan, N. (2021). Op. cit.
([157]) McCrea, B. (2019). What is Artificial Intelligence's Role in the Supply Chain? https://www.sourcetoday.com/supply-chain/article/21867397/what-is-artificial-intelligences-role-in-the-supply-chain.
([158]) McCrea, B. (2019). Op. cit.
([159]) McCrea, B. (2019). Op. cit.

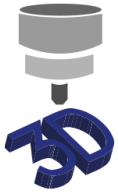
safety; productivity; delivery; and customer service ([160]). On top of this, AI will drastically transform supply chain decisions by using advanced analytics and modelling techniques to help decision-makers evaluate alternatives against complex and dynamic threats and constraints ([161]).

Among its other uses, AI can be used in adaptive robotics, processing Internet of Things (IoT) device information and a large amount of structured and unstructured data to help robots learn and make autonomous decisions ([162]). Other AI applications, such as natural language processing tools, have been developed to process human speech and react accordingly. Predictive analytics are being used in the fields of responsiveness, inventory and network optimisation, preventative maintenance, and digital manufacturing ([163]). Complex coordination performance can be achieved using search and pattern recognition algorithms, which are designed to analyse real-time data, enabling supply chains to respond to machine-generated, augmented intelligence while increasing visibility and transparency ([164]). Visibility refers not only to the internal aspects of the supply chain, but also to visibility among partners, which allows collaborative decision-making ([165]).

ML might also be used in making baseline forecasts for new products, identifying changing demand behaviours, optimising inventory levels, and managing product life cycles ([166]). It might apply algorithms to large operational data feeds to identify insights that enable the tracking and prediction of supply chain disruptions, recommending alternative actions in unexpected circumstances such as transport disruptions ([167]). In other areas such as manufacturing, AI-based collaborative robots can perceive their environment and move safely around humans working alongside them in production ([168]).

([160]) McCrea, B. (2019). Op. cit.
([161])Butner, K. (2017). AI is reshaping the supply chain. https://www.ibm.com/thought-leadership/institute-business-value/report/cognitivesupplychain.
([162]) Butner, K. (2017). Op. cit.
([163]) Butner, K. (2017). Op. cit.
([164]) Butner, K. (2017). Op. cit.
([165]) Butner, K. (2017). Op. cit.
([166]) Butner, K. (2017). Op. cit.
([167]) Butner, K. (2017). Op. cit.
([168]) Butner, K. (2017). Op. cit.

The adoption of AI in the supply chain can improve its general management and security. In the scenarios in Chapter 5, expert systems are used to optimise and, in some cases, automate the decision-making process in the supply chain. These scenarios also show how AI can be used in the supply chain for infringement. For example, AI in robotics can be used to optimise the mass production of infringing products and the processes in their supply chain.



4.7 AI in 3D printing

The 3D printing or additive manufacturing (AM) process begins with a digital file, in which the item to be printed is using either 3D printing software or a 3D scanner. This digital file is then exported to a 3D printer, which uses dedicated software to assemble the digital model into a physical object by building liquid material up in layers that then harden until the finished object emerges. ([169]).3D printing makes it technically possible to replicate nearly any object, with or without the authorisation of those who hold the rights to it ([170]).

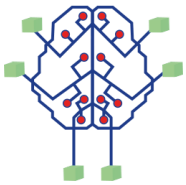
There are various possible benefits of 3D printing for innovation-intensive companies. It allows them to reduce their overheads when creating, designing, and testing new items or improving existing ones. In addition, the technology can be used to avoid paying for expensive prototypes, since it can quickly and cheaply produce multiple iterations of complex components using in-house 3D printers ([171]). 3D printing is a complex process, and AI could improve it considerably and make it even more efficient. The combination of AI and 3D printing could lead to new applications of the additive manufacturing technology, and more ([172]).

([169]) Malaty E., Rostama G. (2017), 3D printing and IP law. WIPO Magazine. February: https://www.wipo.int/wipo_magazine/en/2017/01/article_0006.html.
([170]) Malaty E., Rostama G. (2017), Op. cit.
([171]) Malaty E., Rostama G. (2017), Op. cit.
([172]) Drupa. (2019). It's a match! how artificial intelligence and 3D printing can work together. drupa. Retrieved from https://blog.drupa.com/en/its-a-match-how-artificial-intelligence-and-3d-printing-can-work-together/.

AI can be used in 3D printing as part of machine vision and machine learning systems. A multi-material inkjet 3D printer can use a vision system that extensively scans each layer of the object while it is being printed to correct errors in real time; at the same time, an ML system can use that information to predict the warping behaviour of materials and create more accurate final products ([173]). Machine learning can be used in additive manufacturing in several ways, including creating designs for 3D printing, tuning materials, optimising processes, carrying out *in situ* monitoring, and providing cloud services and cybersecurity ([174]). Moreover, ML data-driven models based on the understanding of the physical processes involved in 3D printing is essential, since these processes can then be optimised using incomplete or partial information ([175]). These data-driven models can also outperform time-consuming physics-based modelling and detect anomalies during in-process monitoring for quality control. In addition, ML affects other elements of 3D printing, such as the design and fabrication processes, qualification, and logistics ([176]).

Customs agencies' scanning processes could be improved by implementing 3D and penetration scanners adapted to large objects, or by applying nanotech. Customs inspections could also focus on inspecting, detecting and controlling the distribution of the most popular 3D printing materials, such as plastic pellets. Shipping of these materials is nevertheless expected to drop as the world adopts a 'circular economy' paradigm where materials are recycled and sourced locally. Nanocodes could be integrated into CAD files and used to track 3D-printed objects, allowing authorities to determine a product's authenticity easily ([177]). AI in 3D printing is a technology with potential in different areas, including in sensitive situations such as those described in the scenarios in the following chapter. However, it can also be used by criminals to facilitate the creation of infringing goods.

([173]) Winn, Z. (2019). A 3-D printer powered by machine vision and artificial intelligence. https://news.mit.edu/2019/inkbit-3d-printer-0604.
([174]) Goh, G. D., Sing, S. L., & Yeong, W. Y. (2020). A review on machine learning in 3D printing: Applications, potential, and challenges. Artificial Intelligence Review, 54(1), 63-94. doi:10.1007/s10462-020-09876-9.
([175]) Goh, G. D., Sing, S. L., & Yeong, W. Y. (2020). Op. cit.
([176]) Goh, G. D., Sing, S. L., & Yeong, W. Y. (2020). Op. cit.
([177])EUIPO (2020). Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020. https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2020_Tech_Watch_paper/2020_IP_Infringement_and_Enforcement_Tech_Watch_Discussion_Paper_Full_EN.pdf, p.35.



4.8 AI and Blockchain

Blockchain refers to a register or large database shared simultaneously by all of its users, all or some of whom may have the capability to enter data, according to specific rules set out in an extremely secure cryptographic computer protocol ([178]). The main features of blockchain include ([179]):

- **immutability**: there is a permanent record of transactions, and once a block is added, the transaction record cannot be altered;
- **decentralisation**: the blockchain is stored in a file that can be accessed and copied by any node on the network;
- **consensus**: each block on the blockchain is independently verified independently by validating consensus models;
- **transparency**: the full transaction history is available, since any party can access the blockchain and audit transactions.

The combination of AI and blockchain technology can be mutually beneficial. Both AI and blockchain use data in diverse ways and are particularly useful in processing and analysing a large amount of data using different tools ([180]). Both AI and blockchain act upon data in various ways; therefore, their combined use takes the manipulation of data to new levels. At the same time, the integration of ML and AI into blockchain, and vice versa, can strengthen blockchain's underlaying architecture and enhance the capacity of AI. Blockchain can be used to make AI more understandable and coherent,

([178]) Assemblée Nationale. (2018). *Mission d'information commune sur les usages des bloc-chaînes (blockchains) et autres technologies de certification de registres*. Assemblée Nationale. https://www2.assemblee-nationale.fr/15/missions-d-information/missions-d-information-communes/chaines-de-blocs.

([179])Sultan, K., Ruhi, U., Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications. arXiv.org. https://arxiv.org/abs/1806.03693.

([180]) Banafa, A. (2019). Blockchain and AI: A Perfect Match? OpenMind BBVA. https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/

including tracing and determining why specific decisions were made by ML. In this case, the ledger in blockchain can record all data and variables involved in ML decision-making ([181]).

Specific applications of AI and blockchain ([182]) can be observed in the following areas (for more information, see Annex):

- increasing smart computing power;
- creating diverse datasets;
- data protection;
- data monetisation;
- ensuring trustworthy AI decision-making.

The use of blockchain and AI can be seen in some of the scenarios in Chapter 5, in which the technology is used to protect unique identifiers and other relevant product information, and to protect registered designs in databases, which can then be shared with law enforcement. However, this combination of technologies can also be used for infringement, for example in AI-based cyberlockers, online-based data hosting services that provide remote file-storing and file-sharing services for various types of files and data within a secure storage architecture ([183]), and AI-supported blockchains that can evade detection.

([181]) Banafa, A. (2019). Op. cit.
([182]) Banafa, A. (2019). Op. cit.
[183] Techopedia. (n.d.). Cyberlocker. Techopedia.com. https://www.techopedia.com/definition/27694/cyberlocker

5. Copyright and design infringement and enforcement scenarios

This chapter will show how AI technologies and tools may be weaponised to facilitate copyright and design infringement, as well as how law enforcement may use these technologies to detect or defend against such infringement. These competing uses of AI are analysed below through fictional scenarios elaborated by the research team. These scenarios reflect the 'Intellectual Property Tech Chain' cycle, in which the exploration of AI as a technology is used as a base from which to analyse the use of that technology in developing an application ('weaponisation') to achieve a goal ('monetisation'), whether this is infringement or enforcement.

Each scenario is based on a thorough analysis of international references on the topic and was discussed with several international experts and with the members of the ad-hoc supporting Expert Group (see Annex 1 List of experts and stakeholders involved in the studyAnnex). However, the 20 scenarios only cover examples of potential uses of AI for infringement and enforcement and are not exhaustive.

To illustrate more clearly how AI tools can be used in practice for infringement or enforcement of relevant IP, two main storylines were created: one concerning physical products and the other involving digital content. This structure divides the 20 scenarios into two groups of 10, one group for each storyline.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

The two storylines are fictional, [184] but have been developed based on existing situations or situations that may be on the horizon given the pace of current technological developments. In particular:

- **Storyline α** concerns the infringement and enforcement of copyright and designs of **physical products** (see paragraph 5.1 Storyline α: infringement and enforcement of physical product copyright and designs);

- **Storyline b** concerns the infringement and enforcement of copyright and designs of **digital content** (see paragraph 5.2 Storyline b – infringement and enforcement of copyright and designs of digital content)

5.1 Storyline α: infringement and enforcement of physical product copyright and designs

This section analyses the use or potential use of AI technologies in 10 scenarios involving the infringement and enforcement of copyright and designs of physical products. Storyline α, described below, provides the context for these scenarios.

Storyline α: a European clothing, accessories and cosmetics company and the organised crime group that seeks to infringe the company's copyrights and design rights.

A well-known European clothing, accessories and cosmetics company, Marcoriana Vittaria (MarcVit), has developed a new clothing line called '*Artsters*' that takes original artistic expressions and places them on never-before-seen designs for shirts and dresses. This

[184] Since the storylines and relevant scenarios are fictional, their content may not be applicable or realistic in all jurisdictions, and will depend on the specific mandate and role assigned to law enforcement and other authorities involved in IP enforcement.

new Artsters clothing line will be marketed to young adults and hipsters in brick-and-mortar stores, and online through MarcVit's own retail website and through e-commerce platforms.
A sophisticated organised criminal group called 'OMD' has learned that MarcVit plans to launch its new clothing line, and OMD intends to make and to sell its own infringing version of Artsters products.

This storyline will be examined through the following 10 scenarios:

1. theft of copyrightable work or design under development
2. design registration fraud
3. mass production of copyright and design-infringing goods
4. importation of copyright and design-infringing goods
5. physical marketing of copyright and design-infringing products – infringer-controlled shop
6. physical marketing of copyright and design-infringing products – third-party-controlled shop
7. trade dress infringement
8. online marketing of copyright and design-infringing products – infringer controlled e-shop
9. online marketing of copyright and design-infringing products – sales on third-party marketplaces (surface web)
10. online marketing of copyright and design-infringing products – sales on third-party marketplaces (dark web).

5.1.1 Theft of copyrightable work or design under development

OMD has learned from a Marcoriana Vittaria (MarcVit) insider that MarcVit plans to launch its new Artsters clothing line in 6 months. OMD intends to use AI technologies to steal MarcVit's copyrightable artwork and innovative shirt and dress designs while they are still under development and, importantly, before MarcVit has the chance to make the Artsters clothing line available to consumers.

To accomplish this goal, OMD uses AI to conduct reconnaissance to identify who it perceives as the weakest and best-placed employee most likely to be duped by a phishing email, such as the executive assistant to the Chief Executive Officer (CEO) of MarcVit. OMD then uses AI to optimise a spear phishing attempt to obtain the CEO's email login and password. Once OMD has the ability to send and receive emails from the MarcVit CEO's email account, it sends an email to the head of MarcVit's design team to obtain the designs for the new Artsters clothing line.

OMD also uses another tactic. It has obtained AI-based software from a Crime-as-a-Service group that allows the user to generate any statement using an almost perfect ('deepfake') copy of someone's voice. Using this software, OMD generates a deepfake version of the CEO's voice and leaves a voicemail with MarcVit's design team lead asking her to email the new Artsters designs to an email account under OMD's control. OMD then stores the stolen designs on an encrypted hard drive.

For its part, MarcVit is concerned about criminals who may seek to steal its original artwork and new shirt and dress designs before the Artsters clothing line is released for sale. For this reason, MarcVit is looking for ways to work with law enforcement to use AI as an enforcement tool to prevent the pre-release theft of its new clothing line.

OMD's efforts are successful, but law enforcement investigates the case and executes a search warrant to obtain OMD's encrypted hard drive. Law enforcement then uses AI-based technology to break the encryption on OMD's hard drive and retrieve the files containing the stolen MarcVit Artsters designs.

AI tools used for infringement:

- Reconnaissance is an AI-supported machine learning technique (see
- 3.2.1 Machine learning (ML)) that learns from social media profiles, in this case by analysing the communication style of the executive assistant to the CEO of MarcVit. By collecting this data

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

using such an AI tool, OMD can weaponise ML to create an alias of an individual trusted by MarcVit.

- AI technologies can be weaponised to make phishing, hacking and brute force attacks more efficient. For example, natural language processing (see 3.2.2 Natural language processing (NLP)) can be adapted to create text, including coherent paragraphs. This NLP-generated text can then be used to create false emails and written communications based on existing information, which OMD could obtain either from open-source data or by scanning the email communications of the CEO's assistant and the CEO.

- Even if the phishing attempt fails, AI-supported hacking, AI-supported password guessing, and AI-supported CAPTCHA breaking can easily be used to predict the correct password and enable OMD to enter the CEO's email account. This AI technology can also be weaponised to predict updates to passwords.

- Deepfakes of someone's voice (like the CEO's voice in this scenario) can be generated by AI generative adversarial networks (see
-
- 3.2.1 Machine learning (ML)).

- Machine learning algorithms and computer speech (see 3.2.3 Computer speech) can also be used by OMD to imitate the CEO's voice, thereby misleading the MarcVit designer. Deep neural networks, in particular, can be used to recognise patterns in speech.

AI tools used for enforcement:

- Machine learning, and in particular supervised learning, can be converted into a functional application by law enforcement to break the encryption used by OMD. In addition, deep learning algorithms, specifically convolution neural networks (CNN), might be used to classify encryption

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

schemes and solve some of the limitations of ML such as the ability to perform an accurate cryptanalysis ([185]).

- In addition, MarcVit could fortify its cybersecurity efforts with AI by using ML to quickly analyse millions of events and identify many different types of threats: for instance, NLP-enabled filters can classify and analyse emails to block phishing attacks. This information can then be provided to law enforcement in support of their investigation.

- AI bots could also be employed by MarcVit to crawl the web to help identify and detect social engineering bots that are targeting MarcVit. These AI bots are self-learning software applications that are programmed with natural language processing and machine learning tools. In the framework of a targeted investigation, a specialised law enforcement department could employ a similar tool and approach.

5.1.2 Design registration fraud

Two types of design registration fraud scenarios are presented below.

5.1.2.1 Design registration fraud where the registration itself is fraudulent

MarcVit intends to register the original shirt and dress designs that will eventually be included in its Artsters clothing line. However, after stealing MarcVit's original shirt and dress designs, OMD hopes to fraudulently register the designs as its own with a national intellectual property office (IP Office).

OMD intends to use AI technologies to 'trick' the IP Office into believing that MarcVit's original designs were actually created by OMD.

([185]) Pan, J. (2017). Encryption scheme classification: a deep learning approach. International Journal of Electronic Security and Digital Forensics, 9(4), 381-395. doi:10.1504/IJESDF.2017.087397.

However, the IP Office plans to use AI technologies of its own to identify and stop fraudulent design registrations.

AI tools used for infringement: 

- Generative adversarial networks and computer vision tools (see 3.2.4 Computer vision) can be weaponised by OMD to produce a fake appplication for registration, replicating very similar applications filed by MarcVit and others in order to trick the IP Office. In particular, a natural language processing tool could replicate the text of the original applications. Generative modelling is an unsupervised learning task in machine learning that automatically acquires information about regularities or patterns in input data to generate new examples that were based on the original information ([186]).

AI tools used for enforcement: 

- Machine learning can be used by the IP Office to create a system that detects if someone is attempting to re-register a previously registered design. GANs could also be trained to determine if a part or parts of several original designs are being combined to create a spurious 'new' design.

- AI-supported blockchain (see AI and Blockchain can be used by the IP Office to protect the information in a registration system from vulnerabilities. In fact, blockchain's cryptography and immutability provide an additional security layer.

- In general, intellectual property offices responsible for national design registrations can use deep learning and convolutional neural networks to analyse and recognise visual imagery in order to

([186]) Brownlee, J. (2019). A gentle introduction to generative adversarial networks (GANs). Machine Learning Mastery. Retrieved from https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/ .

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

scan shapes and patterns for similarities. The model could be optimised to identify infringement even if the image is taken from a different angle.

5.1.2.2 Design registration fraud where the registration invoices are fraudulent

MarcVit registers its original shirt and dress designs with a national IP Office ("IP Office"). When the time comes for MarcVit to renew its design registrations, MarcVit must pay a renewal fee to the IP Office. Knowing this, OMD sends MarcVit an invoice that looks like it came from the EUIPO, but includes a payment address that OMD controls, so that OMD, rather than the IP Office, receives MarcVit's re-registration fee.

