325DT71
Webinar on Computer Crimes

Table of Contents:

Co-funded by the European Union

Computer Crimes

TRAINING FOR DEFENCE LAWYERS

Online, 2 July 2025

ONLINE

EXCELLENCE IN EUROPEAN LAW

Speakers

Ciprian Băban, Defence Lawyer, Zamfirescu Racoti Vasile & Partners, Bucharest

Ramin Farinpour, Senior Lawyer, European Criminal Law Section, ERA, Trier

Dr Elena Lazăr, Associate Professor, Public Law Department, University of Bucharest

Key topics

- EU current and future legislative framework on cybercrime, Council of Europe Budapest Convention on Cybercrime
- E-evidence, its admissibility, access to it and handling in court and the defence's role in challenging such evidence

Language
English

Event number
325DT71

Organiser
Ramin Farinpour (ERA)

Co-funded by the European Union

european.law

Computer Crimes

Wednesday, 2 July 2025

14:40 Connecting to the videoconference platform

15:00 **Opening of the webinar**
Ramin Farinpour

I. CURRENT AND FUTURE EUROPEAN AND EU FRAMEWORKS TO COUNTER COMPUTER CRIMES

Chair: Ramin Farinpour

15:05 **Council of Europe cybercrime standards and EU standards on information systems, fraud and non-cash payments**
- Council of Europe Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol
- Directive 2013/40/EU on attacks against information systems
- Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment
- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, EU Cybersecurity Act, EU Cyber Resilience Act and EU cybersecurity certification framework

Elena Lazar

15:45 Discussion

16:00 **EU standards to combat the sexual exploitation of children online, child pornography and violence against women and domestic violence**
- Directive 2011/93/EU on combatting the sexual abuse and sexual exploitation of children and child pornography and its proposed recast
- Regulation (EU) 2024/1307 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse
- Proposal for a Regulation laying down rules to prevent and combat child sexual abuse
- Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) and its provisions on the online protection of minors
- Directive (EU) 2024/1385 on combatting violence against women and domestic violence

Elena Lazar

16:45 Discussion

II. E-EVIDENCE

Chair: Ramin Farinpour

17:00 **Online investigations and the challenges of dealing with electronic evidence in criminal proceedings and in court**
- Principles of dealing with electronic evidence
- Common procedures for recognising and handling evidence on digital devices
- International investigations (search and seizure – obtaining evidence from the internet, admissibility)
- Collection of evidence located abroad and the challenges of cross-border access to data
- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Ciprian Băban

17:45 Discussion

18:00 End of the webinar

For programme updates: **www.era.int**
Programme may be subject to amendment

Apply online for
"Computer Crimes":
www.era.int/?133426&en

Objective

This three-hour long webinar, which forms a part of a larger project on European Criminal Law for Defence Lawyers, focuses on computer crimes and practical matters in applying measures to counter it.

It will explain and take a look at the current and future EU legislative framework, the Council of Europe's Budapest Convention on Cybercrime, and provide an analysis of the various forms of cybercrime. Using e-evidence to counter cybercrime will be explained and, within this context, its admissibility, access to it and handling in court and the defence's role in challenging such evidence. Insights from practitioners familiar with these instruments will be shared.

Who should attend?

Criminal defence lawyers

Interactive online seminar

The online seminar will be hosted on the Zoom videoconference platform. You will be able to interact immediately and directly with our top-level speakers and other participants. We will make the most of the technical tools available to deliver an intensive, interactive experience. The highest security settings will be applied to ensure that you can participate safely in this high-quality online conference.

Your contacts

Ramin Farinpour
Senior Lawyer
E-Mail: rfarinpour@era.int

Venla Gilles
Assistant
E-Mail: vgilles@era.int
Tel.: +49 (0)651 937 37 325

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). Participation in the full programme of this event corresponds to **3 CPD hours**.
A certificate of participation for CPD purposes with indication of the number of training hours completed will be issued on request. CPD certificates must be requested at the latest 14 days after the event.

Times indicated are CEST
(Central European Summer Time)

Computer Crimes

TRAINING FOR DEFENCE LAWYERS
Online, 2 July 2025

Terms and conditions of participation

- No registration fee.
- Participation is only open to lawyers in private practice from eligible EU Member States (Denmark does not participate in the EU Justice Programme) Albania, Bosnia and Herzegovina, Kosovo* and Ukraine.
- A list of participants including each participant's address will be made available to all participants unless ERA receives written objection from the participant no later than one week prior to the beginning of the event.
- The participant will be asked to give permission for their address and other relevant information to be stored in ERA's database in order to provide information about future ERA events, publications and/or other developments in the participant's area of interest.
- A certificate of attendance will be issued after the webinar to all those that participated for the entire event.

* This designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ opinion on the Kosovo declaration of independence.

Apply online for
"Computer Crimes":
www.era.int/?133426&en

Save the date

The scope and application of the EU Charter of Fundamental Rights
Riga, 5-6 June 2025

Instruments of mutual recognition: EAW, EIO
Budapest, 25-26 September 2025

The role of the CJEU for defence lawyers
Trier, 8-10 October 2025

Further information about the European Criminal Law for Defence Lawyers project:

https://training-for-defence.era.int/

Try out our new e-Learning course – for free!

Introduction to EU Criminal Law

This 3-hour e-learning course on EU criminal law is a guide through the fundamental characteristics of EU criminal law and aims to provide insight into what EU criminal law entails and what it does not entail.

Further information:
www.era.int/?131631&en

www.era.int/elearning

COUNCIL OF EUROPE CYBERCRIME STANDARDS AND EU STANDARDS ON INFORMATION SYSTEMS, FRAUD AND NON-CASH PAYMENTS

BY LAZAR ELENA

Co-funded by the European Union

RELEVANT INSTRUMENTS

- Council of Europe Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol
- Directive 2013/40/EU on attacks against information systems
- Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment
- NIS 2 Directive
- EU Cybersecurity act

- Classification-cyber operations generally refer to the employment of cyber capabilities to achieve objectives in and through cyberspace
- MOST COMMON CYBEROPERATIONS methods-Denial of service, logical bomb, Abuse tools, Sniffer, Trojan horse, Virus, Worm, Send spam, and Botnet.
- Types of cyberoperations:
- Cybercrimes
- Cyber attacks
- Cyberwarfare
- cyberterrorism

METHODS USED FOR CYBEROPERATIONS

Method	Description
Denial of Service	A hacker consumes all server resources, so access to the service is not possible for system users.
Man-in-the-Middle	Where a hacker puts himself between the victim device and the router to eavesdrop on or change data packets.
Malware	Malware is a way in which victims come in contact with worms or viruses and their devices become infected.
Phishing	It is a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information.

- Cyber attacks
- A deliberate offensive or malicious action carried out via cyberspace and intended to cause damage (in terms of availability, integrity or confidentiality) to data or the systems that treat them, posing a threat to the national security of state, which may consequently harm the activities for which they are the medium.
- Cyberwarfare
- Any cyberoperation which is carried out in, and in connection with, an armed conflict situation, and constitutes an act of violence, whether offensive or defensive, against another party to the conflict, is an attack within the meaning of Article 49 of AP I to the Geneva Convention
- For example, the destruction of adversary military offensive cyber or conventional capabilities by disruption or the creation of major damage is an attack within the meaning of IHL. The same applies to neutralisation actions which damage adversary cyber or conventional military capabilities by destroying ICT equipment or systems or altering or deleting digital data or flows such as to disable a service essential to the operation of such capabilities

- Cyberterrorism
- Any planned, politically motivated attack on information systems, programs, and data that makes violent threats or actually causes violent acts is commonly referred to as cyber terrorism. Sometimes the phrase is broadened to cover any cyberattack that causes fear or intimidation among the target population. Attackers frequently accomplish this by destroying or impairing vital infrastructure.

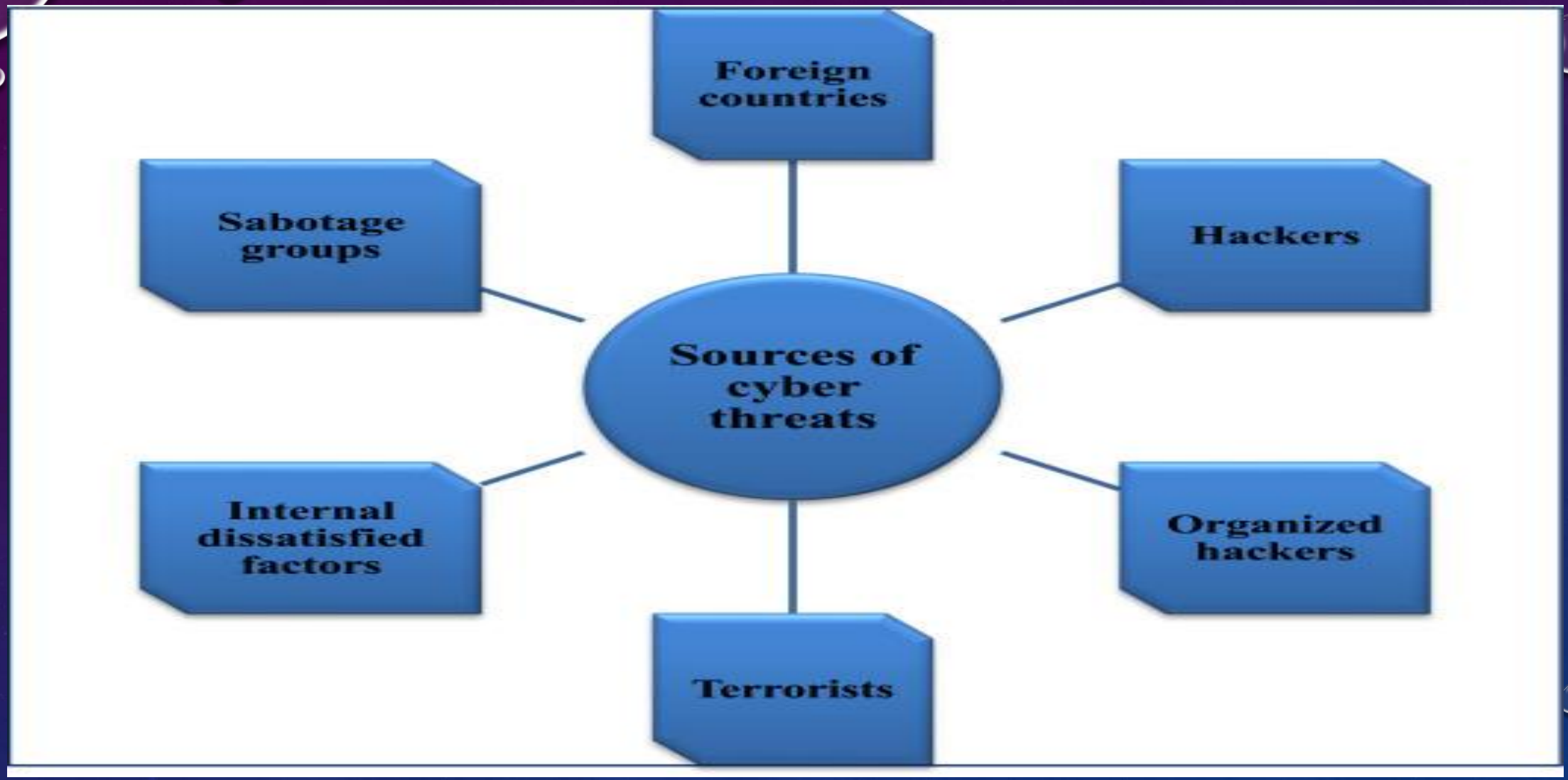
- CYBERCRIME
- -Cyber actions taken by non-governmental attackers, pursuing economical gains

- Europol (2018) differentiates cybercrime into *cyber-dependent* operations (i.e., "any crime that can only be committed using computers, computer networks or other forms of information communication technology;" McGuire and Dowling, 2013, p. 4; Europol, 2018, p. 15) and *cyber-enabled* operations (i.e., traditional crimes facilitated by the Internet and digital technologies). The key distinction between these categories of cybercrime is the role of ICT in the offence - whether it is the target of the offence or part of the *modus operandi* (or M.O.; i.e., method of operation) of the offender (UNODC, 2013, p. 15). When ICT is the target of the offence, this cybercrime negatively affects the *confidentiality*, *integrity* and/or *availability* of computer data or systems (UNODC, 2013).
- "new" cyberoperations (i.e., *cyber-dependent* crimes) are primarily those that target systems, networks, and data, and seek to compromise their *confidentiality* (i.e., systems, networks, and data are protected and only authorized users can access them), *integrity* (i.e., data is accurate and trustworthy and has not been modified) and *availability* (i.e., data, services, and systems are accessible on demand). These cybercrimes include hacking; malware creation, possession, and distribution; denial of service (DoS) attacks; distributed denial of service (DDoS) attacks; and website defacement (i.e., a form of online vandalism targeting the content of websites).

INTERNATIONAL LAW APPLIES TO (AND IN) CYBERSPACE

- With few exceptions (most notably, the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace. Moreover, the technology is both novel and dynamic. Thus, for several years, there were open questions about whether existing international law applied to cyberspace at all. Today, most states and several international organizations, including the UN General Assembly's First Committee on Disarmament and International Security, the G20, the European Union, ASEAN, and the OAS have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states.

- Issues surrounding international law's application to cyberspace may be broken into five discrete categories: (i) silence; (ii) existential disagreements; (iii) interpretative challenges; (iv) attribution; and (v) accountability.
- International law only regulates its subjects of international law (for example, states). It does not usually direct the behavior of ICT companies or individuals (who are usually subject to one or more domestic legal orders). To apply international law in cyberspace, therefore, it is necessary to know the identity of whoever is responsible for the activity in question: is it a state or state-sponsored actor subject to international law or is it an individual(s) engaged in behavior outside international law's ambit? Such identifications are, however, difficult in cyberspace given well-known challenges in technical attribution—identifying the origins of malicious cyber behavior is often difficult and time-consuming.


Foreign countries
Sabotage groups
Hackers
Sources of cyber threats
Internal dissatisfied factors
Organized hackers
Terrorists

CYBERCRIMES

- The Council of Europe Convention on Cybercrime (also known as the Budapest Convention), which was opened for signatures in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime. After 20 years, it still remains the most significant one in the area. Currently, 75 countries are Parties to the Convention on Cybercrime, including 26 EU Member States
- In 2003, the Convention was extended by an Additional Protocol covering offences of racist or xenophobic propaganda. Following the evolution of information and communication technologies, the Second Additional Protocol to the Convention on Cybercrime on enhanced international cooperation and disclosure of evidence was adopted
- In States that have adopted legislation based on the Budapest Convention any investigation making use of such legislative provisions may be attributed to this treaty. However, prosecutions and court decisions will refer to the articles of domestic law and not to the Budapest Convention except for instances where evidence has been obtained through international cooperation provisions.

