Information and Communication Technology Law

Lecture 1

Title: Introduction to IT and Data Protection Law

Diploma in Law (Malta)

Lecturer: Alexia Valenzia
Date: 02 April 2025

What is ICT Law?

Information and Communications Technology Law

- *Information* – (or data) in paper or electronic format
- *Communication* – in person or electronically (electronic communications), in writing or voice, telecommunications, and broadcasting
- *Information technology* (IT) – including software, hardware and electronics
- *Communications technology* – including protocols, software and hardware

What topics are covered under ICT law?

- Data protection and confidentiality of data
- Intellectual property
- Contracts to purchase computer hardware or software
- New (disruptive) technologies
- Electronic commerce
- Computer crime
- Protection of IT products / services

ICT Law is a distinct field of law

- Made up of different branches of the law such as:
  - contract law
  - consumer protection law
  - criminal law
  - intellectual property law
  - banking law
  - privacy and data protection law
  - freedom of expression law
  - tax law
  - telecommunications law
  - Employment law
- Includes contentious and non-contentious matters
- Civil as well as criminal matters

Digitisation: What is it?

Industrial Economic Model (19th/20th Centuries)

- Economic value within physical goods (*atoms*)
- Economies of scale & Mechanisation

Information Economy – present time

- Economic value sited within information *(bits*)
- Information collected, stored, processed
- Provision of services – banking, financial etc
- Information society – encoding: *atoms to bits*

Digitisation: What is it?

- Atoms used in the physical world to construct everything.
- Digitization = Conversion from *atoms to bits* (0 or 1)
- Bits = building blocks of the information society.

Digitisation:

- Cheaper to store and distribute goods/services
- New models to market and deliver products/services
- New avenues for communication, exchange of ideas
- Non-rivalrous goods versus rivalrous goods
  - ❑ Non-rivalrous goods/informational goods = intangibles, consumed by several consumers at the same time
  - ❑ rivalrous goods/ "Atomic" – those goods whose consumption by one consumer prevents simultaneous consumption by other consumers.

- Cross-border effects of information transfers on law – jurisdiction, identification of lawbreakers

Digitisation: What is it?

We have experienced a move from industrial based society to an information society

- Shift from ownership or control *of things* to ownership of or control *over information*
  - Information is important. e.g. a UK newspaper can be instantly printed anywhere in the world if the information (e.g. in a file) is available. No need to transport newspaper from country A to country B – disintermediation.

- New and revolutionary models to market and deliver products/services
  - Example music or film streaming services e.g. SoundCloud, Netflix

The Internet

Difference of opinions on how to regulate the Internet

The internet is a free and open space that requires no regulation and/or is incapable of being regulated

vs.

The internet today is completely regulated because of the prevalence of state surveillance and any ‘freedom’ is an illusion

Digitisation: What is it?

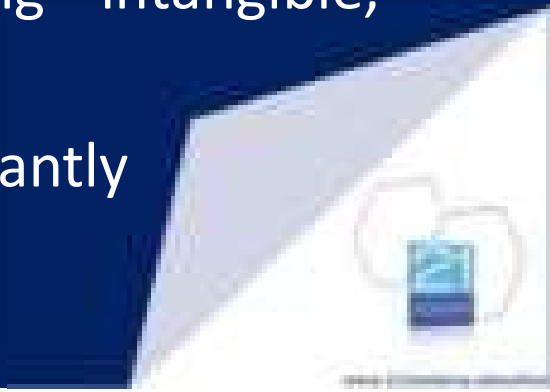
Even though digital information, the internet and applications like YouTube or social networking tools like Instagram, X or Facebook may seem to be simply part of the fabric of a 21st century world, legal systems find these developments to be extremely disruptive.

They are also innovative.

Legal challenges of the information society

- Traditional legal values based on valuable goods being physical, tangible and rivalrous or intangible goods (protected by intellectual property rights) fixed to a tangible carrier (CDs, books etc)

- With digitisation - possible to replace all previous information storage forms/media with bits
  - Valuable content (non-rivalrous goods) separated from traditional carrier (which was rivalrous)
  - Undermines traditional legal models for enforcing intangible, intellectual property rights
  - Legal challenge to protect information that is instantly replicable, transmissible and infinitely scalable.



Digitisation: What are its drivers?

