Information & Communication Technology Law

Lecture Title: The implications of IT Law on legal processes (II)

Diploma in Law (Malta)

Lecturer: Veronica Campbell

Date: 4th May 2023

CAMILLERI PREZIOSI
ADVOCATES

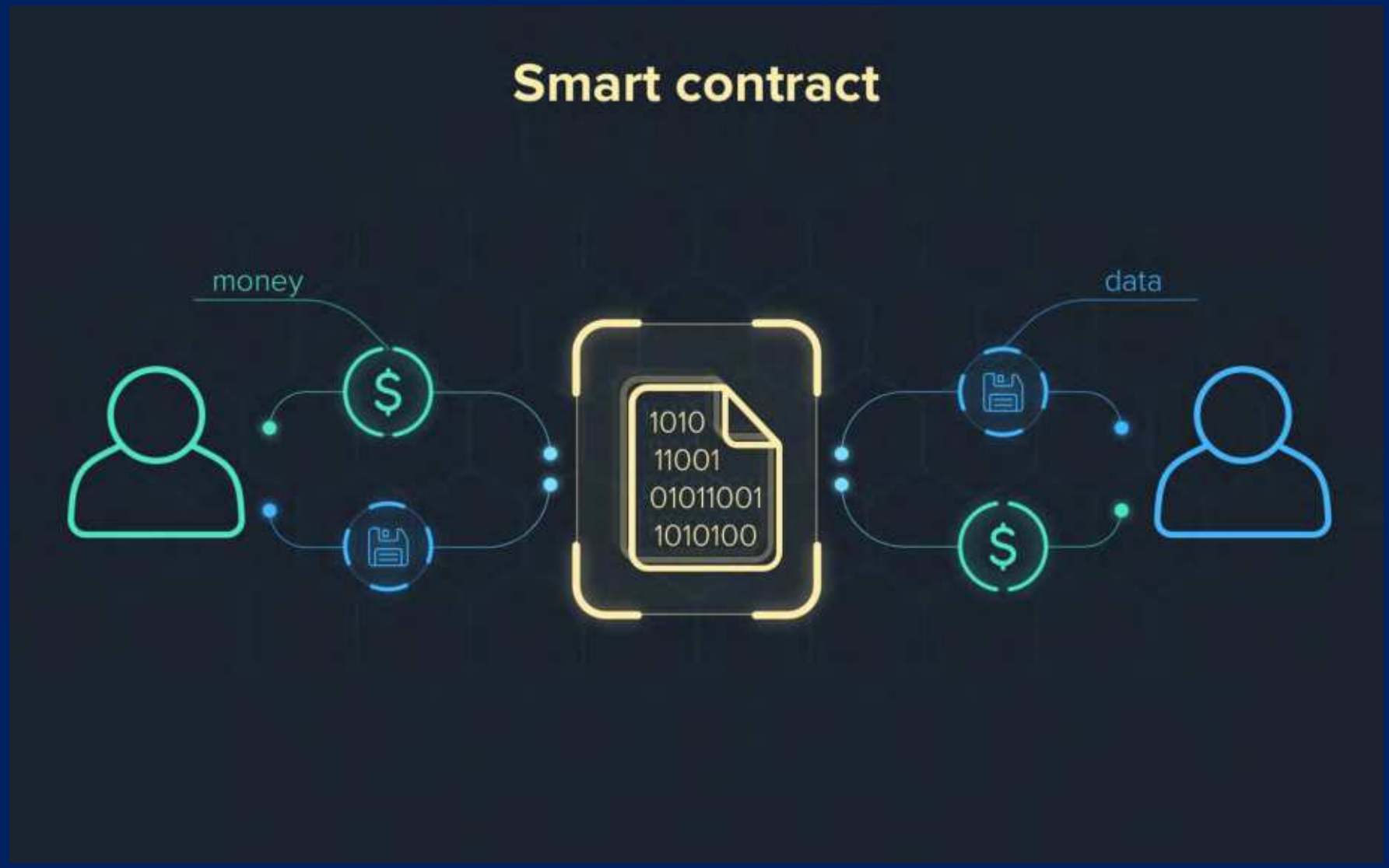
Lex Specialis

- *Lex Specialis* means 'specific law' and is derived from the Latin maxim '*lex specialis derogat legi generali*'.

- In essence, this doctrine means that sector-specific rules will prevail over more general rules, should there be a conflict in interpretation between both laws.

- For example, S.L.586.11 (Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations) provides that the processing of personal data of a child in relation to such services shall be lawful where the child is thirteen years of age.

Smart Contracts



Smart Contracts

- Nick Szabo first introduced the concept of ‘smart contracts’ in a peer-reviewed journal in 1997.
- He defined a smart contract as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”.
- Like in a physical contract, one party binds itself (promises) to perform an obligation (be it a sale or service) for the other party.
- The performance characteristics usually linked with blockchain are also directly linked to smart contacts: transparent, immutable, irrevocable, programmable, no single point of failure and time-stamped.

Smart Contracts - Legislation

- The primary legislative instruments which regulate smart contracts and other innovate technologies are:
  - The Malta Digital Innovation Authority Act (Chapter 591, Laws of Malta); and
  - The Innovative Technologies Arrangement and Services Act (Chapter 592, Laws of Malta – the "ITAS Act").

- The MDIA Act provides for the constitution of the Malta Digital Innovation Authority and outlines the Authority's scope, functions and powers. In essence, this is to enhance the development of innovative technology arrangements and services within Malta, while providing for legal and technical assurances.

- The Authority acts as a certification body for DLT platforms and how these are to be managed. This provides certainty to users that any platform used has legal backing, and has been developed in accordance with industry standards, best practices and legal norms.

Validity of Contracts

- The prerequisites for the validity of a contract under Maltese law are as follows:
  - Capacity to contract;
  - Consent of the parties;
  - Causa – subject matter; and
  - Lawful consideration.

- The absence of any one of these requirements will render the contract null and void in the eyes of the law.

Issues Relating to Smart 'Contracts'

- Predominantly code-based, so not the typical form of a contract one may imagine.
- Depending on the information within the code, may not strictly adhere to the contractual requirements, therefore, would not be considered as a contract regardless of the obligations therein.
- 'Consent' may be difficult to obtain and prove.

What are DLTs?

- Distributed ledger technologies (DLTs) are digital systems for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledgers have no central data store or administration functionality.

- Defined as “a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof” within the MDIA Act.

- While having their benefits from the technical perspective, legally speaking, DLTs face certain discrepancies within National and EU Laws.

Smart Contracts – ITA Guidelines

- The MDIA issued guidelines (the "Guidelines") in 2018, which all Innovative Technology Arrangements ("ITAs") should abide by, in order to obtain the appropriate certification.

- The general requirements within Section 5 of the Guidelines are as follows:
  - Legality of the purpose and function of the ITA;
  - Integrity of the Applicant (including Administrator and Qualifying Shareholders);
  - Transparency to users regarding the functions and limitations of the ITA;
  - Compliance with all applicable legal obligations;
  - Accountability by identifying and defining the responsibilities of who will be fulfilling the roles within the ITAS Act.

ITA Guidelines – Special Requirements

- ITA certification shall only be issued by the MDIA where the system meets the following specific requirements (Article 8(4) of the ITAS Act):
  - Fit and properness of the ITA and Applicant;
  - Positive assurance from Systems Auditor;
  - Appointment of Technical Administrator;
  - Compliance with applicable and mandatory law; and
  - Adequate disclosures to users.

Fit and Properness

- The ITA must be fit and proper for the purposes declared within the certification application and have the qualities, attributes, features, behaviour or aspects as declared.

- Upon application, the applicant must submit a blueprint which shall include:
  - The reasons for which the ITA was created;
  - The specific characteristics that the ITA offers to users;
  - The specific elements or boundaries of the ITA;
  - Distinctive functional capabilities;
  - The inherent capabilities of the ITA;
  - How the ITA responds to unexpected processes and inputs; and
  - Technical/Operational restrictions.

- The appointed Administrator and any Qualifying Shareholders must also be declared fit and proper persons.

Positive Assurance

- The Systems Auditor is required to opine as to whether the ITA meets the standards as set out by the Authority, including those within:

  - The previously mentioned blueprints;
  - Any rules and regulations within the ITAS Act;
  - Guidelines issued by the Authority;
  - Any requirements established by the Authority in a particular case.

Technical Administrator

- An ITA shall have a Technical Administrator, duly registered with the Authority, in office at all times.

- The Technical Administrator must be able to satisfy any certification pre-requisites, continuously meet standards and vary the ITA's parameters or functionality where necessary to meet mandatory legal requirements.