Substantive criminal law: offences	Procedural law to secure evidence and investigate	International cooperation
Art. 2 – Illegal access Art. 3 – Illegal interception Art. 4 – Data interference Art. 5 – System interference Art. 6 – Misuse of devices Art. 7 – Computer-related forgery Art. 8 – Computer-related fraud Art. 9 – Child pornography Art. 10 – IPR offences Art. 11 – Attempt, aiding, abetting Art. 12 – Corporate liability	Art. 14 – Scope of procedural provisions Art. 15 – Conditions and safeguards Art. 16 – Expedited preservation Art. 17 – Expedited preservation and partial disclosure of traffic data Art. 18 – Production order Art. 19 – Search and seizure Art. 20 – Real-time collection traffic data Art. 21 – Interception of content data	Art. 23 – General principles Art. 24 – Extradition Art. 25 – General rules Art. 26 – Spontaneous information Art. 27 – MLA in absence of treaty Art. 28 – Confidentiality Art. 29 – Expedited preservation Art. 30 – Partial disclosure traffic data Art. 31 – MLA accessing data Art. 32 – Transborder access Art. 33 – MLA collection traffic data Art. 34 – MLA interception content Art. 35 – 24/7 point of contact

The Council of Europe’s Convention on Cybercrime (the ‘Convention’, and its additional Protocol) lists the following as categories of cybercrime offences:

- • Offences against the confidentiality, integrity and availability of computer systems and data (illegal access and interception, data and system interference, and misuse of devices)
- • Computer-related offences (forgery and fraud)
- • Content-related offences (child pornography)
- • Offences related to infringements of copyright and related rights
- • Acts of a racist and xenophobic nature (including threats and insults) committed through computer systems, also including denial, gross minimisation, approval or justification of genocide or crimes against humanity

THE HOW OF THE OFFENSES PROVIDED BY THE CYBERCRIME CONVENTION

- THROUGH MALAWARES FOR EXAMPLE

- A MALAWARE REPRESENTS…..WORMS, VIRUSES AND TROJANS, DDoS
- Eg. Cybercriminals gained unauthorized access to the system of a Lithuanian plastic surgeon and obtained sensitive information about patients from different parts of the world, procedures they undertook, naked photos of the patients, and medical data, among other forms of information. The cybercriminals then threatened each patient with the release of this information if the ransom was not paid. So we have both illegal access to data and interference with data and computer related fraud

- A *distributed denial of service attack* (or DDoS attack) refers to the use of multiple computers and other digital technologies to conduct coordinated attacks with the intention of overwhelming servers and/or intermediaries to prevent legitimate users' access . An example of how one type of DDoS attack works is as follows : Imagine many computers trying to connect to a single computer (the server) all at the same time. The single computer has a limited amount of processing power and network bandwidth. If too many computers try to connect at the same time, the server cannot respond to each connection quickly enough. The result is that the server may not be able to respond to *real* users because it is too busy with *fake* requests-in this case we have system interference
- DDoS attacks can be conducted by an individual, group, or state. States can target critical infrastructures, which are deemed essential to the functioning of society. For example, Country A experienced a series of DDoS attacks perpetrated by Country B on its financial sector. As a result of these cyberattacks, citizens of Country A were unable to access online banking, and ATMs within this country were intermittently working.s

Relevant Articles	Examples
Artide 2 – Illegal access	Malware can be used to access computer systems.
Artide 3 – Illegal interception	Malware can be used to intercept non-public transmissions of computer data to, from, or within a computer system.
Artide 4 – Data interference	Malware damages, deletes, deteriorates, alters or suppresses computer data.
Artide 5 – System interference	Malware may hinder the functioning of a computer system.
Artide 6 – Misuse of devices.	Malware is a device as defined in Article 6 (parties that take reservations to Article 6 must still criminalize the sale, distribution or making available of covered devices). This is because it will normally be designed or adapted primarily to commit the offences established by Artides 2 through 5. In addition, the article criminalizes the sale, procurement for use, import, distribution or other making available of computer passwords, access codes, or similar data by which computer systems may be accessed. These elements are frequently present in malware prosecutions.
Artide 7 – Computer-related forgery.	Malware may input, alter, delete, or suppress computer data with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Artide 8 – Computer-related fraud.	Malware may cause one person to lose property and cause another person to obtain an economic benefit by inputting, altering, deleting, or suppressing computer data and/or interfering with the function of a computer system.
Artide 11 – Attempt, aiding and abetting	Malware may be used to attempt or to aid or abet several crimes specified in the treaty.
Artide 13 – Sanctions	The effects of new forms of malware vary widely. Some malware is relatively trivial; other malware is dangerous to people, to critical infrastructures, or in other ways. The effects may differ in different countries for technical, cultural or other reasons. A Party may foresee in its domestic law a sanction that is unsuitably lenient for malware attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Artide 13, that criminal offences related to such attacks "are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty". For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions.

DIRECTIVE 2013/40 - ATTACKS AGAINST INFORMATION SYSTEMS

- This directive introduces new rules harmonising criminalisation and penalties for a number of offences directed against information systems. These rules include outlawing the use of so-called botnets -- malicious software designed to take remote control of a network of computers. It also calls for EU countries to use the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology.
- The main types of criminal offences covered by this directive are attacks against information systems, ranging from denial of service attacks designed to bring down a server to interception of data and botnet attacks.

The second half of the 2000s marked a decisive change of pace in the EU fight against cybercrime. After the Estonian cyber attack in April-May 2007, the European Union started focussing on issues such as ‘large scale cyber attacks’ and ‘botnets’. The objectives of the Directive are to approximate the criminal law of the Member States in the area of attacks against information systems and to improve cooperation between competent authorities.

Variations in national criminal law and procedure may give rise to differences in investigation and prosecution, leading to differences in how these crimes are dealt with. Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools (‘malware’ and ‘botnets’), while offering offenders anonymity and dispersing responsibility across jurisdictions.”

As compared to the previous Framework Directive, the Directive includes the penalisation of illegal access, illegal system interference, and illegal data interference, and introduces the following elements:

- penalisation of the use of tools (such as malicious software, e.g. botnets, or unrightfully obtained computer passwords) for committing the offences Introduction of ‘illegal interception’ of information systems as a criminal offence
- Improvement of European criminal justice/police cooperation by strengthening the existing structure of 24/7 contact

The present directive requires the approximation of criminal law systems between EU countries and the enhancement of cooperation between judicial authorities concerning:

- illegal access to information systems
- illegal system interference
- illegal data interference
- illegal interception.

In all cases, the criminal act must be committed intentionally.

Instigating, aiding, abetting and attempting to commit any of the above offences will also be liable to punishment.

The Directive goes further than the Convention, which allowed some margin of discretion to Member States just like the Framework Decision. In fact, the Convention not only allows States to exclude offences not committed by infringing security measures or are unrelated to a computer system that is connected to another computer system, but also permits them to narrow criminal liability through the introduction of subjective elements, such as requiring ‘dishonest intent’.

- The first category of offence, stipulated by Article 3 of the Directive, refers to illegal access to information systems. This category of offence comprises a series of computer attacks, also known in the literature as hacking. The offence consists in committing intentionally the access without right to the whole or to any part of an information system, by infringing a security measure. The offence of illegal access to information systems must not be a minor case
- For illegal system interference, the most known attack against an information system affecting the information system interference is Denial of Service-DOS- attack. In this form of attack, the offender tries to deny to authorized users the access to specific information, information systems and the network itself. DOS attack is in fact an attempt of the offender to make information resources unavailable for legitimate users. The purpose of such attack may be simply the prevention of access to target information system or the attack may be used with other actions in order to obtain unauthorized access to an information system or computer network.
- The third type of offence refers to illegal data interference. Thus, the offence of illegal data interference stipulated by Article 5 of the Directive consists in deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible. Article 4 of the Directive comprises the offence of illegal system interference, by manipulation of computer data on the information system. On the other hand, the provisions of article 5 refer to computer attack having as target only the computer data.

- The fourth category of offence refers to illegal interception. Article 6 of the Directive contains the provisions relating to illegal interception, consisting in intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data. The activity of interception by technical means, requires listening, supervising of the content of communications, procurement of computer data either directly, by accessing and using the information system, or indirectly, by using some listening and/or recording electronic devices. The technical means are devices fixed on communication lines or devices designed to collect and record wireless communications
- Article 7 of the Directive refers to tools used for committing offences mentioned at articles 3 to 6. Thus, according to Article 7 of the Directive, the Member States are required to adopt the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence

To fight cybercrime better, the directive calls for greater international cooperation between judicial and law enforcement authorities. To this end, EU countries must:

- have an operational national point of contact,
- use the existing network of 24/7 contact points ,
- respond to urgent requests for help within 8 hours to indicate whether and when a response may be provided,
- collect statistical data on cybercrime.

WHAT IS AN INFORMATION SYSTEM?

the definition provided in Directive 2013/40/EU refers to ‘computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance’.

- Elements of IS

The existence of a device or a group of interconnected or functionally related devices. This narrows the definition only to physical entities, such as electronic equipment– e.g. laptops, PCs, smartphones, etc. Considering this criterion, a virtual machine (VM) does not qualify as an information system; it is instead software that emulates an information system within a physical one. Likewise, an operating system (OS), whether it is Windows, iOS, Android, or another, is not an information system in itself but a computer program that manages different functions and re sources, within an information system. We argue that a network (e.g. the Internet or a Wi-Fi network) does not constitute an information system, even if it operates by using them. Thus, a router is an information system, but the Wi-Fi network provided by the router has an intangible nature and is incompatible with the definition of an information system.

- ii. The capability of performing automatic processing of data. It is important to emphasise that not all electronic equipment qualifies as an information system. For a device to be considered an information system, it must be able to process data automatically. This criterion is necessary to be able to distinguish between information systems and computer data storage mediums. In this context, we argue that a storage medium could be qualified as an autonomous information system if it has a function for data encryption. Thus, the mere fact that such a physical device can store computer data is not enough to conclude that it is an information system. It is questionable whether a group of interconnected hardware constitutes an in formation system when it lacks the necessary functional components. For instance, a PC lacking a motherboard becomes unusable. If a perpetrator attempts to access a non-functional PC by pressing the start button, it raises questions about the rea sonableness of holding them liable for attempting illegal access to an information system

- iii. The automatic processing of data must be conducted using a computer program. We acknowledge that firmware can play this role, even though this raises the potential risk of broadening the definition and potentially include all electronic devices equipped with firmware– such as electronic toys or IoT devices. However, denying that firmware is capable of processing data automatically according to a com puter program can lead to significant consequences. For instance, if a perpetrator uses a victim's PC that lacks a storage medium and an operating system, some might argue that the remaining interconnected hardware components do not constitute an information system. This argument is both incorrect and dangerous. The perpetrator could access the BIOS (Basic Input/Output System), making changes to the information system that could restrict the victim's access (via a password), or they could boot an operating system (e.g. Kali Linux) from an external storage medium, utilising the RAMtotemporarily store data.

EXAMPLES OF CRIMES

- Using a skimmer device at anATM- It is a common modus operandi for perpetrators to install a skimmer device inside an ATM to copy data from the magnetic strip of electronic payment instruments. In this scenario, the victim unwittingly interacts with the skimmer by inserting their electronic payment instrument into the ATM reader, allowing the perpetrator to copy the necessary data for counterfeiting the electronic payment instrument. It is important to note that in this case, the skimmer device copies data from the magnetic stripe without any logical interaction with the ATM. Similarly, the perpetrator only physically interacts with the ATM to install the skimmer device.
- However, installing a skimmer device, a video camera, or a modified keyboard-type device on an ATM does not constitute access, as it lacks direct interaction with the information system by the perpetrator.

- Accessing an Internet or mobile banking account -We argue that accessing an Internet or Mobile banking account is similar to accessing an ATM by using an electronic payment instrument and is different from using such an instrument to make a payment at a POS terminal. The differentiating element refers to the control gained by the perpetrator over the information system. In the case of making payments at a POS terminal, there is only a transmission of computer data, without the perpetrator gaining control over the functions or resources of an information system (so we would only be talking about theft).
- On the other hand, accessing an Internet banking account gives the perpetrator the ability to exercise a limited control over the functions of an information system– namely, the bank server. Thus, by gaining such access, the perpetrator can carry out various financial operations fraudulently or make various changes to the account, which could either restrict access to it or facilitate future unauthorised access (so in this case we could have illegal access and theft). Additionally, accessing the Internet Banking service may compromise the confidentiality of personal data, including bank balances.

DIRECTIVE (EU) 2019/713 ON COMBATING FRAUD AND COUNTERFEITING OF NON-CASH MEANS OF PAYMENT

- The Directive above all harmonizes the criminal conduct of natural or legal persons in relation to non-cash means of payment. The reform of the Framework Decision was considered particularly necessary in order to update the EU response to new technologies involving payment instruments that are beneficial to business and consumers, on the one hand, but also increasingly benefit criminals, on the other. As a result, the new rules must also be seen in the context of the EU's efforts to provide better cybersecurity.
- Directive 2019/713 includes common definitions in the areas of fraud and the counterfeiting of non-cash means of payment. Criminal liability has now also been extended to virtual currencies (insofar as they can be commonly used to make payments) and digital wallets.

The Directive defines the constituent elements of criminal conducts, which have been categorized as follows:

- fraudulent use of a stolen or forged non-cash payment instrument
- theft, forgery, and unlawful possession or procurement (including sale) of physical forms of payment, such as payment cards (‘corporeal non-cash payment instruments’);
- illegal receipt, forgery and unlawful possession or procurement (including sale) of digital forms of payment, such as mobile payments, electronic wallets and virtual currencies (‘non-corporeal non-cash payment instruments’);
- hacking into information systems or manipulating computer data to transfer illegally a person’s money;
- inciting or aiding and abetting any of the above offences.

The Directive clarifies that incitement, aiding and abetting, and attempt of any of the above-mentioned offences must also be made punishable as a criminal offence

Non-cash payment instrument: protected devices and procedures, physical or virtual, enabling the user to transfer money or monetary value without using coins or notes.

- With the term “corporeal” non-cash payment instruments the Directive aims to cover classical forms of conduct, like fraud, forgery, theft and unlawful appropriation that had in the view of the legislator already been shaped by national law before the era of digitalisation.
- In contrast, the Directive also aims to cover forms of conduct in the digital sphere by also protecting non-corporeal payment instruments. The Directive requires Member States to prohibit various kinds of conduct that have the aim of obtaining control of a non-cash payment instrument as well as to provide for sanctions.