- Fall in cost of storing digital information (bits).
- Fall in cost and speed of transmitting bits across computer networks.
- Rise in consumer demand for greater storage capacity and multi-platform support in digital devices.

Digitisation: What are its drivers?

Information / data is:

- Easier to generate, manipulate, transmit and store
- Cheaper to collect, manipulate and transmit

Furthermore:

- Nature of electronic information has developed an intrinsic value in itself
- Operation of IT systems and networks generate additional digital information (backup copies, cache copies etc)

Digitisation: Information disintermediation

- Traditional distribution: standard chain of manufacturer – carrier (middleman) – e.g. consumption from a shop

- Modern distribution: direct delivery from producer to consumer (*disintermediation*)
  - Direct downloading of products online
  - Middle man in supply chain cut off
  - Push media (websites) vs social networking tools

Digitisation: Convergence

The technological merger of several industries - computers, communications, consumer electronics, entertainment, and mass media - through various devices that exchange information in common electronic, or digital, formats.

ICT Regulation: What is Law?

- **Regulation** – creates, limits, or constrains a right; creates or limits a duty; or allocates a responsibility.
    - Many forms: laws, rules, obligations, social norms etc.
- **Law** – A set of rules that guides/govern our conduct in society and is enforceable through public bodies.

Why is Law important in the ICT sector?

- *Responsibility* (the liability for damages arising from breaches of the law).

- *Trust* (the commercial and personal trust necessary for electronic transactions).

Examples of laws fostering trust: The General Data Protection Regulation (EU Regulation 2016/679) & the Digital Services Act (EU Regulation 2022 2022/2065) and the Digital Markets Act (EU Regulation 2022/1925)

- *Ownership* (of intellectual property and information).

Examples of laws ensuring ownership: Trademarks Act (Chapter 597 of the Laws of Malta), Patents and Designs Act (Chapter 417 of the Laws of Malta) & Copyrights Act (Chapter 415 of the Laws of Malta)

The application of IT in the Legal Sector

1. Automated processes
2. Electronic Identification
3. Ease of research
4. Better resource management
5. Decline in risk of errors
6. Increased transparency
7. Introduction of new legal products/services

Practical Uses

1. Electronic case management
2. Online filing of documents
3. Legal Databases
4. Better client handling and delivery of services
5. Billing Software
6. Due Diligence

Tech Governance: Network Neutrality

"The principle that data packets on the internet should move impartially without regard to content, destination or source." (Murray, 2013)

You do not arbitrarily interfere in the transmission of data packets in an unclear and discriminatory fashion

- Modern routers allow network carriers to prioritise certain traffic over others
- Network providers argue that they can make more efficient use of the limited resources available to them with everyone receiving the best service possible
- Critics argue that it also allows network providers to discriminate against certain applications or data types

Net Neutrality: Advocates

Includes: Consumer groups, content providers, Internet founders

- The internet should be a free an open technology.
- Internet plurality – everyone has the right to free, open access
- Preserves fundamental internet standards
- Preserves end-to-end principle of the Internet
- A tiered system will favour large, well-established content providers who can afford to pay a premium
- Tiered system will lead to Premium service vs degraded service
- Preferential treatment of certain internet traffic will affect competition and innovation (esp. new entrants)
- Discrimination against certain applications or data types.

Net Neutrality: Opponents

Includes: Many ISPs, Telecoms companies, network operators

- Rise of Internet traffic puts burden on infrastructure hence best to control data rates for different types of content
- Allow allocation of bandwidth for more urgent applications
- Have a tiered system that would prioritise certain types of traffic for those able to pay.
- Revenue gained by premium payers can be used to invest in better networks and improve bandwidth
- Make more efficient use of the network (a limited resource)

Net Neutrality: Regulation

- EU Regulation No. (EU) 2015/2120 of 27th Nov 2015
  - states the principle of open internet access or “net neutrality” for the first time under European law
  - clarifies the set of rights and obligations associated with this principle. Gives some exceptions from basic net neutrality premise.
  - Came into force on 30th April 2016.

Net Neutrality: Regulation

1. Enshrines an **end-user's right** to be "free to access and distribute information and content, use and provide applications and services of their choice".
   - Specific provisions ensure that national authorities can enforce this new right.