- ITAs must have in-built technology features to enable the Technical Administrator to intervene in a transparent and effective manner in the event of a material cause of loss to any user or a material breach of law.

Compliance

- Applicant must show how the ITA will meet applicable law obligations, such as those relating to:
  - AML/FT;
  - Personal data protection;
  - Consumer Rights; and
  - Cybersecurity.

- Within the application, it must be specified whether the above obligations will be met within the ITA's functionalities or outside its boundaries. In the former case, blueprints should clearly indicate how compliance will be achieved.

Adequate Disclosure

- The following information regarding the ITA must be adequately disclosed to all users in English and in an easily accessible and intelligible format:
  - Specific purposes
  - Qualities
  - Features
  - Attributes
  - Limitations
  - Conditions
  - Terms of service and behaviours or aspects of the ITA and on the basis of which a user is invited to participate in, rely on or use the ITA.

Virtual Financial Assets

VFA Framework

- In tandem with the previously mentioned laws, Malta has promulgated legislation regulating virtual currencies. These are the Virtual Financial Assets Act (Chapter 590, Laws of Malta – the "VFA Act") and the Virtual Financial Assets Regulation (S.L 590.01).

- The VFA Act sets out the general legal framework regulating the issuance of DLT tokens in or from Malta, and the operation of certain DLT-related activities in Malta. It collectively refers to assets which intrinsically depend on or which utilise DLT as DLT assets.

- Being the primary legislative tool, the VFA Act sets out the four categories under which DLT assets may be classified in terms of Maltese law. The Act itself regulates Virtual Financial Assets ("VFAs"), those being DLT assets that are not classified as being utility tokens, electronic money or financial instruments in terms of the Act.

- In addition, the VFA Act regulates several aspects of the DLT environment including, inter alia, initial VFA offerings, admission of VFAs to trading on DLT-based exchanges and the operation of VFA exchanges. The operation of such exchanges is restricted to entities licenced as VFA Service Providers by the MFSA under the VFA Act.

Initial Coin Offerings

- The Financial Instruments Test must be carried out compulsorily by the issuer and their VFA Agent, prior to the Initial Coin Offerings ("ICO") on the exchange. This is the issuer (or "Applicant")'s first port-of-call in obtaining a licence.

- The VFA Act states that no person shall provide, or hold itself out as providing, a VFA service in or from within Malta unless such person is in possession of a valid licence granted under the Act by the MDIA.

The Financial Instruments Test

- The Malta Financial Services Authority ("MFSA") introduced a Financial Instruments Test (the "Test"), to determine whether a DLT asset:
  1. Falls under EU legislation such as Directive 2014/65/EU (MiFID II);
  2. Is encompassed within the VFA Act;
  3. Is exempt.

- The Test is applicable to issuers offering DLT assets to the public (or within exchanges) and persons providing any services and/or performing any activity within the context of the VFA Act or traditional financial services.

- The Test's objective is to offer legal clarity regarding the distinction between types of assets, in order to determine the asset's nature and the respective applicable legal framework based on the token's features.

Categorising Assets

- The VFA Act defines a VFA as “any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not electronic money, a financial instrument or a virtual token”.

- A ‘virtual token’ is “a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms”.

Categorising Assets

- MiFID II provides for an exhaustive list of 'financial instruments' such as transferable securities, money-market instruments, units in collective investment undertakings, options, derivative instruments for the transfer of credit risk etc within Section C of Annex I.

- The Financial Institutions Act (Chapter 376 Laws of Malta) defines 'electronic money' ("E-money") as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer", such as PayPal.

Responsibilities

- The VFA Act creates the role of the VFA agent. All issuers must have a VFA agent in place at all times. The VFA agent is a person registered with the MFSA who can offer legal counsel to the VFA service provider and submit documents and information to the MFSA as requested.

- Must confirm that the DLT asset qualifies as a VFA and must note any assumptions which it has made when submitting the test.

- An annual compliance report must be drawn up by the issuer, and will be reviewed by the VFA agent to ensure compliance with the VFA Act and other regulations and rules issued by the MFSA.

VFA Rulebook – Requirements for Issuers

- The MFSA has published a rulebook which includes requirements that all VFA Issuers must comply with, prior to the ICO. This is split into the following sections:

1. General Requirements;
2. Board of Administration;
3. Functionaries;
4. Cybersecurity;
5. Record-keeping; and
6. IT Infastructure

- This above encompass all the requirements for Issuers and identifies the Functionaries such Issuers must appoint, while detailing the Issuer's obligations towards said Functionaries.

General Requirements

- An Issuer (other than a Public Sector Issuer) must be a legal person duly formed under Maltese Law and must be subject to the 'dual control' principle.

- The Issuer shall commence the offering of its VFA to the public or shall proceed with the admission of its VFA to trading on a DLT exchange within six months from the date of registration of the whitepaper with the MFSA.

- In determining whether a DLT asset qualifies as a VFA, an Issuer of a DLT asset shall, prior to offering such DLT asset to the public in or from within Malta, or applying for its admission on a DLT exchange, undertake the Financial Instruments Test, which shall be signed by its Board of Administration, and endorsed by its VFA Agent.

General Requirements - Compliance

- An Issuer shall be required to draw up, on an annual basis, a compliance certificate in relation to its business, which is to include the following:
  - confirmation that all the local AML/CFT requirements have been satisfied and that there are adequate systems in place to identify suspicious transactions;
  - confirmation that the ITA complies with qualitative standards issued by the MDIA;
  - a statement as to whether the Issuer is a fit and proper person, confirmed by the VFA Agent; and
  - a statement as to whether there have been any breaches of the VFA Act.

General Requirements – AML/CFT

- The Issuer shall, on an annual basis, engage an independent auditor to draw up a report which shall include:

  a) confirmation that the AML/CFT/KYC systems the Issuer purports to have in place are indeed in place; and

  a) review of the operations of the Issuer from an AML/CFT perspective.

General Requirements – Public Disclosures

- Issuer must ensure that the whitepaper contains *inter alia* a detailed description of the past and future milestones, including any deliverable in any private placements and its effect on the public offering to the investors.

- Issuer shall provide investors with regular and comprehensive updates on the progress being achieved with respect to the milestones set out in the whitepaper to enable them to assess the deliverables in the whitepaper. Such updates are to be made by means of public announcements.

- An Issuer shall ensure that the identities of the Functionaries it appoints are appropriately disclosed within the whitepaper. Provided that where any Functionary is removed or replaced, this shall be so stated in a public announcement.

General Requirements – Supervisory Fees

- An Issuer shall, upon the submission of the compliance certificate by its appointed VFA Agent, pay to the Authority the applicable supervisory fees in accordance with the Virtual Financial Assets Regulations.

General Requirements – Cap on Investable amount

- An Issuer shall ensure that an investor does not invest more than EUR 5,000 in its Initial VFA Offerings over a 12-month period.
- Provided that this Rule shall not apply to Experienced Investors.

Board of Administration

- Responsible for ensuring that the Issuer complies with its obligations within the Rulebook.
- Obligation to acquire and maintain sufficient knowledge and understanding of the Issuer's business.
- Must:
  - Act honestly and in good faith;
  - Exercise reasonable care, skill and diligence,
  - Not misuse their powers,
  - Act independently;
  - Monitor the execution of the Functionaries;
  - Identify and manage risk;
  - Monitor compliance;
  - Avoid conflicts of interest;
  - Establish a good governance framework; and
  - Be responsible for the Issuer's AML/CFT compliance.

Board of Administration

- Issuer is liable towards the unitholders for any damages incurred as a result of wilful misconduct or negligence, including the failure to perform its obligations.

- Issuer to ensure that the BoA's minutes are held in Malta at its registered address or any placed agreed upon by the MFSA.

Functionaries

- An Issuer shall appoint and have at all times in place the following Functionaries:
  - A Systems Auditor to review and audit the ITA & cybersecurity arrangements;
  - A VFA Agent;
  - A Custodian;
  - An Auditor; and
  - A Money Laundering Reporting Officer ("MLRO").

- The role of the Custodian may be performed through the use of a smart contract if this is duly certified by the systems auditor.

Record-keeping

- An Issuer shall arrange for documents to be kept to enable MFSA to monitor compliance with the requirements under these Rules. This does not exonerate the Issuer from its record-keeping obligations under any other law.

- Documents shall be kept for at least 5 years, however, the MFSA may request that such are kept for up to 7 years.

- Additional requirements:
  - MFSA must be able to access them readily and to reconstitute each key stage of the processing of each transaction;
  - it must be possible for any corrections or other amendments, and the contents of the documents prior to such corrections or amendments, to be easily ascertained; and
  - it must not be possible for the documents otherwise to be manipulated or altered.