The Directive also includes rules on the following issues:

- Jurisdiction and conflicts of jurisdiction;
- Investigative tools to effectively investigate fraud and the counterfeiting of non-cash means of payments;
- Exchange of information by national points of contact that are available 24/7;
- Establishment of channels that facilitate reporting of the offences described in the Directive;
- Encouragement for financial institutions and other legal persons to report suspected fraud or counterfeiting to law enforcement authorities.

- An example for a non-cash payment instrument is a mobile payment application and a corresponding authorisation (e.g. a password). The Directive only covers instruments which put the holder or user of the instruments in the position to enable a transfer of money or to initiate a payment order. In that respect, unlawfully obtaining a mobile payment application without the necessary authorisation is not an unlawful obtainment of a non-cash payment instrument.
- In addition, the Directive covers fraud in relation to **information systems**, which are defined as devices that, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device for the purposes of its or their operation, use, protection and maintenance.

EXAMPLE OF CRIMES

- Payment cards have a chip inside them that recognises radio waves, if a card holder wishes to pay contactless. It is based on Radio-Frequency Identification technology – known as RFID.

- To pay with a contactless payment card, for example, in a supermarket or in a restaurant, the customer holds their card near to the reader, i.e. RFID reader. Consequently, the reader can communicate with the card's microchip. Further, the reader sends to the card the details regarding transaction, the card sends back the payment details and then the payment processor processes the contactless payment.
- It is easy to misuse RFID chip in payment card. Anyone with a fake RFID scanner, even homemade scanner, can "send" signal. That means that anyone with a scanner can walk down the street and "scan" cards of people without realising it. Of course, PIN technology can reduce such danger, but it is not always working. Many cards using RFID technology have set limits for automatic approvals of payments, for example, up to 20 EUR. Any wireless or contactless technology has the chance to be hacked, including RFID.

NIS 2 DIRECTIVE

- The old NIS directive (Directive 2016/1148) also specified cybersecurity for critical infrastructure, but it did not manage to introduce the same level of cybersecurity across all Member States, resulting in a fragmented approach.
- The new NIS2 introduces a wider array of industries (sectors) that must be compliant, better cooperation between the Member States, new timelines for reporting incidents, more focus on supply chains, the responsibility on the top management of entities, stricter penalties, etc. NIS 2 replaces the old NIS on October 18, 2024.

Why is NIS 2 important?

- NIS 2 is important because it sets very strict cybersecurity requirements for a large number of companies in the European Union – by some estimates, more than 100,000 companies in the European Union will have to become NIS 2 compliant.
- Even though NIS 2 does not apply to as many companies as, e.g., the EU GDPR, it will certainly become a de facto standard for critical infrastructure that other (non-EU) countries will emulate – a very similar scenario has happened already in non-EU countries with privacy regulations that are very similar to the EU GDPR.

WHO DOES NIS2 APPLY TO?

- There are 3 criteria that define which organizations (NIS 2 calls them “essential entities” and “important entities”) must comply with NIS 2:
- 1) Location – if they provide services or carry out activities in any country of the European Union (no matter if they are based in the EU or not); and
- 2) Size – if they have more than 50 employees and have more than 10 million euro in revenue; and
- 3) Industry – if they operate in any of these sectors: Energy, Transport, Banking, Financial market infrastructures, Health, Drinking water, Waste water, Digital infrastructure, ICT service management (business-to-business), Public administration, Space, Postal and courier services, Waste management, Manufacture, production, and distribution of chemicals, Production, processing, and distribution of food, Manufacturing, Digital providers, Research

LOCATION

If the organization provides services or carries out activities in any country in the European Union

WHO DOES NIS 2 APPLY TO?

Three criteria that define which organizations must comply with NIS 2

SIZE

If the organization has more than 50 employees and has more than 10 million euro in revenue

INDUSTRY

If the organization operates in any of the 18 sectors specified by NIS 2

WHAT ARE ESSENTIAL AND IMPORTANT ENTITIES, AND WHAT IS THE DIFFERENCE?

“Essential entities” and “important entities” are what NIS 2 calls companies and other organizations that need to comply with NIS 2. Essential entities are as follows:

- Companies that have more than 250 employees or 50 million euro of revenue and that are in one of the following sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration, or space
- Trust service providers
- DNS service providers
- Public electronic communication networks
- Public administration entities
- Any critical entity according to Critical Entities Resilience (CER) Directive (EU) 2022/2557
- Other entities specified by Member States

Important entities are all other organizations that are not essential entities, but that fall under the 3 criteria mentioned PREVIOUSLY

What are the reporting obligations of essential and important entities?

Essential and important entities must send notifications about significant incidents to:

- A computer security incident response team (CSIRT) or competent authority
- Recipients of their services
- Entities need to submit several types of reports to the CSIRT: an early warning, an incident notification, an intermediate report, a final report, and a progress report.

NIS 2 certification- NIS 2 does not require essential and important entities to get certified. However, Member States (or the EU commission) may require those entities to use particular IT products or services that are certified in accordance with the European cybersecurity certification scheme according to the Cybersecurity Act (EU Regulation 2019/881).

WHAT IS THE DIFFERENCE BETWEEN NIS 2 AND DORA?

	NIS 2	DORA
Type	Directive (companies comply with local legislation that is published)	Regulation (directly applicable to financial institutions)
Applies to	Organizations that are considered essential and important entities	Financial institutions
Protection	Emphasis on cybersecurity measures	Besides cybersecurity measures, the emphasis is also on overall resilience of financial institutions
Effective from	October 18, 2024	January 17, 2025

CYBERSECURITY ACT AND CERTIFICATION SCHEMES

What is the EU Cybersecurity Act?

The EU Cybersecurity Act is a landmark legislation adopted in 2019 due to the increasing landscape of global cyber threats and the need for consistent cybersecurity standards across the Union.

Key Objectives of the EU Cybersecurity Act- The EU Cybersecurity Act is broken down into two main objectives:

- Strengthen the mandate of the European Union Agency for Cybersecurity (ENISA).
- Establish a common cybersecurity certification framework for ICT products, services, and processes.

The problem is that we live in the EU and have a single European market, and the same rules must apply to all market participants. So one country cannot simply introduce a mandatory cybersecurity certificate on its own.

That is why there is the Cybersecurity Act (EU 2019/881). Among other things, it regulates how uniform European cybersecurity certificates can be issued. The Cybersecurity Act is not to be confused with the Cyber Resilience Act (EU 2024/2847), which defines mandatory security requirements and a CE mark for products with digital elements.

- The second objective of the EU Cybersecurity Act establishes a cybersecurity certification framework for Information and Communication Technology (ICT) products and services. Because of the unique nature of the European Union, providing a consistent framework for ICT products, services, and processes helps member states maintain cohesive cybersecurity measures. Once a product or service passes this conformity assessment in one EU country, it will be recognized across all member states.
- The cybersecurity framework provides European cybersecurity certification schemes, which include rules, technical requirements, standards, and procedures to evaluate the security properties of an ICT-based product or service throughout its lifecycle. Each European scheme must specify the following:

- Category of Product or Services Covered
- Cybersecurity Requirements
- Type of Evaluation (Self-Assessment or Third Party)
- Intended Level of Assurance

Levels of Assurance- Within the cybersecurity framework, levels of assurance are used to help inform users of the cybersecurity risk of an ICT product or service. The three levels of assurance are:

- **Basic:** Poses a low cybersecurity risk. A self-assessment by the manufacturer or service provider is usually sufficient for this level.
- **Substantial:** Poses a significant cybersecurity risk where protection measures against known attack scenarios are needed. Requires a comprehensive evaluation by a third party.
- **High:** Poses a high cybersecurity risk with scenarios where the impact of an attack could be severe. Rigorous evaluation and testing by a third party are mandated for this level.

So, the Cybersecurity Act describes how and from whom products in the EU can obtain an EU-wide cybersecurity certificate.In this context, you need to know an important term: The assurance level. It indicates how thoroughly the product has been tested!!

The idea is that the higher the assurance level, the greater the certainty that the product can withstand cyber attackers with high capabilities and resources. If this sounds familiar, the same idea is behind the “security level” of ISA/IEC 62443.

- At a low assurance level, only technical documentation is checked and, depending on the certification scheme, a self-assessment is sufficient.
- At medium and high levels, an external assessment must be carried out, the product must be tested for vulnerabilities and the correct implementation of security functions must be checked.
- For the high level, a penetration test simulating a competent attacker must also be carried out, and the security functions must correspond to the latest state of the art. The certification authorities must also meet special requirements before they can award this level of assurance.

European Cybersecurity Certification Group (ECCG)

- The European Cybersecurity Certification Group (ECCG) was established under the EU Cybersecurity Act to assist the Commission in developing and implementing the new cybersecurity certification framework. The ECCG comprises representatives from each EU member state, and together, the group acts as a bridge between member states and the European Commission while also acting as an assessment body for the certification frameworks.
- The EU Cybersecurity Act also requires every EU member state to identify at least one National Cybersecurity Certification Authority (NCCA) in their country, which may also contribute to the ECCG.

WHO MUST COMPLY WITH THE EU CYBERSECURITY ACT?

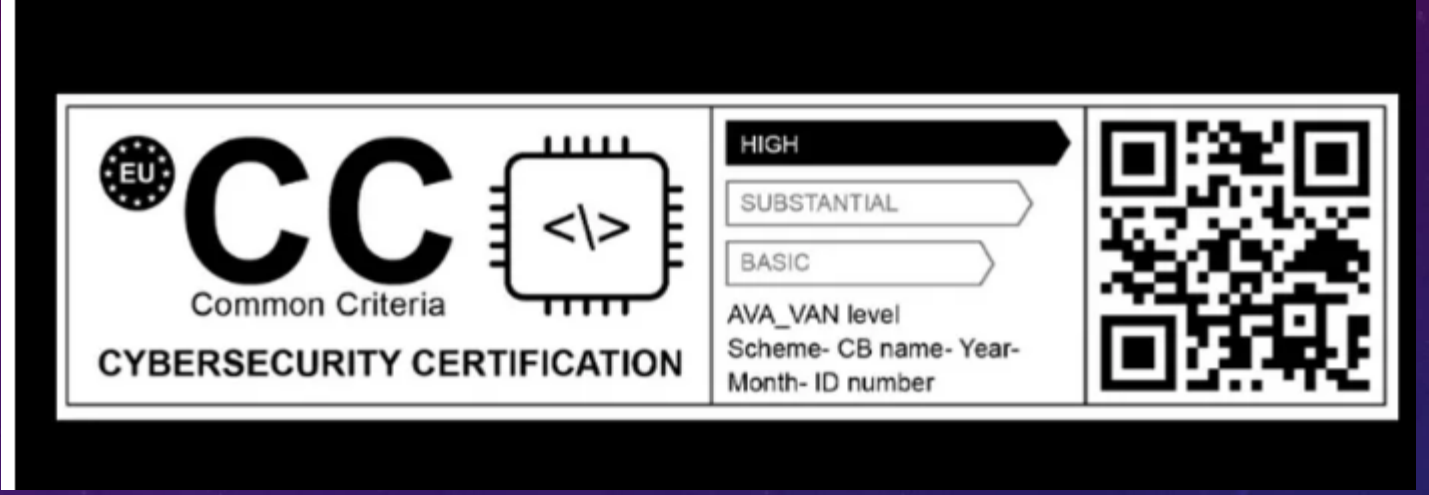
- The certification framework focuses on Information and Communication Technology (ICT) products, especially its certification framework services and processes. Unlike other cybersecurity regulations, compliance with the certification framework is not mandatory, and organizations are not forced to certify their ICT products, services, or processes. Mandatory requirements may be introduced in the future, with possible penalties for infringements.
- Parties encouraged to comply with the EU Cybersecurity Act include the following:

- **Manufacturers and Developers:** Any business that creates ICT products and services for the European market or imports into the EU.
- **Service Providers**: Providers of ICT digital services, including online marketplaces, cloud computing services, and search engines.
- **Critical Infrastructure Operators:** Entities that operate essential services (energy, transport, banking, health) if they use ICT products or services. While the EU Cybersecurity Act does not mandate compliance with the certification framework, other regulations, like the NIS Directive, may encourage them to use certified products or services.
- **Public Sector and Government Agencies:** In specific situations, organizations in the public sector or government may be required to use certified ICT products or services.

CERTIFICATION SCHEME?

- It has been and still is a long way from the Cybersecurity Act to the certificate. This is because a certificate requires a certification scheme — it specifies which requirements products must meet and how these can be checked, conformity assessment bodies that check conformity with these requirements and, for the highest assurance level, certification bodies that issue the certificate.
- **The first certification scheme, which was published as an implementing regulation (2024/482) for the Cybersecurity Act, has been in force since February 27,** 2025. It is based on Common Criteria, a catalog of criteria and procedures for cybersecurity certification internationally standardized as ISO/IEC 15408 and therefore called “EUCC” for short — EU Cybersecurity Certification Scheme on Common Criteria.
- Under the EUCC, there are only the assurance levels “medium” and “high”, and self-assessment is not possible. Manufacturers must therefore undergo an assessment by an external conformity assessment body and a certification body for the “high” level.