2. **ISPs are prohibited from blocking or slowing down of internet traffic**, except where necessary. Exceptions are limited to:
   - traffic management to comply with a legal order,
   - to ensure network integrity and security,
   - to manage exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

Net Neutrality: Regulation

- Internet access providers can implement **reasonable traffic management measures** to enable an efficient use of network resources and the optimization of overall transmission quality.

- '**reasonable**' means:
  - Must be transparent, non-discriminatory and proportionate,
  - Must not be based on commercial considerations but only on objectively different technical quality of service requirements.
  - Must not monitor the specific content of traffic.
  - Must not be maintained for longer than necessary.

Net Neutrality: Regulation

One of the exceptions to basic neutrality premise:

'**Specialised services**': providers of certain services will have access to special transmission quality if there is network capacity and there will not be an adverse effect on overall internet access. E.g. critical services such as remote surgery, driverless cars and preventing terrorist activities

Regulating the Information Society

Atoms → bits

- Should the provision of ‘real world’ laws apply to the online world?
- Implications of the Metaverse

https://www.youtube.com/watch?v=6dYVFSZcXb0&t=162s

Regulating the Metaverse

- Privacy concerns
- Liability concerns
- Defamation and freedom of speech (amongst other fundamental rights)
- Tax and financial rules

Regulating the Information Society: Ethical Concerns

- Proper and lawful use of data
- Spreading of false information
- Covert tracking
- Accountability
- Liability

Regulating the Information Society: Ethical Concerns

- Bias in AI systems
- Deepfakes
- Autonomous vehicles
- Facial recognition
- Health tracking & automated decision-making
- Neurotechnology
- Genetic engineering
- Weaponization of technology

Regulating the Information Society: Social Issues

- Right to internet access
- Right to disconnect
- Identity theft
- Gaming & Gambling

Regulating the Information Society: Social Issues

- Lack of acceptance and trust in technology
- Facilitation of crime
- Social media addiction
- Anxiety and depression on the rise
- Health and fitness declining
- Lack of socialising
- Education


Break

Brief overview of the topics to be discussed in this module

Lecture	Topics
Lecture 2:	Computer Misuse and Cybercrime
Lecture 3:	MiCA, AI Regulation and IP laws
Lecture 4:	Electronic commerce, Digital Services and the Digital Markets Act
Lecture 5:	Data privacy, freedom of information and media and defamation
Lecture 6:	The GDPR
Lecture 7:	E-privacy regulation, Cookie war and SCCs

Computer Misuse & Cybercrime

Computer Misuse: Legal Issues related to Computers

- Hacking
- Encryption
- Censorship
- Harassment and DOS Attacks
- Defamation
- Copyright & Trademark infringement
- Privacy & data protection
- Illegal Content

Computer Misuse as a Crime

A crime is an act that violates a political, religious, or moral command considered important in protecting the interests of the State or the welfare of its citizens or subjects.

Computer Misuse: The FreeHour Issue

- It was reported that in April 2023, four students were arrested after exposing a security flaw in FreeHour's application
- FreeHour is a student & youth platform which simplifies daily student life with an array of academic and youth-oriented offerings - https://www.freehour.eu/
- Students identified a vulnerability in the app which they say could be exploited by malicious hackers
- Emailed FreeHour and asked for a 'bug bounty'. They also gave FreeHour a three-month deadline to secure the vulnerability before they would disclose it to the public
- Were arrested a month later and had their computer equipment seized

Computer Misuse: The FreeHour Issue

- Students say that the vulnerability allowed them to request whatever type of information they wanted from FreeHour's servers.
- Normally, a server would see a request for private data, check who is requesting it – in this case, it was the students – and deny access as the user does not have the required authorisation.
- The students are being investigated under Article 337 of the Criminal Code, which makes it illegal to access an application without being "duly authorised by an entitled person".
- The crime carries a punishment of up to four years in prison and a maximum fine of €23,293.

Computer Misuse: The FreeHour Issue

- FreeHour said that on receipt of the email, FreeHour contacted the office of the Information and Data Protection Commissioner (IDPC) and the Cyber Crime Unit for advice.

- Issue touches upon cybercrime as well as data protection laws

Computer Misuse: The Criminal Code

- Malta's Criminal Code (Chapter 9, Laws of Malta) regulates computer misuse through 337B-337H
- Based on the UK Computer Misuse Act and the Budapest Cybercrime Convention
- Drafted and defined broadly to account for 'all' scenarios

Unlawful access to, or use of, information – Art. 337C

A person who without authorisation does any of the following acts shall be guilty of an offence

a) **uses** a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;

b) **outputs** any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

c) **copies** any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

d) **prevents** or **hinders access** to any data, software or supporting documentation;

e) **impairs** the operation of any system, software or the integrity or reliability of any data.