Cybersecurity

- Issuer must establish a cybersecurity framework which shall *inter alia* include:
  1. Information and data security roles and responsibilities;
  2. Access management policy;
  3. Sensitive data management policy;
  4. Threats management policy;
  5. Business continuity plan;
  6. Response and recovery plan; and
  7. Security education and training

- Naturally, the above may vary depending on the nature, scale and complexity of the Issuer's business. In any case, the framework must comply with international cybersecurity standards and be in line with the GDPR.

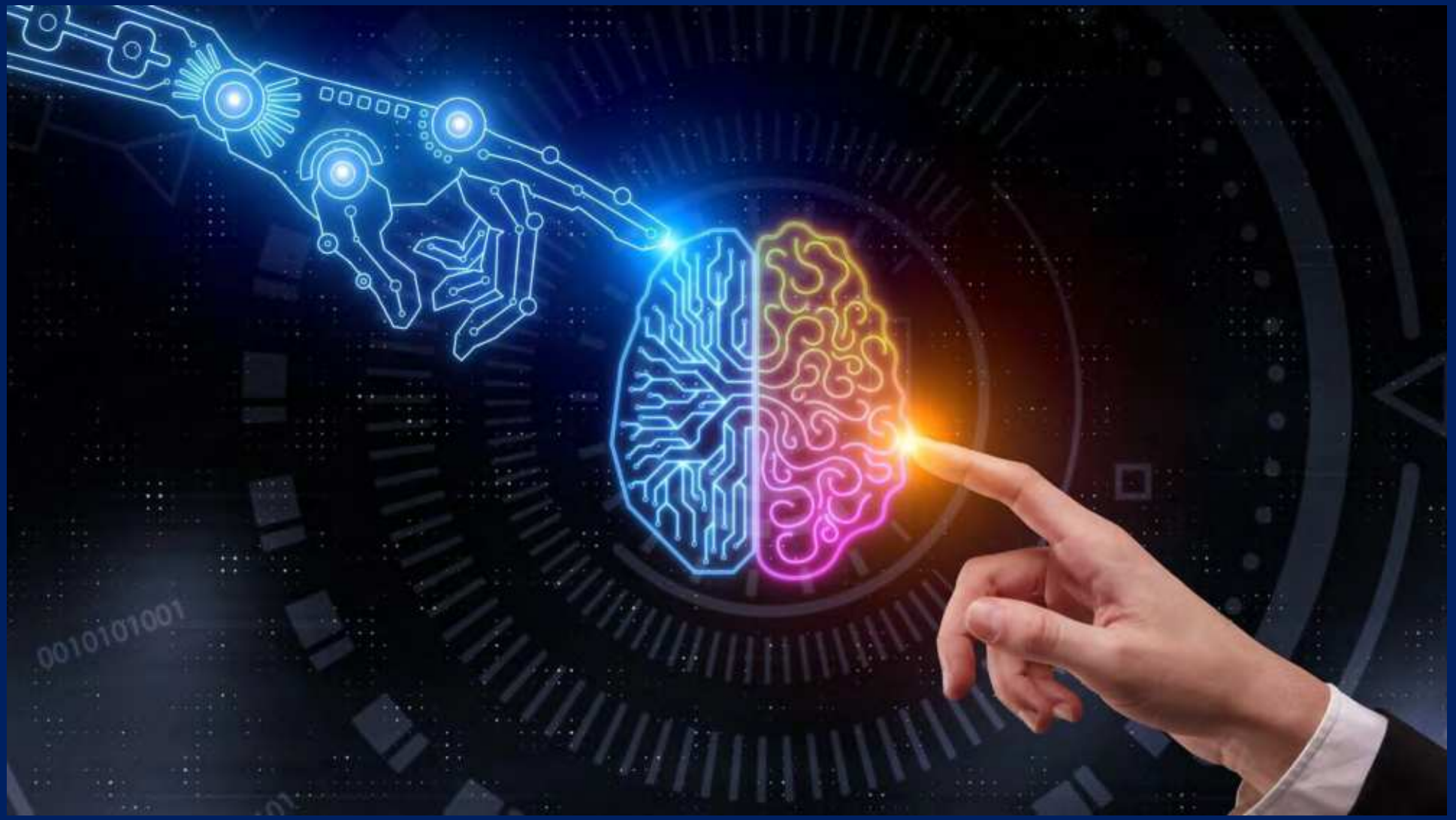
IT Infrastructure

- The Issuer shall ascertain that its IT infrastructure ensures:
  - the integrity and security of any data stored therein;
  - availability, traceability and accessibility of data; and
  - privacy and confidentiality.

- The Issuer shall ensure that its IT infrastructure is located in Malta and/or any EEA member state and/or any other third country jurisdiction wherein the Authority is satisfied that the above can be satisfied.

- Where not held in Malta or located in a cloud environment, the Issuer shall ensure that data is replicated real time by virtue of a live replication server located in Malta.

Artificial Intelligence



What is 'AI'?

- The proof of concept was initialized through Allen Newell, Cliff Shaw, and Herbert Simon's *Logic Theorist*.

- The Logic Theorist was a computer program designed to mimic the problem-solving skills of a human and was funded by Research and Development (RAND) Corporation.

- It's considered by many to be the first artificial intelligence program and was presented at the Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) hosted by John McCarthy and Marvin Minsky in 1956.

Practical uses of AI systems

- The private, transport, health, and education sectors stand to gain the most through prevalent use of AI systems, at least in the short term. In the private sector, AI becomes especially useful in conducting client due diligence assessments. AI's main strength lies within its ability to effectively recognise patterns and deduce outcomes to an effective degree of certainty.

- Researchers at the University of Malta have conducted a study into the feasibility of introducing 'driverless' vehicles in Malta using AI systems under Malta's Introduction of Shared Autonomous Mobility ("MISAM") project.

- Within the health sector, certain local companies have partnered with entities outside of Malta to enhance the electronic patient record system and to provide patients in the UK with the accessibility to set hospital appointments, reschedule or cancel them in real time.

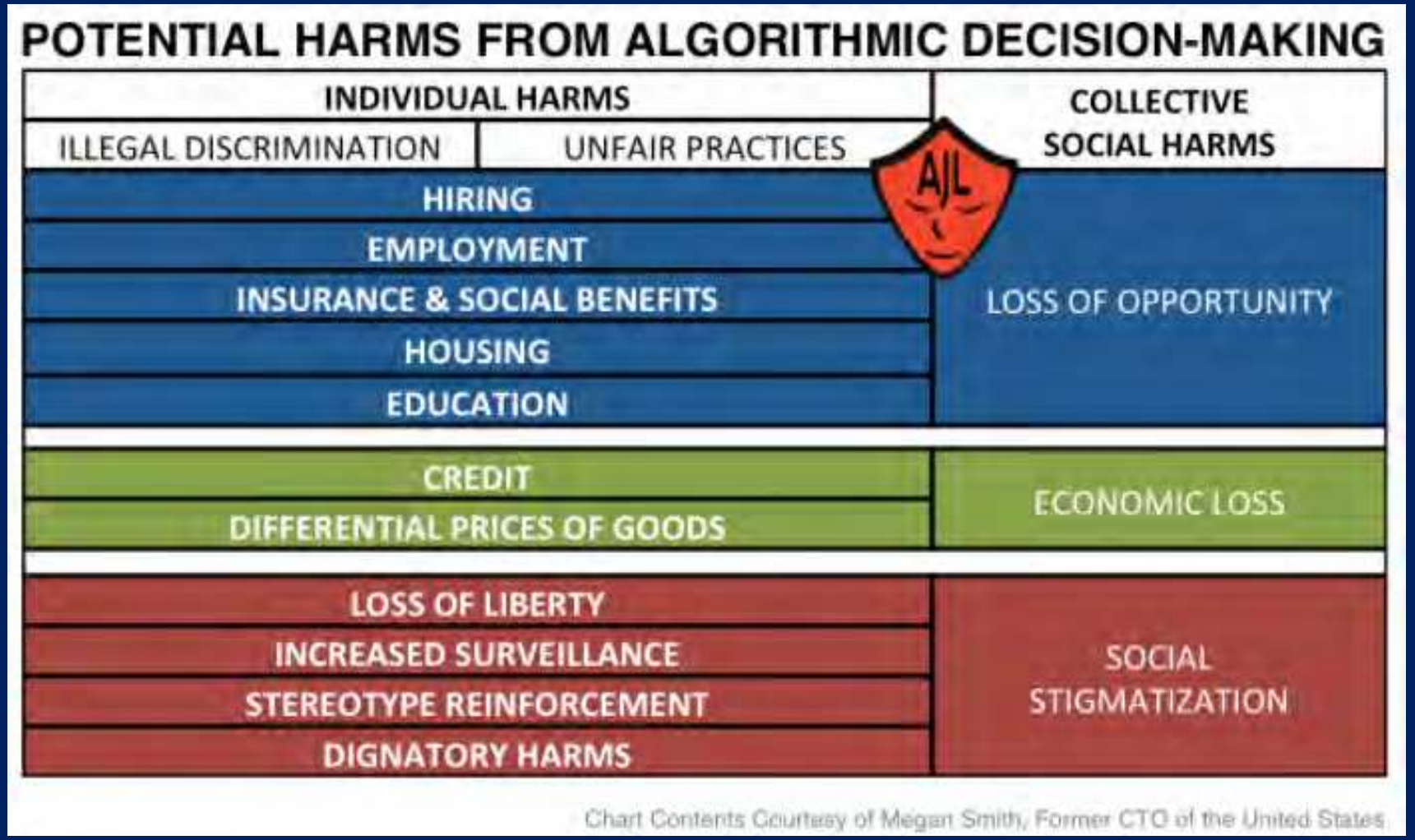
- Within the education sector, the University of Malta and the Ministry for the Economy and Industry have partnered up with the MDIA to run three projects using AI. One of the three projects, 'Edu AI', targets children aged between 8 to 10 years of age and uses AI-powered puppets during shared reading sessions. The AI system includes language and literacy tasks and games involving speech and text recognition.