CERTIFICATION SCHEME

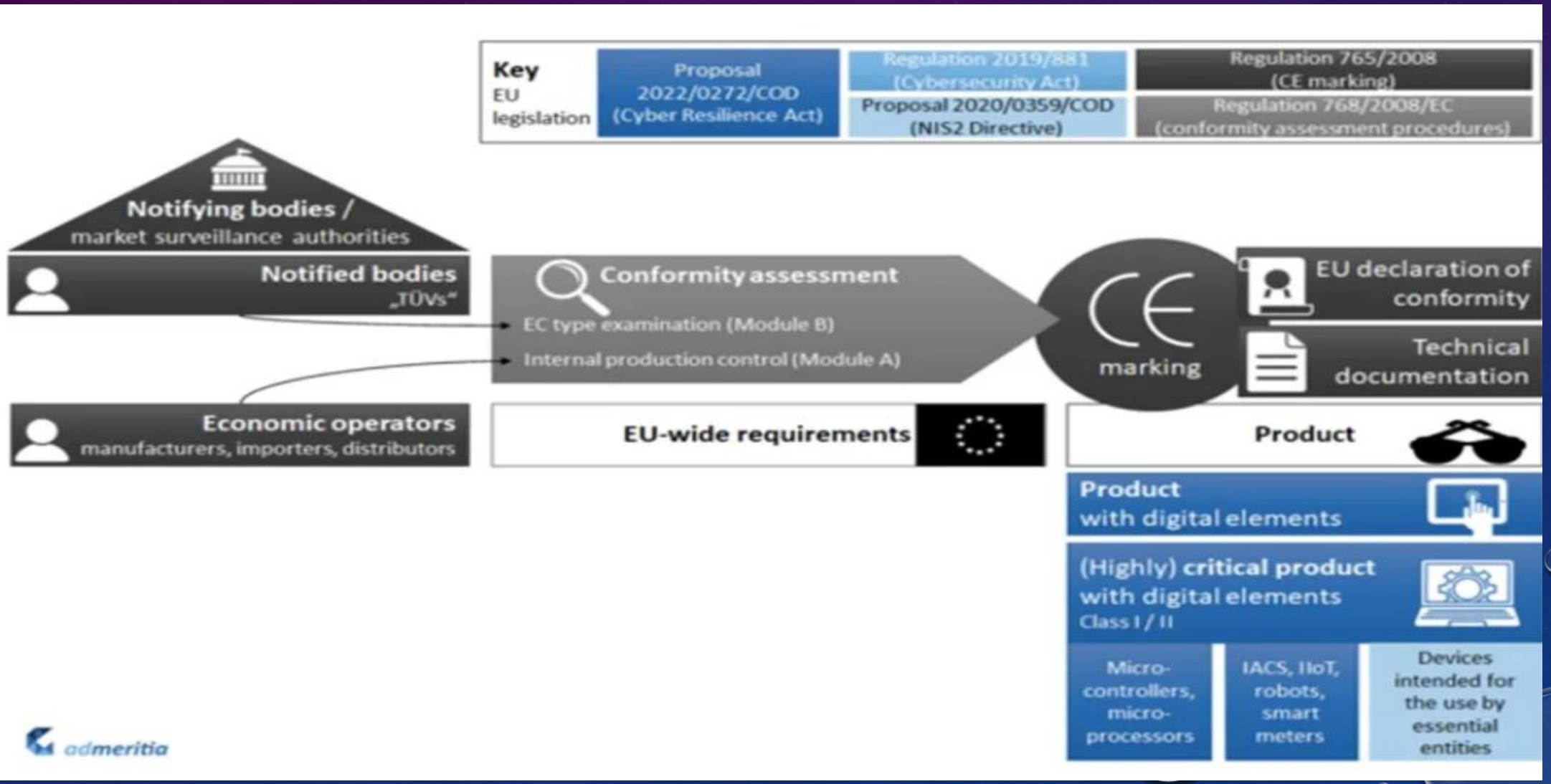


The EU Cybersecurity Certification Scheme on Common Criteria (EUCC)

- The first scheme adopted under the Cybersecurity Act certification framework is based on the renowned international standard Common Criteria, used to issuing certificates in Europe for almost 30 years now. The scheme takes advantage of the high reputation of European vendors and certifiers using the Common Criteria-based certification across the world.
- The scheme will apply EU-wide, on a voluntary-basis, and focuses on certifying the cybersecurity of ICT products in their lifecycle, including:

- Biometric systems
- Firewalls (both hardware and software)
- Detection and response platforms
- Routers
- Switches
- Specialised software (such as SIEM and IDS/IDP systems)
- Data diodes
- Operating systems (including for mobile devices)
- Encrypted storages
- Databases
- Smart cards and secure elements included in all sorts of products, such as in passports daily used by all citizens.

HOW DOES IT WORK?



CYBERSECURITY ACT VS CYBER RESILIENCE ACT?

- The **Cybersecurity Act** is needed to enable a standardized EU-wide certificate with a standardized external audit.
- And the **Cyber Resilience Act** is needed to make such a certificate mandatory for certain products.

A Cybersecurity Certificate in accordance with the Cybersecurity Act is one way to comply with the Cyber Resilience Act.

For most products with digital elements that fall under the CRA, this is not relevant as the manufacturer's self-declaration is sufficient. But for "important" or "critical" products in Annex 3 or 4 of the CRA, a conformity assessment with an external assessment is mandatory. And one possibility for such an external conformity assessment is the certificate.

EU STANDARDS TO COMBAT THE SEXUAL EXPLOITATION OF CHILDREN ONLINE, CHILD PORNOGRAPHY AND VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE

BY LAZAR ELENA

Co-funded by the European Union

DIRECTIVE 2011/93/EU

- The Directive covers prosecuting offenders, protecting victims and preventing offences as well as blocking and taking down websites that hold and distribute child sexual abuse material. The Commission is working closely with EU Member States to make sure that the directive is implemented fully.
- When implementing Directive 2011/93/EU, Member States are bound to respect the rights enshrined in the Charter of Fundamental Right of the European Union. Respect of the Charter includes that penalties imposed upon persons may not be disproportionate to the criminal offence of which they are convicted.

WHAT IS THE AIM OF THE DIRECTIVE

It aims at improving the protection of children from sexual abuse and exploitation. To achieve this, it obliges EU countries to:

- adopt prevention measures;
- protect child victims;
- investigate and prosecute offenders.

DEFINITIONS

- (a) 'child' means any person below the age of 18 years;
- (b) 'age of sexual consent' means the age below which, in accordance with national law, it is prohibited to engage in sexual activities with a child;
- (c) 'child pornography' means:
- (i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;
- (ii) any depiction of the sexual organs of a child for primarily sexual purposes;
- (iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or
- (iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes

INCRIMINATED OFFENSES

- The directive indeed criminalises the act of engaging in sexual activities with a child who has not reached the age of sexual consent, as well as the act of coercing, forcing or threatening a child into sexual activities with a third party (Article 3). Article 4 covers offences concerning sexual exploitation, while Article 5 is dedicated to offences related to child sexual abuse content and material. Article 6 explicitly criminalises the solicitation of children online for the purpose of sexual abuse and exploitation (often referred to as 'online grooming'). The directive also envisages aggravating circumstances (Article 9), including: offences committed against a child in a particularly vulnerable situation; offences committed by a member of the child's family, a person cohabiting with the child, or a person who has abused a recognised position of trust or authority; or offences committed by several persons acting together

Offences and sanctions	• About twenty criminal offences identified divided into four categories: sexual abuse, sexual exploitation, child pornography and the solicitation of children online for sexual purposes • Thresholds for maximum terms of imprisonment • Incitement to commit an offence also punishable and a legal person may be held liable and sanctioned • Aggravating circumstances are provided for (such as the abuse of a vulnerable child, when the abuse is committed by a member of the child's family or where the offender holds prior convictions of the same nature
Professional activities involving contact with children	• Employers exercising employment involving direct and regular contact with children must be able to request information on the existence of a conviction or a disqualification from exercising this type of employment. This information must also be sent to other Member States

- The directive provides that Member States are required to take ‘appropriate measures, such as education and training, to discourage and reduce the demand that fosters all forms of sexual exploitation of children’, as well as ‘appropriate action, including through the internet, such as information and awareness-raising campaigns, research and education programmes, where appropriate, in cooperation with relevant civil society organisations and other stakeholders, aimed at raising awareness and reducing the risk of children, becoming victims of sexual abuse or exploitation’ (Article 23). The directive also aims at adopting measures against advertising abuse opportunities and child sex tourism (Article 21).
- Sex offender registries- In Recital 43, the Child Sexual Abuse Directive provides that ‘Member States may consider adopting additional administrative measures in relation to perpetrators, such as the registration in sex offender registers of persons convicted of offences referred to in this directive. Access to those registers should be subject to limitation in accordance with national constitutional principles and applicable data protection standards, for instance by limiting access to the judiciary and/or law enforcement authorities’.

INTERNET AND CHILD ABUSE

The Internet has brought about a dramatic increase in child sexual abuse in that:

- it facilitates the sharing of child sexual abuse material, by offering a variety of distribution channels such as the web, peer-to-peer networks, social media, bulletin boards, newsgroups, Internet relay chats and photo-sharing platforms, among many others. Sharing is also facilitated by access to a worldwide community of like-minded individuals, which is a source of strong demand and mutual support;
- it provides technical means and security measures that can facilitate anonymity;
- as a consequence of the strong demand for child sexual abuse material, children continue to be at risk of becoming victims, while anonymity can obstruct the investigation and prosecution of these crimes; and
- new child sexual abuse materials have become a currency. To obtain and maintain access to forums, participants frequently have to submit new materials on a regular basis, which encourages the commission of child sexual abuse.

Objectives and scope of Article 25

- The main objective of Article 25 of the Directive is to disrupt the availability of child pornography. Such provisions were first introduced with the Directive, as they were not included in the main legislative instruments in the area, i.e.:
- the Framework Decision that the Directive replaces;
- the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, from which the Directive draws inspiration in other areas; or
- the Council Decision to combat child pornography on the Internet, which was one of the first legal instruments at EU level that addressed child pornography.

Article 25 is one of a number of provisions in the Directive to facilitate prevention and mitigate secondary victimisation. Together with provisions on the prosecution of crimes and protection of victims, they are part of the holistic approach required to tackle child sexual abuse, child sexual exploitation and child pornography effectively.

- Article 25 reads as follows:
- *1. Member States shall take the necessary measures to **ensure the prompt removal** of web pages containing or disseminating child pornography hosted in their territory and to **endeavour** to obtain the removal of such pages hosted outside of their territory.*
- *2. Member States may take measures to **block access** to web pages containing or disseminating child pornography towards the Internet users within their territory. These measures must be set by transparent procedures and provide adequate **safeguards**, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress* See also recitals 46 and 47 of the Directive concerning the measures referred to in Article 25.

- It therefore:
  - obliges Member States to **remove** promptly material on websites hosted within their territory;
  - obliges them to **endeavour to secure the removal** of material on websites hosted elsewhere; and
  - offers the **possibility** to **block access** to child pornography by users within their territory, subject to a number of **safeguards**.
- It is important to note that Article 25 refers to 'measures', which may not necessarily involve legislation. As recital 47 of the Directive states:
- *"… The measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other. In that context, this Directive is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States…"*

What does this mean/imply in practice? Who bears responsibility?

The parties involved in disrupting the availability of child sexual abuse material online are:

- **information society service providers (ISSPs)**, including providers of access, hosting and online platforms. As criminals abuse the services and the infrastructure they provide, ISSPs are well placed to cooperate in the implementation of Article 25. For example, hosting providers are ultimately able to remove material hosted on their servers and access providers such as internet service providers (ISPs) can block access;
- **Internet users**, who may come across child sexual abuse material online (intentionally or unintentionally) and decide to report it to the ISSP directly if the technology to do so is in place, e.g. through a 'report abuse' button on the web page or browser. Users may also report to a dedicated hotline run by a civil society organisation, or to the LEA responsible;
- **dedicated hotlines**, usually run by an NGO or an association of ISSPs or media companies, which allow anonymous reporting by users who may not feel comfortable reporting to the police and cannot or do not wish to report to the ISSP directly. In many cases, reports received in one country refer to material hosted by providers in another. Its removal requires international cooperation, which INHOPE facilitates;
- **LEAs**, whose work is supported by reports passed on by hotlines and directly from Internet users. They also share reports with each other in Europe (directly and through Europol and its European Cybercrime Centre) and beyond (through Interpol); and
- the **judiciary**, which ensures application of the law in each Member State. In some countries, court orders are needed to remove or block material. Eurojust helps coordinate judicial cooperation in criminal matters across Member States.

- Member States have adopted two types of measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in a Member State's territory: measures based on Directive 2000/31/EC (E-commerce Directive), and measures based on national criminal law.

1. Measures based on the E-commerce Directive (and DSA)

- The E-commerce Directive defines the liability limitations of an Internet intermediary providing services consisting of mere conduit, caching and hosting (articles 12-15)

Under the 'mere conduit' exemption, ISS providers are not liable for the information transmitted of their communication network, if the provider:

- Does not initiate the transmission;
- Does not select the receiver of the transmission; and
- Does not select or modify the information contained in the transmission.

The 'caching' exemption exempts an ISS provider from liability for the automatic, intermediate and temporary storage of information provided by a recipient of the ISS, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request, if the provider:

- Does not modify the information transmitted;
- Complies with conditions on access to the information;
- Act expeditiously to remove or disable access to the information it has stored upon obtaining knowledge of the fact that a court has ordered the removal or disablement of the information.

Finally, under the 'hosting' exemption, an ISS provider is exempt from liability for the information it stores at the request of the recipient of the service, if it:

- Does not have actual knowledge of illegal activity or information; The Recitals clarify that this implies that the ISS provider plays a merely technical and passive role with regard to the hosted information. Under Art. 14 ECD, a platform operator is not liable for information stored at the request of a user, subject to the satisfaction of two alternative conditions. First, if “the provider does not have actual knowledge of illegal activity or illegal content”. Second, if “the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the illegal content”. According to well established case law of the European Court of Justice, the applicability of these safe harbor provisions depends on whether the intermediary has played a “neutral role” or an “active role”.
- Acts expeditiously upon obtaining such knowledge to remove or to disable access to the information.
- In addition to these three exemptions, the e-Commerce Directive specifies that Member States are not allowed to impose a general obligation on ISS providers to monitor or actively seek for illegal activity.

2. Measures based on national criminal law

- Member States have notified two types of criminal law provisions which also allow the removal of illegal content hosted in their territory:
- general provisions that allow the seizure of material relevant to criminal proceedings, e.g. material used in the commission of an offence: **AT, CZ, HU, IT, LU, NL, SE** and **SK**; and
- specific provisions on the removal of child pornography: **CY, EE, EL, ES, SE**, and **UK (Gibraltar)**.

DID YOU KNOW?

- What is Top-level domain hopping?

"Top-level domain hopping" is when a site (e.g. 'badsite.ru') keeps its second-level domain name ('badsite') but changes its top-level domain ('.ru'), creating a whole new website with different hosting details but retaining its 'name brand'. So from 'badsite.ru', the additional sites 'badsite.ga', 'badsite.ml' or 'badsite.tk' could be created. This allows instances of a website to persist online after the original has been taken down while keeping the website recognisable and easy to find.

- What are commercial disguised websites?

child sexual abuse websites which display child sexual abuse imagery only when accessed by a 'digital pathway' of links from other websites. When the pathway is not followed, or the website is accessed directly through a browser, legal content is displayed. This means it is more difficult to locate and investigate the criminal imagery. This trend for concealing the distribution of criminal imagery has increased since 2021. some image host sites requiring a 'digital pathway' for the first time - meaning a particular route had to be taken to access a single image of child sexual abuse. These images would have appeared as blank webpages without following the necessary pathway.