The IP Office has learned about this type of design registration fraud scheme and uses AI technologies to anticipate when certain design registrants, like MarcVit, are being targeted by groups like OMD. It warns MarcVit and other registrants of OMD's fraud scheme and reiterates the proper address to which OMD should send the re-registration fees. MarcVit makes the information available to law enforcement.

AI tools used for infringement: 

- Machine learning with pattern recognition and computer vision tools can be used by OMD to produce a fake re-registration invoice virtually identical to the original issued by the IP Office.

- Natural language processing can be weaponised by OMD to create text that resembles an authentic invoice or other 'official' document.

AI tools used for enforcement: 

- NLP-enabled filters can classify and analyse emails received by MarcVit to block phishing attacks. This information can be shared by MarcVit with the IP Office, which can then increase

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

its security measures, and with law enforcement, to support the investigations against the organised criminal group.

5.1.3 Mass production of copyright and design-infringing goods

MarcVit intends to mass produce its Artsters clothing line so it can be distributed on a global scale in 6 months. MarcVit is concerned that infringers may produce copyright and design-infringing versions of their new line before they are released to the public.

OMD wants to use AI technologies, including AI-supported robotics, to optimise its own illegal manufacture of infringing versions of the copyright-protected artistic works and unique clothing designs that make up MarcVit's Artsters clothing line.

MarcVit has alerted law enforcement to its concerns, and law enforcement intends to use AI technologies to stop criminal groups like OMD from mass-producing infringing copies of the Artsters clothing line.

AI tools used for infringement:

- Generative design-based tools (see **Error! Reference source not found.**can be weaponised by OMD to more efficiently mass-produce infringing copies of the Artsters clothing line.
- AI in robotics (see AI in roboticscan be used to optimise the mass production of the Artsters products and the processes in their supply chain.
- OMD could also use neural-style transfer techniques to create additional designs that replicate MarcVit's original designs.

AI tools used for enforcement: 

- A platform can be developed using deep learning and convolutional neural networks (CNN) to analyse and recognise visual imagery in order to scan shapes and patterns for similarities. This model could identify infringement even if OMD presents an image taken at a different angle to avoid discovery by less advanced AI tools.

- AI-supported blockchain can also be used by MarcVit to protect the registered designs in a common database, maintained by rights holders, providing a reliable tool to store information that can be shared with law enforcement in support of the investigation against OMD.

- Machine learning tools can be then adopted to quickly process and classify the data, which can then be shared with law enforcement authorities investigating the case.

5.1.4 Importation of copyright and design-infringing goods

OMD intends to sell its infringing versions of MarcVit's Artsters clothing line all over the world. To accomplish this goal, OMD will have to find a way to avoid customs authorities in the countries to which it will export its infringing goods. OMD will use AI to evade customs inspections and avoid seizure of their infringing goods. Specifically, OMD hopes AI will help it:

- identify and create shell corporations in different countries, so customs authorities will not know that OMD is behind the imports of infringing goods;
- engage in 'port shopping' whereby OMD chooses ports where customs authorities are least likely to seize OMD's infringing goods;
- optimise its concealment of the infringing goods in shipping containers;
- find the best trade route between its illicit factories and ports of entry.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

The customs authorities, meanwhile, use AI to identify the real importer of infringing goods behind the shell corporations and expose importers engaged in 'port shopping'. The customs authorities also use AI software to scan shipping containers for hidden infringing goods.

AI tools used for infringement: 

- OMD can weaponise machine learning to create a system that identifies the quickest trade route between its illicit factories and ports of entry, chooses ports, and helps to conceal infringing goods in containers, limiting the risk of being detected by customs authorities. The system is constantly updated.

- OMD can also weaponise expert systems (see 3.2.6 Expert systems (ESs)) to optimise the decision-making process it uses for its supply chain.

- Adversarial machine learning can be used by OMD to evade detection. Specifically, OMD can implement this AI-based technique to change trade routes and optimise its concealment of infringing copies of MarcVit products. Adversarial ML is a technique that can be weaponised to deceiving ML models designed to detect the illegal activities of an organised criminal group such as OMD. For instance, OMD could use adversarial ML techniques to provide deceptive input data, or 'false flags', to cause a malfunction in the ML model being used by customs authorities, making it generate inaccurate information.

- To use adversarial ML effectively, OMD would have to have extensive knowledge of customs authorities' use of AI to detect infringements. If an ML model is used by law enforcement or customs authorities, OMD could use an ML model extraction attack to obtain information on its functioning. This 'reverse engineering' strategy could be used to identify and potentially even reproduce the neural network ([187]).

([187]) Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing Machine Learning Models via Prediction APIs. USENIX. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

AI tools used for enforcement: 

- ML pattern recognition tools can be used by customs authorities to identify risk indicators related to the importation of IP-infringing goods.

- In more complex cases, customs and law enforcement authorities can potentially use quantum computing in AI (see 3.2.5 AI quantum) to recognise patterns in large datasets and identify similarities (e.g. specific characteristics of shipments to predict infringement). The processing power of quantum computing could enable the analysis of a large amount of data, at a regional or even global level.

- Expert systems [see 3.2.6 Expert systems (ESs)] can be used to decide which strategy and vulnerabilities are most appropriate to the situation.

5.1.5 Physical market sale of copyright and design-infringing products – infringer-controlled shop

MarcVit uses AI to generate unique visual anti-counterfeiting technology on the labels of its Artsters clothing line, so customers can use MarcVit's app to scan and confirm that what they are buying in markets and elsewhere is authentic. MarcVit periodically changes this visual anti-counterfeiting technology to make duplication more difficult.

OMD hopes to use AI technologies to replicate and track changes to MarcVit's visual anti-counterfeiting technology so that OMD can successfully sell its infringing goods in stores that OMD controls.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

MarcVit is sharing data about its AI-generated visual anti-counterfeiting technology with law enforcement, so national authorities can use their own AI to detect OMD's fakes when they investigate infringer-controlled stores.

AI tools used for infringement:

- Pattern recognition, computer vision and/or machine learning can be used by OMD to detect and replicate the patterns in the visual anti-counterfeiting technology.

AI tools used for enforcement:

- AI-supported blockchain (see AI and Blockchaincould be adopted by MarcVit to create and secure a label, code, or image that would enable its clients to verify the authenticity of a product, and which the company can share with law enforcement authorities investigating the case. Once it is independently verified by national investigators, this would also provide important evidence for the prosecutor to present in court.

- Machine learning can be adopted in the creation of the visual identity that will be protected. Law enforcement will be able to identify OMD's infringing copies using computer vision tools.

5.1.6 Physical market sale of copyright and design-infringing products – third-party-controlled shop

MarcVit strictly manages the wholesale prices that it charges third-party controlled stores for its Artsters clothing line. MarcVit will charge different wholesale prices in different countries.

To select prices for its infringing versions of Artsters clothes that are just below MarcVit's wholesale prices, OMD uses AI to track when MarcVit's prices change and how they vary from country to country.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

To combat these efforts, MarcVit shares its sensitive pricing data with law enforcement so national authorities can use their own AI to develop a price comparison tool that will detect infringing Artsters goods based on price.

AI tools used for infringement:

- OMD can weaponise machine learning and natural language processing to analyse the different prices of Artsters clothes in different countries and track the changes in these prices, consequently adjusting its marketing policy.

AI tools used for enforcement:

- Law enforcement can use machine learning to create its own platform that works as a price comparison tool.
- Law enforcement can implement deep learning tools to obtain insights into infringement patterns in order to detect and prevent the crime.
- Expert systems (see 3.2.6 Expert systems (ESs)) can be developed to create an interface that uses the generated data to analyse patterns and determine which decisions could prevent future criminal activities.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

5.1.7 Trade dress infringement

To accompany its Artsters clothing line, MarcVit has launched an Artsters cosmetics line that includes shapes and colours for the cosmetics containers that are not functional but unique, distinctive, and difficult to replicate.

As with the Artsters clothing line, OMD will use AI to try and infringe the unique shapes and colours of MarcVit's Artsters cosmetics containers and then sell them in stores and online.

MarcVit is providing data to law enforcement on the components of the unique colours of the Artsters cosmetics containers, so law enforcement can use its own AI to distinguish the authentic colours from attempts by groups like OMD to infringe them.

AI tools used for infringement:

- OMD can weaponise computer vision to identify and replicate the unique colours and shapes of the new Artsters cosmetics line.
- AI can be integrated into robotics [see AI in roboticsto improve the manufacturing process, enabling OMD to create the infringing copies in an easier and faster way.

AI tools used for enforcement:

- Law enforcement can implement computer vision technology to identify the unique colours and shapes of the new Artsters cosmetics line and distinguish them from OMD's infringing copies of MarcVit's trade dress.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

- Deep learning-based optical character recognition (OCR) tools can identify and distinguish infringing copies of the Artsters cosmetics line sold online from the authentic products.

- Web crawlers automated with AI can find patterns in the data (e.g. domain names, content of websites with fakes, websites or products with similar names, or Javascript) used by OMD to market infringing goods. Web crawling is a procedure in which data on web pages is indexed using a program or automated script by copying pages for processing, which are then indexed by a search engine ([188]). One of the main objectives of a crawler is to understand the content of a website. Law enforcement can apply machine learning (ML) technology to identify the unique underlying patterns of websites, including changes in their structures over time.

- Finally, law enforcement can use natural language processing to analyse users' behaviour and the content they share to identify the fraudsters.

5.1.8 Online marketing of copyright and design infringing products – infringer-controlled e-shop

MarcVit markets and sells its Artsters clothing line online through its own retail website and through e-commerce platforms.

OMD uses AI to scan MarcVit's online listings of shirts and dresses in the Artsters clothing line to identify the most popular Artsters clothes and then uses this information to sell infringing versions of these products on OMD-controlled e-shops. OMD stores this information on encrypted hard drives and servers.

([188]) Dilmegani, C. (2021). What is web Crawling? How it works in 2021 & examples. AIMultiple. https://research.aimultiple.com/web-crawler/.

Law enforcement uses AI to systematically identify, seize, and take down servers storing OMD's information. Law enforcement also uses AI to break the encryption that OMD uses on its hard drives and servers.

AI tools used for infringement: 

- Web crawlers using machine learning, computer vision, and speech technologies can all be weaponised by OMD to scan websites and identify (and then infringe) the most popular Artsters product designs.

AI tools used for enforcement: 

- Law enforcement can use machine learning (ML) to automate web crawlers to find patterns (e.g. domain names, content of websites with fakes, websites or products with similar names, or Javascript) used by OMD.
- Deep learning-based optical character recognition (OCR) tools can used to identify and distinguish infringing copies of the Artsters clothing line sold by OMD online from the authentic products.
- The marketing of the infringing products can be tracked using computer vision, in particular natural language processing text recognition, to identify the characters and their similarity to the originals.
- NLP can also be used to analyse users' behaviour and the content they share.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

- ML can be used to break the encryption used by OMD. Deep learning algorithms, specifically convolution neural networks (CNN), might be used to classify encryption schemes and solve some of the limitations of ML, such as the ability to perform an accurate cryptanalysis.

- Machine translation in natural language processing can also aid in the translation of websites and identify infringing content in other languages.

5.1.9 Online marketing of copyright and design-infringing products – sales on third-party marketplaces (surface web)

MarcVit markets and sells its Artsters clothing line online through popular third-party e-commerce platforms.

OMD uses AI to scan MarcVit's online listings of Artsters shirts and dresses and identify MarcVit's most popular clothes. OMD then uses this information to sell infringing versions on popular third-party e-commerce platforms.

National product safety authorities and other law enforcement authorities purchase and use third-party AI-enabled products to: (1) identify third-party sellers such as OMD group members who attempt to sell infringing products and (2) take down listings for infringing products. In this way, authorities identify OMD members who are infringing MarcVit's copyright and design rights.

AI tools used for infringement: 

- Machine learning, computer vision and natural language processing can all be weaponised by OMD to scan websites and identify the most popular designs, which it will later infringe and sell online.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

- OMD could also use AI with virtual reality (VR) / augmented reality (AR) to develop an online persona to promote infringing products on social media marketplaces. In this case, OMD members would hide their identities while launching different marking campaigns.

AI tools used for enforcement: 

- Law enforcement can use machine learning (ML) to automate web crawlers to find patterns (e.g. domain names, content of websites with fakes, websites or products with similar names, or JavaScript) used by OMD.

- Law enforcement can use AI tools for probabilistic guessing, such as predicting the next word in a text or recognising suspicious text from a website based on whether such text has been seen before.

- Deep learning-based optical character recognition tools can be also used by MarcVit in collaboration with the law enforcement authorities investigating the case.

- NLP can analyse users' behaviour and the content they share.

- The marketing of the infringing products can also be tracked using computer vision and NLP text recognition to identify the characters and their similarity to the originals. Once the listings are identified, law enforcement can seek an order compelling the third-party e-commerce platform to take down the listing.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

5.1.10 Online marketing of copyright and design-infringing products – sales on third-party marketplaces (dark web)

OMD uses the same AI for its sales on the surface web to automate the sale of infringing versions of the most popular Artsters clothes on third-party marketplaces on the dark web. On the dark web, OMD only accepts cryptocurrency as payment.

Law enforcement hires computer forensics experts or creates its own 'cyber patrol' unit that specialises in cryptocurrency to analyse OMD's cryptocurrency transactions and identify members of the group.

Law enforcement also uses AI tools to find similarities between OMD-affiliated users selling infringing Artsters clothes on different platforms on the dark web and, if possible, track such sellers across dark web and surface web platforms.

AI tools used for infringement: 

- Machine learning (ML) and computer vision tools can be used by OMD to scan websites and identify the most popular Artsters designs, which will be later copied and sold to the public on the dark web.

AI tools used for enforcement: 

- A cyber patrol unit could be involved in the investigation, making full use of advanced technologies including AI tools. In many EU countries, as well as in countries outside Europe, specialised law enforcement units or 'cyber patrols' are trained to conduct investigations against serious crimes conducted using the internet and the dark web. These units also investigate counterfeiting and piracy cases.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

- Law enforcement can use machine learning (ML) to automate web crawlers to find patterns (e.g. domain names, content of websites with fakes, websites or products with similar names, or Javascript) used by OMD in its sales of infringing goods.

- Law enforcement can use AI tools for probabilistic guessing, such as predicting the next word in a text or recognising suspicious text from a website based on whether such text has been seen before.

- Deep learning-based optical character recognition tools can also be used by cyber patrol units investigating the case.

- Natural language processing can look for specific information on a website, and exploratory analysis (mathematical analysis) can find correlations in datasets. This AI-enabled tool could also be used to identify similar domains/sellers on the dark web.

- Advanced analytical techniques based on machine learning (ML) could be used by law enforcement to determine the identity of the cryptocurrency address holders. In particular, supervised ML can identify the cryptocurrency cluster and assign it a category to help identify controlling entities. Deep learning and neural networks can be used for latent representations on a graph or network structure.

- AI can also use graph analysis to 'follow the money' by detecting correlations between addresses on the blockchain.

5.2 Storyline b – infringement and enforcement of copyright and designs of digital content

This section will analyse 10 different scenarios concerning the infringement and enforcement of copyright and designs of digital content, based on storyline b below.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

Storyline b: a multinational media conglomerate producing a variety of digital media and the organised criminal group that seeks to infringe the conglomerate's copyrights and design rights.

A multinational media conglomerate, Mottanna, produces a variety of digital media, including music, movies, television broadcasts, software, and video games. Mottanna markets its popular digital content all over the world.

A sophisticated online organised criminal group called the InterGalactics, or 'the IGs', is one of the most successful online infringers and distributors of copyright-protected digital works.

This storyline will unfold through the following 10 scenarios:

1. hacking media accounts
2. computer icon / virtual commodity infringement
3. social media offences
4. sales of hacked media accounts on the dark web
5. media sharing platform offences
6. virtual/gaming world offences
7. P2P and BitTorrent
8. live streaming – sports broadcast link aggregator (advertising-based)
9. IPTV crime – unauthorised access to subscription-based IPTV service
10. training an AI application.

5.2.1 Hacking media accounts

Two types of media account hacking scenarios are suggested in this section.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

5.2.1.1 Hacking movie streaming media accounts

Members of the InterGalactics purchase a database of existing movie streaming service customers and use this information to execute an AI-based brute force attack to hack the accounts of these customers and stream movies without authorisation.

Law enforcement uses AI-based machine learning to track changes to IP addresses, MAC addresses, content selection and other non-human behaviour on the movie streaming service accounts to identify accounts that are under the IGs' control.

Law enforcement also uses AI bots to crawl the web to identify online attempts at social engineering.

AI tools used for infringement: 

- AI technologies can be employed by the IGs to hack databases through brute force attacks and AI-supported password guessing. The same technologies, along with AI-supported CAPTCHA breaking, could be used to hack the user accounts found in the hacked databases.

- Although malware does not necessarily require the use of AI, AI-enabled technologies could be weaponised by the IGs to create more sophisticated malware that can imitate trusted system components and deceive movie streaming account users into providing their login information.

- Machine learning can be used to carry out 'smart' phishing attacks, where a baseline of data exclusive to the user being targeted is used to make the phishing attack look more legitimate and authentic. Machine learning can be further misused by organised criminal groups like the IGs to learn patterns and exploit other personal information.

AI tools used for enforcement: 

- Law enforcement can use deep learning tools to identify online attempts at social engineering.
- Convolutional neural networks (CNN) for image and pattern recognition can be used for the same purpose by law enforcement.
- A machine learning-based system could be developed to scan images and identify fake login pages, phishing behaviours, or other suspicious activities. Computer vision, natural language processing, and machine learning could recognise these activities and block them. These AI tools would be able to carry out real-time scanning of inbound links, using visual indications to determine the authenticity of a login page.

5.2.1.2 Hacking music streaming media accounts

The InterGalactics upload infringing copies of Mottanna's sound recordings to music streaming services using song titles that are confusingly similar to Mottanna's actual song titles. The IGs claim that they are the owners of the sound recording copyright and therefore entitled to the royalties for streams of their pirated version of Mottanna's sound recordings. The IGs' goal is to increase the number of streams of these pirated sound recordings and thereby maximise the royalties they can receive for these streams.

The IGs then use AI to:

- hack into and take over actual accounts on music streaming services to play/stream their pirated versions of Mottanna's sound recordings that they had previously uploaded on these services
- create free trial accounts with music streaming services for the sole purpose of streaming/playing their pirated versions of Mottanna's sound recordings
- artificially inflate the number of streams of their pirated versions of Mottanna's sound recordings on music streaming services by waiting more than 30 seconds before replaying the streams of the songs

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

Law enforcement uses AI-based pattern recognition technology to monitor the misuse of music streaming media accounts to identify and to track the accounts that have been hacked and the IG members who control the hacked music streaming accounts.