Concerns with AI

- The main concerns with implementing AI systems is the lack of legal certainty surrounding such systems, as our current legislative framework does not cater for complex issues which may arise.

- Currently, AI systems bring about lacunae within Maltese Law, which does not cater for certain scenarios, such as:
  1. Discrimination and Bias within the AI system;
  2. Civil Liability;
  3. Intellectual property rights; and
  4. Competition Law.

Discrimination and Bias



Discrimination and Bias

- A core concern with AI systems is the innate human bias of its developers which is embedded within the system per se. If one views code as an expression of the developer's self, it is not difficult to understand how such bias arises within AI systems.

- This has been identified as a major challenge related to the use of algorithms and automated decision-making. The principle of non-discrimination as enshrined in Art. 21 of the Charter of Fundamental Human Rights of the European Union is not to be taken lightly and must be at the forefront of any system.

- Potential examples of discrimination relate to candidates for job interviews, scores in creditworthiness or during trials, amongst others.

Discrimination and Bias

- In August 2019, Malta published a draft Ethical AI Framework: 'Towards Trustworthy AI', which aims to establish a set of guiding principles and trustworthy AI governance and control practices.
- The intention is for the Malta Ethical AI Framework to support AI practitioners in identifying and managing the potential risks of AI, while also serving to identify opportunities to encode a higher ethical standard into AI.
- There is also the IEEE P7003 standard for algorithmic bias considerations which provides a development framework to avoid unintended, unjustified, and inappropriately differential outcomes for users.

Civil Liability

- Maltese legislation does not currently provide for non-contractual liability for damages cause by AI or other alternative digital technologies.

- In lieu of this, one must fall back on the provisions of the Civil Code (Chapter 16 of the Laws of Malta) to determine liability from a traditional tort-based perspective.

- Therein, article 1031 establishes the principle that every person is liable for damages caused through their own fault. The standard of proof in determining such fault is that of the bonus paterfamilias ("reasonable man").

Civil Liability

- It would appear that the developer of an AI system would be deemed to be the legal person against whom claims for damages may be brought.

- This thinking would currently apply to damages arising both as a result of the use of the AI system itself, as well as the reliance on any of the outcomes of that system, even if such outcomes arose from the system's own processes.

- This is because ultimately, it is the developer who implemented the system's 'cognition'. When coupled with the concept of the bonus paterfamilias, this entails that the developer should be liable for not implementing appropriate 'fail-safes' or be found liable for producing a defective product.

- This would also suffice for the sake of practicality. A natural person would not be able to seek legal redress against an AI system, unless a separate legal personality is attributed to it, or some form of agency status is recognised, as a minimum.

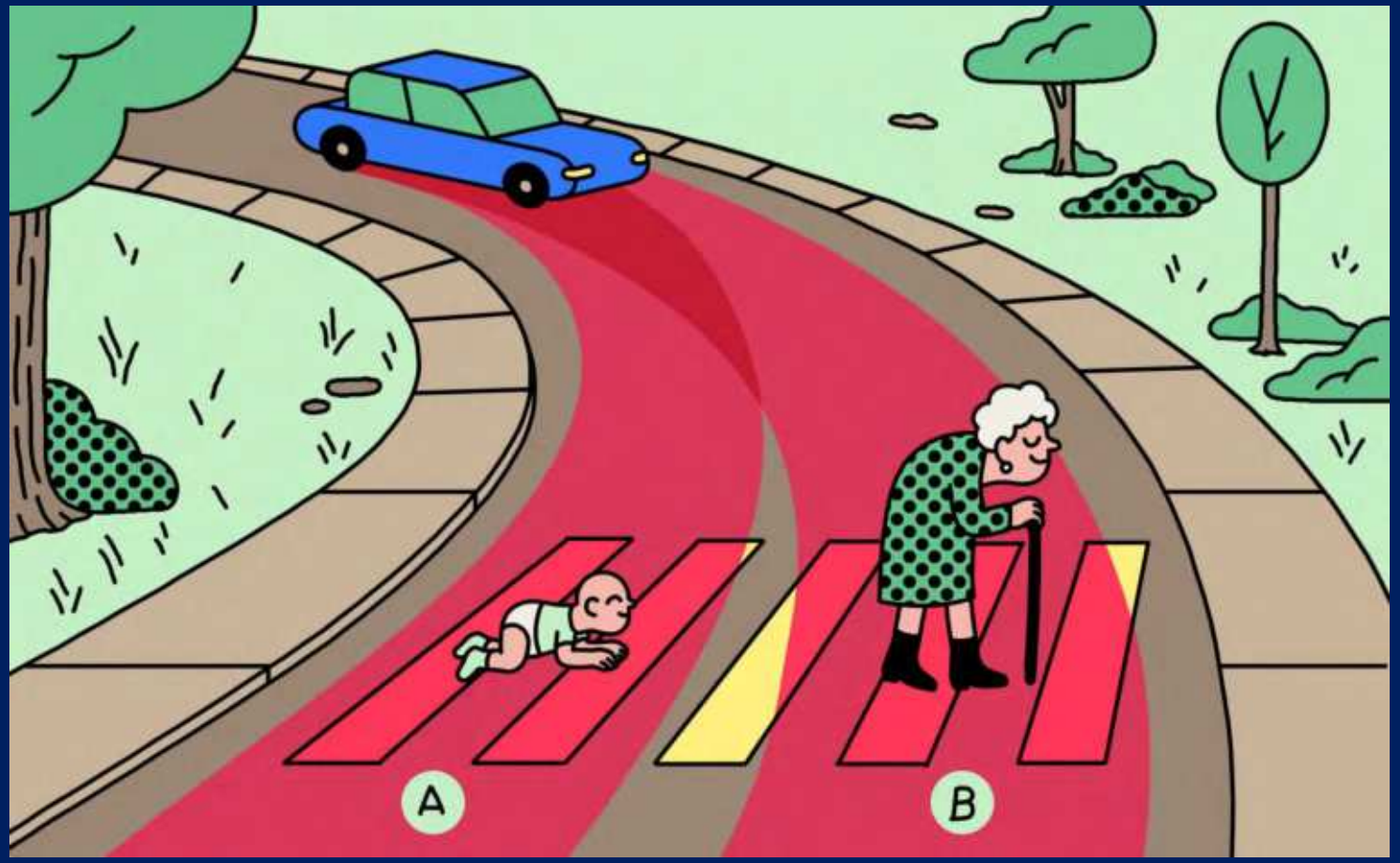
Civil Liability

- This standard is evident within article 1032 of the Civil Code, which provides that a person is deemed to be at fault where they fail to exercise the attention, diligence and prudence of a “reasonable man”. The extent of reasonableness is only determined by the Courts, which must exercise discretion in their determination.

- Moreover, article 1033 of the Civil Code further provides that any person who with or without intention to injure, voluntarily or through negligence, imprudence, or want of attention, is guilty of an act or omission which breaches the duty of care as imposed by law, will be liable for any damage resulting from their negligence.

- This begs the question as to whether, if an AI system acts of ‘its own’ volition and through no prior instructions of the developer, the owner would be indirectly liable for creating a system which gives rises to the damage.