CSAM –ONLINE DANGERS

Text-to-video CSAM

- Perpetrators watch the latest advancements with interest. On a dark web forum, AI CSAM perpetrators discuss AI-generated videos:
- "*How long until we can use this new Sora software to make whatever video we want? I want to put my sister's photos in from when she was a kid and make her do nasty things*"
- *"Am seeing the video trailers that were generated by AI, and my mind is blown… The ability to create any child porn we desire… our wildest fantasies… in high definition.*

- Some deepfake CSAM videos shared in dark web forums take an adult pornography video and add a child's face. Others take existing CSAM videos and add a different child's face to them. Because the original videos are of real children, and have, therefore, real child anatomical proportions, they can be especially convincing. One impressed forum user says:
- *"I knew about deepfakes… This is so on point! The colours, the shadings, no glitch. Truly mind blowing."*

PROPOSALS FOR A RECAST OF THE DIRECTIVE AND FOR A REGULATION

Proposal for a Regulation to prevent and combat child sexual abuse

On 11 May 2022, the Commission proposed a Regulation on preventing and combatting the sexual abuse and sexual exploitation of children to require online services providers to detect and report child sexual abuse material and grooming. This new legislation aims to help EU countries detect and report child sexual abuse online, prevent it from taking place and support victims of child sexual abuse.

The new rules will safeguard children by establishing:

- mandatory risk assessments
- targeted detection obligations (based on a detection order)
- stronger safeguards concerning detection.
- clear reporting obligations
- effective removal of forbidden content
- lower risks of exposing children to grooming
- solid oversight mechanisms and judicial redress

- The proposed Regulation relies on the Directive for the definition of what is a criminal offence because it constitutes child sexual abuse material and solicitation. The Directive constitutes the criminal law pillar upon which the proposed Regulation stands.
- The two instruments would reinforce each other to jointly provide a more comprehensive response to the crime of child sexual abuse and exploitation, both offline and online

Timeline

29/04/2024	The Council adopts a regulation to prolong a child sexual abuse protection measure
15/02/2024	Council and Parliament agree to prolong an interim measure to combat online child sexual abuse
08/12/2022	Progress report on proposal for a regulation to prevent and combat child sexual abuse
09/06/2022	Conclusions on the rights of the child
01/06/2022	Examination of the proposal for rules to prevent and combat child sexual abuse

Interim Regulation

- On 14 July 2021 the Commission adopted an interim Regulation to allow providers of electronic communications services to continue their voluntary practices to detect child sexual abuse in their systems beyond 21 December 2020. The interim Regulation puts in place a temporary and strictly limited derogation from the application of some provisions of the e-Privacy Directive, with the aim of detecting, reporting and removing child sexual abuse. This legislation, which was initially set to expire on 3 August 2024, has been extended until 3 April 2026, to ensure that there is no legal gap in the voluntary detection of child sexual abuse online until a more permanent solution is put in place.

- The interim Regulation requires providers to communicate to the Commission the names of organisations acting in the public interest to which they report online child sexual abuse. They are also obliged to submit a report on the processing of personal data under this Regulation.

- Regulation (EU) 2021/1232 laid down temporary and strictly limited rules derogating from certain obligations laid down in Directive 2002/58/EC - also known as the *ePrivacy Directive* - with the objective of enabling providers of certain number-independent interpersonal communications services to use specific technologies for the processing of personal and other data to the extent strictly necessary to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services.The Regulation was put in place to provide a temporary solution pending the adoption of a long-term legal framework to tackle child sexual abuse at EU-level.

Recast of Directive 2011/93/EU to strengthen criminal law

- On 6 February 2024, the Commission proposed a recast of Directive EU 2011/93 to strengthen criminal law on child sexual abuse and sexual exploitation. The revised rules expand the definitions of offences, seeking to harmonize these definitions among Member States. For example, these new offences include livestreaming of child sexual abuse and the possession and exchange of paedophile manuals. The proposal introduces higher penalties for the perpetuators of abuse and will set a longer time period during which victims can report the sexual abuse they suffered and seek action against the offender.

To **facilitate the prosecution of offenders**, the directive:

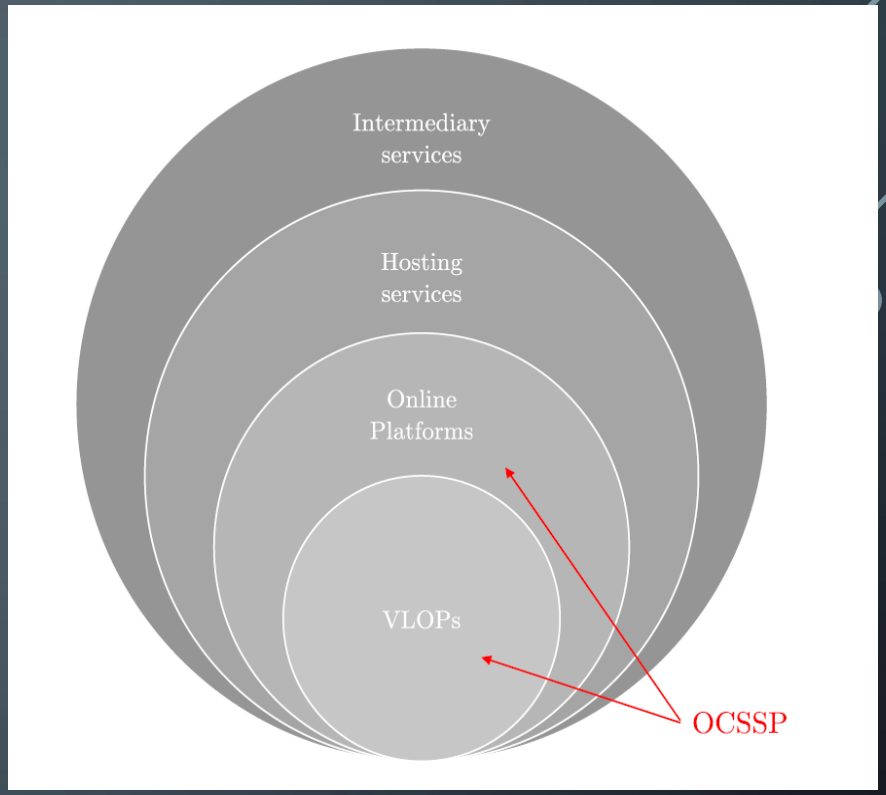
- **criminalises** a wide range of situations of sexual abuse and exploitation (20 offences and attempts);
- **Introduces increased levels of penalties.** Maximum levels set by national legislation must not be lower than levels going from 1 to 10 years of prison, depending on the seriousness of the offence. A number of aggravating circumstances should also be considered;
- **extends the statute of limitation** after the victim has reached adult status;
- **removes confidentiality obstacles** to reporting by professionals whose main duty is to work with children;
- **introduces extraterritorial jurisdiction** for offenders who are nationals, so that they can also be prosecuted in their country for crimes they commit abroad;
- requires that **procedural obstacles** to prosecuting crimes committed abroad **are removed**;
- ensures that **effective investigative tools must be available to the police**, such as those used against organised and serious crime, and special units must be set up to identify victims of child pornography.

DSA ACT

- The Digital Services Act (DSA) is a new set of EU-wide rules for digital services acting as intermediaries for consumers and goods, services, and content. In the context of the DSA, digital services refer to intermediary services such as host providers, online marketplaces, and social media networks.
- The Digital Services Act (DSA) applies to all online intermediaries and platforms in the EU, for example, online marketplaces, social networks, content sharing platforms, app stores, and online travel and accommodation platforms.
- Small and micro-enterprises are exempted from some rules that might be more burdensome for them. The Commission will carefully monitor the effects of the new Regulation on SMEs.
- Very large online platforms and search engines (VLOPs and VLOSEs) have additional obligations.

TO WHOM THE DSA APPLIES

- DSA retains in Article 2(a) the definition of "information society services" of the e-Commerce Directive that underpins the notion of an information society service provider. For the purposes of due diligence obligations, it then proposes a distinction between four categories of services, from the general to increasingly more specific:
- (1) intermediary services; (2) hosting services; (3) online platforms; and (4) VLOPs



- Intermediary services – the broadest category – comprises “mere conduit”, “caching” or hosting services. Hosting services consist of “the storage of information provided by, and at the request of, a recipient of the service”. Online platforms are defined as providers of “a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation”

WHAT ARE VLOP AND VLOSE?

- Very large online platforms and search engines are those whose average users reach or exceed 10% of the EU population. This is equivalent to having 45 million users or more.
- Why is it relevant to know which entities are VLOPs and VLOSEs?- because they have to respect supplementary obligations according to the DSA

OBLIGATIONS UNDER THE DSA | TIERED OBLIGATIONS FOR ISPS AND ONLINE PLATFORMS

The DSA categorizes intermediary services into different tiers or levels based on their size, impact, and responsibilities. The DSA introduces these levels to tailor obligations and requirements to the specific characteristics of each type of service provider. The levels of intermediary services under the DSA include:

Tier 1 - Basic DSA Obligations: Tier 1 includes the basic obligations that apply to all intermediary services, regardless of their size or specific role. Primarily, these obligations ensure transparency and protection of fundamental rights. They include:

- Cooperating with authorities, such as making information available for identification and communication
- Designating and making public a single point of contact for service recipients
- Including information regarding content moderation policies and procedures in the terms of service
- Making comprehensive reports on content moderation activities publicly available at least once a year
- Preserving liability exemptions for intermediary services while clarifying rules and responsibilities based on the nature of their activities

Tier 2 - Additional Obligations for Hosting Services: Tier 2 introduces additional obligations for hosting services, which include services that store and make content available online. These DSA obligations aim to ensure a safer online environment and include:

- Implementing a notice and action mechanism to remove online content in response to user notifications
- Reporting suspicions of criminal offenses involving threats to a person's life or safety to law enforcement

Tier 3 - Additional Obligations for Online Platforms: Tier 3 obligations apply to online platforms. The additional obligations include:

- Providing a complaint handling system and redress mechanisms for users
- Responding preferentially and expeditiously to notices from trusted flaggers regarding illegal content
- Increasing transparency in recommendation algorithms by ensuring users have a choice not to receive recommendations based on profiling
- Prohibiting the use of dark patterns in online interfaces to manipulate or deceive users
- Enhancing transparency in advertising presentation and prohibiting targeted advertising to minors based on sensitive category data

- **Obligations for online platform providers**

The DSA clarifies that services limited to **closed groups, specific user groups and micro or small enterprises will not be considered online platforms**. In addition to the obligations set out in the previous sections, in accordance with the DSA, online platforms will have obligations relating to:

- **Internal complaint resolution system**
- **Alternative dispute resolution**
- **Trusted flaggers**
- **Measures and protection against misuse**
- **Transparency reports**
- **Designing and organizing online interfaces**
- **Online advertising**
- **Cooperation on orders**
- **Protecting minors online**

- VLOPs and VLOSEs due to their size and the potential impact they can have on society must identify, analyse, and assess systemic risks that are linked to their services. They should look, in particular, to risks related to:
- illegal content
- fundamental rights, such as freedom of expression, media freedom and pluralism, discrimination, consumer protection and children's rights
- public security and electoral processes
- gender-based violence, public health, protection of minors, and mental and physical wellbeing
- Once the risks are identified and reported to the Commission for oversight, VLOPs and VLOSEs are obliged to put measures in place that mitigate these risks. This could mean adapting the design or functioning of their services or changing their recommender systems. They could also consist of reinforcing the platform internally with more resources to better identify systemic risks.

Those designated as VLOPs or VLOSEs (see art. 34) will also have to:

- establish an internal compliance function that ensures that the risks identified are mitigated
- be audited by an independent auditor at least once a year and adopt measures that respond to the auditor's recommendations
- share their data with the Commission and national authorities so that they can monitor and assess compliance with the DSA
- allow vetted researchers to access platform data when the research contributes to the detection, identification and understanding of systemic risks in the EU
- provide an option in their recommender systems that is not based on user profiling
- have a publicly available repository of advertisements

Article 34(1), VLOPs should also conduct risk assessments that cover the dissemination of illegal content through their services and any actual or foreseeable negative effects on human dignity

- DSA requires platforms to put in place measures to counter the spreading of illegal goods, services or content online, such as mechanisms for users to flag such content and for platforms to cooperate with 'trusted flaggers'. More specifically, recital 87 refers explicitly to providers of very large online platforms (VLOPs) 'used for the dissemination to the public of pornographic content'. Such platforms should meet all their obligations under the DSA with regard to ensuring that victims can effectively exercise their rights to have content representing non-consensual sharing of intimate or manipulated material removed 'through the rapid processing of notices and removal of such content without undue delay'

- As part of its implementation of the DSA, in December 2023 the EU added three porn websites – Pornhub, Stripchat and XVideos – to the list of VLOPs facing increased control under the Act. The designation is the result of Commission investigations concluding that the three services fulfil the threshold of 45 million average monthly users in the EU. However, the three websites are contesting their designation and have sued6 the Commission at the Court of Justice of the EU.
- In addition to the general DSA obligations, these websites have to fulfil additional obligations within four months from their date of designation, including (according to the Commission's website) mitigating the risk of dissemination of illegal content online, such as child sexual abuse material, and content affecting fundamental rights, such as the right to human dignity and private life in case of non-consensual sharing of intimate material online or deep-fake pornography. These measures can include adapting their terms and conditions, interfaces, moderation processes, or algorithms, among other things.

DSA AND CHILDREN ONLINE PROTECTION

- On May 13, 2025, the European Commission issued its draft Guidelines on the protection of minors online under the DSA ("the Guidelines"). The Guidelines aim to support providers of online platforms that are "accessible to minors" with meeting their obligation to ensure "a high level of privacy, safety, and security" for minors under Article 28(1) of the Digital Services Act("DSA").

The Guidelines are addressed to providers of online platforms whose services are “accessible to minors”. Recital 71 DSA clarifies that an online platform can be considered as “accessible to minors” when “*its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors*”.

The Commission considers that platforms may be considered as “accessible to minors” in the following circumstances, among others:

- A platform’s terms and conditions restrict access to minors, but the provider does not implement any effective measures to prevent access;
- The provider already processes users’ personal data for purposes other than age verification, and that data reveals the user’s age; or
- Types of platforms that are known to appeal to minors, offer similar services to those used by minors, or promote their services to minors.

- While the Guidelines are not legally binding, once finalized, they will constitute a “significant and meaningful benchmark”, which the Commission will rely on in the context of its enforcement of the DSA. Nevertheless, the Commission has clarified that implementing the recommended measures, in part or in full, will not automatically amount to a presumption of compliance with Article 28(1) DSA.
- **Risk Review**
- The Commission recommends that providers of platforms accessible to minors (hereinafter, “providers”) carry out a “risk review”. This review aims to assess and determine what measures are most appropriate and proportionate to meet the provider’s obligations under Article 28(1) DSA.