AI tools used for infringement: 

- AI-enabled malware can be used by hackers to identify potential vulnerabilities in the music streaming service, infect the service with malicious code, and then gain access to a music streaming service account in order to use existing accounts on the service at a later time. The attack is not immediate, but rather is triggered by specific actions at a certain time. This approach can maximise the impact of the attack, since it would not necessarily raise suspicion at first.

- AI can be used to create malware that imitates trusted system components, which could improve stealth attacks. In this case, hackers could use AI malware programs to automatically learn the services' computation environment, patch update lifecycle, and preferred communication protocols, as well as the moments when the systems are least protected.

- The IGs can also use AI-enabled bots to automate the creation of free accounts on the music streaming services and automatically replay the songs they previously uploaded for more than 30 seconds, so that each replay generates royalties.

AI tools used for enforcement: 

- Machine learning could be used to model and monitor users' behaviour, raising an alert if there are any anomalies. The same technology could detect infringement patterns to identify larger networks of IP infringers.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

- AI can detect duplicate copies of sound recordings on the service containing suspect ownership data, and copyright owners can help law enforcement identify which uploads are authentic and which are infringing.

5.2.2 Computer icon / virtual commodity infringement

One of Mottanna's top artists is giving a virtual 3D concert on a popular Mottanna gaming platform. Mottanna sells tens of thousands of tickets to fans who will attend the virtual concert using their avatars. The IGs create an avatar of their own and use it to sell virtual hats and T-shirts bearing the Mottanna logo and an image of the Mottanna musician for EUR 1 per virtual item of clothing without Mottanna's authorisation.

Law enforcement purchases AI that identifies the IGs' avatar as well as the unauthorised use of logos that are identical or very similar to Mottanna's logo.

AI tools used for infringement: 

- The IGs can weaponise machine learning and computer vision tools using Mottanna's logos to produce new and infringing images: neural networks can produce images similar to a specific image, such as the one developed by Mottanna. This includes colour alteration and pixelisation of images. Pattern recognition, as well as text, video, and audio recognition tools, can be used to create a new item.

- The IGs can also create AI-based bots to test the commercial viability of their infringing virtual commodities and then (if viable) to promote them. AI bots are self-learning bots programmed with natural language processing and machine learning. The initial stage of training and building

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

an AI bot takes a long time, but once weaponised and used during training, they are highly efficient in terms of time and costs ([189]).

- Adversarial machine learning can be weaponised by fraudsters to overcome detection. This technique could be used by the IGs to change how they present their infringing copies online and evade detection. To accomplish this, IP infringers would first illegally obtain extensive knowledge about authorities' use of AI to detect infringement. Using this stolen information, fraudsters would then implement adversarial machine learning to identify and circumvent the authorities' detection patterns.

- If law enforcement uses an ML model, an ML model extraction attack could obtain information on its functioning. This "reverse engineering" strategy could be used to identify and potentially reproduce the neural network ([190]).

AI tools used for enforcement: 

- Computer vision or pattern recognition applications can be used to detect the specific logo used by the IGs on their avatars or digital items.

- Neural networks can be used by the authorities to find images similar to a specific image through pattern recognition. Convolutional neural networks can be used for image and pattern recognition.

- NLP can search for specific information on a website, and exploratory analysis (mathematical analysis) can be adopted by law enforcement to find correlations in datasets.

([189]) Joshi N. (2020) Choosing Between Rule-Based Bots And AI Bots. https://www.forbes.com/sites/cognitiveworld/2020/02/23/choosing-between-rule-based-bots-and-ai-bots/.

([190]) Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing Machine Learning Models via Prediction APIs. USENIX. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

5.2.3 Social media offences

Members of the InterGalactics have successfully developed AI that seems to perfectly impersonate the voices of popular singers and musicians who have signed to Mottanna's music label. These voices then appear to sing 'samples' of copyright-protected songs composed by other artists. The IGs seek to incorporate these impersonations into 'deepfake' music videos.

The IGs have also successfully used social engineering to hack into the social media accounts of Mottanna's singers and musicians. The IGs hope to legitimise their deepfake videos by broadcasting them on the musicians' hacked social media accounts and later monetising or selling copies of the deepfake videos elsewhere online.

Law enforcement works with third-party companies to develop AI that can distinguish between a musician's true voice and an impersonation.

AI tools used for infringement: 

- Generative adversarial networks and deep learning can be weaponised by the IGs to create the imitation 'samples' of music videos of singers signed to Mottanna.

- Social engineering is a type of hacking carried out through human interactions, whereby an attacker uses psychological manipulation that leads innocent people to make mistakes and unwittingly reveal information that they should not ([191]). AI can be used for social engineering through voice cloning, deepfakes, and natural language processing phishing bots that could improve the hacking techniques used on Mottanna's singers and musicians.

([191]) Analytics India Magazine (2019) How AI Is Helping Combat Social Engineering Attacks. https://analyticsindiamag.com/how-ai-is-helping-combat-social-engineering-attacks/ .

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

AI tools used for enforcement: 

- Convolutional neural networks can be used by law enforcement authorities for image and pattern recognition to identify the IGs' deepfake music videos.
- Pattern recognition can be used by IT professionals to identify social engineering risks, which can then be communicated to law enforcement authorities investigating the IG case.
- Once the deepfakes have been identified, law enforcement can use AI bots, such as automated cyber patrols, to look for images on social media that contain copyright and design infringement.

5.2.4 Sales of hacked media accounts on the dark web

The InterGalactics have successfully used social engineering to hack into the social media accounts and cloud storage accounts of Mottanna's singers and musicians. Now they intend to use AI to identify the best dark web forums to advertise the sale of the stolen credentials used to hack the accounts.

The IGs also will try to use AI to build up their reputation on dark web forums to maximise the sale of the stolen credentials. The IGs target their marketing of the stolen credentials to operators of dedicated music piracy websites and pre-release networks who intend to use their access to these accounts (and the private direct messages they contain) to look for and to obtain copies of sound recordings before they are commercially released.

Law enforcement uses AI to find and track the IGs' attempts to sell the stolen credentials across different forums on the dark web so authorities can conduct a coordinated takedown of all the IGs' attempted sales.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

AI tools used for infringement: 

- AI-supported internet bots can be weaponised by the IGs to look for the dark web forums that are most likely to allow them to advertise the sale of the stolen credentials on the dark web and elsewhere.

- The IGs are in possession of directories containing links to hidden services that exist on the dark web as well as on the surface web. They implement web crawling tools to identify where to post their advertisements.

AI tools used for enforcement: 

- Deep learning-based optical character recognition tools can be used by law enforcement to track the IGs' attempts to sell the credentials that the IGs stole. This AI tool could also be combined with natural language processing.

- Convolutional neural networks for image and pattern recognition can also be used to track the IGs' attempts to sell the credentials they stole.

- Finally, NLP that looks for specific information on a website, or exploratory analysis (mathematical analysis), can be adopted to find correlations in datasets.

5.2.5 Media sharing platform offences

Two types of media sharing platform offences are described in the following two scenarios.

5.2.5.1 Uploading deepfake music videos

The InterGalactics make copies of deepfake music videos they have created using AI technologies and upload them to online video services, hoping to make money from the online advertising that these deepfake videos generate.

Law enforcement uses AI-enabled text-based and content-based pattern recognition and image recognition technology to identify the deepfake videos and automate the takedown of the IGs' infringing uploads.

AI tools used for infringement: 

- Generative adversarial networks can be weaponised by organised criminal groups operating online, such as the InterGalactics, to create deepfake music videos.

AI tools used for enforcement: 

- AI-improved algorithms can detect if music is copyright protected: computer vision programs can recognise if the image has been uploaded before. AI software can also analyse photos and videos, providing a signal (a 'confidence score') about whether the material is likely to have been artificially created.

- Computer vision can analyse the sequence of images in the video.

- Web crawlers can find patterns (e.g. domain names, content of websites with fakes, similar names, Javascript) that show that the IGs are behind the deepfake videos.

- Machine learning, and in particular deep learning-based fingerprinting of media content, could also be used by Mottanna as a precautionary measure. The fingerprint data could be shared with law enforcement to identify infringing music videos and support takedown orders. The fingerprinting technique can be adopted by content-sharing platforms to identify the unauthorised use or monetisation of copyright-protected content, as well as to apply specific policies defined by content rights holders, including blocking ([192]).

- Convolutional neural networks can also be used for image and pattern recognition.

- NLP that looks for specific information on a website, or exploratory analysis (mathematical analysis), can be used by enforcement authorities investigating the case to find correlations in datasets to show that that IGs are behind the uploaded deepfake videos.

5.2.5.2 Unauthorised streaming of movies and sports broadcasts

The InterGalactics use AI to automate the unauthorised streaming and online distribution of copyright-protected Mottanna movies and sports broadcasts over popular media sharing platforms.

Law enforcement uses AI-based image recognition to identify the type of streamed or distributed content and quickly determine which content belongs to Mottanna and other copyright owners. Once identified, law enforcement can also use AI to automate the takedown of the IGs' infringing streams and seize the servers used to distribute infringing copies of Mottanna's copyrighted content online.

([192]) European Union Intellectual Property Office (EUIPO). (2020). Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP.' EUIPO. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Automated_Content_Recognition/2020_Automated_Content_Recognition_Discussion_Paper_Full_EN.pdf.

AI tools used for infringement: 

- Machine learning can be weaponised by the IGs to identify and eliminate simple digital dots and digital watermarks used by Mottanna to track the distribution of unauthorized copies of its movies online. Generative adversarial network could also be used to incorporate certain effects into livestreams to prevent automatic content recognition by adding new logos, removing original logos, watermarks, and fingerprinting, or enhancing content. The IGs can then proceed with the distribution of fake livestreams.

AI tools used for enforcement: 

- AI-based web crawlers can find patterns (e.g. domain names, content of websites with fakes, websites or products with similar names, or Javascript) to identify criminal actors, techniques and trends.

- Machine learning can carry out an analysis of the sequence of images in the video to identify copyright infringing content.

- Machine learning- or deep learning-based fingerprinting of media content can also be used by Mottanna. Convolutional neural networks can be employed for image and pattern recognition.

- NLP that looks for specific information on a website, or exploratory analysis (mathematical analysis), can find correlations in datasets.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

5.2.6 Virtual/gaming world offences

The InterGalactics have developed 'cheats' for Mottanna's massive online gaming platform that the IGs then sell to Mottanna's most competitive customers, who can then use those cheats to 'steal' (i.e. copy without authorisation) virtual items (copyright-protected code) that they would otherwise have to earn or pay for in the game, in order to gain a competitive edge against their opponents.

The IGs use AI to identify vulnerabilities in the game to maximise the effectiveness of these illegal cheats and, in turn, how much they can charge Mottanna's customers for the cheats.

Law enforcement use AI-based machine learning to distinguish and identify those Mottanna customers who are using cheats, which will then facilitate identifying the IGs member who sold those cheats.

AI tools used for infringement: 

- Machine learning and computer vision can be weaponised by the IGs to infringe a videogame copyrights by modifying the game's colours, icons, video, or audio.
- Natural language processing and machine learning bots can be used to sell articles online.
- AI-supported hacking could allow the IGs to obtain the access keys to Mottanna's online gaming platform. They could hack servers or obtain second-hand keys from online resale markets for this purpose. ML can be weaponised to target and circumvent authentication and identity validation, including voice and visualisation-based hacking attempts.
- Mottanna's skins in the game can be imitated with the help of computer vision tools.
- IGs could even develop AI-empowered bots to use as mules during an illegal transaction in the game to cover their tracks.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

AI tools used for enforcement: 

- Computer vision and text recognition can identify similar images, names, and content across the internet, especially on marketplaces and gaming platforms, as in this scenario.

- Convolutional neural networks could alternatively be employed by law enforcement for image and pattern recognition.

- AI algorithms can efficiently deal with large amounts of data through pattern recognition ([193]). AI-supported big data analysis can identify suspicious behaviours globally, for example, if new accounts have been created by an app. ML can then compare existing user accounts to others to distinguish those that have been detected as suspicious, or that have suspicious or unusual patterns.

- Law enforcement could implement an AI-enabled tool to analyse players' behaviour – such as their moves, trades, and playing times, and the time between their logins and logouts – to distinguish between real players and bots.

5.2.7 P2P and BitTorrent-like applications

The InterGalactics members often use tools to share infringing copies of Mottanna's movies efficiently and anonymously among themselves. In particular, they use AI to develop and run a decentralised file-sharing network, called IGFlix, that is similar to existing P2P networks, but more fragmented in its distribution of packets than typical BitTorrent or P2P technology. This file-sharing network is connected to a cryptocurrency blockchain, enabling the IGs to sell premium IGFlix accounts (i.e. user accounts with privileges) and anonymously pay rewards to members who occasionally upload infringing content to IGFlix.

([193]) Melnichuk A. (2020). How Big Data and AI Work Together. Ncube. https://ncube.com/blog/big-data-and-ai .

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

The IGs also use AI to quickly circumvent the technological protection measures that Mottanna uses to prevent unauthorised access and copying of its copyright-protected movies.

Law enforcement uses AI-based pattern recognition technology to find common patterns between members of the IGs, users of the IGFlix peer-to-peer technology, and cryptocurrency transactions occurring on the associated blockchain. Finding these patterns will help them establish which members of the IGs are distributing infringing copies of Mottanna's movies.

AI tools used for infringement: 

- AI-supported blockchain [see AI and Blockchain] can be weaponised by the IGs to evade detection by Mottanna.
- AI and machine learning could also eliminate digital dots and digital watermarks that Mottanna adds to its copyright-protected movies to track the distribution of unauthorized copies of its movies online.
- Generative adversarial networks could also be used to incorporate certain effects into livestreams to prevent automatic content recognition by adding new logos, removing original logos, watermarks, and fingerprinting, or enhancing content.

AI tools used for enforcement: 

- Mottanna can use an image watermarking system based on deep neural networks. Data could be shared with the law enforcement to help investigations.
- Machine learning- or deep learning-based fingerprinting of media content can also be employed for the same purpose.

LEGEND

ML NLP Vision Speech Expert systems Robotics Quantum computing XAI

- AI-supported big data analysis can analyse suspicious behaviours and find patterns to promptly detect the distribution of infringing movie copies on the P2P network and dubious transactions on the cryptocurrency blockchain.

- Convolutional neural networks can be used for image and pattern recognition.

5.2.8 Livestreaming – sports broadcast link aggregator (advertising-based)

The InterGalactics members are big fans of Mixed Martial Arts (MMA), so they use AI to create a link aggregator that finds and posts all the links that other groups have created so other MMA fans can watch Mottanna's MMA programming for free. The IGs generate revenue from advertising on the website where it posts the aggregated links.

To combat these efforts, Mottanna has developed an AI of its own that automates the generation of requests for notice-and-takedown orders. For its part, law enforcement has developed AI to quickly generate requests for dynamic and live blocking orders.

AI tools used for infringement: 

- Machine learning can be weaponised by the IGs to identify and scan the most popular and most relevant websites and social media and then suggest infringing links to Mottanna's MMA programming. ML can then also find and automatically extract the links to infringing streams, before reposting them on the IGs' own website.

AI tools used for enforcement: 

- Machine learning can be employed by law enforcement officials to increase the efficiency of an automatic content recognition tool. This refers not only to the recognition of images and videos, but also to the content's audio footprint.

- Expert systems could be employed by law enforcement authorities to generate requests for dynamic and live blocking orders.

- A platform could be developed using deep learning and convolutional neural networks to analyse the content of the website and detect patterns. The data thus gathered could enable law enforcement to predict future infringements and detect links between infringing websites so they can take down mirrors of blocked websites more easily and create a blacklist of infringing sites.

- The marketing of the infringing streams can also be tracked by using computer vision to identify the content and its similarity to the original content.

5.2.9 IPTV crime – unauthorised access to subscription-based IPTV service

Members of the InterGalactics want to offer access to Mottanna's copyright-protected television programming without having to pay the subscription fee for this service. Therefore, they develop and sell an AI-enabled IPTV application (or 'app') that customers can buy and then download onto their smart televisions.

The IGs' IPTV app circumvents Mottanna's technological protection measures, enabling purchasers to avoid paying for Mottanna's television subscription and watch all of its television programming for free.

Mottanna works with law enforcement to develop AI software that analyses the behavioural patterns of Mottanna's television viewers to identify those who have failed to pay a subscription. They also develop AI that identifies whether Mottanna's copyright-protected programming is being streamed using the IGs' IPTV app.

AI tools used for infringement: 

- The IGs could weaponise an AI-enabled machine learning tool to identify the protection measures Mottanna has applied to its IPTV service to break into the system and gain access to its IPTV content. Circumvention methods are then shared with the IGs' app customers in an adaptive way, so that they can access Mottanna's service without paying.

- The IGs could also use AI tools to identify broken links or streams with lag spikes and then reroute the source of the stream or forward a working link to the IPTV service customers.

AI tools used for enforcement: 

- Convolutional neural networks can allow Mottanna to (1) track the tools the IGs have created to offer illicit access to copyright-protected content and (2) collect data for behavioural analysis, all of which can then be shared with law enforcement for their investigation.

- ML can also analyse the behavioural patterns in users' account activity to recognise unknown users or unusual consumption patterns, such as account details being used in several locations within a short period. This would also enable the detection – either retroactive or predictive – of any correlation or pattern in the IGs' infringement methods.

- The IGs' marketing of the infringing services can also be tracked using computer vision to identify the content and its similarity to the original content.

5.2.10 Training an AI application

The InterGalactics want to create an AI application that successfully impersonates one of Mottanna's most successful musical artists. To train this AI application, the IGs make infringing copies of dozens of the artist's most popular sound recordings and feed this data into the AI application. Based on the data (i.e. the infringing copies of the artist's sound recordings), the AI's artificial neural network can create near-perfect copies of the artist's voice. The IGs can in turn use these copies to create and sell deepfake music videos of other artists' songs without authorisation, violating those artists' copyright as the composers of these songs.

Mottanna works with law enforcement to develop AI that not only determines when a music video is using a fake copy of an artist's voice, but also identifies the AI application that was 'trained' to generate the fake copy.

AI tools used for infringement:

- Generative adversarial networks can be weaponised by the IGs to recognise successful artists and impersonate a specific artist's voice.