Civil Liability - Example



Civil Liability - Example

- Part of the previously mentioned MISAM project sets out to explore the current legislative framework, and to propose initial solutions in respect of any gaps currently found within our law, such as liability for any collisions or accidents which autonomous vehicles may cause.

- These are issues which will undoubtedly strain current concepts and the application of civil liability and will introduce moral dilemmas, which may not be entirely addressed through traditional legal means.

- What do you think the 'moral approach' would be in choosing between the young child and the old woman in the picture?

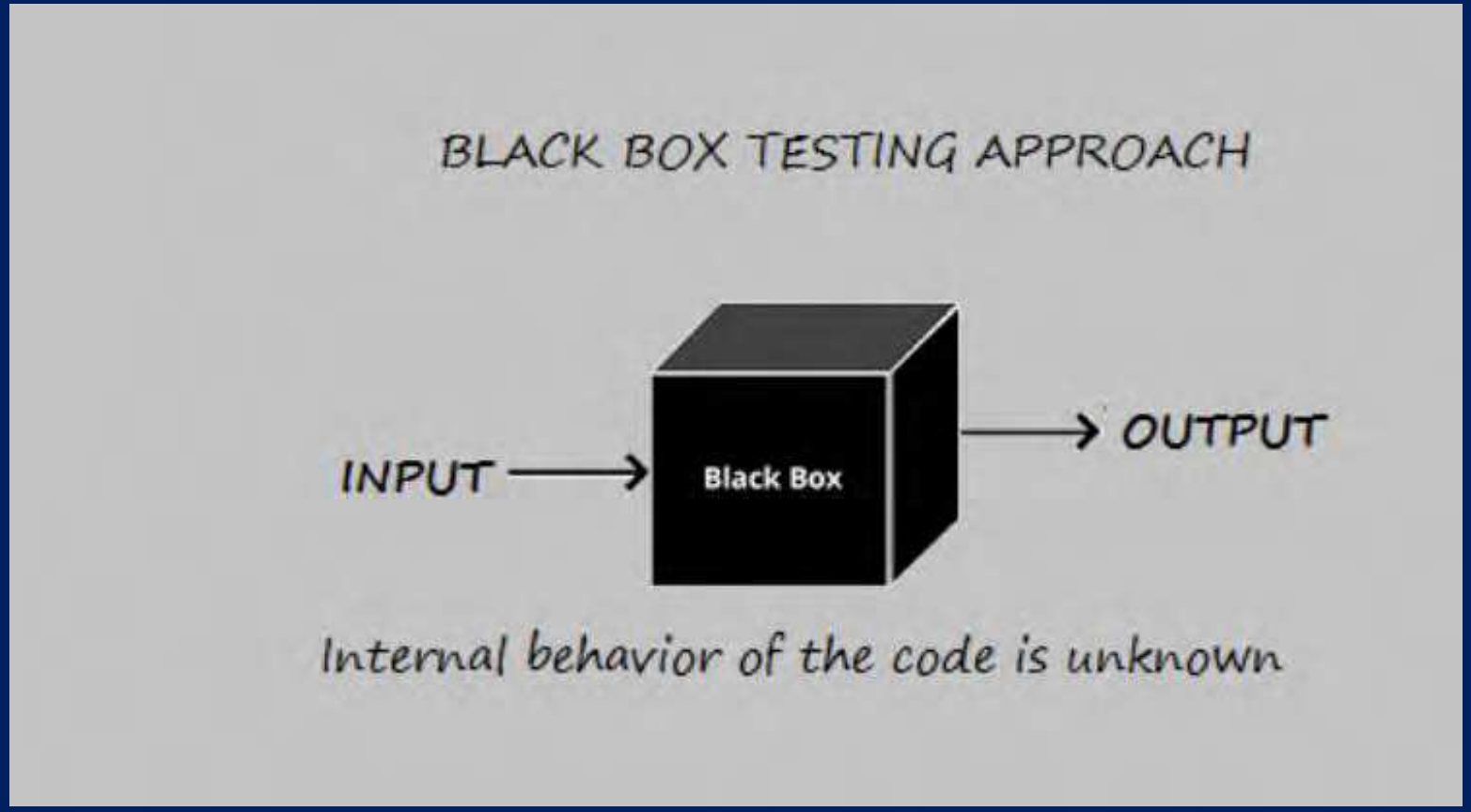
The Product Liability Directive

- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products and the Consumer Affairs Act (Chapter 378 of the Laws of Malta) and its subsidiary legislation.

- It is evident that current liability rules do not fit 'black-box' systems such as AI, which results in a number of legal complexities, particularly when it comes to proving any defects and the causal link between such defects and the damage incurred.

- The EU Product Liability Directive is being revised, with the aim of a new Directive covering all products and adapting to the rules of the digital age and the circular economy.

Intellectual Property Rights



Intellectual Property Rights

- Code is predominantly based on arithmetic expression. Hence, AI (being code for the most part) is protected through the Maltese Copyright Act (Chapter 415 of the Laws of Malta) as a literary work, provided that the work satisfies the definition of 'computer program' found therein.

- Issues will arise for any work generated by the AI system because Maltese copyright law defines an 'author' as a natural person who created the work, thus excluding the possibly of automated systems as 'authors'.

- The main argument is whether the AI system was developed specifically to generate the work in question and if so, whether the system was merely a 'tool' utilised by the author and therefore, the system would not be deemed to be an author itself.

- Hence, while the developer of the AI system would be the owner of that system in terms of our Copyright Act, any subsequent works generated by this system fall within a lacuna which is not currently catered for in national legislation.

Intellectual Property Rights

- In terms of Maltese patent law, ownership over such patented ideas or processes is bestowed upon the applicant, who must be a legal person in order to fulfil the criteria of the patent legislation.

- While this is understandable when an AI system is developed using one's intellectual endeavours, matters become increasingly complex when that system generates its own 'content' or solution, without the intervention of a legal person. If the AI system generates any invention without any human intervention, current patent law would not consider such an invention as being patentable.

- It is therefore necessary to update current legislation to provide for ownership of IP generated entirely by automated systems or to bestow such ownership rights to agents and consider having an agency status allocated to AI automated systems.

Competition Law Concerns

- Big data in combination with AI has not changed the basic tenets of competition law. However, under certain circumstances, the two feature as a contributing factor to competition concerns, including:
  1. increasing market power and facilitating exploitative or exclusionary practices by dominant firms;
  2. facilitating collusion; and
  3. merger control issues.

- Determining any alleged illegality depends on the factual context of each case and the legislative framework in the particular jurisdiction.

- Maltese (and EU) courts are yet to decide on such matters.

Algorithmic Pricing

- One relevant issue faced in the competition sector, for example, is that of algorithmic pricing, wherein an AI system utilizes 'big data-sets' and machine learning techniques to automatically re-calibrate prices based on internal or external factors. These include supply and demand variables, competitor's prices, or external market data (which is typically purchased by the respective undertaking).

- Algorithmic pricing is not deemed illegal per se where the information is obtained legitimately, and if the AI system was developed independently. Should, however, the system be a result of collusion or collaboration between competing undertakings to set prices then regardless of whether the price setting was conducted orally, through correspondence or through algorithms, the basic tenets of Maltese / EU competition law remain true in an online environment as well, including that prohibiting the setting of unlawful pricing among competitors.

Proposal for a Regulation on Harmonised AI Rules

- On the 21st of April 2021, the European Commission set out their proposal for the regulation of artificial intelligence ("AI") systems (the "Regulation").

- The aim of the Regulation is to set harmonised standards of ethical usage of AI while promoting its development in various practical use-cases.

- Through the Regulation, the EU seeks to define AI systems using a risk-based approach, ranging from minimal risk to unacceptable risk. The latter is a clear attempt to prohibit AI systems which evaluate persons based on their 'trustworthiness' or social behaviour.

- Different levels of risk attract corresponding compliance requirements. The risk categories include:
    1. unacceptable risk (these AI systems are prohibited);
    2. high-risk;
    3. limited risk; and
    4. minimal risk.

Proposal for a Regulation on Harmonised AI Rules

- The main provisions of the AI Regulation are the introduction of:
  1. Binding rules for AI systems that apply to providers, users, importers, and distributors of AI systems in the EU, irrespective of where they are based.
  2. A list of certain prohibited AI systems.
  3. Extensive compliance obligations for high-risk AI systems.
  4. Fines of up to EUR 30 million or up to 6% of annual turnover, whichever is higher, for breaches.