At a minimum, providers should identify and assess the following elements:

- Likelihood of minors accessing their service;
- The risks that the platform may pose to the privacy, safety and security of minors, based on the "5Cs typology of risks" developed by the OECD. The aim is to identify certain types of risks which may infringe minors' rights;
- The measures already implemented to prevent and mitigate these risks, and their potential positive and negative effects on minors' rights;
- Any additional measures identified in the review.
- With regards to providers of "very large online platforms" and "very large online search engines", as defined by the DSA, the Commission clarifies that this risk review should be carried out as part of, and complement, the risk assessment required by Article 34 DSA.

• DIRECTIVE (EU) 2024/1385 ON COMBATING VIOLENCE AGAINST WOMEN AND DOMESTIC

- Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence reflects the EU's commitment to ensuring gender equality (the Gender Equality Strategy 2020-2025) and protecting human rights. The Directive supports the EU and Member States' international commitments to combat and prevent violence against women, such as the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) and the International Labour Organization's Convention concerning the elimination of violence and harassment in the world of work (C190)

FROM WHEN DO THE RULES APPLY?

- The directive has to be transposed into national law by 14 June 2027. The rules contained in the directive should apply from the same date. The new rules will come into force twenty days after their publication in the EU Official Journal, and member states have three years to implement the provisions.

- the document is the first EU legislative act to mention that VAW is rooted in “historically unequal power relations” and that still existing perceptions about the “inferiority of women” need to be eradicated. The directive, hence, emphasises the centrality of understanding VAW as a form of structural discrimination and eliminating harmful gender stereotypes that underlie it.
- Recognising that women politicians, journalists, and human rights defenders constitute a group especially vulnerable to violence is another key development that deserves mentioning. This is all the more important when viewed in combination with the criminalisation of certain acts in cyberspace, as women belonging to this group are often victims of vicious online attacks and harassment because of their political and social views and their support for gender equality or feminist ideas and principles.

INCRIMINATED OFFENSES

- The Directive criminalises the following offences across the EU:
  - **female genital mutilation,**
  - **forced marriage,**
  - **non-consensual sharing of intimate images,**
  - **cyberstalking,**
  - **cyberharassment, and**
  - **cyber incitement to hatred or violence.**

- In addition, other forms of violence, such as intersex genital mutilation and forced sterilisation, were ultimately not criminalised in the Directive. Intersex genital mutilation affects intersex individuals, who are one of the most discriminated groups among the LGBTI population

CYBERTHREATS WHEN IT COMES TO WOMEN

- One of the difficulties in tackling cyber violence against women is the intersection between it and real-life violence, where acts in the digital world lead to physical violence either inspired by or as a continuation of cyber violence.
- Deep-fake technology, which impersonates a person's voice, face, body or actions, has by now attracted most public attention for its abusive potential and has led to legislative action to stop and prevent it. Women are the primary targets of deep-fakes, particularly of 'nudification' – the creation of naked images of individuals without their consent. More than 90 %2 of all deep-fake videos online are pornographic in nature, and their victims are almost exclusively women – often cultural, media and political personalities.
- AI can facilitate identity theft as well as stalking – for example, by impersonating contacts known to the person. It can be a very powerful tool for surveillance of victims' private life in online and offline settings, and can enable tracking through cameras, analysis of digital data (such as email and messages) and predictive location, all dangerous tools in the hands of stalkers

- One key aspect is the requirement for EU countries to criminalise female genital mutilation (Art. 3) and forced marriage (Art. 4). This demonstrates the Directive`s firm stance that these issues are not merely products of cultural distinctions but are rather gender-related crimes.
- Moreover, the Directive places a significant emphasis on addressing cyber-related violence. It considers the non-consensual sharing of intimate or manipulated material as a criminal offence (Art. 5), providing a safety measure to protect women, which also encompasses instances like deepfakes. Additionally, cyber stalking (Art. 6), cyber harassment (Art. 7), and cyberincitement (Art. 8) are recognised as punishable criminal offences. The Directive also addresses issues such as cyber stalking that have previously not been adequately covered in EU legal regulations, thereby filling a legal gap and for the first time criminalising various forms of cyber violence that predominantly target and impact women due to their gender.

- Articles 3 and 4 of the Directive, which expressly mandate that female genital mutilation and forced marriage are criminalized.
- Genital mutilation includes all forms of procedures that deliberately change or cause injury to the female genital organs for non-medical reasons, while forced marriage can generally be defined as the union of two people in marriage without the full, free and informed consent of one or both parties, which is the result of the application of force.

WHAT IS TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE?

- Technology-facilitated gender-based violence refers to any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms.
- While many other terms – such as digital or online violence – are commonly used, "technology-facilitated gender-based violence" better reflects how technology can enable harm, both online and offline.
- Take doxing, for example, which is the act of sharing someone's personal information online. It can lead to real-life consequences such as stalking, threats, and even physical violence. Or consider deepfake abuse, where manipulated images or videos of someone published online can then result in offline reputational damage with lasting and devastating effects on a person's life. These examples show the complexities of technology-facilitated gender-based violence and how its scope can be harder to define, as harm often permeates both online and offline spaces.

Non-consensual sharing of intimate or manipulated material

- Member States shall ensure that the following intentional conduct is punishable as a criminal offence: (a) making accessible to the public, by means of information and communication technologies ('ICT'), images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person; (b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person; (c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act

- Doxing (also spelled doxxing) consists of searching, collecting and publicly sharing personally identifiable information against a target's will. This includes personal details and sensitive data such as home address, photographs, the victim's name or the names of the victim's family members.
- The information shared online can also be used by a large number of perpetrators in campaigns of harassment and threats with significant psy chological consequences. As information usually allows victims to be physically located, doxing can also be a precursor for violence in the physical world
- Methods employed to acquire such information include searching publicly available databases and social media websites as well as hacking and social engineering

Table 1: Non-consensual intimate image abuse: samples of variations in definitions across platforms

Platform	Definitions related to NCII abuse
Reddit	'Rule 3 prohibits sharing intimate or sexually explicit media of a person created or posted without their permission. Intimate media include a depiction of the person in a state of nudity or engaged in any act of sexual conduct, including depictions that may have been AI-generated or faked. Images or video of intimate parts of a person's body, even if the person is clothed or in public, if contextualized in a salacious manner (e.g. "creepshots" or "upskirt" imagery), are also prohibited. The Rule applies to leaked, stolen or privately shared images of an individual where the individual, or their representative, reports that they do not consent to the public sharing of the images. Additionally, images or video of another person posted for the specific purpose of faking explicit content or soliciting "lookalike" pornography (e.g. "deepfakes" or "bubble porn") is also against the Rule' ([22]). The guidance on this point goes on to provide explicit examples of content that violates Rule 3, before providing links to where users can report non-consensual intimate media and where users can find more information and support. The support signposted includes StopNCII and the international resources page of the US-based Cyber Civil Rights Initiative, which provides links to organisations focused on image-based sexual abuse in 10 Member States (Belgium, Denmark, Germany, Ireland, Spain, France, Italy, the Netherlands, Austria, Finland) ([23]).
TikTok	'Image-based sexual abuse is the creation, manufacture, or distribution of nude, partially nude, or sexually explicit content without the consent of the person in the content, for the purpose of sexualizing their body, or portraying them in a sexual manner' ([24]). This definition is accompanied by a link through which users can report content; a link to sexual assault resources, including advice for victims of sexual assault and their friends and family; and links / contact details for specialist local (i.e. country-specific) organisations, including in 11 Member States (e.g. Violences Femmes Info and Solidarité Femmes in France, or NANE Egyesület in Hungary).
Tinder	'Don't post images or private messages from other people unless you've been given consent to do so' ([25]).

Cyber stalking

- Member States shall ensure that the intentional conduct of repeatedly or continuously placing a person under surveillance, without that person's consent or a legal authorisation to do so, by means of ICT, to track or monitor that person's movements and activities, where such conduct is likely to cause serious harm to that person, is punishable as a criminal offence.
- Cyber stalking is a form of stalking perpetrated using electronic or digital means. It is methodical and persistent in nature and involves repeated incidents. It is perpetrated by the same person and undermines the victim's sense of safety. Behaviours include (1) emails, text messages (SMS) or instant messages that are offensive or threaten ing; (2) offensive comments posted on the internet; and (3) intimate photos or videos shared on the internet or by mobile phone (FRA, 2014)
- Abusers may attach global positioning system (GPS) devices to their victims' vehicles, append geo location spyware on their phones and obsessively track their victims' location through social media (check-ins, photos or other updates)

Cyber harassment

- Member States shall ensure that the following intentional conduct is punishable as a criminal offence: (a) repeatedly or continuously engaging in threatening conduct directed at a person, at least where such conduct involves threats to commit criminal offences, by means of ICT, where such conduct is likely to cause that person to seriously fear for their own safety or the safety of dependants; (b) engaging, together with other persons, by means of ICT, in publicly accessible threatening or insulting conduct directed at a person, where such conduct is likely to cause serious psychological harm to that person; (c) the unsolicited sending, by means of ICT, of an image, video or other similar material depicting genitals to a person, where such conduct is likely to cause serious psychological harm to that person;
- Cyber harassment is a persistent and repeated course of conduct targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm
- Can involve requests to the victim for sexual favours or any unwelcome con tent that is regarded as offensive, humili ating, degrading or intimidating. • Can incorporate threats of physical and/ or sexual violence and hate speech or inappropriate, offensive advances on social media platforms or in chat rooms

Cyber incitement to violence or hatred

- 1. Member States shall ensure that intentionally inciting violence or hatred directed against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating, by means of ICT, material containing such incitement is punishable as a criminal offence. 2. For the purposes of paragraph 1, Member States may choose to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting
- Online hate speech targeting women usually involves sexualisation, objectification and body-shaming comments, as well as degrading comments and rape threats, often from members of incel communities
- Often considered a form of cyber harassment, trolling is a deliberate act of luring others into useless circular discussion, with the result of interfering with the positive and useful exchange of ideas in online discussion sites. It involves post ing off-topic material in large quantities, as well as inflammatory, insensitive, aggressive or con fusing messages.

- While cyber bullies are likely to have an existing relationship with victims, perpetrators of trolling are usually anonymous
- Trolling ‘may function to establish an aggressive online area, rejecting new posters and discouraging the advancement of online communities’ .
- Gendertrolling is a term used to refer to gender-based insults, vicious language and rape and death threats by a coordinated group of trolls to humiliate women, particularly those who assert their opinion online

Computer Crimes – Training for Defence Lawyers

ONLINE, 2 JULY 2025

Ciprian Băban – Criminal Defence Attorney

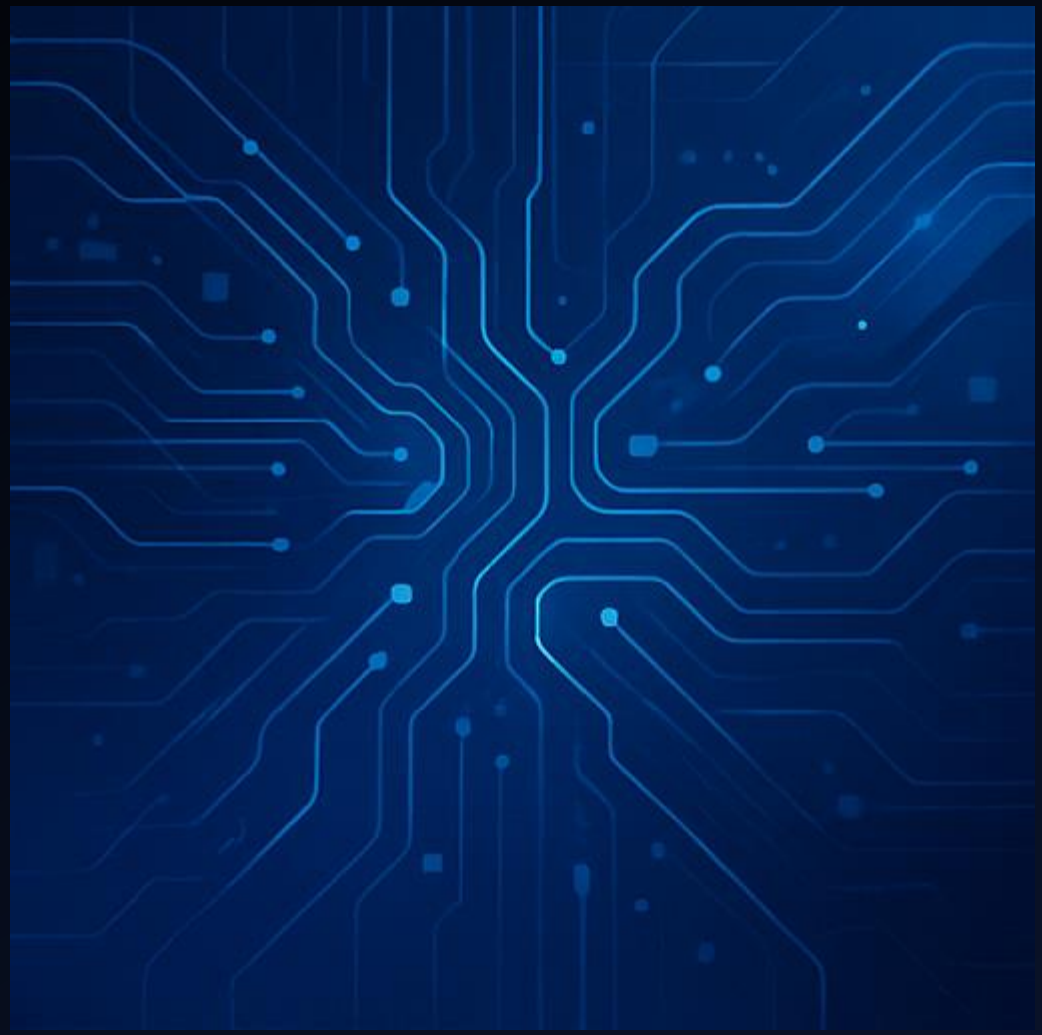
Co-funded by the European Union

Online investigations and the challenges of dealing with electronic evidence in criminal proceedings and in court

“In God we trust; all others must bring data."
W. Edwards Deming

- Principles of dealing with electronic evidence
- Common procedures for recognising and handling evidence on digital devices
- International investigations (search and seizure – obtaining evidence from the internet, admissibility)
- Collection of evidence located abroad and the challenges of cross-border access to data
- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Principles of dealing with electronic evidence