AI tools used for enforcement:

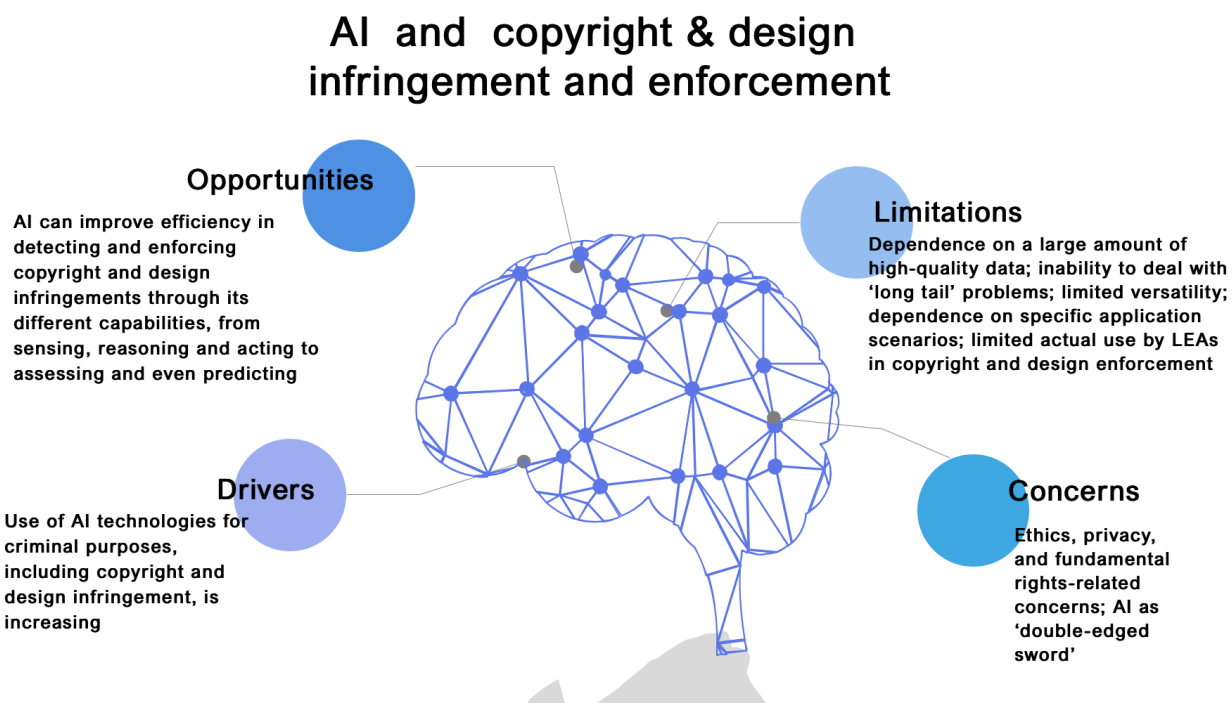
- Law enforcement can use convolutional neural networks to identify the AI application that the IGs trained to generate the fake artist's voice and create their deepfakes.

Conclusions

The findings of this study allow some general conclusions based on existing AI technologies and their current applications in the infringement and enforcement of copyright and designs of both physical products and digital content. It examined those technologies that – based on the current pace of technological advancements – will plausibly be used for the same purposes in the near future. The use and transformation of AI was analysed using the 'Intellectual Property Tech Chain', from the exploration of the existing and developing subfields and tools, through the conversion of the technology to adapt to certain goals and the development of specific applications at the weaponisation stage, to the monetisation stage, in which AI is used to protect, enforce or infringe IP.

In conclusion, the results regarding the use of AI in the infringement and enforcement of copyright and designs can be summarised under the headings 'Opportunities', 'Drivers', 'Risks', and 'Concerns'.

Figure 15 – AI and copyright and design infringement and enforcement



Opportunities

AI can perform a number of different functions, ranging from sensing, reasoning and acting, to assessing and even predicting. Currently, the main areas of development are machine learning, natural language processing, computer vision, and expert systems. Explainable AI is another field that is currently receiving increased attention from experts and policy makers. Other technologies that can be enhanced by AI, such as quantum computing, blockchain, 3D printing, generative design, cloud services, and robotics, also have great potential. AI can identify and prioritise risks, instantly spot malware on a network, guide incident responses, and detect intrusions before they occur ([194]).

([194]) Balbix (n. d.). Using Artificial Intelligence in Cybersecurity https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.

As described in the scenarios presented in Chapter 5, machine learning has become one of the key AI subfields in the development of possible tools for law enforcement in the field of copyright and design protection. Some of the most common uses of machine learning for the enforcement of copyright and design include analysing large amounts of information to detect threats, identifying social engineering bots, scanning images to detect false pages or illicit content, improving ACR tools, and providing insights to find infringement patterns.

Natural language processing can analyse and block cyberattacks like phishing, identify the behaviour of fraudsters, and create a correlation analysis to promptly identify copyright and design infringements. Computer speech and computer vision can also be successfully employed in this field. Some of their uses include pattern recognition to predict future infringements, detecting the marketing of infringing goods, and detecting and analysing fraudulent logos or other images. Quantum computing could improve AI tools, enabling them to process larger amounts of data. For example, AI and quantum computing can be used by customs and law enforcement authorities to recognise patterns in large datasets and identify similarities. Expert systems, alternatively, can be used by law enforcement to decide which strategy is more adequate to protect a system from specific vulnerabilities, including those linked to copyright and design infringement. Customs and law enforcement authorities should continuously monitor the new technology landscape to ensure their preparedness to use new tools that may support identifying, limiting and investigating IP violations.

Finally, it is worth keeping in mind that there is always a human being behind any AI algorithm and its practical application vectors ([195]). Explainable AI, although it does not solve all possible issues, could be used by law enforcement authorities to increase the use of innovative tools – including AI – for analysis and prediction, while at the same time helping to achieve the prerequisites of fairness, accountability and transparency. The use of AI in law enforcement and the judiciary should in any case always be subject to strong safeguards and human oversight ([196]), through built-in human control ([197]).

([195]) Balaban D. (2021). How AI is Mishandled to Become a Cybersecurity Risk. https://www.eweek.com/security/how-ai-is-mishandled-to-become-a-cybersecurity-risk/.
([196]) European Parliament, Civil Liberties Committee (2020). Artificial Intelligence in policing: safeguards needed against mass surveillance. Press Release. https://www.europarl.europa.eu/news/de/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance.
([197]) Wassink J. (2018). Human control of artificial intelligence. Delft Outlook. https://www.tudelft.nl/en/delft-outlook/articles/human-control-of-artificial-intelligence/.

Drivers

On the infringement side, fraudsters and criminal groups involved in copyright and design infringement employ, or could possibly employ, the same AI techniques used by enforcement agencies in order to overcome cybersecurity measures and evade detection. This is known as the 'AI/cybersecurity conundrum' ([198]): as AI matures and is increasingly used in the field of cybersecurity, the potential downsides of this technological advancement increase as well.

Adversarial machine learning can help to spot and overcome cybersecurity measures in place. AI can be trained to break through defences and develop dynamic malware to evade detection. Phishing, hacking and brute force attacks do not have to involve AI, but AI technologies can evidently be employed to make such attacks more efficient, as in the case of AI-supported password guessing and CAPTCHA breaking. AI-enabled malware can be used to conceal malicious codes in benign applications – an attack triggered by specific actions or at a certain time, which can maximise the impact of the attack without raising suspicion.

Natural language processing tools can be used to produce deepfake music videos, and generative design-based tools can aid in the manufacturing of infringing copies. In addition, pattern recognition, computer vision and/or machine learning can detect, eliminate, or replicate the patterns of anti-counterfeiting technologies (like digital dots and digital watermarks).

Limitations

AI as a tool still faces certain limitations, including, in particular: its dependence on a large amount of high-quality training data; its inability to deal with 'long tail' problems; its limited versatility; its dependence on specific application scenarios; and the inherent biases of its developer.

([198]) Khan A. (n.d). Using Artificial Intelligence in Cybersecurity. https://medium.com/@ak180404/using-artificial-intelligence-in-cybersecurity-53786d56e5f0.

More powerful machine learning algorithms can learn complex nonlinear relationships between input and output data, but to do so they require a large amount of quality data. Machines still need to understand the world perceptual and cognitive learning in a more accurate manner, enabling them to simulate real-world scenarios through reinforcement learning to perceive information; they can then transform the perceived information into abstract knowledge through attention, memory, and understanding. This might be achieved through the intersection, integration, and optimisation of algorithms and the continuous improvement of academic studies. Further developments could improve AI's creative abilities, its general-purpose use, and its understanding of objects in the world. The accessibility of computing power is another current limitation: quantum computing, for instance, is still not widely available.

Finally, although the use of innovative technologies in law enforcement is increasing, according to the interviews for this study, their actual use in the enforcement of copyright and designs is still generally limited. It is clear, though, that AI can help companies, IT experts and law enforcement to identify and mitigate risks and threats, predict attack vectors, block and take down infringing sites, and try 'to shrink the attack surface instead of constantly chasing after malicious activity' ([199]). Experts involved in the study underlined the need for increased awareness of technological developments and continuous training of law enforcement and customs authorities on the ways AI tools can be used for infringement and for enforcement.

Concerns

As AI and related technologies are used to make determinations and predictions in areas of great importance, such as combatting copyright and design infringement, AI has the potential to impact fundamental human rights in profound ways.

AI algorithms are powered by data collected and processed by technologies that are increasingly surrounding us, in every single minute of every person's life. As a result, the fundamental human rights

([199]) Gant V. (2018). How Machine Learning and AI in Cybersecurity is Shaping IT. https://biztechmagazine.com/article/2018/06/roleartificialintelligencecybersecurity#:~:text=Artificial%20intelligence%20%28AI%29%20and%20machine%20learning%20%28ML%29%2can,BizTech%20newsletter%20in%20your%20inbox%20every%20two%20weeks%21.

of privacy and data protection must be duly considered when data is collected by law enforcement authorities. AI increases the possibility that mass surveillance will become more widespread. The international debate concerning its impact on fundamental human rights, and more generally on the ethical aspects of AI, is very lively.

Nevertheless, the experts highlighted that use of AI in the justice system also presents many opportunities to figure out how to effectively use it without violating individual privacy and affecting fundamental rights. Explainable AI could also ensure that authorities can clarify to the court how the algorithms work, and which datasets they work on.

Concerns regards the potential dual use of AI technologies, as depicted in the 'double-edged sword' metaphor mentioned in Chapter 1, suggest that there can be weaknesses in each side's application of technologies that can be exploited by the other.

Many experts argue that AI algorithms must be built to align with overarching human goals. The EU Parliament, in its recent Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), has clearly stated that 'AI should not be seen as an end in itself, but as a tool, with the ultimate aim of increasing human well-being, human capabilities and safety' ([200]). As a result, the fundamental human right to privacy must be duly considered when data is collected by law enforcement authorities. Algorithms and AI should be 'ethical by design', with no built-in bias, in a way that guarantees maximum protection of fundamental rights. The EU Parliament, in the same Resolution, therefore invites 'European stakeholders, including the Member States and the Commission, to ensure, through international cooperation, the engagement of partners outside the EU in order to raise standards at international level and to find a common and complementary legal and ethical framework for the use of AI' ([201]). Policy makers are invited to be actively involved and to draw the legal boundaries within which these technologies are allowed to operate. Retroactive deconstruction of the algorithm could be required in order to assess the factors that influence a model's predictions.

([200]) European Parliament (2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html.
([201]) European Parliament (2021). Op. cit., p. 13.

The proposed new EU regulatory framework on AI, currently under discussion, is intended to ensure that AI systems used in the EU market are safe and respect existing law on fundamental rights and values. Further considerations may arise if or when the text is approved by the Parliament.

In conclusion, great investment is flowing into AI research and development along with machine learning technologies, and this trend is predicted to continue over the next years. Therefore, the availability and use of these tools and technologies, for both legal and illegal purposes, can be expected to increase. A wide range of AI-related tools and technologies are currently or potentially in use in copyright and design infringement and enforcement. There is clearly a need for better understanding, increased awareness and enhanced capacities on the part of all stakeholders, including policymakers, IP protection entities, companies and law enforcement authorities.

Bibliography

Agrawal S. (2021). Logistic Regression – Supervised Learning Algorithm for Classification. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/05/logistic-regression-supervised-learning-algorithm-for-classification/

AI World Society Innovation Network (2020). Marvin Minsky and Dean Edmonds built SNARC, the first artificial neural network. https://aiws.net/the-history-of-ai/this-week-in-the-history-of-ai-at-aiws-net-marvin-minsky-and-dean-edmonds-built-snarc-the-first-artificial-neural-network/

Alam M. (2020). Multiple regression as a machine learning algorithm. With full implementation in Python using Sci-kit Learn module. https://towardsdatascience.com/multiple-regression-as-a-machine-learning-algorithm-a98a6b9f307b

Albus J. S. (1991). Outline for a theory of intelligence. IEEE Transactions on Systems, Man, and Cybernetics, 21(3), 473–509. https://doi.org/10.1109/21.97471

Analytics India Magazine (2019). How AI Is Helping Combat Social Engineering Attacks. https://analyticsindiamag.com/how-ai-is-helping-combat-social-engineering-attacks/

Anderson H. (1986). Metropolis, Monte Carlo, and the MANIAC. In Los Alamos Science, Fall. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-86-2600-05

Andreu Perez J., Deligianni F., Ravi D., and Yang G. (2017). Artificial Intelligence and Robotics. https://www.researchgate.net/publication/318858866_Artificial_Intelligence_and_Robotics

Anyoha R. (2017). The History of Artificial Intelligence. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Assemblée Nationale (2018). Mission d'information commune sur les usages des bloc-chaînes (blockchains) et autres technologies de certification de registres. https://www2.assemblee-nationale.fr/15/missions-d-information/missions-d-information-communes/chaines-de-blocs

Autodesk (n.d.). What is generative design? https://www.autodesk.com/solutions/generative-design

Balaban D. (2021). How AI is Mishandled to Become a Cybersecurity Risk. https://www.eweek.com/security/how-ai-is-mishandled-to-become-a-cybersecurity-risk/

Balbix (n.d.). Using Artificial Intelligence in Cybersecurity. https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

Banafa A. (2019). Blockchain and AI: A Perfect Match? OpenMind BBVA. https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match

Barredo Arrieta A., Díaz-Rodríguez N., Del Ser J., Bennetot A., Tabik S., et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, pp. 82-115 doi:10.1016/j.inffus.2019.12.012

BBVA (2020). How may quantum computing affect Artificial Intelligence? https://www.bbva.com/en/how-may-quantum-computing-affect-artificial-intelligence/

Bhatia V. (2020). The Role of Artificial Intelligence in Cloud Computing. https://www.goodfirms.co/blog/role-of-ai-in-cloud-computing

Botelho B. (2018). What is cognitive computing? https://searchenterpriseai.techtarget.com/definition/cognitive-computing

Brownlee J. (2019). A gentle introduction to generative adversarial networks (GANs). Machine Learning Mastery. https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/

Brownlee J. (2017). How Much Training Data is Required for Machine Learning? Machine Learning Process. https://machinelearningmastery.com/much-training-data-required-machine-learning/

Buchanan B. G. (2005). A (very) brief history of artificial intelligence. AI Magazine, 26(4), pp. 53-60. https://www.researchgate.net/publication/220605666_A_Very_Brief_History_of_Artificial_Intelligence

Butner K. (2017). AI is reshaping the supply chain. https://www.ibm.com/thought-leadership/institute-business-value/report/cognitivesupplychain

Caldwell M., Andrews J.T.A., Tanay T., et al. (2020). AI-enabled future crime. Crime Sci 9, 14. https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8

CERN (n.d.). Recommendations about Viruses What is a virus? Why virus are bad? How not to get a virus? How to get rid of a virus? https://espace.cern.ch/winservices-help/NICESecurityAndAntivirus/VirusHoaxesAndSpyware/AboutViruses/Pages/default.aspx

CISCO (2013). The Internet of Everything, Global Private Sector Economic Analysis. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf

Computer Security Resource Center (CSRC) (n.d.). Malware. https://csrc.nist.gov/glossary/term/malware

Corporate Finance Institute (n.d.). What is Moore's Law? https://corporatefinanceinstitute.com/resources/knowledge/other/moores-law/

CrowdStrike (n.d.). Spear-Phishing definition. https://www.crowdstrike.com/cybersecurity101/phishing/spearphishing/?utm_campaign=dsa&utm_content=dach&utm_medium=sem&utm_source=goog&utm_term=&gclid=Cj0KCQjwseDBhC7ARIsAI8YcWL2yDufFJRZP1_8_4nKXYDWyL3HYHeTHMnJFh4ED1_8PT2Eelw1HM0aAlj8EALw_wcB

Culatta R. (2021). General Problem Solver (A. Newell & H. Simon). In InstructionalDesign.org. https://www.instructionaldesign.org/theories/general-problem-solver/

Dartmouth (n.d). Artificial Intelligence (AI) Coined at Dartmouth. https://250.dartmouth.edu/highlights/artificial-intelligence-ai-coined-dartmouth

DBI (n.d). Globalization 4.0 – The role and impact on the economy of emerging technologies in the paradigm of Globalization 4.0. Economistas #165. https://www.dbi.srl/the-role-and-impact-on-the-economy-of-emerging-technologies-in-the-paradigm-of-globalization-4-0/

DeAngelis S. F. (2015). Artificial intelligence: How algorithms make systems smart. https://www.wired.com/insights/2014/09/artificial-intelligence-algorithms-2/

Deloitte (n.d). The future of policing. The policing innovations shaping the future of law enforcement. https://www2.deloitte.com/us/en/pages/public-sector/articles/future-of-policing-and-law-enforcement-technology-innovations.html

Dilmegani C. (2021). What is web crawling? How it works in 2021 & examples. AIMultiple. https://research.aimultiple.com/web-crawler/.

Dinesh G., Harkut and Kashmira Kasat (2019). Introductory Chapter: Artificial Intelligence - Challenges and Applications, Artificial Intelligence - Scope and Limitations, Dinesh G. Harkut, IntechOpen, DOI: 10.5772/intechopen.84624. https://www.intechopen.com/books/artificial-intelligence-scope-and-limitations/introductory-chapter-artificial-intelligence-challenges-and-applications

Drexl J., Hilty R., Desaunettes-Barbero L., Globocnik J., Gonzalez Otero B., Hoffmann J., Kim D., Kulhari S., Richter H., Scheuerer S., Slowinski P. R., and Wiedemann K. (2021). Artificial Intelligence and intellectual property law - position statement of the Max Planck Institute for

Innovation and Competition of 9 April 2021 on the current debate. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3822924

Drupa (2019). It's a match! how artificial intelligence and 3D printing can work together. drupa. Retrieved from https://blog.drupa.com/en/its-a-match-how-artificial-intelligence-and-3d-printing-can-work-together/.