Unlawful access to, or use of, information – Art. 337C

f) **takes possession** of or makes use of any data, software or supporting documentation;

g) **installs**, **moves**, **alters**, **erases**, **destroys**, varies or adds to any data, software or supporting documentation;

h) **discloses** a password or any other means of access, access code or other access information to any unauthorised person;

i) **uses another person's** access code, password, user name, electronic mail address or other means of access or identification information in a computer;

j) **discloses** any data, software or supporting documentation unless this is required in the course of his duties or by any other law.

Unlawful access to, or use of, information – Art. 337C

- Any person who performs any type of operation on a computer system or network, **without authorisation**, shall be guilty of an offence under the Criminal Code if convicted.

- Article 337C provides an exhaustive list of such operations. That said, Art. 337C was drafted in such a manner so as to include any **unauthorised** possession, alteration (not limited to impairment), use or distribution of the system of network.

- Therefore, one should note that the regulator's intention with this clause was to prevent any form of **unauthorized** activity to the computer system or network.

- This has broad implications, ranging from employee activity on their employer's system, intellectual property rights within software, and also criminal activity aimed at hindering such systems.

Data Protection & Privacy

What is Personal Data?

Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Key Definitions

Special Categories of Personal Data

Personal Data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life

Principle is that special categories of personal data cannot be processed

Processing

Use	Blocking	Retrieval	Destruction
Recording	Erasure	Storage	Gathering
Dissemination	Combination	Disclosure	Collection
Alignment	Adaptation	Organisation	Alteration

Data Controller

A natural or legal person, public authority, agency or other body which, alone or jointly with other, determines the purposes and means of the processing of personal data

Principles of Accountability – Art 5 GDPR

1. **Fair** and **lawful** processing
2. Data collected for **specific, explicitly stated, and legitimate purposes**
3. Data not processed for any purpose that is **incompatible** with the reason for collection
4. Processing **adequate** and **relevant** for the purposes of processing
5. No more data is processed **than is necessary** and is **not kept for a period longer than necessary**
6. **Correct** and **up-to-date**
7. All reasonable measures are taken to **complete**, **correct**, **block** or **erase** data to the extent that such data is incomplete or incorrect
8. processed in a manner that **ensures appropriate security** of the personal data

Lawfulness of Processing – Art 6 GDPR

Six available lawful bases for processing:

- Data Subject Consent

or

- Processing 'necessary' for:
  - The performance of a contract; or
  - Compliance with a legal obligation at law on DC; or
  - Vital interests of the DS; or
  - Performance of a task carried out in the public interest; or
  - Legitimate interest of the data controller or a third party.

Data Subject Rights

- ✓ Right to Information (Privacy Notices)
- ✓ Right to Access (DSARs)
- ✓ Right to Rectification
- ✓ Right to Withdraw Consent
- ✓ Right to Erasure (to be Forgotten)
- ✓ Right to Portability
- ✓ Right to know about Profiling
- ✓ Right to Object

Security and Data Breaches

- A Data Breach

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

- Notification to the IDPC

(72 hours from awareness)

- Notification to Data Subjects

High risk

Cross-Border Transfers Limitation

Principle:

No transfer of data to countries outside the EU that do not offer an "adequate level of protection"

Cross-Border Data Transfers may only take place if:

- the transfer is made to an Adequate Jurisdiction;
- the data exporter has implemented a lawful data transfer mechanism; or
- or an exemption or derogation applies

FROM POLITICO PRO

EU hits Meta with record €1.2B privacy fine

Tech giant transferred Europeans' data to the US unlawfully, Irish privacy regulator said.

Meta’s record fine

- This fine, which is the largest GDPR fine ever, was imposed for Meta’s transfers of personal data to the U.S. on the basis of standard contractual clauses (SCCs) since 16 July 2020. Furthermore, Meta has been ordered to bring its data transfers into compliance with the GDPR.

- Given the seriousness of the infringement, the EDPB found that the starting point for calculation of the fine should be between 20% and 100% of the applicable legal maximum.