- The AI Regulation proposes a broad regulatory scope, covering all aspects of the lifecycle of the development, sale and use of AI systems. The AI Regulation will apply to:
  1. providers that place AI systems on the market or put AI systems into service, regardless of whether those providers are established in the EU or in a third country;
  2. users of AI systems in the EU; and
  3. providers and users of AI systems that are located in a third country where the output produced by the system is used in the EU.
  4. Therefore, the AI Regulation will apply to actors both inside and outside the EU as long as the AI system is placed on the market in the EU or its use affects people located in the EU.

Defining AI systems

- The Regulation defines an 'artificial intelligence system' ("AI system") as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

- The abovementioned techniques and approaches are as follows:
  1. Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
  2. Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; or
  3. Statistical approaches, Bayesian estimation, search and optimization method.

Prohibited AI systems

- AI systems that deploy subliminal techniques to exploit vulnerabilities of a specific group of persons to distort their behaviour, causing physical or psychological harm.

- The use of AI systems by public for the evaluation or classification of the trustworthiness of persons based on their social behaviour where the score generated leads to the detriment of certain groups – think of the social-scoring system in North Korea.

- Real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement, unless strictly necessary for a targeted crime search or prevention of substantial threats. This came about in connection with a facial recognition app 'Clear View' to allow clients such as US law enforcement agencies to match photos of unknown persons to images of them found online.

High-risk AI Systems

- AI systems intended to be used as a safety component of products (or as the product *per se*) within:
  1. Machinery;
  2. Recreational craft and personal watercraft;
  3. Lifts;
  4. Protective systems in potentially explosive atmospheres;
  5. Radio equipment;
  6. Marine equipment;
  7. Pressure equipment;
  8. Cableway installations;
  9. Personal protective equipment.

High-risk AI Systems

- Stand-alone AI systems whose use may have an impact on the fundamental rights of natural persons, such as:
  1. Biometric identification systems;
  2. Education and vocational training;
  3. Employment;
  4. Law enforcement;
  5. Migration;
  6. Asylum and border control;
  7. Administration of justice.

High-risk systems – General Requirements

- Transparency: High-risk AI systems must be designed and developed to ensure that the system is sufficiently transparent to enable users to interpret its output and use it appropriately;

- Human oversight: High-risk AI systems must be designed and developed in such a way that there is human oversight of the system, aimed at minimising risks to health, safety and fundamental rights;

- Risk management system: A risk management system must be established and maintained throughout the lifetime of the system to identify and analyse risks and adopt suitable risk management measures;

High-risk systems – General Requirements

- Training and testing: Data sets used to support training, validation and testing must be subject to appropriate data governance and management practices and must be relevant, representative, accurate and complete;

- Technical documentation: Complete technical documentation that demonstrates compliance with the AI Regulation must be in place before the AI system is placed on the market and must be maintained throughout the lifecycle of the system; and

- Security: A high level of accuracy, robustness and security must consistently be ensured throughout the lifecycle of the high-risk AI system.

High-risk systems – Specific Requirements

- Compliance with the general requirements;
- Registration: Register the AI system in the EU AI database to be managed by the European Commission;
- Conformity assessment: Ensure the system undergoes the relevant conformity assessment procedure;
- Corrective action and notification: Immediately take corrective action to address any suspected non-conformity and notify relevant authorities of such non-conformity;

High-risk systems – Specific Requirements

- Quality management system: Implement a quality management system, including a strategy for regulatory compliance, and procedures for design, testing, validation, data management, and record-keeping;

- Post-market monitoring: Implement and maintain a post-market monitoring system, by collecting and analysing data about the performance of the high-risk AI system throughout the system's lifetime.

- Monitoring obligations include reporting any serious incident or any malfunctioning of the AI system, which would constitute a breach of obligations under EU laws intended to protect fundamental rights.

High-risk systems – User Requirements

- use the systems in accordance with the instructions of the provider and implement all technical and organisational measures stipulated by the provider to address the risks of using the high-risk AI system;
- ensure all input data is relevant to the intended purpose;
- monitor operation of the system and notify the provider about serious incidents and malfunctioning; and
- maintain logs automatically generated by the high-risk AI system, where those logs are within the control of the user.

Non High-Risk Systems

- AI systems which do not qualify as prohibited or high-risk AI systems are not subject to any specific requirements.
- Limited risk AI-systems are subject to transparency obligations, particularly if they are intended to interact with people, such as chatbots.
- All other minimal risk AI systems can be developed and used subject to existing legislation without additional legal obligations.

Enforcement

- Member States must designate national competent authorities and a national supervisory authority responsible for providing guidance and advice on the AI Regulation.
- The Regulation provides for the establishment the European Artificial Intelligence Board ("EAIB"), to advise and assist the Commission in connection with the AI Regulation.
- The EAIB facilitate cooperation between the national supervisory authorities and the Commission, coordinate and contribute to guidance by the Commission and assist the national supervisory authorities and the Commission to ensure consistent application of the Regulation.

Sanctions

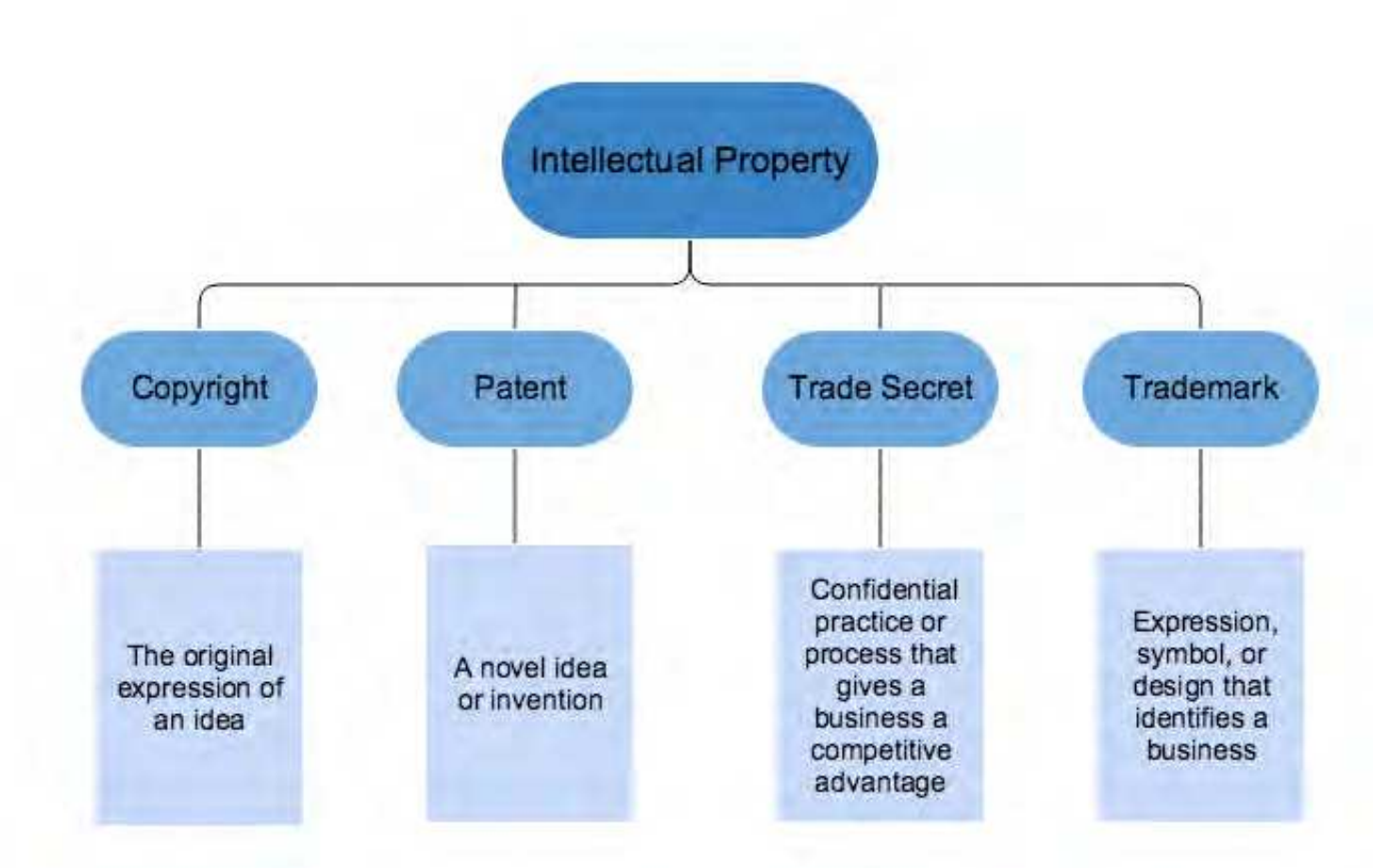
- Infringement of the AI Regulation is subject to financial sanctions of up to €10m – €30m or 2% – 6% of the global annual turnover, whichever is higher.