Encyclopædia Britannica (n.d.). Marvin Minsky. Britannica. https://www.britannica.com/biography/Marvin-Lee-Minsky.

European Commission. (2021). Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

European Commission (2021). Coordinated Plan on Artificial Intelligence 2021 Review. https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe

European Commission (2020). White Paper on Artificial Intelligence - A European approach to excellence and trust. 19 February. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Commission (2020). Call for tender for a study on copyright and new technologies: copyright data management and artificial intelligence. https://ec.europa.eu/digital-single-market/en/news/call-tender-study-copyright-and-new-technologies-copyright-data-management-and-artificial

European Commission (2019). 'A definition of Artificial Intelligence: main capabilities and scientific disciplines'. https://ec.europa.eu/digital-singlemarket/en/news/definition-artificial-intelligence-main-capabilities-and-scientificdisciplines

European Commission (2018). Communication from the Commission: Artificial Intelligence for Europe. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

European Commission for the Efficiency of Justice (CEPEJ) (2019). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Council of Europe. February. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

European Observatory on Infringements of Intellectual Property Rights (EUIPO) (2021). International Judicial Cooperation in Intellectual Property Cases Study on Legislative Measures Related to Online Intellectual Property Infringements – Phase 2

European Observatory on Infringements of Intellectual Property Rights (EUIPO), Impact of Technology Expert Group. (2020). Intellectual Property Infringement and Enforcement Tech Watch Discussion Paper 2020 (Rep.). https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Tech_Watch_paper/2020_IP_Infringement_and_Enforcement_Tech_Watch_Discussion_Paper_Full_EN.pdf

European Union Intellectual Property Office (EUIPO). (2020). Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP.' EUIPO. https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2020_Automated_Content_Recognition/2020_Automated_Content_Recognition_Discussion_Paper_Full_EN.pdf.

European Parliament, Civil Liberties Committee (2020). Artificial Intelligence in policing: safeguards needed against mass surveillance. Press Release. https://www.europarl.europa.eu/news/de/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance

European Parliament (2021). European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)). p. 7. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0238_EN.pdf

European Union Agency for Cybersecurity (ENISA). (2021). ENISA Threat Landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Europol (2021). Internet organised crime threat assessment (IOCTA) 2021. Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Europol (2020). Internet organised crime threat assessment (IOCTA) 2020. Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Europol, Eurojust (2021), Third Report of the Observatory Function on Encryption. June. https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf

Evans-Greenwood P., Hanson R., Goodman S., and D. Gentilin (2020). A moral license for AI. Ethics as a dialogue between firms and communities. https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/artificial-intelligence-impact-on-society.html/#endnote-sup-12

FAT/ML (n.d). Principles for Accountable Algorithms and a Social Impact Statement for Algorithms. FAT/ML http://www.fatml.org/resources/principles-for-accountable-algorithms

Formlabs (n.d.). Generative design 101. https://formlabs.com/blog/generative-design/#What%20Is%20Generative%20Design%3F

Frankenfield J. (2020). Artificial neural Network (ANN). https://www.investopedia.com/terms/a/artificial-neural-networks-ann.asp

FRONTEX (2021). Artificial Intelligence -Based Capabilities for The European Border and Coast Guard Final Report.

https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

Gant V. (2018). How Machine Learning and AI in Cybersecurity is Shaping IT. https://biztechmagazine.com/article/2018/06/roleartificialintelligencecybersecurity#:~:text=Artificial%20intelligence%20%28AI%29%20and%20machine%20learning%20%28ML%29%2can,BizTech%20newsletter%20in%20your%20inbox%20every%20two%20weeks%21

Gaumond E. (2021). Artificial Intelligence Act: What Is the European Approach for AI? https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai

Geske U, Hannebauer M. (2000). History of Artificial Intelligence. Part II: Achievements: Exhibition ECAI 2000.

Giles M. (2018). Six cyber threats to really worry about in 2018. https://www.technologyreview.com/2018/01/02/146501/six-cyber-threats-to-really-worry-about-in-2018/

Gillis A. (2019). Turin Test. https://searchenterpriseai.techtarget.com/definition/Turing-test

Goh G. D., Sing S. L., Yeong W. Y. (2020). A review on machine learning in 3D printing: Applications, potential, and challenges. Artificial Intelligence Review, 54(1), 63-94. doi:10.1007/s10462-020-09876-9

Google Developers. (n.d.). Generative Adversarial Networks. https://developers.google.com/machine-learning/gan

Green A. (2020). What is User Behavior Analytics?.Varonis. https://www.varonis.com/blog/what-is-user-behavior-analytics/

Griffith E. (2020). What is cloud computing? https://uk.pcmag.com/networking-communications-software/16824/what-is-cloud-computing

Hernández I., Rivero C.R. and Ruiz, D. (2019). Deep Web crawling: a survey. World Wide Web 22, 1577-1610. https://doi.org/10.1007/s11280-018-0602-1

High-Level Expert Group on Artificial Intelligence set up by the European Commission. (2019). A definition of AI: Main capabilities and disciplines. https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf

Hochreiter S., Schmidhuber J. (1997). Long Short-Term Memory. https://www.mitpressjournals.org/doi/pdf/10.1162/neco.1997.9.8.1735

Honda (n.d.). Honda global: ASIMO. https://global.honda/innovation/robotics/ASIMO.html

Horowitz J. H. (2020). Speech Recognition in AI. https://itchronicles.com/speech-to-text/speech-recognition-in-ai/

Hosch W. L. (2017). Web 2.0. Encyclopedia Britannica. https://www.britannica.com/topic/Web-20

IBM Cloud Education. (2020). What is machine learning? https://www.ibm.com/cloud/learn/machine-learning

IBM (n.d.). Deep blue. https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/

IBM (n.d). FORTRAN. The Pioneering Programming Language. https://www.ibm.com/ibm/history/ibm100/us/en/icons/fortran/

IBM (n.d.). What is computer vision? https://www.ibm.com/topics/computer-vision

IBM (n.d.). Explainable AI. https://www.ibm.com/watson/explainable-ai

International Federation of Robots (IFR). (n.d.). International robot standardization within ISO. https://ifr.org/standardisation

Institute for Quantum Computing, University of Waterloo. (n.d.). Quantum computing 101. https://uwaterloo.ca/institute-for-quantum-computing/quantum-101#What-is-quantum-computing

Javapoint (n.d.). Expert systems in artificial intelligence. https://www.javatpoint.com/expert-systems-in-artificial-intelligence

Javapoint (n.d.). Random Forest Algorithm. https://www.javatpoint.com/machine-learning-random-forest-algorithm

Javapoint (n.d). K-Nearest Neighbor (KNN) Algorithm for Machine Learning. https://www.javatpoint.com/k-nearest-neighbor-algorithm-for-machine-learning

Javed A. (2018). Impact of Artificial Intelligence on the Future Labor Market. Xorlogics. http://www.xorlogics.com/2018/10/15/impact-of-artificial-intelligence-on-the-future-of-labor-market/

Joshi N. (2020) Choosing Between Rule-Based Bots and AI Bots. https://www.forbes.com/sites/cognitiveworld/2020/02/23/choosing-between-rule-based-bots-and-ai-bots/

Katwala A. (2020). Quantum computing and quantum supremacy, explained. https://www.wired.co.uk/article/quantum-computing-explained

Khan A. (n.d). Using Artificial Intelligence in Cybersecurity. https://medium.com/@ak180404/using-artificial-intelligence-in-cybersecurity-53786d56e5f0

Kostadinov S. (2019). Understanding backpropagation algorithm. https://towardsdatascience.com/understanding-backpropagation-algorithm-7bb3aa2f95fd#:~:text=The%20algorithm%20is%20used%20to,parameters%20(weights%20and%20biases)

Korean Institute of Criminology, International Center of Comparative Criminology (2018). Artificial Intelligence in the Context of Crime and Criminal Justice. A Report for the Korean Institute of Criminology. https://www.ciccicc.org/public/media/files/prod/publication_files/ArtificialIntelligenceintheContextofCrimeandCriminalJustice_KICICCC_2019.pdf

Kranzberg M. (1986). 'Technology and Culture', Vol. 27, No. 3, July, pp. 544-560. The Johns Hopkins University Press

Kraus P. (2021). Will AI malware change the game? https://www.securitymagazine.com/articles/94757-will-ai-malware-change-the-game

Kreutzer R. (2020). Understanding artificial intelligence: Fundamentals, use cases and methods for a corporate AI journey. Cham, Switzerland: Springer

Lessig L. (1999). Code and Other Laws of Cyberspace. Basic Books

Liaqat S., Ullah S., Dashtipour K., Zahid A., Arshad K., Assaleh K., and Ramzan N. (2021). AI-powered IoT for Intelligent Systems and Smart Applications. https://www.frontiersin.org/research-topics/15144/ai-powered-iot-for-intelligent-systems-and-smart-applications

Lighthil J. (1973). Lighthill Report: Artificial Intelligence: A paper symposium. http://www.chilton-computing.org.uk/inf/literature/reports/lighthill_report/contents.htm

Lodewijckx I. (2019). What is the difference between artificial and collective intelligence? CitizenLab. https://www.citizenlab.co/blog/civic-engagement/what-is-the-difference-between-artificial-and-collective-intelligence/.

Lopez Yse, D. (2019). Your Guide to Natural Language Processing (NLP). https://towardsdatascience.com/your-guide-to-natural-language-processing-nlp-48ea2511f6e1

Ma E. (2019). How does your Assistant device work based on Text-to-Speech technology? https://becominghuman.ai/how-does-your-assistant-device-work-based-on-text-to-speech-technology-5f31e56eae7e

Madali N. (2020). Hopfield Networks. https://medium.com/swlh/hopfield-networks-ff2d96e1e19c

Malaty E., Rostama G. (2017). 3D printing and IP law. WIPO Magazine. https://www.wipo.int/wipo_magazine/en/2017/01/article_0006.html

Malwarebytes Labs. (2019). When artificial intelligence goes awry: Separating science fiction from fact. https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf

Marenus M. (2020). Gardner's Theory of Multiple Intelligences. https://www.simplypsychology.org/multiple-intelligences.html

Marr B. (n.d). How Quantum Computers Will Revolutionise Artificial Intelligence, Machine Learning and Big Data. https://www.bernardmarr.com/default.asp?contentID=1178

Massachusetts Institute of Technology (MIT) (n.d.). Cog project overview. http://www.ai.mit.edu/projects/humanoid-robotics-group/cog/overview.html

Massachusetts Institute of Technology (MIT) (2001). MIT team building social robot. In MIT News. https://news.mit.edu/2001/kismet

McCarthy J., Minsky M. L., Rochester N., Shannon C. E. (1955). A proposal for the Dartmouth summer research project on artificial intelligence. http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

McCrea B. (2019). What is Artificial Intelligence's Role in the Supply Chain? https://www.sourcetoday.com/supply-chain/article/21867397/what-is-artificial-intelligences-role-in-the-supply-chain

McKinsey Global Institute (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. Discussion Paper. https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy

Melnichuk A. (2020). How Big Data and AI Work Together. *Ncube*. https://ncube.com/blog/big-data-and-ai

Microsoft (n.d.). What is a virtual machine (VM)? An intro to virtualization and the benefits of VMs. https://azure.microsoft.com/en-us/overview/what-is-a-virtual-machine/

National Academy of Sciences (1994). Voice Communication Between Humans and Machines. Washington, DC: The National Academies Press. https://doi.org/10.17226/2308.

Newquist H. P. (1994). The brain makers: Genius, ego, and greed in the quest for machines that think. Indianapolis, IN: Sams Publ.

Norman J. (n.d). Marvin Minsky's SNARC, Possibly the First Artificial Self-Learning Machine. HistoryofInformation.com. https://www.historyofinformation.com/detail.php?id=3884

Norman J. (n.d). Newell, Simon & Shaw Develop the First Artificial Intelligence Program. HistoryofInformation.com. https://www.historyofinformation.com/detail.php?id=742

OECD (2019). Artificial Intelligence in Society. OECD Publishing. Paris, https://doi.org/10.1787/eedfee77-en

OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD legal instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Ohri A. (2021). LaSSO Regression: A Complete Understanding (2021). https://www.jigsawacademy.com/blogs/ai-ml/lasso-regression

Oracle (n.d.). What is the Internet of Things (IoT)? https://www.oracle.com/internet-of-things/what-is-iot/

Overby S. (2020). Artificial intelligence (AI) vs. natural language processing (NLP): What are the differences? https://enterprisersproject.com/article/2020/2/artificial-intelligence-ai-vs-natural-language-processing-nlp-differences

Pan J. (2017). Encryption scheme classification: a deep learning approach. International Journal of Electronic Security and Digital Forensics, 9(4), 381-395. doi:10.1504/IJESDF.2017.087397

Pathmind (n.d.). A beginner's guide to Generative Adversarial Networks (GANs). https://wiki.pathmind.com/generative-adversarial-network-gan

Press G. (2017). Artificial intelligence (AI) defined. Forbes. https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai defined/?sh=5826d9337661

Raj M., Seamans R. (2019). Primer on artificial intelligence and robotics. https://jorgdesign.springeropen.com/articles/10.1186/s41469-019-0050-0

Ray S. (2017). 6 Easy Steps to Learn Naive Bayes Algorithm with codes in Python and R. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2017/09/naive-bayes-explained/

Ray S. (2017). Understanding Support Vector Machine(SVM) algorithm from examples (along with code). Analytics Vidhya. https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example-code/

Rehan A. (2020). About the long tail. Medium. https://medium.com/swlh/about-the-long-tail-113e98ce8717.

Richardson, R., Schultz, J. and Crawford, K. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law

Review Online, https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

Russell S., Norvig P. (1995). A modern, agent-oriented approach to introductory artificial intelligence. ACM SIGART Bulletin, 6(2), 24–26. https://doi.org/10.1145/201977.201989

Sample I. (2020). What are deepfakes – and how can you spot them? *The Guardian*. https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

SAS (n.d.). Computer vision: What it is and why it matters. https://www.sas.com/en_us/insights/analytics/computer-vision.html#technical

Schuchmann S. (2019). History of the first AI Winter. https://towardsdatascience.com/history-of-the-first-ai-winter-6f8c2186f80b

Schuchmann S. (2019). History of the Second AI Winter. https://towardsdatascience.com/history-of-the-second-ai-winter-406f18789d45

Sharma A., (2021) Machine Learning 101: Decision Tree Algorithm for Classification. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/02/machine-learning-101-decision-tree-algorithm-for-classification/

Sharma G. (2021). 5 Regression Algorithms you should know – Introductory Guide!. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/05/5-regression-algorithms-you-should-know-introductory-guide/

Silverio-Fernández M., Renukappa S., and Suresh S. (2018). What is a smart device? - a conceptualisation within the paradigm of the internet of things. Visualization in Engineering, 6(1). doi:10.1186/s40327-018-0063-8

Somers M. (2020). Deepfakes, explained. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

Sponsor Rep. Delaney, J. (2017). H.R.4625 - FUTURE of Artificial Intelligence Act of 2017. https://www.congress.gov/bill/115th-congress/house-bill/4625/text

Sultan K., Ruhi U., Lakhani R. (2018). Conceptualizing Blockchains: Characteristics & Applications. arXiv.org. https://arxiv.org/abs/1806.03693

Techopedia. (n.d.). Cyberlocker. Techopedia.com. https://www.techopedia.com/definition/27694/cyberlocker

Telatnik M. (2020). How To Scrape the Dark Web. May. https://towardsdatascience.com/how-to-scrape-the-dark-web-53145add7033

Tencent Research Institute, CAICT, Tencent AI Lab, Tencent open platform (Ed.). (2021). Artificial Intelligence: A National Strategic Initiative. Palgrave Macmillan, Singapore. doi:https://doi.org/10.1007/978-981-15-6548-9

ThinkAutomation (n.d.). What is an algorithm? An 'in a nutshell' explanation. https://www.thinkautomation.com/eli5/what-is-an-algorithm-an-in-a-nutshell-explanation/

Tramèr F., Zhang F., Juels A., Reiter M. K., and Ristenpart T. (2016). Stealing Machine Learning Models via Prediction APIs. USENIX. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer

Trend Micro, the United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol. (2020). Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-—-and-it's-not-just-deep-fakes

UNICRI, INTERPOL (2020). Towards responsible artificial intelligence innovation. Second INTERPOL-UNICRI Report on Artificial Intelligence for Law Enforcement. http://www.unicri.it/towards-responsible-artificial-intelligence-innovation

United Nations (2021). Resource Guide on Artificial Intelligence (AI) Strategies. New York. https://sdgs.un.org/sites/default/files/2021-06/Resource%20Guide%20on%20AI%20Strategies_June%202021.pdf

University of Fullerton (n.d.) (1999). Eliza, the Rogerian Therapist. http://psych.fullerton.edu/mbirnbaum/psych101/eliza.htm

University of Missouri-St. Louis. (n.d.). Expert systems and applied artificial intelligence. https://www.umsl.edu/~joshik/msis480/chapt11.htm

University of Reading (2014). Turing test success MARKS milestone in computing history. http://www.reading.ac.uk/news-archive/press-releases/pr583836.html

US National Science and Technology Council, Committee on Technology (2016). Preparing For The Future Of Artificial Intelligence https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

Wassink J. (2018). Human control of artificial intelligence. Delft Outlook. https://www.tudelft.nl/en/delft-outlook/articles/human-control-of-artificial-intelligence/

West S.M., Whittaker M. and Crawford K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI Now Institute. https://ainowinstitute.org/discriminatingsystems.pdf

Winn Z. (2019). A 3-D printer powered by machine vision and artificial intelligence. https://news.mit.edu/2019/inkbit-3d-printer-0604

World Economic Forum (WEF) (2016). The Fourth Industrial Revolution: what it means, how to respond https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

World Intellectual Property Organization (WIPO). (2019). WIPO Technology Trends 2019: Artificial Intelligence. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf

World Intellectual Property Organization Secretariat (WIPO). (2020). WIPO conversation on intellectual Property (IP) and Artificial Intelligence (AI). https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.docx

Zhao N., Liu Y., Jiang Y. (2017). CAPTCHA Breaking with Deep Learning. CS 229 Final Project. http://cs229.stanford.edu/proj2017/final-reports/5239112.pdf

Annex 1 List of experts and stakeholders involved in the study

The experts interviewed by the research team who agreed to be mentioned in the study are as follows:

1. Magnus ALGRHEN, Swedish Patent and Registration Office
2. Dani BACSA, Motion Picture Association (MPA)
3. Panagiotis BELLONIAS, Creative Technology Department, Bournemouth University
4. Maurizio BORGHI, Bournemouth University
5. Primavera DE FILIPPI, Berkman Klein Center for Internet & Society, Harvard University
6. Véronique DELFORGE, European Union Intellectual Property Office (EUIPO)
7. Nicolas DOUARCHE, European Patent Office (EPO)
8. Graeme GRANT, International Federation of the Phonographic Industry (IFPI)
9. Jordi IPARRAGUIRRE, EURid
10. Marc KAUFMAN, Rimon Law
11. Eamonn KELLY, European Union Intellectual Property Office (EUIPO)
12. Jean-Marie LE GOFF, European Organization for Nuclear Research (CERN)
13. Luis Carlos LINARES Jr, Recording Industry Association of America
14. Michael LUND, Nordic Content Protection
15. Yulia MORENETS, Together against Cybercrime
16. Constantin REHAAG, Dentons
17. Barry SCANNELL, Irish Music Rights Organisation (IMRO)
18. Gianluca SENSIDONI, Expert.ai
19. Andrii SHALAGINOV, Norwegian University of Science and Technology (NTNU)
20. Per STRÖMBÄCK, Enfant Terrible, Netopia
21. Geo VAN LANGENHOVE, EURid
22. Benjamin VAN BAVEL, European Union Intellectual Property Office (EUIPO)
23. Marc VAN WESEMAEL, EURid
24. Didier WANG, High Authority for the Distribution of Works and the Protection of Rights on the Internet (Hadopi)

25. Norbert WIENOLD, European Patent Office (EPO)
26. Erwin VAN UFFEL, Internet Investigations, Belgian Customs
27. Cristina MARTINEZ TERCERO, Padima
28. Marie-Ange BOYER, Nike
29. Rahul BHARTIYA, European Union Intellectual Property Office (EUIPO)
30. Stephane ROBINOT, European Union Agency for Law Enforcement Cooperation (EUROPOL)
31. Krisztian TOTH, European Union Intellectual Property Office (EUIPO)
32. Martin Lykkeskov BAHR, Danish Safety Technology Authority
33. Peter SZYSZKO, White Bullet
34. Michael ELLIS, Ellis & Associates Ltd.
35. Christine MAURY-PANIS, Viaccess-Orca
36. Oliver PRIBRAMSKY, DFL Deutsche Fußball Liga GmbH
37. Knud WALLBERG, Zacco

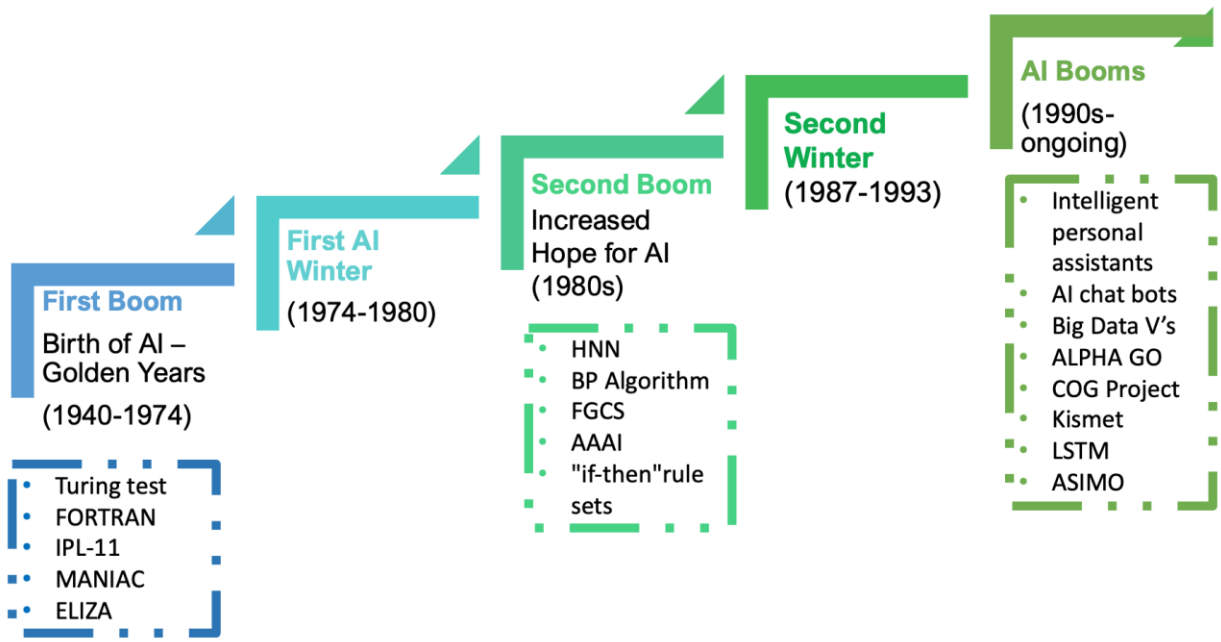
Annex 2 Additional information on AI

This annex includes additional information complementing Chapters 3 and 4 of the core part of the study that will give the reader a deeper understanding of the concepts and topics introduced therein.

1 Phases in the history of artificial intelligence

AI technologies have gone through five different phases of development, dating back to the late 1940s or early 1950s. Even in periods of reduced activity in this field (the so-called 'AI winters'), the technology never regressed, but previous achievements were in fact consolidated, preparing for the next 'boom' phase.

Figure 16 - Phases in AI History



The Birth of AI - the Golden Age (1940-1974)

The initial stage of development took place from the 1940s to 1974 and is known as the **'Golden Age of AI'**. Artificial intelligence was born as a field of scientific study in 1956, when the term was coined at a conference organised at Dartmouth College in New Hampshire, US. The Dartmouth Summer Research Project on Artificial Intelligence ([202]) was initially created to discuss the simulation of learning or any other feature of intelligence by a machine. This included automatic computers, i.e. those programmed to use language, neuron nets, self-improvement, abstractions, randomness, and creativity, or to grasp the theory of the size of a calculation ([203]).

Before the term was formally coined, several technologies and theories related to the future development of AI originated in the post-World War II period. One of the most relevant examples is the creation of the **Turing test** (or 'imitation game') by Alan Turing in 1950, who proposed a model to validate whether a computer or other machine can be programmed to behave intelligently to the extent that it can convince a human that it too is a human ([204]).

Other milestones in the evolution of AI were: Marvin Minsky ([205]) and Dean Edmonds' **first artificial neural network** in 1951 ([206]); the **first transistor computer**, introduced by IBM in 1955; the creation of the **first AI language** (IPL-II) by Allen Newell, J. C. Shaw and Herbert Simon in 1955 ([207]); the invention of the **first scientific programming language** (Formula Translator or FORTRAN) by John Backus in 1956 ([208]); and the development of MANIAC I (Mathematical Analyzer, Numerical Integrator,

---

([202]) For more information see: Dartmouth (n.d). Artificial Intelligence (AI) Coined at Dartmouth. https://250.dartmouth.edu/highlights/artificial-intelligence-ai-coined-dartmouth

([203]) McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955). A proposal for the Dartmouth summer research project on artificial intelligence. http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

([204]) For more information on this test see: Gillis A. (2019). Turin Test. https://searchenterpriseai.techtarget.com/definition/Turing-test

([205]) Norman J. (undated). Marvin Minsky's SNARC, Possibly the First Artificial Self-Learning Machine. In *HistoryofInformation.com*. https://www.historyofinformation.com/detail.php?id=3884

([206]) AI World Society Innovation Network (2020) Marvin Minsky and Dean Edmonds built SNARC, the first artificial neural network. https://aiws.net/the-history-of-ai/this-week-in-the-history-of-ai-at-aiws-net-marvin-minsky-and-dean-edmonds-built-snarc-the-first-artificial-neural-network/

([207]) Norman J. (undated). Newell, Simon & Shaw Develop the First Artificial Intelligence Program. In *HistoryofInformation.com.* https://www.historyofinformation.com/detail.php?id=742

([208]) IBM (undated). FORTRAN. The Pioneering Programming Language. https://www.ibm.com/ibm/history/ibm100/us/en/icons/fortran/

and Computer), the first computer program to beat a human being at chess, by a group of H-bomb researchers in Los Alamos, USA ([209]) in the same year.

The study of AI took a multidisciplinary approach even before the development of concrete AI tools, being influenced by disciplines such as psychology, mathematics and statistics, philosophy, and linguistic and communication theories ([210]). Technology advanced in different areas, especially in relation to the storage, capability and affordability of computers and the improvement of algorithms, which could be seen in the presentation of the **General Problem Solver** computer by Newell and Simon ([211]) and the **natural language processing** computer program ELIZA by Weizenbaum ([212]) ([213]).

The successful development of these technologies, and advocacy by researchers, contributed to the flourishing of AI and the funding of AI research by government agencies such as the **Defense Advanced Research Projects Agency** (DARPA) ([214]). Research in the Golden Age was mainly based on logic-based problem-solving approaches. However, between 1966 and the early 1970's, the limitations of AI had already become clear when machine translation did not provide the expected results, and the connectionist approach was abandoned ([215]).

The First AI Winter (1974-1980)

This initial stage of growth was followed by a period known as an 'AI winter', which occurred from 1974 to 1980. The early successes encountered several obstacles, which eventually led to a period

([209]) Anderson H. (1986). Metropolis, Monte Carlo, and the MANIAC. In *Los Alamos Science,* Fall. https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-86-2600-05
([210]) Buchanan, B. G. (2005). A (very) brief history of artificial intelligence. AI Magazine, 26(4), 53-60.https://www.researchgate.net/publication/220605666_A_Very_Brief_History_of_Artificial_Intelligence
([211]) Culatta R. (2021). General Problem Solver (A. Newell & H. Simon). In InstructionalDesign.org. https://www.instructionaldesign.org/theories/general-problem-solver/
([212]) Anyoha, R. (2017). The History of Artificial Intelligence. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/
([213]) University of Fullerton (n.d.) (1999). Eliza, the Rogerian Therapist. http://psych.fullerton.edu/mbirnbaum/psych101/eliza.htm
([214]) Anyoha, R. (2017). Op. cit.
([215]) Connectionism is a movement that seeks to explain intellectual abilities using artificial neural networks. Neural networks are simplified models of the brain composed of large numbers of units (the analogs of neurons) together with weights that measure the strength of connections between the units.

of stagnation. The First AI Winter was caused by several factors, including the capacity of computers at the time and a number of disappointments in regard to machine translation.

The publication of the **Lighthill report** ([216]) in 1973 concluded that AI researchers' promises concerning the technology's development were exaggerated, which provoked cuts in government funding, first in the United Kingdom and later in the rest of Europe and the United States ([217]). As in the case of other technologies, the AI Winter was a result of initial excitement caused by overinflated promises by developers, unrealistically high expectations on the part of end-users, and extensive promotion in the media ([218]).

Renewed hope for AI (1980s)

The field of AI was revived in the 1980s, when an increase in funding and the expansion of the algorithmic toolkit reignited interest in the technology ([219]). During this period, several relevant advances were achieved, such as the popularisation of deep learning techniques that enabled computers to learn from previous experience.

In 1982, Hopfield revived the concept of the **recurrent artificial neural network** with the Hopfield neural network (HNN) ([220]), which also provides a model for understanding human memory. In 1986, Hinton, Rumelhart and Williams published the **backpropagation training algorithm**, which trained a neural network through a method called a chain rule; this means that after each forward pass through a network, backpropagation performs a backward pass while adjusting the model's parameters ([221]). Furthermore, Edward Feigenbaum introduced expert systems, which mimicked the decision-making process of a human expert; in this case, the program would ask an expert in a field how to respond in

([216]) For more information see: Lighthill, J. (1973). Lighthill Report: Artificial Intelligence: A paper symposium. http://www.chilton-computing.org.uk/inf/literature/reports/lighthill_report/contents.htm
([217]) Schuchmann, S. (2019). History of the first AI Winter. 12 May. https://towardsdatascience.com/history-of-the-first-ai-winter-6f8c2186f80b
([218]) Newquist, H. P. (1994). *The brain makers: Genius, ego, and greed in the quest for machines that think*. Indianapolis, IN: Sams Publ.
([219]) Anyoha, R. (2017. Op. cit.
([220]) Madali N. (2020). Hopfield Networks. https://medium.com/swlh/hopfield-networks-ff2d96e1e19c
([221]) Kostadinov, S. (2019). Understanding backpropagation algorithm. https://towardsdatascience.com/understanding-backpropagation-algorithm-7bb3aa2f95fd#:~:text=The%20algorithm%20is%20used%20to,parameters%20(weights%20and%20biases)

a given situation, and once this was learned for virtually every situation, non-experts could receive advice from that program based on the experience of experts ([222]).

These technological advances were accompanied by other circumstances that increased the flourishing of AI in this period. In 1982, the Japanese Ministry of International Trade and Industry (MITI) launched the **Fifth Generation Computer Systems** (FGCS) initiative with the objective of revolutionising computer processing, implementing logic programming, and improving artificial intelligence. The high level of investment in the technology's development by the Japanese government (USD 400 million between 1982 and 1990) led to an increase in investment by other actors, such as the British government ([223]). Despite these efforts, the project did not have the expected results.

Other important factors included the founding of the **American Association for the Advancement of Artificial Intelligence** (AAAI) ([224]) in 1979, and the organisation of conferences on related topics, which enhanced the visibility of AI. Moreover, the commercialisation of AI, especially of expert systems, contributed to increased interest in the technology.

Expert systems were created by surveying experts using **'if-then' rule sets** and were implemented in fields like financial planning, medical diagnosis, geological exploration, and microelectronic circuit design ([225]). However, as with the initial period of hype regarding AI's potential, the fact that the technology did not achieve the expected results in a short period led to another era of stagnation.

Second AI Winter (1987-1993)

The Second AI Winter occurred from 1987 to 1993, when another decrease in funding adversely affected AI research: interest on the topic declined when it could not meet unrealistic expectations

([222]) Anyoha, R. (2017). Op. cit.
([223]) Anyoha, R. (2017). Op. cit.
([224]) Founded in 1979, the Association for the Advancement of Artificial Intelligence (AAAI) (formerly the American Association for Artificial Intelligence) is a nonprofit scientific society devoted to advancing the scientific understanding of the mechanisms underlying thought and intelligent behavior and their embodiment in machines. https://www.aaai.org/
([225]) Schuchmann, S. (2019). History of the Second AI Winter. https://towardsdatascience.com/history-of-the-second-ai-winter-406f18789d45

regarding the technologiy's capacity, which coincided with the collapse of the market for some of the early general-purpose computers and reduced government funding.

The expert systems that had been one of the main sources of interest in previous years started to show their limitations; in particular, many AI-related tasks were too complicated to design rules around them manually, and systems for vision and speech recognition contained too many edge cases ([226]). During these years, many AI companies closed, and attendance at the AAAI conference significantly diminished in 1991. Similarly, a decrease in the publication of AI-related articles was observed, starting in 1987 and reaching a nadir in 1995 ([227]).

AI Booms (late 1990s-ongoing)

In the 1990s, advances in computation power and storage generated new funding and interest in AI ([228]). In this decade, several developments facilitated AI's next period of flourishing. In 1995, the **Artificial Linguistic Internet Computer Entity** (A.L.I.C.E) was created by Richard Wallace. Based on Joseph Weizenbaum's 1964 ELIZA program, it was able to hold basic conversations with humans. During this period there were other major advances in all areas of AI, with significant demonstrations in machine learning, intelligent tutoring, case-based reasoning, multi-agent planning, scheduling, uncertain reasoning, data mining, natural language understanding and translation, vision, virtual reality, games, and other fields ([229]).

The 1990s saw other relevant events that demonstrated the development of AI. The **COG Project** at MIT ([230]) made significant progress in building a humanoid robot, while IBM created the chess-playing computer Deep Blue, which defeated world champion Garry Kasparov ([231]). In 1997, the speech recognition software **Dragon Naturally Speaking** was launched by Dragon Systems to be

([226]) Schuchmann, S. (2019). Op. cit.
([227]) Schuchmann, S. (2019). Op. cit.
([228]) OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en
([229]) Buchanan, B. (2005). A (Very) Brief History of Artificial Intelligence. AI Magazine. 26. 53-60.
([230]) For more information see: Massachusetts Institute of Technology (MIT) (n.d.). Cog project overview. http://www.ai.mit.edu/projects/humanoid-robotics-group/cog/overview.html
([231]) For more information see: IBM. (n.d.). Deep blue. https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/

implemented on Windows personal computers. In the same year, Dr. Cynthia Breazeal developed the **robot head Kismet** at MIT ([232]), which was able to recognise and display emotions ([233]).

In 1995, Cortes and Vapnik published the current **standard for the support vector machine**, a system for mapping and recognising similar data through classification and regression analysis, while in 1997 Hochreiter and Schmidhuber developed the **long short-term memory** (LSTM) for recurrent neural networks ([234]). Both contributions were essential for the evolution of deep learning. These advances were possible due to improvements in processing and storage capacity, which had previously been the main limitation in achieving the expected results ([235]).

The increased development of AI-related technologies after the 1990s was due to the interaction of many factors and drivers, particularly the exponential development in the performance of IT systems and technologies based on them, the advance of digitalisation and dematerialisation into more and more areas of value creation, and increasing connectivity between objects, processes, and human beings. In time this has led not only to the development of the Internet of Things (IoT) ([236]) but to an Internet of Everything (IoE) ([237]). Gordon Moore explained this phenomenon in what became known as **Moore's Law** ([238]), which describes the exponential growth of integrated circuits by estimating that the speed and memory of computers doubles every year. These doublings are currently occurring at

([232]) Massachusetts Institute of Technology (MIT) (2001). MIT team building social robot. In MIT News. https://news.mit.edu/2001/kismet

([233]) Anyoha, R. (2017). Op. cit.

([234]) Hochreiter S., Schmidhuber J. (1997). Long Short-Term Memory. https://www.mitpressjournals.org/doi/pdf/10.1162/neco.1997.9.8.1735

([235]) Anyoha, R. (2017). Op. cit.

([236]) The Internet of Things (IoT) describes the network of physical objects —"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. See, Oracle. (n.d.). What is the Internet of Things (IoT)? https://www.oracle.com/internet-of-things/what-is-iot/

([237]) Internet of Everything (IoE) is bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before-turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries. See CISCO. (2013). The Internet of Everything, Global Private Sector Economic Analysis. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf See also Kreutzer, R. (2020). Understanding artificial intelligence: Fundamentals, use cases and methods for a corporate AI journey. Cham, Switzerland: Springer

([238]) For more information see: Corporate Finance Institute (undated). What is Moore's Law? https://corporatefinanceinstitute.com/resources/knowledge/other/moores-law/

an already very high level of performance, and the next massive boost is expected from quantum computing ([239]).