- The punishment was imposed in relation to a legal challenge brought by an Austrian privacy campaigner, Max Schrems, over concerns resulting from the Edward Snowden revelations that European users’ data is not sufficiently protected from US intelligence agencies when it is transferred across the Atlantic.

- Meta said it would appeal against the decision and seek a stay on the data transfer order.

Electronic Commerce

E-Commerce issues: Smart Contracts

An Important Blockchain Application

- Smart contracts are automated agreements that allow us to transfer money, data, property deeds, shares, or anything else of value in a transparent conflict–free way without the services of a middleman. A smart contract is always essentially based on an if/then construct. The ***Ethereum*** platform runs smart contracts.
  - *Example 1*: Tom & Bob enter into a bet for £40 on the outcome of a game. They do not trust each other so will need an escrow agent (middleman) to hold the money. Instead of the escrow agent they can agree to use a code on a blockchain (smart contract) that executes automatically to award the money to Tom or Bob based on the outcome of the match
  - *Example 2*: A soft drinks machine that automatically orders new drinks when the machine is almost empty
    - **IF Number of bottles of soft drink = < 10**
      THEN Send order to soft-drink supplier

Smart Contracts

A Legal Issue related to Blockchain Technologies = Can we enforce smart contracts?

Smart contracts are prewritten software codes, and their use may present enforceability questions if attempting to analyse them within the traditional ‘contract’ definition. This is particularly true where smart contracts are built on permissionless blockchains (no central controlling authority)

Intellectual Property

Intellectual Property Law

- **IP** - The results of intellectual activity in the industrial, scientific literary or artistic fields. Creations of the mind – e.g. inventions, artistic works, literary works, designs, images etc.

- **IP - intangible assets, different to physical property**
  - Non-rivalrous – consumption of asset by X does not affect consumption by Y.
  - Non-exclusive – X cannot prevent Y from consuming asset.

- **An IP right is a right:** (i) That can be treated as property (ii) To control particular uses and (iii) of a specified type of intangible asset.

- IP rights granted to creator(s) of work and enforced by both civil and criminal law.

Intellectual Property Law

- In Favour: *Granting of IP Rights*

  - To reward authors for their work
  - To prevent someone taking credit for the work of another
  - To encourage & facilitate innovation, creativity & individuality.

- Against

  - Creating monopoly situations in the market place
  - Inadequate supply to meet demand in the market.

Intellectual Property Law

Main Forms:

- Patents
- Copyright
- Database Right
- Trademarks
- Registered Designs
- Trade Secrets
- Breach of confidence
- Passing off

Intellectual Property Law: Copyrights

- Copyright Act, Chapter 415 Laws of Malta
- Copyright is a property right that exists in works that can be protected by copyrights. Examples:
  - (a) paintings, drawing, maps, plans, sculptures etc
  - (b) audiovisual works
  - (c) computer programs
- Copyright cannot be used to protect an 'idea'
- Copyright protection is available only once the idea/work exists in some tangible or permanent form (written or recorded) = fixation

Intellectual Property Law: Copyrights

The owner of the copyright in a work has the exclusive right to prevent others from doing the following (amongst others):

- copy the work
- issue copies of the work to the public
- rent or lend the work to the public
- perform, show or play the work in public

Intellectual Property Law: Copyrights

- Moral rights relate to the ability of authors to control the eventual fate of their works.
- They cannot be sold/transferred but can be waived.
- They must be asserted by the copyright owner.

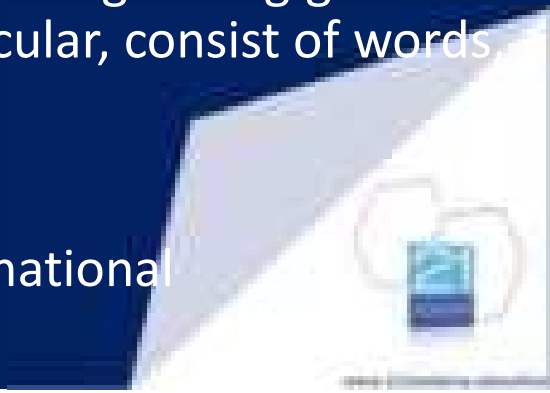
Intellectual Property Law: Copyrights

Exceptions to Copyright : Fair Dealing example

- Reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightsholders receive fair compensation which take account of the application or non-application or technological measures to the work or subject-matter concerned.