- The level of fine imposed depends on the nature of the infringement, granting a degree of discretion to the supervisory authority in handing out sanctions.

Questions

- How does the EU intend to regulate AI systems?
- What are the different levels of risk associated with AI systems?
- What are the main risks associated with AI systems? How can these be mitigated?

Intellectual Property



Intellectual Property - General

- Intellectual property ("IP") refers to intangible assets that are products of the mind. IP assets are not physical in nature. Rather, they are the ideas, knowledge and creativity that go into making a product, service, process or business.

- IP is incredibly valuable for businesses as it gives them a competitive edge. Therefore, organizations protect intellectual property assets with legal safeguards.

- Having legal protection over one's IP means that the proprietor has certain rights which:

1. Can be treated as property;
2. Allow the proprietor to control the use of their IP;
3. Amounts to a specified type of intangible asset;
4. Can be enforced by civil, commercial and competition law.

Copyright – Applicable Legislation

- In so far as copyright is concerned, the relevant legislation is as follows:
  - The Copyright Act (Cap 415);
  - S.L 415.01 on Control for the Establishment and Operations of Societies for the Collective Administration of Copyright,
  - S.L 415.02 on Revival of Rights and Neighbouring Rights and the Exhaustion of Distribution Rights;
  - S.L 415.03 on Artists' Resale Rights;
  - S.L 415.08 on Copyright and related rights in the Digital Single Market Regulations.

- In 2009, Malta also acceded to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

Copyright - General

- Copyright (or author's right) 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, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings.

- In the majority of countries, and according to the Berne Convention, copyright protection is obtained automatically without the need for registration or other formalities. That said, having voluntary registration systems can help solve disputes over ownership or creation, as well as facilitate financial transactions, sales, and the assignment and/or transfer of rights.

Copyright - Rights

- There are two types of rights under copyright:
  1. economic rights, which allow the rights owner to derive financial reward from the use of their works by others; and
  2. moral rights, which protect the non-economic interests of the author.

- This protection remains valid for a period of 70 years after the end of the year in which the author dies, irrespective of the date when the work is lawfully made available to the public.

- In the case of performers, such protection generally expires 50 years from the publication of the performance.

Copyright – Rights

- Such rights include the right of the author to authorise and prevent third parties from reproducing the entirety (or a substantial part of) the protected work. Another of such rights includes the right to alter, adapt, distribute, or communicate the work to the public. Hence, the main protection is that of protecting the author against the commercial exploitation of the copyrighted work, without prior approval.

- Protection arises automatically once a work which is eligible for copyright is created. This hinges upon the essential elements of copyright coexisting, which require the work in question to be:

1. a work eligible for copyright protection;
2. original in character; and
3. certain works must also be reduced to writing.

- Seeing as there is no need to register copyrighted work for the author to benefit from such protection, there is currently no register available locally to register copyrighted works.

Copyright - Rights

- There is no such thing as an international copyright since copyright protection is a territorial concept. This means that each country regulates copyrights according to their own set of local regulations.

- In other words, if an IPR is recognised in Malta, this does not necessarily mean that such an IPR would be recognised in any other jurisdiction.

- Although there are international efforts to set minimum standards for copyright and patent protection, the different requirements in national laws can present a challenge for global organisations.

The Database Directive

- Directive 96/9/EC on the legal protection of databases (the “Database Directive") provides for two different form of protection:
  - That based on copyright, which extends to databases “by reason of the selection or arrangement of their contents, constituting the author's own intellectual creation”; and
  - *Sui generis* rights over the database *per se* since making such databases requires “the investment of considerable human, technical and financial resources” (Recital 7 of the Directive).

- Note that the former does not extend to the content of the database itself while the latter prohibits the extraction and re-use of substantial part of the contents of the database.

- To be awarded protection under the Database Directive, the makers of the database must show that there was a substantial investment in obtaining, verifying or presenting the contents of a database.

The Database Directive

- Rights holders may only stop data from being extracted from databases or reused when the conduct they are complaining of affects their investment in obtaining, verifying or presenting the information that makes up databases.

- AG Szpunar (Attorney General of the Court of Justice of the European Union) opines that there must be:
    1. A balance of interests of the database operators with those of content aggregators and users of content aggregation services; and
    2. Preventing database rights being used to exclude others from the same market as those in which the database right holder operates in.

- The aim of this opinion is not to afford protection against all competition, but rather, to avoid commercial parasitism.

Copyright in Software

- The Copyright Act provides protection to computer programs as a literary work, as per Directive 2009/24/EC (the “Software Directive”).

- Therefore, software copyright is protection granted over the source codes and/ or object code which enables a computer to perform a specific task.

- As copyright protects the original work, any software which is an original creation of the programmer, is eligible for Copyright protection.

Source Code vs. Object Code

- Source code represents an original code of a program written in a particular programming language. The source-code is independent of the platform so that it does not refer to certain types of processors or operating system. Access to the source code allows understanding of the techniques and the programming technology.

- Object code is expressed in binary form, meaning a series of zeroes and ones, and is the compilation of the source code through a compiler.

- A part of these elements, such as the formulae included in the source code, the implemented algorithms, the architecture of the information system or the database structure, may be protected by both copyright and trade secret, as long as it has economic value and retains secret character.

Patents

- Patents are governed by the Patents and Designs Act (Cap 417) and are a form of IP which confer upon the inventor exclusive rights over the subject-matter within the patent application.

- The protection granted hinges upon the valid registration of the patent within the register of patents kept under the Patents and Designs Act (unlike copyright). It should be noted that the register contains national patents and information related to European patents validated in Malta.

- Patent protection may be conferred over a product or a process. Accordingly, protection is conferred over the inventive idea which may be embodied within a product or process, not the actual product or process *per se*.

- Entitles the inventor to an exclusive right over his invention, which is essentially deemed to be a product or process which is employed in an innovative manner or which offers a new technical solution to a problem.

- The term of a patent is (20) years from the filing date of the application.

Patents

- Under the Act, inventions are patentable in Malta if they:
    1. Are novel (not forming part of the prior art);
    2. Involve an inventive step; and
    3. Are susceptible to industrial applications.

- However, not all forms of inventions are eligible for patent protection. The following are all excluded from the scope of patent eligibility:
    a. Discoveries, scientific theories and mathematical methods;
    b. Aesthetic creations;
    c. Presentations of information;
    d. Rules, and methodologies for performing mental acts, playing games or doing business; and
    e. computer programs.

Issues with Software Patentability

- Maltese law does not protect computer programs and technically, they shall not be considered as inventions and are thus not eligible for patent protection.

- That said, the exclusion within Art. 4(3) “shall exclude the patentability of the subject matter or activities… only to the extent to which a patent application or patent relates to such subject matter or activities **as such**”.

- The European Patents Office (“EPO”) has considered various jurisprudence in determining the benchmark for software to be considered as patentable.

Jurisprudence - Vicom

- Vicom (T 0208/84) is an early (1986) legal decision which helped define the EPO's approach to software inventions in the 1980s and 1990s. In this decision, it was stated that: "Decisive is what technical contribution the invention as defined in the claim when considered as a whole makes to the known art." (T 208/84, Reasons 16)

- If a claimed invention makes a technical contribution that goes beyond the exclusions to patent eligibility, then the exclusions to patent eligibility are avoided.

- This approach was followed by the EPO and led to a large volume of case law concerning what can be considered to be "technical", much of which is still relevant today.

Jurisprudence – Comvik and Hitachi

- Through Comvik (T641/00) and Hitachi (T258/03), EPO case law began to evolve away from the "technical contribution" approach of Vicom, into what became known as the 'Comvik approach':
  1. Differentiate between features having technical character ("technical" features) and features lacking technical character ("non-technical" features);
  2. If the claim includes any technical features, the patent eligibility exclusions are avoided;
  3. Assess the inventive step of technical features using the EPO's 'problem-and-solution approach', whilst allowing non-technical features to be incorporated into the technical problem that is to be solved.

Jurisprudence – Comvik and Hitachi

- The assessments of patent eligibility and inventive step are tightly coupled together. The non-technical features are considered to be part of the prior art, and can be used to attack the inventive step of the remaining technical features.

- This is a dramatic shift away from the Vicom approach, but means that patent eligibility and inventive step analyses are based on the same set of technical features.

Differences between the Comvik and Vicom approaches

- Under Vicom, the assessment of patent eligibility and inventive step were performed separately, allowing a gap to exist between the set of claimed features used as the basis for arguing that the invention provides a “technical contribution”, and the set of claimed features used as the basis for arguing inventive step.