AI became more complex at the beginning of the 21st century, with an approach centred on developing tools that can interact and cooperate with people. The **humanoid robot ASIMO** (Advanced Step in Innovative Mobility) ([240]), which could perform basic interactions, was presented by Honda in 2000. AI was also commercialised in items for daily use, such as the robotic vacuum cleaner Roomba in 2002.

In 2001, Doug Laney proposed the **'Three Vs of big data'**: volume, velocity and variety. In 2005, O'Reilly published '**What is Web 2.0**', thereby popularising this term, which was devised to differentiate the post-dotcom bubble World Wide Web, with its emphasis on social networking, user-generated content, and cloud computing, from that which came before ([241]). Machine reading was also refined with the improvement of the autonomous understanding of text.

After that, AI technologies started to become more accessible for everyday use. In 2010, Apple introduced the intelligent personal assistant **Siri** in its iPhone 4S, followed by Amazon's intelligent personal home assistant **Alexa** in 2014. **Machine-learning chatbots** also became a common tool for customer service. In 2014, the chatbot Eugene Goostman passed the Turing test for the first time, convincing 33 % of the judges that it was human ([242]).

Advancements were observed in other areas of AI research. In 2016, the **Google DeepMind Challenge Match** showcased the computer Go program **AlphaGo**'s defeat of the world's best Go player, Lee Sedol. AlphaGo was later programmed to play against itself using a trial-and-error pattern, which led to the creation of an improved version of AlphaGo Zero that trained itself faster and was able to beat the original AlphaGo by 100 games to 0 ([243]).

([239]) Quantum computing is essentially harnessing and exploiting the laws of quantum mechanics to process information. A traditional computer uses long strings of "bits," which encode either a zero or a one. A quantum computer, on the other hand, uses quantum bits, or qubits. See Institute for Quantum Computing, University of Waterloo. (n.d.). Quantum computing 101. https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101#What-is-quantum-computing and Kreutzer, R. (2020). Understanding artificial intelligence: Fundamentals, use cases and methods for a corporate AI journey. Cham, Switzerland: Springer.
([240]) For more information see: Honda. (n.d.). Honda global: ASIMO. https://global.honda/innovation/robotics/ASIMO.html
([241]) Hosch, W. L. (2017). Web 2.0. Encyclopaedia Britannica. https://www.britannica.com/topic/Web-20
([242]) University of Reading. (2014). Turing test success MARKS milestone in computing history. Retrieved from http://www.reading.ac.uk/news-archive/press-releases/pr583836.html
([243]) OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en

In the last few years, the increasing availability of big data and cloud computing and the associated computational and storage capacity, as well as advances in machine learning, have rapidly boosted the power, attainability, growth, and impact of AI technologies ([244]). The **improvement in sensors** and the reduction in their cost has also contributed to the growth of AI, and resulted in enhanced research in core AI areas such as natural language processing, autonomous vehicles and robotics, computer vision, and language learning.

2 Definitions of AI throughout its history

But what is AI? To date, there is no widely agreed-upon and precise definition of the concept. As mentioned in the main part of the study, AI is computer code (comprising both software and hardware) that dynamically adapts according to algorithmic rules while processing large datasets to predict phenomena and assist decision-making.

Over the course of AI's history, numerous definitions have been given of what 'AI' actually means. While the term 'artificial intelligence' has entered common parlance and is widely used, there is no single definition of AI that is universally accepted. Some define AI loosely as a computerised system that exhibits behaviour commonly thought of as requiring intelligence. Others define AI as a system capable of rationally solving complex problems or taking appropriate actions to achieve its goals in whatever real-world circumstances it encounters ([245]).

The term 'artificial intelligence' was coined by Professor John McCarthy in 1955, who defined it as 'Machines behaving in ways that would be called intelligent if a human were so behaving' ([246]). The following box showcases the changing definition of AI over the years since the term was invented.

([244]) OECD (2019), Op. cit.
([245]) US National Science and Technology Council, Committee on Technology (2016). Preparing For The Future Of Artificial Intelligence https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

([246]) Press, G. (2017). Artificial intelligence (AI) defined. Forbes. https://www.forbes.com/sites/gilpress/2017/08/27/artificial-intelligence-ai-defined/?sh=5826d9337661

Box 1 – Examples of definitions of AI over the years

'AI is the science of making machines do things that would require intelligence if done by men'. (M. Minsky, 1969) ([247])
'The ability of a system to act appropriately in an uncertain environment, where appropriate action is that which increases the probability of success, and success is the achievement of behavioural subgoals that support the system's ultimate goal.' (J.S. Albus, 1991) ([248])
'The main idea unifying theme is the idea of an intelligent agent. We define AI as the study of agents that receive precepts from the environment and perform actions. Each such agent implements a function that maps percept sequences to action.' (S. Russell et P. Norvig, 1995) ([249])
'[…] activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment.' (Nils Nilsson, The Quest for Artificial Intelligence, Cambridge, 2010)
'Any artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance…In general, the more human-like the system within the context of its tasks, the more it can be said to use artificial intelligence.' (Fundamentally Understanding the Usability and Realistic Evolution of AI (Future of AI) Act of 2017) ([250])
'[…] a set of technologies that enable computers to perceive, learn, reason and assist in decision-making to solve problems in ways that are similar to what people do.' (Microsoft, (2018)
'Artificial intelligence refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems)

([247]) Encyclopædia Britannica. (n.d.). Marvin Minsky. Britannica. https://www.britannica.com/biography/Marvin-Lee-Minsky.
([248]) Albus, J. S. (1991). Outline for a theory of intelligence. IEEE Transactions on Systems, Man, and Cybernetics, 21(3), 473–509. https://doi.org/10.1109/21.97471
([249]) Russell, S., Norvig, P. (1995). A modern, agent-oriented approach to introductory artificial intelligence. ACM SIGART Bulletin, 6(2), 24–26. https://doi.org/10.1145/201977.201989
([250]) Sponsor Rep. Delaney, J. (2017). H.R.4625 - FUTURE of Artificial Intelligence Act of 2017. https://www.congress.gov/bill/115th-congress/house-bill/4625/text

or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications), European Commission Communication on AI ([251]). An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.' (OECD, 2019) ([252])
'Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)' (Independent High-Level Expert Group on AI set up by the European Commission, 2019) ([253])
'Artificial intelligence (AI) is a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention.' (WIPO Conversation on IP and AI, 2020) ([254])

3 Additional technical insights into AI

([251]) European Commission. (2018). Communication from the Commission: Artificial Intelligence for Europe. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

([252]) OECD. (2019). Recommendation of the Council on Artificial Intelligence. OECD legal instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

([253]) High-Level Expert Group on Artificial Intelligence set up by the European Commission. (2019). A definition of AI: Main capabilities and disciplines. https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf

([254]) World Intellectual Property Organization Secretariat. (2020). WIPO conversation on intellectual Property (IP) and Artificial Intelligence (AI). https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.docx

Algorithms are, as mentioned earlier, the basis of AI, enabling the development of different tools that can be used for the protection of copyright, designs, and other IP, as well as for enforcement purposes. Algorithms can enhance the capabilities of existing tools and expand their use to other areas.

Different algorithms are used for different purposes. The **Naive Bayes algorithm** ([255]) has a group of prior probabilities (calculated with previously gathered data) for each class. Once data is provided, it updates these probabilities to constitute a posterior probability ([256]). Another category is the **decision tree algorithm**, which belongs to the family of supervised machine learning algorithms ([257]) and resembles a flowchart where nodes represent the test on an input attribute and branches represent the outcome of the test. Similarly, the **random forest algorithm** ([258]), is a ML algorithm that belongs to the supervised learning technique and can be used for classification as well as for regression problems in ML. It acts as group of trees, where input dataset is subclassified and fed into various decision trees to finally average all outputs ([259]). In the same category, **support vector machines** (SVMs) ([260]) are mostly used in classification problems. SVMs classify data using a hyperplane, ensuring that the space between the hyperplane and support vectors is maximal, whereas a **K Nearest Neighbours** (KNN) ([261]) – one of the simplest machine learning algorithms based on the supervised learning technique – uses multiple data points divided into classes to predict the class of a new sample data point ([262]).

Regression algorithms ([263]) are another type of supervised machine learning algorithm, used in AI to predict the output values based on the input information points in a database ([264]). Some of the main applications of these algorithms include predicting stock market prices and forecasting weather,

([255]) Ray S. (2017). 6 Easy Steps to Learn Naive Bayes Algorithm with codes in Python and R. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2017/09/naive-bayes-explained/
([256]) DeAngelis, S. F. (2015). Op. cit.
([257]) Sharma A., (2021) Machine Learning 101: Decision Tree Algorithm for Classification. 25 February. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/02/machine-learning-101-decision-tree-algorithm-for-classification/
([258]) JavaPoint (n.d.). Random Forest Algorithm. https://www.javatpoint.com/machine-learning-random-forest-algorithm
([259]) DeAngelis, S. F. (2015). Op. cit.
([260]) Ray S. (2017). Understanding Support Vector Machine (SVM) algorithm from examples (along with code). 13 September. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example-code/
([261]) JavaPoint (n.d). K-Nearest Neighbor(KNN) Algorithm for Machine Learning. https://www.javatpoint.com/k-nearest-neighbor-algorithm-for-machine-learning
([262]) DeAngelis, S. F. (2015). Op. cit.
([263]) Sharma G. (2021). 5 Regression Algorithms you should know – Introductory Guide! 26 May. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/05/5-regression-algorithms-you-should-know-introductory-guide/
([264]) DeAngelis, S. F. (2015). Op. cit.

among others ([265]). Algorithms in this category include linear regression algorithms that measure genuine qualities by taking into account consistent variables, which is achieved by identifying the best linear-fit relationship in a dataset among independent and dependent variables ([266]). Other examples are the **Lasso regression algorithm** ([267]), which – like other regression algorithms – obtains the subset of predictors that minimises prediction error for a response variable; the **logistic regression algorithm** ([268]) for binary classification; the **multivariate regression algorithm** ([269]) used when there is more than one predictor variable, and the **multiple regression algorithm**, which applies a combination of linear regression and non-linear regression algorithms using multiple explanatory variables as inputs ([270]).

Finally, to complement the information in Chapter 3, it may be added that international studies and literature on the topic divide AI systems into three main categories, two of which are currently only hypothetical.

1. **Artificial narrow intelligence (ANI)** is the current state of the technology, also known as applied AI. It is designed to accomplish a specific problem-solving or reasoning task. It cannot replicate the versatility of a human mind, but is able to generalise pattern recognition such as by transferring knowledge learned in the field of image recognition to speech recognition tasks ([271]).

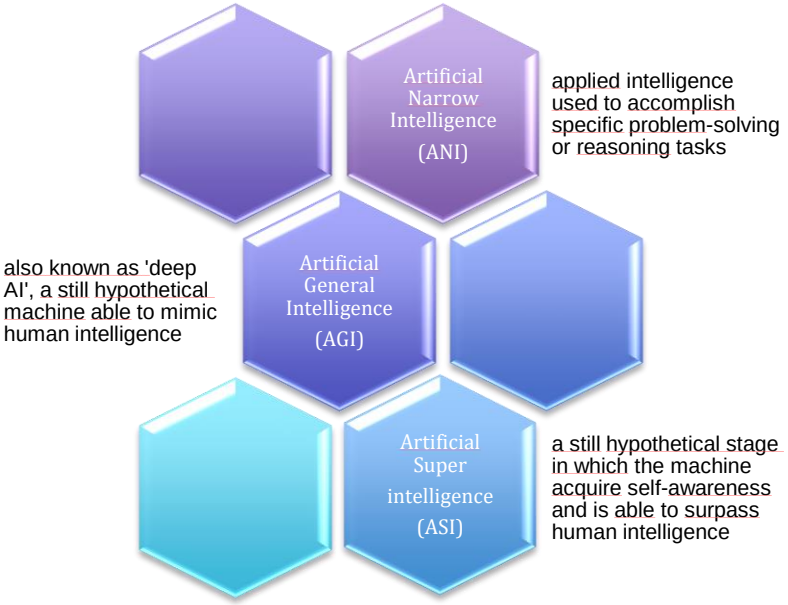
2. **Artificial general intelligence (AGI)**, also called 'strong AI' or 'deep AI', refers to a machine with general intelligence that is able to mimic human intelligence while greatly improving upon it, intelligence to solve problems that go beyond the resolution of specific tasks. AGI can think, understand, and act in a way that is indistinguishable from that of a human in any given situation.

([265]) DeAngelis, S. F. (2015). Op. cit.
([266]) DeAngelis, S. F. (2015). Op. cit.
([267]) Ohri A. (2021). LASSO Regression: A Complete Understanding (2021). 9 March. https://www.jigsawacademy.com/blogs/ai-ml/lasso-regression
([268]) Agrawal S. (2021). Logistic Regression- Supervised Learning Algorithm for Classification. 23 May. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/05/logistic-regression-supervised-learning-algorithm-for-classification/
([269]) Alam M. (2020). Multiple regression as a machine learning algorithm. With full implementation in Python using Sci-kit Learn module. https://towardsdatascience.com/multiple-regression-as-a-machine-learning-algorithm-a98a6b9f307b
([270]) DeAngelis, S. F. (2015). Op. cit.
([271]) OECD (2019), Artificial Intelligence in Society, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en

It would be capable of generalising and abstracting learning across different cognitive functions, with a strong associative memory, judgment and decision making ([272]).

3. **Artificial superintelligence (ASI)** is the last hypothetical stage of the technology, in which the machine will have self-awareness and will be able to surpass the capacity of human intelligence ([273]). For this stage, quantum computing will most probably be needed.

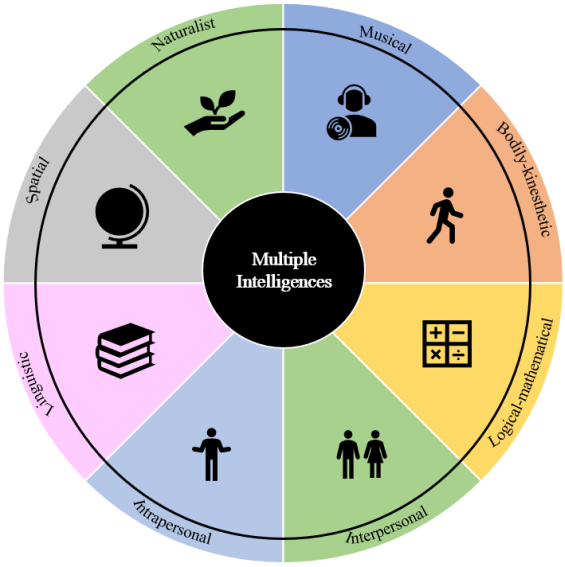
Figure 17 – Categories of AI



([272]) OECD (2019), Op. cit.
([273]) OECD (2019), Op. cit.

The core of AI is the manifestation of multiple intelligence approaches based on human intelligence, which Gardner ([274]) describes as encompassing linguistic, musical, logical-mathematical, spatial, physical-kinaesthetic, intrapersonal, interpersonal, and naturalistic-existential intelligence ([275]).

Figure 18 – Gardner's Theory of Multiple Intelligences



In this sense, the field of AI covers two main areas: the analysis of how 'intelligent' behaviour can solve problems, and subsequently, based on the knowledge obtained during this process, the 'intelligent' solutions suggested by the systems ([276]).

([274]) Marenus M. (2020). Gardner's Theory of Multiple Intelligences. https://www.simplypsychology.org/multiple-intelligences.html
([275]) Kostadinov, S. (2019). Understanding backpropagation algorithm. https://towardsdatascience.com/understanding-backpropagationalgorithm7bb3aa2f95fd#:~:text=The%20algorithm%20is%20used%20to,parameters%20(weights%20and%20biases)
([276]) Kostadinov, S. (2019). Op. cit.

4 Overview of AI technologies' impact on the economy and labour market

As mentioned in the study, AI has profound implications for individuals, societies, economies, and the environment. The EU Parliament, in its resolution of 6 October 2021 ([277]), has underlined that, while innovative technologies in general, and AI in particular, hold extraordinary promise, with the potential to generate substantial benefits in efficiency, accuracy, and convenience for the European economy and society, they also pose a number of challenges and threats to fundamental rights and democracies based on the rule of law.

At the global level, the United Nations has put in place several important initiatives related to the role of AI in sustainable development. While it is widely acknowledged that AI technologies may support breakthroughs in achieving the Sustainable Development Goals (SDGs), they may also have unanticipated consequences that will exacerbate inequalities and negatively impact individuals, societies, economies and the environment ([278]). The UN Secretary-General has underlined the need to ensure that AI becomes a force for good. The UN systems' work on the ethics of AI builds on a long history of engagement with ethical concerns related to the development and use of information and communication technologies (ICTs).

In discussing AI, it is important to briefly mention the impact that these technologies are having today and may have in the future on the economy and the labour market.

4.1 Impact on the economy

A lot has been written concerning AI's impact on the economy, and the debate is ongoing. A report published by the McKinsey Global Institute ([279]) attempts to simulate AI's impact on the world economy. According to this simulation, AI has the potential to deliver additional global economic

([277]) European Parliament (2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

([278]) United Nations (2021). Resource Guide on Artificial Intelligence (AI) Strategies. DESA. New York. June. https://sdgs.un.org/sites/default/files/2021-06/Resource%20Guide%20on%20AI%20Strategies_June%202021.pdf

([279]) McKinsey Global Institute (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. Discussion Paper. https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy

activity of around USD 13 trillion by 2030, or about 16 % higher cumulative GDP than today, equivalent to 1.2 % additional GDP growth per year.

A number of factors, including **labour automation, innovation, and new competition**, have an impact on AI-driven productivity growth. Micro factors, such as the pace of adoption of AI, and macro factors, such as a country's global connectedness or labour-market structure, both contribute to the size of this impact. With regard to the impact on the supply chain, the McKinsey study reports that 61 % of executives have observed decreased costs and 53 % increased revenues as a direct result of introducing artificial intelligence into their supply chains.

The World Economic Forum highlights the impressive advance in AI technologies in recent years, boosted by exponential increases in computing power and by the availability of massive amounts of data, from software used to discover new drugs to algorithms used to predict our cultural interests ([280]). Technological innovation will also increase the **efficiency and productivity of the global supply chain**, as transportation, logistic and communication costs all drop. On the other hand, as artificial intelligence systems are introduced into our core infrastructures, the risks posed by errors and blind spots increase.