Intellectual Property Law: Trademarks

- Trademarks Act, Chapter 597 of the Laws of Malta
- They allow consumers to distinguish between competing products and services in a market economy
- Distinctive - Goods marks / service marks
- Signs capable of being represented graphically which is capable of distinguishing goods or services of one undertaking from another. A trademark may, in particular, consist of words slogans, designs, combined marks etc.
- Different methods of trademark protection: national, EU-wide, international



Intellectual Property Law: Trademarks

- Infringement: use of identical/similar mark in relation to identical/similar goods

Existing Trade Mark vs Proposed Mark	Goods/Services	Other Factor
Identical	Identical	N/A
Identical	Similar	Likelihood of Confusion
Similar	Identical or Similar	Likelihood of Confusion
Identical or Similar	Identical, Similar or Different	Reputation in & use for unfair advantage, detriment to reputation

Intellectual Property Law: Patents

An exclusive right to use and exploit an invention provided that that the essential elements for patentability exists where the invention:

- is new (Novelty)
- involves an inventive step going beyond state of the art
- is capable of industrial application

Exclusions – Non-patentable material :

- a discovery
- scientific theory
- mathematical method
- any aesthetic creation (e.g. artistic, musical work)
- any method of performing a mental act, playing a game or doing business
- the presentation of information

Lex Specialis

Examples:

- E-signature laws (EIDAS)
- VFA Framework / MiCA
- EU AI Regulation

Electronic Signatures

- **Electronic signature**: “data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”

- Very broad term and can take many different forms, including:

  - Typing a name into a contract or into an email containing contract terms
  - Clicking an “I accept” button on a website.
  - Pasting a signature (in the form of an image) into an electronic contract.
  - Using a web-based electronic signature platform to generate:
    - an electronic representation of a handwritten signature; or
    - a **digital signature** using public key encryption technology and backed by a digital certificate from the provider (or a trusted third party) verifying the identity of the signatory.

Electronic Signatures

- “Digital signatures” are a specific technology implementation of electronic signatures
  - Uses public key infrastructure (PKI) technology to associate a signer with a document & to protect the signed document.
  - It imprints ‘time’ into the signature stamp.
  - It is unique, Impossible to forgery, easy to authentication, impossibility of denial etc.

VFA Framework

- A framework supporting innovation and new technologies for financial services in the area of crypto-assets.

- Chapter 590 of the Laws of Malta – Virtual Financial Assets Act definitions:

  - "Distributed Ledger Technology" means "*a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes as further described in the Act (chapter 590 of the Laws of Malta).*"

  - "DLT asset" means *"(a) a virtual token; (b) a virtual financial asset; (c) electronic money; or(d) a financial instrument, that is intrinsically dependent on, or utilises, Distributed Ledger Technology*".

MiCA Regulation

- Markets in Crypto Assets Regulation
- Entered into force in June 2023 – applicable as from 30 June 2024 for Stablecoins and 30 December 2024 for all other aspects
- Divides crypto assets into 3 categories: (i) Asset referenced tokens, (ii) Electronic money tokens and (iii) ‘other’ tokens (that are not ART or EMT)
- Crypto - asset service providers are also regulated

MiCA Regulation

Fallen 'Crypto King' Sam Bankman-Fried gets 25 years for fraud

A timeline of cryptocurrency exchange FTX's historic collapse

Bankman-Fried received a sentence of 25 years in prison on Thursday.

EU Law on AI

- Proposed law
- Focuses on 2 areas: excellence in AI and trustworthy AI.
- The European approach to AI will 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.

- Commission published its AI package in April 2021, proposing new rules and actions to turn Europe into the global hub for trustworthy AI. This package consists of:

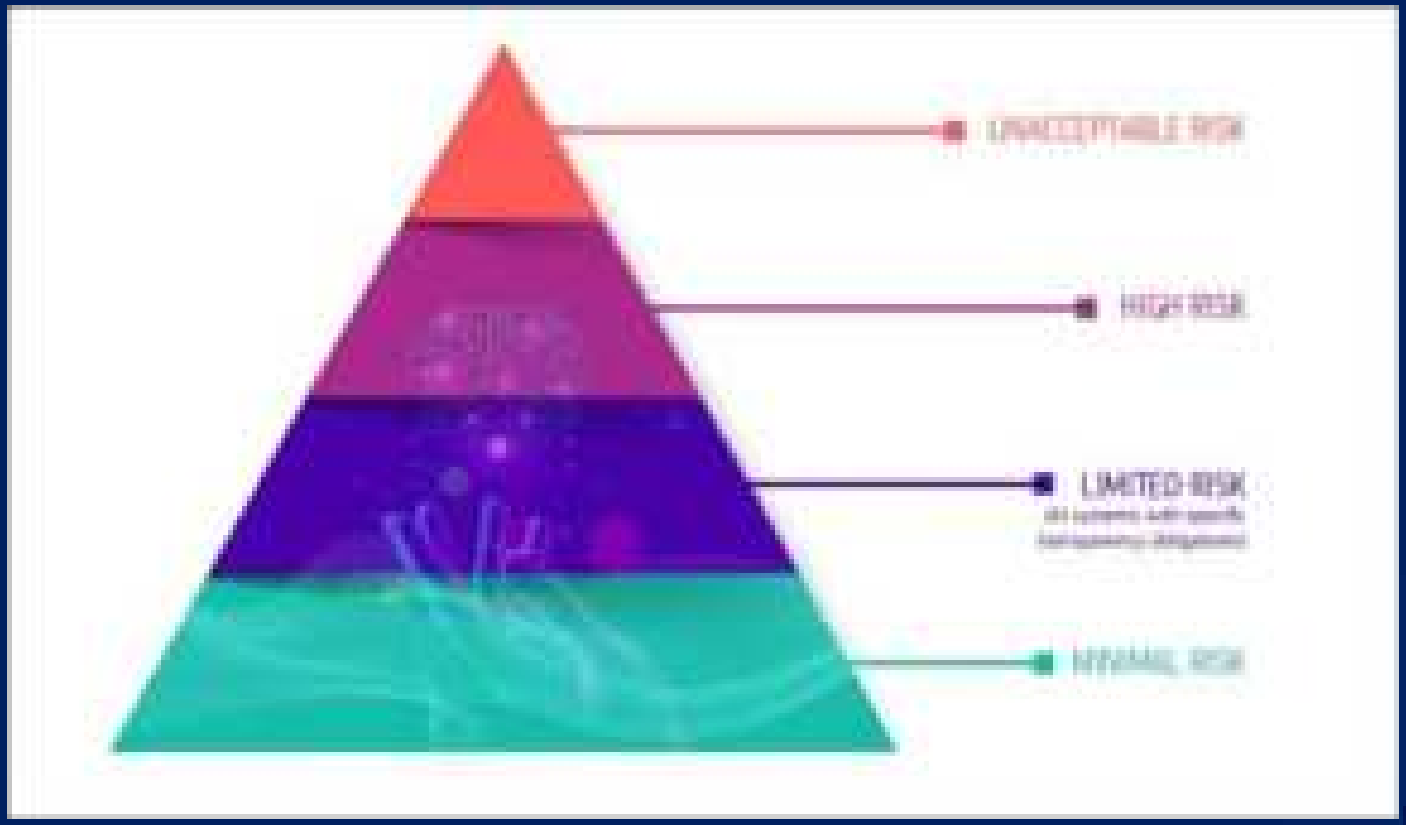
  - a Communication on Fostering a European Approach to Artificial Intelligence;
  - the Coordinated Plan with Member States: 2021 update; and
  - a proposal for an AI Regulation laying down harmonised rules for the EU (Artificial Intelligence Act).

EU Law on AI

The AI Regulation:

- Lays down harmonised rules for the EU (Artificial Intelligence Act)
- Was announced by the Commission in April 2021
- Addresses risks of specific uses of AI, categorising them into 4 different levels:
  - unacceptable risk;
  - high risk;
  - limited risk; and
  - minimal risk.

EU Law on AI



EU Law on AI

Unacceptable Risk / Prohibited AI practices

- Social Scoring
- Exploiting vulnerabilities/vulnerable groups
- Manipulation aiming at/effecting in the distortion of behaviour
- Real-time remote biometric identification systems in publicly accessible spaces

EU Law on AI

High Risk

Safety component in a product/ is a safety product

and

Safety product/ AI has to undergo third party conformity assessment

Listed in a critical area

and

Significant risk for health/ safety/ fundamental rights

EU Law on AI

Any Questions?

21 ACADEMY

Diploma in Law (Malta)