- Under Comvik, patent eligibility and inventive step are argued based on the same set of technical features:
  - What claimed features can be considered technical; and
  - can those technical features be considered non-obvious to a skilled person armed, not only with the prior art, but also with knowledge of any “non-technical” features of the claim.

Technical Character

- In order to have a technical character, and thus not be excluded from patentability, a computer program must produce a "further technical effect" when run on a computer.

- A "further technical effect" is a technical effect going beyond the "normal" physical interactions between the program (software) and the computer (hardware) on which it is run.

- The normal physical effects of the execution of a program, e.g. the circulation of electrical currents in the computer, are not in themselves sufficient to confer technical character to a computer program

Domain Names

- Domain names are registered at a domain name registrar. The process usually takes three to four days from application to access the domain. Part of the process requires a physical signature on a document sent by the Maltese Network Information Centre, which needs to be sent back before it is processed.

- The registrars ensure that the requested domain name is available and, if so, match the domain name with an IP address. The registrant can use the domain name for as long as the renewal fee is paid to the registrar and as long as the registration of the domain name does not infringe the rights of others.

- Anyone can own an ".mt" domain and there is no need for the applicant to be established in Malta. The applicant must declare the right to use the domain name, ideally via a trade mark or a business name.

Protecting One's Domain – Cease & Desist

- Sending a formal 'Cease and Desist' letter to the Website's owner as a first step. In practice, it is typical for Cease and Desist letters to be circulated to the alleged infringer before any further action is taken in order to give the recipient fair notice of the proceedings which may be filed against them and to give the recipients time to regularise their position.

- The Cease and Desist letter would essentially assert that the Website infringes the domain holder's registered trademarks and its registered domain name, and that the use and operation of this Website constitutes passing off in terms of article 32 of the Commercial Code and article 6bis of the Paris Convention.

- Letter should be sent to the operator of the Website as well as the registrant. Following the implementation of the GDPR, the Register no longer displays contact details of the persons behind the websites and this means that it can be difficult to find contact details which we could use to send out such legal letters.

Protecting One's Domain – UDPR

- The Uniform Domain Name Dispute Resolution Policy ("UDPR") involves arbitration to resolve disputes concerning the abusive registration of the domain name and where successful, the domain name in question may be cancelled or transferred to the complainant. An abusive registration is one where:
  1. The domain name is identical or confusingly similar to the complainant's trademark;
  2. The registrant has no rights or legitimate interests in the trademark;
  3. The registration has been made and is being used in bad faith.

- Model Complaint Form to be sent via e-mail to domain.disputes@wipo.int.

- Once a complaint is filed, the WIPO Centre requests the concerned registrar to "lock" the disputed domain name so that the domain name will not be transferred to another registrant during the UDRP proceeding. Within two business days of receiving the Centre's request, the registrar must confirm that a lock has been applied and that the disputed domain name will remain locked during the pendency of the UDRP proceeding.

- The required payment should be made to the WIPO along with the submission of the complaint. Depending on whether 1 or 3 Panellists were chosen to assist in the procedure, the administrative fees vary from $ 1,500 to $ 4,000, respectively.

Trademarks

- A trademark is any sign capable of being represented graphically and of distinguishing the goods and services of one undertaking from those of another. It may consist of words, figurative elements, letters, numerals or the shape of goods or their packaging.
- Trademark registration offers the following benefits, such as prohibiting:

- the use of an identical or similar sign in the course of trade in relation to similar or identical goods or services; and
- the use of an identical or similar sign in the course of trade where the goods or services are not similar, but the trademark has a reputation in Malta and such use take unfair advantage of or is detrimental to the distinctive character or the repute of the trademark.

- Trademark registration covers the classes of goods and/or services (under the Nice Classification) designated in the application.

Trademarks

- A trademark will not be registered if:

- It lacks distinctive character;
- It is made up entirely of signs/indications which may serve, in trade, to designate the kind, quality, intended purpose, value, geographical origin, time of production of goods or rendering of services, or other characteristics of goods or services;
- It consists entirely of signs or indications which have become customary in the current language or in the bona fide and established practices of trade;
- Its shape results from the nature or shape of the goods themselves and said shape gives substantial value to the goods;
- It is contrary ot public policy or morality;
- It is of such a nature as to the deceive the public as to the nature, quality or geographical origin of the goods/services;
- Its use is prohibited in Malta by any law;
- It consists of or contains any signs, arms, armorial bearings or flags; or
- It is made in bad faith.

- A trademark registration has a duration of 10 years, following which it can be renewed for further periods of 10 years.

Intellectual Property - Summary

	Trademarks	Copyright	Patent	Designs
Example	Logos	Computer programs	Inventions	The shape of a Coca-cola bottle
Registerable?	Yes	No	Yes	Yes
Requirements for Registration	List of Goods and Services	N/A	Completed patent application	Completed Design application form
Term of Protection (Malta)	10 years from the date of filing of the application with the possibility of renewing protection for further 10 year periods.	For works other than audio-visual works, 70 years after the end of the year in which the author dies, irrespective of the date when the work is lawfully made available to the public.	The term of a patent shall be 20 years from the filing date of the application.	5 years with the possibility of renewing such registration for a maximum period of 25 years.
Fees for Registration	€115 per class per mark (Malta)	N/A	Application is subject to the payment of a filing fee amounting to €58.23and a further €58.23 shall become due upon the grant of the patent.	€46.59

Questions

- What does copyright/patents seek to protect? How does the protection differ?
- Is any protection provided to Databases?
- Is software patentable?
- What are the key differences between the Vicom and Comvik Approaches?
- How can one protect their domain name?

IT & Competition Law

- The Treaty on the Functioning of the European Union (the "TFEU") sets out the EU's antitrust policy under Articles 101 and 102.

- Article 101 prohibits anti-competitive agreements between two or more independent market operators. This covers both horizontal agreements (between actual or potential competitors at the same level of the supply chain) and vertical agreements (between undertakings operating at different levels e.g. a manufacturer and distributor). The most blatant example of illegal conduct breaching Article 101 is the creation of a cartel between competitors, which may involve price-fixing and/or market sharing.

- Article 102 prohibits abusive behaviour by companies holding dominant position on any given market, such as charging unfair prices or limiting production.

Competition – Antitrust Cases

- On 2 May 2022, the Commission sent a Statement of Objections to Apple. In its preliminary view, Apple restricted competition in the market for mobile wallets on Apple devices by limiting access to the NFC functionality for payments in stores in the EEA.

- The Commission's preliminary findings have shown that Apple enjoys significant market power in the market for smart mobile devices and a dominant position on mobile wallet markets.

- By restricting access to the NFC functionality, Apple has reserved the market to itself. Apple's full control over its closed ecosystem enabled its proprietary payment solution, Apple Pay, to remain the only player with access to the necessary NFC input.

- The exclusion of competitors leads to less innovation and less consumer choice for mobile wallets on Apple devices. If confirmed, this conduct would infringe Article 102 of the Treaty on the Functioning of the European Union (TFEU) that prohibits the abuse of a dominant market position.

Competition – Antitrust Cases

- In 2017, the European Commission fined Google EUR 2.42 billion for abusing dominance in order to give illegal advantage to its own comparison shopping service.
- In 2004, Google introduced a product initially named Froogle, then renamed to Google Product Search and subsequently to Google Shopping, which allows consumers to compare products and prices online.
- Google was found to have systematically given prominent placement to its own comparison shopping service, while also demoting rival services in its search results.

Competition – Antitrust Cases

- In 2019, The European Commission fined Google EUR 1.49 billion for abusing its market dominance by imposing a number of restrictive clauses in contracts with third-party websites. This misconduct lasted over 10 years and prevented Google's rivals from placing their search adverts on these websites.

- Google was by far the strongest player in online search advertising intermediation in the EEA, with a market share above 70% from 2006 to 2016. Through "AdSense" for Search, Google functions as an intermediary between advertisers and owners of publisher websites.

- The Commission's investigation found that:
  - Starting in 2006, Google included exclusivity clauses in its contracts, thus prohibiting publishers from placing any search adverts from competitors on their search results pages;
  - As of March 2009, Google gradually began replacing the exclusivity clauses with so-called "Premium Placement" clauses. As a result, Google's competitors were prevented from placing their search adverts in the most clicked on parts of the websites' search results pages; and
  - As of March 2009, Google also included clauses requiring publishers to seek written approval from Google before making changes to the way in which any rival adverts were displayed. This enabled Google to control how attractive competing search adverts could be.

21 ACADEMY

Diploma in Law (Malta)

CAMILLERI PREZIOSI
ADVOCATES