4.2 Impact on labour

The profound business transformation caused by the quick, efficient and accurate processing of large amounts of data will greatly affect employment and labour. With regard to the labour market, experts worldwide concur that AI will certainly cause our workforce to evolve. Automation and early-stage AI systems are already changing the nature of employment and working conditions in multiple sectors. AI tools, for instance, can limit errors caused by human fatigue and improve the efficiency and accuracy of work. Some have emphasised the loss of jobs to machines, although other sources underline that other jobs will be created. In this case, the concept of 'collective intelligence' would combine the accumulated knowledge of a group of people with the use of AI.

([280]) World Economic Forum (2016). Op. cit.

The McKinsey study suggests that around 30 % of global working hours could be automated by 2030 ([281]), AI can help by **taking over repetitive or dangerous tasks** from employees, who in turn can focus on the types of work that **require a more strategic or analytical approach**. However, this also requires the retraining of the existing workforce at a certain level ([282]). Moreover, many AI predictive statistics applications call for data input that requires extensive manual labour to prepare ([283]); this is in contrast to the idea that AI can make sense of disorganised data.

At the same time, technological advances could yield greater inequality, particularly in labour markets. As automation substitutes for labour across different economic sectors, the displacement of workers by machines may exacerbate the gap between returns to capital and returns to labour. On the other hand, it is also possible that the displacement of workers by technology will, in aggregate, result in a net increase in safe and rewarding jobs. This may give rise to a job market increasingly segregated into **'low-skill/low-pay' and 'high-skill/high-pay'** segments, which in turn could lead to increased social tensions ([284]). In parallel, there is likely to be increased demand for experts in designing and delivering training on AI solutions.

5 Overview of the main AI-affected areas relevant for the study

For the purpose of this study, three areas in which AI technologies have a significant impact are particularly relevant: crime, law enforcement and criminal justice. Across these last two areas, ethical, fundamental rights and privacy concerns are clearly at stake.

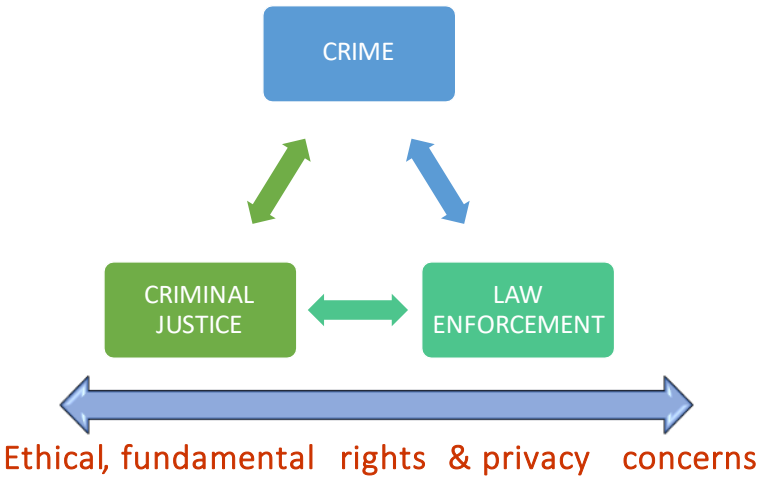
([281]) McKinsey Global Institute (MGI) (2017). Jobs Lost, Jobs Gained: Workforce Transitions In A Time Of Automation. December. https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Executive-summary-December-6-2017.pdf p.2.

([282]) Javed A. (2018). Impact of Artificial Intelligence on the Future Labor Market. *Xorlogics*. http://www.xorlogics.com/2018/10/15/impact-of-artificial-intelligence-on-the-future-of-labor-market/

([283]) EUIPO (2020), Intellectual Property Infringement and Enforcement. Tech Watch Discussion Paper 2020. p. 48.

([284]) World Economic Forum (2016). Op. cit.

Figure 19 – Main AI-affected areas relevant for the study



5.1 Impact on crime

As discussed in the core of the study, legitimate AI applications and technologies also present a great potential for misuse in criminal activities. The various capabilities of AI described in Chapter 3 make it attractive for malicious actors. AI can emulate many actions performed by humans, and in some instances can exceed human performance in terms of efficiency and scalability. With AI, certain crimes can be performed on a much larger scale, targeting thousands of victims simultaneously ([285]). It is clear that, as AI technologies expand in capability and deployment, so too do the risks of criminal exploitation ([286]), as described in the scenarios presented in Chapter 5.

([285]) Korean Institute of Criminology, International Center of Comparative Criminology (2018). Artificial Intelligence in the Context of Crime and Criminal Justice A Report For The Korean Institute Of Criminology. https://www.cicc-iccc.org/public/media/files/prod/publication_files/ArtificialIntelligenceintheContextofCrimeandCriminalJustice_KICICCC_2019.pdf

([286]) Caldwell, M., Andrews, J.T.A., Tanay, T. et al. (2020). AI-enabled future crime. Crime Sci 9, 14. https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8

Some of the international reports reviewed for this study suggest that the interlinkages between criminality and AI can be threefold, as shown below.

1. **AI as a tool for crime**: criminals use the capabilities described in the study (see 3.2 AI subfields) to facilitate their criminal actions in the real world, such as the production and sale of copyright and design-infringing goods or digital content; AI prediction technologies are used to forecast the behaviour of people or institutions to discover and exploit vulnerabilities; AI-generated fake content or videos is used to deceive and extort, etc. Chapter 4 provides a wide range of scenarios regarding copyright and design infringements of both physical products and digital content.

2. **AI systems targeted by criminals**: circumventing protective systems to commit a crime (e.g. CAPTCHA breaking, detecting and removing digital watermarks, etc.); evading detection or prosecution for crimes already committed; or making trusted or critical systems fail or behave erratically in order to cause damage or undermine public trust.

3. **AI as context for a crime**: a number of fraudulent activities are based on the victim's belief that a particular AI functionality is possible, even though it is not, or that it is possible, but not actually used in the fraud ([287]).

A single crime may fall into two or three of the above categories simultaneously: an attack on an AI system is often carried out using another AI system, while the fraudulent simulation of non-existent AI capabilities might be executed using other existing AI technologies. Moreover, it is worth emphasising that while a various limits and barriers are being introduced with regard to the legitimate use of AI technologies, these are of course not relevant for criminals, who are going to exploit the capabilities of these innovative tools without any legal, ethical or other limits, and ultimately take advantage of the respect for these limits that society legitimately requires on the part of law enforcement and other authorities.

([287]) Caldwell, M., Andrews, J.T.A., Tanay, T. et al. (2020). Op. cit.

5.2 Impact on law enforcement and criminal justice

The wide range of existing legitimate AI applications includes systems for crime prevention and detection. AI tools analyse sounds, objects, faces, and DNA and uncover digital traces of crimes. AI is also being developed to predict and prevent crime, and not merely detect what has occurred. There are several tools available or under development in numerous jurisdictions to inform initial sentencing, parole, and decisions regarding post-release monitoring and rehabilitation ([288]).

As AI and related technologies are used to make determinations and predictions in high-stakes domains such as criminal justice and law enforcement, they have the potential to impact basic fundamental rights and liberties in profound ways. AI will enhance the uncovering and investigation of criminal activities. Facial recognition and fingerprint technology are increasingly being used. Mass surveillance is also more and more possible.

The UNICRI-INTERPOL report 'Artificial Intelligence and Robotics for Law Enforcement' analyses the contribution AI and robotics can make in policing ([289]) and examines use cases at various stages of development by national law enforcement authorities, demonstrating that the use of AI in this context is a present reality ([290]). Some interesting examples of AI use cases for law enforcement include the following:

1. autonomously researching, analysing and responding to requests for international mutual legal assistance;

2. advanced virtual autopsy tools to help determine causes of death;

3. forecasting where and what type of crimes are likely to occur (predictive policing and crime hotspot analytics) to optimise law enforcement resources;

([288]) Korean Institute of Criminology, International Center of Comparative Criminology (2018). Op. cit., p.87.
([289]) Deloitte (n.d). The future of policing The policing innovations shaping the future of law enforcement. https://www2.deloitte.com/us/en/pages/public-sector/articles/future-of-policing-and-law-enforcement-technology-innovations.html
([290]) UNICRI, INTERPOL (2018). Artificial Intelligence and Robotics for Law Enforcement. http://213.254.5.198/artificial-intelligence-and-robotics-law-enforcement

4. computer vision software to identify stolen cars;

5. tools that identify vulnerable and exploited children;

6. behaviour detection tools to identify shoplifters;

7. fully autonomous tools to identify and fine online scammers;

8. crypto-based packet tracing tools enabling law enforcement to tackle security without invading privacy ([291]).

The recent Frontex report 'Artificial Intelligence-Based Capabilities for the European Border and Coast Guard' provides insights into the current landscape of AI-based capabilities in border security through a number of case studies, as well cross-cutting barriers and enablers for future AI adoption ([292]).

Law enforcement and border guards should continuously monitor the new technology landscape to ensure preparedness to appropriately respond. Moreover, as is widely discussed at international level, law enforcement authorities and the criminal justice system should ensure fairness, accountability, transparency and that the use of AI is effectively communicated to the public. Experts highlight that the use of AI in the justice system also presents many opportunities to figure out how to effectively use it without violating an individual's privacy ([293]).

With regards to criminal justice, numerous examples can be found of judicial systems making use of AI tools in criminal proceedings. According to international studies on the topic, AI is currently employed in the US, for instance, to assess the risk of future unwanted behaviour by an accused person (e.g. committing a new crime or the same crime, or failure to appear in court) ([294]). Some countries also use automated risk assessment tools in the criminal justice system, though their use may be questioned. In fact, some technological solutions, such as those for estimating a criminal

([291]) UNICRI, INTERPOL (2018). Artificial Intelligence and Robotics for Law Enforcement, Op. cit. p. v.
([292]) FRONTEX (2021). Artificial Intelligence -Based Capabilities For The European Border And Coast Guard Final Report. https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf
([293]) World Economic Forum (2016). Op. cit.
([294]) Korean Institute Of Criminology, International Center of Comparative Criminology (2018). Op. cit., p.116.

defendant's risk of recidivism have been considered biased against less privileged groups, exacerbating structural inequalities in society and institutionalising this disadvantage. In fact, data reflect the social, historical and political conditions in which they were created and collected. AI systems 'learn' based on the data they are using. This, along with many other factors, can lead to biased, inaccurate, and unfair outcomes. The quality and quantity of data is therefore essential in limiting possible bias ([295]). In addition, human control over the final decision must always be ensured.

In this context, in December 2018, the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe adopted the 'Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment' ([296]), which encompasses the following five principles:

1. **principle of respect for fundamental rights**: ensure that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights;

2. **principle of non-discrimination**: specifically prevent the development or intensification of any discrimination among individuals or groups of individuals;

3. **principle of quality and security**: with regard to the processing of judicial decisions and data, use certified sources and intangible data with models elaborated in a multi-disciplinary manner, in a secure technological environment;

4. **principle of transparency, impartiality and fairness**: make data processing methods accessible and understandable, and authorise external audits;

5. **principle of 'user control'**: eschew a prescriptive approach and ensure that users are informed actors and in control of the choices made ([297]).

([295]) West, S.M., Whittaker, M. and Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI Now Institute. https://ainowinstitute.org/discriminatingsystems.pdf, and Richardson, R., Schultz, J. and Crawford, K. (2019). Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. New York University Law Review Online, https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/

([296]) European Commission for the Efficiency of Justice (CEPEJ) (2019). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Council of Europe. February. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c p.7.

([297]) European Commission for the Efficiency of Justice (CEPEJ) (2019). Op. cit., p.7.

5.3 Ethical, fundamental rights and privacy concerns

All of the above points raise an increasing number of ethical, fundamental rights and privacy concerns. The ongoing debate is very lively globally as well as within the EU. As mentioned above, AI algorithms are powered by data that are collected and processed by technologies that increasingly surround us at every minute of our lives. This process raises privacy and ethical concerns. Explainable AI could allow authorities to clarify to the court how the algorithms work, and which datasets they are working from.

Many experts argue that AI algorithms must be built to align with overarching human goals. The EU Parliament, in its Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, clearly stated that 'AI should not be seen as an end in itself, but as a tool, with the ultimate aim of increasing human well-being, human capabilities and safety' ([298]). It also stressed that algorithms and AI should be '**ethical by design**', with **no built-in bias**, in a way that guarantees maximum protection of fundamental rights ([299]). Therefore, regulatory agencies shall be actively involved and fix the legal boundaries within which these technologies are allowed to operate. Retroactive deconstruction of the algorithm could be required to assess the factors that influence a model's predictions.

At first, it was thought that regulation could control the way AI is used: open letters were sent to governments with long lists of signatories attached, asking for regulation to be enacted. This approach has failed to bear fruit. More recently, the focus has been on developing ethical principles to guide the development of AI-enabled solutions. These principles are useful indications of what we expect from AI (and what we wish to avoid), but they are not enough, as they fall short of describing how particular solutions should adhere to them.

([298]) European Parliament (2021). European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI). Op. cit. p.3.
([299]) European Parliament (2021). European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)). p.7. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0238_EN.pdf

The most recent expectation is that design (and design methodologies) will enable us to apply these principles, but whether this will suffice is not yet clear ([300]). AI algorithms must be built to align with overarching human goals. The debate is still open and will necessarily evolve with the evolution of technology.

With regard to citizens' fundamental rights and the avoidance of potential liability, the use of AI in law enforcement should ensure that it respects the following key guiding principles.

- **Responsibility**: ensure the availability of measures to redress adverse individual or social effects of an algorithmic decision system, and designate a person responsible for the timely remedy of such issues.
- **Fairness**: the use of technology should not breach rights such as the right to due process, the presumption of innocence, freedom of expression, and freedom from discrimination.
- **Accountability**: a culture of accountability must be established at an institutional and organisational level.
- **Transparency**: the path taken by the system to arrive at a certain conclusion or decision must not be a 'black box'.
- **Explainability**: the decisions and actions of a system must be comprehensible to human users ([301]).

6 AI Regulation in the European Union

In 2020, the EC's white paper on 'AI - A European approach to excellence and trust' ([302]) set out policy options for promoting AI while addressing the risks associated with certain uses. In this context, the proposed regulatory framework on AI has the objectives of ensuring that AI systems used in the EU

([300]) Evans-Greenwood P., Hanson R., Goodman S., and D. Gentilin (2020). A moral license for AI. Ethics as a dialogue between firms and communities.https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/artificial-intelligence-impact-on-society.html/#endnote-sup-12
([301]) FAT/ML (n.d). Principles for Accountable Algorithms and a Social Impact Statement for Algorithms. FAT/ML (Website). http://www.fatml.org/resources/principles-for-accountable-algorithms
([302]) European Commission. (2021). European Commission (2021). White Paper. On Artificial Intelligence - A European approach to excellence and trust https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

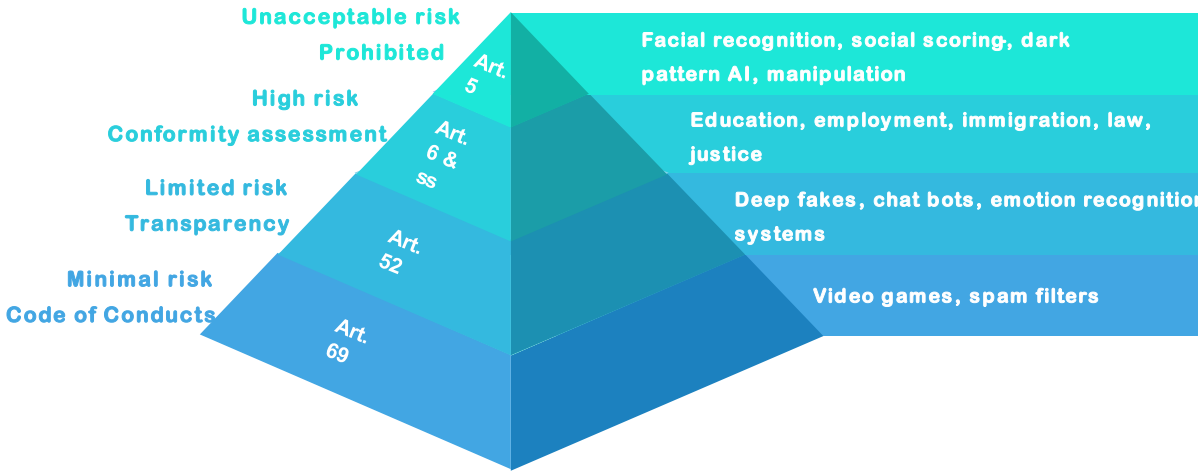
market are safe and respect existing law on fundamental rights and values; ensuring legal certainty to facilitate investment and innovation in AI; enhancing governance and efficient enforcement of existing law on fundamental rights and safety requirements of AI systems; and facilitating the creation of a single market for lawful, safe and trustworthy AI applications, while preventing market fragmentation ([303]).

In April 2021, the European Commission published the first proposal for a legal framework on AI, namely the draft Artificial Intelligence Act ([304]). This proposed AI Act addresses the risks stemming from the various uses of AI systems while at the same time promoting AI innovation, to find a proper balance between the need to preserve individual safety and fundamental rights without overly inhibiting AI innovation. To this end, the draft AI Act envisages a risk-based approach that prohibits specific unacceptable uses of AI, heavily regulates some other uses entailing significant risks, and encourages the adoption of codes of conduct regarding uses of AI that present limited or no risk ([305]).

The gradation of risks is represented using a four-level pyramid: unacceptable risks, high risks, limited risks and minimal risks.

([303]) European Commission. (2021). Op. cit.
([304]) European Commission (2021). Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN
([305]) Gaumond E. (2021). Artificial Intelligence Act: What Is the European Approach for AI? https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai

Figure 20 – Gradation of risks of the proposed AI Act



Additional efforts in this area include several external border management initiatives and the exploration of how emerging technologies, including artificial intelligence, might be adopted ([306]):

1. Regulation (EU) 2016/1624 on the European Border and Coast Guard (EBCG), which proposes general principles for European integrated border management, and Regulation (EU) 2019/1896, strengthening the mandate of the European Border and Coast Guard Agency (Frontex) ([307]);
2. the European Commission's 2018 European Strategy and Coordinated Plan on AI, which proposes a European perspective on the diverse technological, ethical, legal and socio-economic implications of AI and principles for its use in the public and private sectors;

([307]) European Border and Coast Guard Agency (FRONTEX). (2021). Artificial Intelligence-Based Capabilities for the European Border and Coast Guard. Frontex. https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

3. the EU Security Union Strategy 2020, which outlines main priorities for improving internal security, including strengthening the provision of data services in the areas of border surveillance and maritime security.

All these policy and regulatory elements will affect the development and use of AI and related technologies by private-sector actors as well as by customs and law enforcement authorities, including in the field of copyright and design enforcement.