Electronic evidence

- VOLATILE
- FRAGILE
- UBIQUITOS

PRINCIPLES

- ✓ AUTHENTICITY
- ✓ RELIABILITY
- ✓ COMPLETENESS
- ✓ INTEGRITY

PRINCIPLES - extra

- ✓ PROPORTIONALITY
- ✓ MINIMALITY

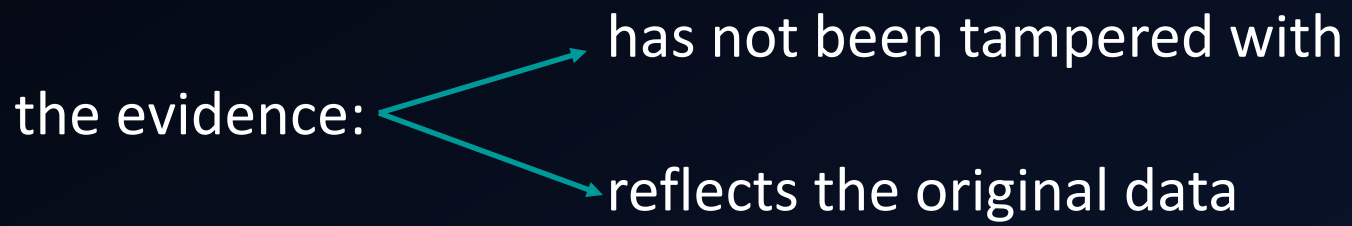
Common Procedures for Recognizing and Handling Evidence on Digital Devices

Phases of Digital Forensics Methodology:

- **Identification** – *where* relevant data is.
- **Preservation/Collection** – clone, bit-by bit, volatile data first.
- **Analysis** – reconstructing state of facts.
- **Documentation** – logs -> who, when, where, what actions, tools description.
- **Reporting/Presentation** – explain methods, conclusion, visual aids

SOPs (standard operating procedures)

- established guidelines for investigations
- Internationally recognised standards (ISO/IEC)



International Investigations: Search and Seizure – Obtaining Evidence from the Internet, Admissibility

SEARCH AND SEIZURE IN A CROSS-BORDER CONTEXT

- **Mutual Legal Assistance Treaties (MLATs)**
- **Direct Cooperation with Service Providers**
- **Emerging Legal Frameworks (Budapest Convention on Cybercrime, e-Evidence Regulation)**

CHALLENGES OF OBTAINING EVIDENCE FROM THE INTERNET

- **Jurisdiction –** 2 or multiple countries
- **Data Localization Laws** – (Germany TGK §113, Russia federal Law 242-FZ, Ukraine Electronic Registers Law - 2017)
- **Privacy Concerns -** GDPR
- **Technical Challenges –** data encryption, anonymization tools, ephemeral online data

ADMISSIBILITY – (STANDARDS OF FORUM COUNTRY)

- **Lawful collection**
- **Chain of custody maintained**
- ***Forensic soundness***
- **Relevance**
- **Human rights and due process**

Collection of Evidence Located Abroad and the Challenges of Cross-Border Access to Data

METHODS OF CROSS-BORDER COLLECTION

- **Mutual Legal Assistance (MLA) –** primary formal mechanisms
- **Direct Access (e.g., CLOUD Act)**
- **Voluntary Disclosure by Service Providers -** emergencies
- **Joint Investigation Teams (JITs) -** EncroChat

CHALLENGES OF CROSS-BORDER ACCESS

- **Sovereignty Conflicts**
- **Differences in Legal Systems and Standards**
- **Data Protection Laws**
- **Technical and Practical Difficulties**
- **Cost and Resources**
- **"Going Dark" Problem**

THE IMPORTANCE OF THE CHAIN OF CUSTODY IN HANDLING EVIDENCE

Unbroken and documented

What is the Chain of Custody?

a chronological, documented history of the electronic evidence from the moment it is collected to its presentation in court

Why is it Critical for Electronic Evidence?

- **Authenticity and Integrity (**precisely what was collected**)**
- **Admissibility -** (broken chain = doubt on integrity)
- **Accountability and Transparency**
- **Preservation of Original State** (analysis on forensic sound copy)

Key Elements of a Strong Chain of Custody

- **Detailed Documentation**

■ Date and time of collection.
■ Name and signature of the person collecting the evidence.
■ Description of the item (make, model, serial number, unique identifiers).
■ Location where the evidence was found.
■ Hash values of the acquired data (MD5, SHA-1, SHA-256 – these are digital fingerprints - cryptographic hash algorithms - that will change if even a single bit of data is altered).
■ Packaging and sealing details.
■ Names and signatures of all individuals who subsequently took possession of the evidence.
■ Dates and times of transfers.
■ Purpose of each transfer (e.g., transport to lab, forensic analysis).

Key Elements of a Strong Chain of Custody

- **Secure Storage** – restricted access
- **Controlled Access** – only authorized personnel
- **Minimized Handling** – lesser risk of contamination

Trial Considerations: Methods of Presentation and Admissibility Tests

Methods of Presentation in Court

- **Expert Witness Testimony –** explain, authenticate, describe, interpret, clarify

- **Visual Aids and Demonstratives:**

■ **Screenshots and Printouts:** Of emails, chat logs, social media profiles, web pages.
■ **Animations and Simulations:** To illustrate complex digital processes or reconstruct events, but with a strong caveat
■ **Timelines and Flowcharts:** To show the sequence of events or the flow of digital communications.
■ **Graphs and Charts:** To present data trends or volumes.
■ **Interactive Presentations:** Using software to navigate through large datasets or demonstrate software functionality.

Methods of Presentation in Court

- **Detailed Forensic Reports**
- **Direct Presentation of Digital Evidence** – when possible

Admissibility Tests for Electronic Evidence

GOVERNED BY PRINCIPLES OF ECHR

- **Legality and Fairness** (art 6 ECHR)
- **Authenticity and Integrity**
- **Reliability –** ISO 27037- digital evidence handling ISO 17025 (lab calibration)
- **Relevance**
- **Proportionality of methods used to obtain digital data**
- **Transparancy**

Admissibility Tests for Electronic Evidence

- **Specific Challenges**
  - **Encryption and Anonymization -** hindrances.
  - **Cross-border Admissibility** – must conform to both the rules of the collecting country and the forum state
  - **Deepfakes and AI-generated Content: -** Expert testimony and advanced forensic to determine original
  - **Attribution:** - anonymity tools.

Philosophical Q:

As technology makes evidence more precise and abundant, will our courts become more just, or will human judgment become overshadowed by digital certainty?

If we increasingly rely on technology for evidence gathering and analysis, are we strengthening fairness in justice or risking the loss of our fundamental human insight and discernment?

Stay cyber-safe!

Ciprian Băban – *Attorney-at-Law*

Specialist White Collar Crime and Cybercrime

ciprian.baban@babanlaw.com

+40753066152

Webinar on Computer Crimes

Training for Defence Lawyers

Online, 2 July 2025 (325DT71)

Background Documentation

Table of Contents with Hyperlinks

Co-funded by the European Union

The table of contents below is hyperlinked, with each entry taking you to the respective document on the web.

A) EU Institutional Framework

Main Treaties and Conventions

A.5	European Convention for the Protection of Human Rights and Fundamental Freedoms and additional protocols (ETS No. 005; 3.5.1953)

B) EU Framework to Counter Computer Crimes

B1) EU Law on Cybercrime and Cybersecurity

B1.1	Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)
B1.2	Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence
B1.3	Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse
B1.4	Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
B1.5	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
B1.6	Regultion (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)
B1.7	Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, COM/2020/568 final
B1.8	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)
B1.9	Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA

B1.10	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
B1.11	Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

B2) EU Law to Combat the Sexual Exploitation of Children Online, Child Pornography and Violence Against Women and Domestic Violence

B2.1	Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence
B2.2	Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance)
B2.3	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)
B2.4	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 11 May 2022
B2.5	Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance)
B2.6	Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA
B2.7	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
B2.8	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

B3) European Commission Communications

B3.1	Communication from the Commission – Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065, 10.10.2025
B3.2	Communicatoin from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, Brussels 24.7.2020 COM(2020) 605 final
B3.3	Communication from the Commission to the European Parliament, the European Council and the Council: Eleventh progress report towards an effective and genuine Security Union, Brussels, 18.10.2017 COM(2017) 608 final
B3.4	Communication from the Commission to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels 13.9.2017 JOIN(2017) 450 final
B3.5	Joint Communcation to the European Parliamet, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels 7.2.2013 JOIN(2013) 1 final

B4) Data Retention

B4.1	Study on the retention of electronic communications non-content data for law enforcement purposes Final report, September 2020

B5) EMPACT

B5.1	EMPACT2023 Results: Factsheets

B6) Child Protection

B6.1	The Digital Services Act (Explained) – Measures to protect children and young people online
B6.2	Eurochild response to European Commission call for evidence on Guidelines to enforce the protection of minors online

B7) European Union Agency for Cybersecurity (enisa)

B7.1	Enisa

C) Council of Europea Convention on Cybercrime

C.1	Convention on Cybercrime, Budapest 23.11.2001
C.2	Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, 17.11.2021

D) EU e-Evidence Legislation

D.1	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings
D.2	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

Co-funded by the European Union

Factsheet on Computer Crimes

Computer crimes in the EU are addressed through a dynamic framework and international cooperation, with evolving rules for handling electronic evidence (e-evidence).

Cybercrime

Cybercrime consists of criminal acts committed online by using electronical communications networks and information systems. The EU has implemented laws and supports operational cooperation through non-legislative actions and funding.

Cybercrime is a borderless issue that can be classified in three broad definitions:

- Crimes specific to the internet, such as attacks against information systems or phishing, e.g. fake bank websites to solicit passwords enabling access to victim's bank accounts.

- Online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.

- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

Many types of crime, including terrorism, trafficking in human beings, child sexual abuse and drugs trafficking, have moved online or are facilitated online. As a consequence, most criminal investigations have a digital component.

Common Challenges in Cybercrime

- **Data volume**: investigations involve massive amounts of complex data, requiring advanced tools and specialised expertise. Many law enforcement agencies lack the capacity, tools, and personnel to handle this efficiently.

- **Loss of data**: the absence of a harmonised EU data retention policy hampers investigation. Data may not be stored long enough or is unavailable due to varying national laws.

- **Access to data**: encryptions technologies, anonymisation services, and legal fragmentation prevent or delay lawful access to critical digital evidence. There is also limited cooperation from some service providers.

- **Anonymisation services**: VPNs, Tor, and decentralised platforms obscure the location of perpetrators and data, making attribution and evidence gathering difficult.

- **Obstacles to international cooperation**: jurisdictional complexity, lack of streamlined mutual legal assistance, and safe havens for cybercriminals complicate cross-border investigations.

- **Public partnership challenges**: collaboration is essential but limited by legal constraints, lack of standard processes and data protection concerns. Trust and information sharing remain problematic.

- **Cryptocurrency and decentralised finance (DeFi)**: criminals use cryptocurrencies and decentralised finance platforms to launder money. Tracing such transactions is technically and legally challenging.

These challenges reflect the evolving complexity of cybercrime and underline the need for coordinated legal, technical, and organisational responses across jurisdictions.

EU laws and actions aim to:

- Improve the prevention, investigation and prosecution of cybercrime and child sexual exploitation

- Build capacity in the law enforcement and the judiciary

- Work with industry to empower the protection of citizens

I. Current and Future European and EU Frameworks to Counter Computer Crimes

1. Council of Europe Conventon on Cybercrime (Budapest Convention) and its Second Additional Protocol

The **Budapest Convention**, adopted in 2001 and entering into force in 2004, was the first and most influential international treaty dedicated to combatting crimes committed via the internet and other computer networks. Drafted by the Council of Europe with the participation of non-European states, it was ratified by all EU Member States and many others countries worldwide, providing a global standard for cybercrime legislation and cooperation.

- **Key objectives and scope:**

  - **Harmonisation of criminal laws:** The Convention requires signatory countries to criminalise a range of cyber offences, ensuring that core definitions and penalties are consistent across borders. Offences covered

include: illegal access to computer systems; illegal interception of data; data and system interference; misuse of devices; computer related forgery and fraud; offences related to child pornography; copyright and intellectual property violations

- **Cross-border cooperation:**
    - **24/7 emergency contact points:** Each party must designate a 24/7 contact point for urgent requests, enabling rapid international cooperation in cybercrime investigations.
    - **The contact points facilitate:** Immediate assistance in securing and sharing electronic evidence; coordination with mutual legal assistance authorities; flexibility for each country to choose the most effective agency for this role, such as a specialised cybercrime unit or a central authority.

➢ **Compatibility with EU frameworks:**

- **Mutual recognition of e-evidence requests:** The Convention's procedural standards are aligned with EU initiatives, such as the e-Evidence Regulation, ensuring that evidence obtained under the Convention is admissible and recognised across EU Member States.
- **Foundation for EU and global policy:** The Budapest Convention serves as the legal and operational backbone for EU cybercrime policy, shaping both national legislation and cross-border cooperation mechanisms.

➢ **Summary:**

- The Budapest Convention is the global benchmark for cybercrime law, enabling harmonised criminalisation, effective investigations and rapid international cooperation, all while upholding fundamental rights and dovetailing with EU legal frameworks.

2. Directive 2013/40/EU on attacks against information systems

The Directive aims to harmonise criminal law across EU Member States by setting minimum penalties for cyber attacks, updating and replacing earlier frameworks. It addresses attacks on information systems that jeopardise availability, integrity, authenticity or confidentiality.

The Directive criminalises five core categories of conduct:

➢ illegal access: gaining entry to an information system without permission;

➢ illegal system interference: seriously disrupting or damaging networks or data;

- illegal data interference: damaging, deleting, deteriorating or altering data;
- illegal interception: unlawful interception of non-public transmissions;
- off-shore-acts: where the perpetrator resides in the EU but commits the offence outside of it.

Offences must be punished by effective, proportionate and dissuasive criminal penalties, including imprisonment or fines. It requires Member States to cooperate and designate points of contact for urgent assistance.

3. Directive (EU) 2019/713 on combatting fraud and counterfeiting of non-cash means of payment

The Directive responds to the evolving digital payment technologies and the rising use of virtual currencies and digital wallets, aiming to keep pace with new fraud risks. It aims to approximate criminal law in the EU to ensure consistent treatment of fraud and the counterfeiting of non-cash means of payment across all Member States. Furthermore, it enhances cross-border cooperation, delegation of jurisdiction, rapid information exchange and support frameworks for victims. Finally, it supports crime prevention and victim assistance, aligning with Directive 2012/29/EU, including identity theft risk and practical awareness initiatives for the public.

4. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, EU Cybersecurity Act, EU Cyber Resilience Act and EU cybersecurity

The Directive focuses on network and information system security for essential services (energy, transport, health and finance). It obligates operators to report major cyber incidents to national authorities. The aim is to align and harmonise cybersecurity legislation across Member States, close gaps from the now no longer in force Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS-1) and strengthen EU-wide resilience.

II. EU Standards to Combat the Sexual Exploitation of Children Online, Child Pornography and Violence Against Women and Domestic Violence

1. EU Strategy for a More Effective Fight Against Child Sexual Abuse

The strategy sets out eight concrete initiatives. It has a three-fold focus on a more effective law enforcement response, better support for victims and improved prevention. It aims to:

- ensure complete implementation of the current rules (particularly Directive 2011/93/EU on combatting sexual abuse and exploitation of children);
- ensure that EU laws enable an effective response;
- identify legislative gaps, best practices and priority actions;
- strengthen the law enforcement efforts at national and EU level;
- enable EU countries to better protect children through prevention;
- establish a European centre to prevent and counter child sexual abuse;
- galvanise industry efforts to ensure the protection of children in their products;
- improve protection of children globally through multi-stakeholder cooperation.

2. The Digital Services Act (DSA) – measures to protect children and young people online

Why the Digital Services Act?

The EU wants to make sure that:

- digital technologies and online platforms respect everyone's rights;
- we can trust the digital services we use
- we are safe and protected online, whatever type of digital service we use.

What does the DSA do?

- It makes sure that all digital services we use, especially the so-called 'Very Large Online Platforms' like Instagram, Snapchat, TikTok and 'Very Large

Online Search Engines' like Google or Bing, do more to protect users' rights, keep us safe and stop the spread of illegal or inappropriate content.

- Different types and sizes of online services, which are used by anyone in the EU, wherever the service is based, are covered. It sets stricter rules for the biggest services.

- Online platforms are required to consider the impact of their services on important issues such as fair elections, public safety, the mental and physical well-being of users, and gender-based violence.

- Online platforms are obliged to respect EU fundamental rights when useres are making use of their services. Among all those listed in the Charter of Fundamental Rights of the European Union, the following are most relevant to the DSA and to protect minors online:
  - the 'best interest of the child' principle;
  - the right to protection for the child;
  - the right to freedom of expression;
  - the right not to face discrimination;
  - the right to protection of personal data;
  - a high level of consumer protection.

How does the DSA protect minors online?

- It states that online platforms that can be used by minors need to make sure that their services offer a high level of privacy, safety and security to young users.

Online Risks for Minors

- Users – children and young people in particular – should be safe from online dangers and risks, such as harassment, bullying, false information, illegal content and/or people pretending to be someone else.

- When considering the risks their service poses to young users, 'Very Large Online Platforms' and 'Very Large Online Search Engines' must consider:

  - if minors will easily understand how the service works;
  - if minors risk finding content that could harm their health, physical, mental and moral development (age-inappropriate content);
  - how design features could cause addiction.

Risk Assessment and Reduction

- Every year, 'Very Large Online Platforms' and 'Very Large Online Search Engines' need to identify and assess the potential online risks for children and young people using their services.

- Just as there are age ratings for films at the cinema, some online content and services are not appropriate for younger age groups. Therefore, platforms must also put measures in place to mitigate these risks, including:

    - parental controls: settings that help parents and carers, for instance, monitor or limit children`s access to the internet, to protect them from online risks and inappropriate content;
    - age verification: a system to check the age of users before they access the service, for instance based on physical identifiers or other forms of identification;
    - tools: to help young people signal abuse or get support.

Child-friendly Complaints and Reporting System

- It is important that the platforms can act on content that could affect people's rights, such as dignity, privacy, and freedom of expression.

- The DSA wants it to be easy for users – including minors – to report and complain when they discover illegal or other content that should not be online.

- Platforms should also act quickly when 'trusted flaggers' report content which they consider illegal or against the terms and conditions of that platform.

Personal Data/Privacy

- The right to privacy and to keep personal information safe also applies online, where platforms should not ask to overshare personal details with them or other users. Personal data must be protected.

- Online platforms used by children should protect the privacy and security of their users. This can be done, for instance, by adopting special privacy and security settings by default.

Child-friendly Information

- Terms and conditions must be written and updated in a way that is easy to understand for everyone, including minors.

- Online services used by minors must make an extra effort to explain things clearly so young users can understand what they are agreeing to.

No Profiling Behind Adverts for Children and Young People

- Companies may collect information about our preferences and interests from the websites which we visit, what we like, links we follow, as well as personal information we provide about, ourselves, such as our age or where we live. The platforms use algorithms and artificial intelligence on this profiling data to decide what adverts to show to have the highest impact on each of us. Some online platforms make money each time we purchase products following

these adverts. If platforms are certain that a user is a minor, they cannot show them any adverts based on profiling.

- 'Very Large Online Platforms' are obliged to make the information about their adverts publicly available, so it is possible for anyone, including researchers, to analyse the potential risks. This information should include for example details on the advert content and who paid for it, especially when targeting minors.

III. E-Evidence: Access, Admissibility and Challenges

Definition and Importance

Electronic evidence, or 'e-evidence', refers to digital data that is used to investigate and prosecute criminal offences. It includes:

- e-mails
- text messages or content messaging apps
- audio-visual content
- information about a user's online account

Such data can be used to identify a person or obtain more information about their activities. In the digital era, criminals are making increasing use of tech services and tools to plan and commit crimes. As a result, e-evidence is becoming essential to fighting crime: currently, 85% of criminal investigations involve digital data.

The issue with cross-border access to e-evidence

Getting access to e-evidence can be a lengthy and complicated process for authorities because it is often saved in another country. Online service providers store user's data on servers which may be located in several countries, both in and outside the EU. This makes it much more difficult for judicial authorities to collect e-evidence as they have to go through lengthy and complicated procedures to obtain access to it. A cross-border request to obtain e-evidence is made in over 50% of all criminal investigations.

Admissibility of e-Evidence

- **Divergent national rules**: currently, each EU Member State applies its own rules on the admissibility of evidence, including electronic evidence, in criminal proceedings. This fragmentation can lead to uncertainty and challenges when e-evidence is shared or used across borders
- **Minimum standards and safeguards**: there is growing support for harmonised minimum standards at the EU level to ensure that e-evidence is

only admitted if it respects fundamental rights and procedural safeguards. These include the protection of privileges, the legality of evidence collection, and respect for human rights as enshrined in the EU Charter and the European Convention on Human Rights

- **Authenticity and integrity**: admissibility also depends on demonstrating the integrity, authenticity, and completeness of e-evidence. This requires proper documentation of the chain of custody, use of forensic standards, and the ability to verify that the evidence has not been tampered with.

EU e-Evidence Legislative Package 2023

- **European Production Order**: allows judicial authorities to order service providers in any Member State to produce or preserve e-evidence directly, within 10 days

- **European Preservation Order**: ensures data is not deleted while a formal request is processed.

- **Direct cooperation**: service providers must comply, reducing delays of traditional mutual legal assistance.

- **Directive (EU) 2023/1544**: requires service providers offering services in the EU to appoint legal representatives for handling orders and ensuring compliance.

Legal Vocabulary: Computer Crimes

active recipient of an online platform	A recipient of the service that has engaged with an online platform by either requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface.
active recipient of an online search engine	A recipient of the service that has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface.
advertisement	Information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and presented by an online platform on its online interface against remuneration specifically for promoting that information.
age of sexual consent	The age below which, in accordance with national law, it is prohibited to engage in sexual activities.
assurance level	The assurance level of 'basic', 'substantial' or 'high' is assigned andis commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.
child	Any person below the age of 18.
child pornography	- Any material that visually depicts a child engaged in real or simulated sexually explicitly conduct. - Any depiction of the sexual organs of a child for primarily sexual purposes. - Any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of

	any person appearing to be a child, for primarily sexual purposes.
child prostitution	The use of a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether that payment, promise or consideration is made to the child or to a third party.
child sexual abuse online	Online child sexual abuse material and solicitation of children.
cloud computing service	A network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
commercial communication	Any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications: - information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address, - communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration.
computer data	Information that can be interpreted and used by computers. It is a collection of facts, such as numbers, words, measurements, observations or even just descriptions of things. In computing, data is typically stored electronically in the form of files or databases.
computer system	Any device or a group of interconnected or related devices, one or more of which,

	pursuant to a program, performs automatic data processing.
conformity self-assessment	An action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of the European cybersecurity certification scheme.
consumer	Any natural person who is acting for the purposes which are outside his or her trade, business, craft, or profession.
content moderation	Activities, whether automated or not, undertaken by providers of intermediary services, that are aimed in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account;
Cross-Border Cyber Hub	A multi-country platform, established by a written consortium agreement that brings together in a coordinated network structure National Cyber Hubs from at least three Member States, and that is designed to enhance the monitoring, detection and analysis of cyber threats to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment.
cybersecurity	The activities necessary to protect network and information systems, the

	users of such systems, and other persons affected by cyber threats.
cyber threat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.
data centre service	A service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control.
digital means of exchange	Any form of electronic money.
Digital Service Coordinator of establishment	The Digital Services Coordinator of the Member State where the main establishment of a provider of an intermediary service is located or its legal representative resides or is established.
dissemination to the public	Making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties.
domain name system / “DNS”	A hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources.
DNS provider	An entity that provides publicly available recursive domain name resolution services for internet end-users; or authoritative domain name resolution services for third-party use, with the exception of root name servers.
domestic violence	All acts of physical, sexual, psychological or economic violence that occur within the family or domestic unit, irrespective of biological or legal family ties, or between former or current spouses or partners, whether or not the offender shares or has shared a residence with the victim.
electronic money	Electronically, including magnetically, stored monetary values as represented by

	a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions.
entity	A natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations.
established service provider	A service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.
European cybersecurity certification scheme	A comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.
Hosting Consortium	A consortium composed of participating Member States, that have agreed to establish and to contribute to the acquisition of tools, infrastructure or services for, and the operation of, a Cross-Border Cyber Hub.
illegal content	Any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law.
incident	An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.
information system	A device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or

	group of devices for the purposes of its or their operation, use, protection and maintenance
intermediary service	One of the following information society services: - a mere conduit service, consisting of the transmission of information provided by a recipient of the service in a communication network, or the provision of access to a communication network. - a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request. - a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service.
large-scale cybersecurity incident	Any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.
internet exchange point	A network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic.
legal person	An entity having legal personality under the applicable law, except for states or public bodies in the exercise of state

	authority and for public international organisations.
managed security service provider	A managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.
managed service provider	An entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.
near miss	An event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise.
network and information system	An electronic communications network: • devices or groups of interconnected devices that automatically process digital data; or • digital data stored, received or transmitted by either of the above, for the purposes of their operation, use, protection and maintenance.
non-cash payment instrument	A non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange.
number-independent interpersonal communications service	An interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a

	number or numbers in national or international numbering plans.
online interface	Any software, including a website or a part thereof, and applications, including mobile applications.
online search platform	An intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.
online platform	A hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation.
online search engine	A digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.
pornographic performance	A live exhibition aimed at an audience, including by means of information and communication technology, of: - a child engaged in real or simulated sexually explicit conduct. - the sexual organs of a child for primarily sexual purposes.
protected device, object record	A device, object or record safeguarded against imitation or fraudulent use, for example, through design, coding or signature.

recipient of the service	Any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible.
recommender system	A fully or partially automated system used by an online platform to suggest specific information to recipients of the service or prioritise that information in its online interface, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed.
research organisation	An entity, the primary goal of which is to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions
risk	Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.
secure network and information systems	The ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.
service provider	Any public or private entity that provides the ability to communicate by means of a computer system to users of its service, and any other entity that processes or stores computer data on behalf of such communication service or users of such service.
significant cyber threat	A cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage.
social networking service platforms	A platform that enables end-users to connect, share, discover and

	communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations.
substantial connection to the Union	A connection of a provider of intermediary services with the Union resulting either from its establishment in the Union or from specific factual criteria, such as: - a significant number of recipients of the service in one or more member states in relation to its or their population, or - the targeting of activities towards one or Member States.
technical specification	A document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process.
terms and conditions	All clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the service.
to offer services in the Union	Enabling natural or legal persons in one or more Member States to use the services of a provider of intermediary services that has a substantial connection to the Union.
trader	Any natural person, or any legal entity, irrespective of whether it is privately or publicly owned, which is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession.
traffic data	Any computer data relating to a communication by means of a computer system, generated by a computer system, that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, data, size, duration, or type of underlying service.
trusted managed security service provider	Managed security service providers selected to be in the EU Cybersecurity Reserve
victim	Any person, regardless of their gender, who has suffered harm directly caused by

	violence, including children who have suffered harm because they have witnessed domestic violence.
violence against women	All acts of gender-based violence directed against a women or a girl because she is a women or a girl, or that affect women or girls disproportionately, that result in or are likely to result in physical, sexual, psychological or economic harm or suffering, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.
virtual currency	A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically.
without right	Conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.

Legal Vocabulary: Cybercrime

age of sexual consent	The age below which, in accordance with national law, it is prohibited to engage in sexual activities.
assurance level	The assurance level of 'basic', 'substantial' or 'high' is assigned andis commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.
child	Any person below the age of 18.
child pornography	- Any material that visually depicts a child engaged in real or simulated sexually explicitly conduct. - Any depiction of the sexual organs of a child for primarily sexual purposes. - Any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes.
child prostitution	The use of a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment in exchange for the child engaging in sexual activities, regardless of whether that payment, promise or consideration is made to the child or to a third party.
child sexual abuse online	Online child sexual abuse material and solicitation of children.
cloud computing service	A network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
computer data	Information that can be interpreted and used by computers. It is a collection of

	facts, such as numbers, words, measurements, observations or even just descriptions of things. In computing, data is typically stored electronically in the form of files or databases.
computer system	Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic data processing.
conformity self-assessment	An action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of the European cybersecurity certification scheme.
Cross-Border Cyber Hub	A multi-country platform, established by a written consortium agreement that brings together in a coordinated network structure National Cyber Hubs from at least three Member States, and that is designed to enhance the monitoring, detection and analysis of cyber threats to prevent incidents and to support the production of cyber threat intelligence, in particular through the exchange of relevant data and information, anonymised where appropriate, as well as through the sharing of state-of-the-art tools and the joint development of cyber detection, analysis, and prevention and protection capabilities in a trusted environment.
cybersecurity	The activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.
cyber threat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.
data centre service	A service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and

	network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control.
digital means of exchange	Any form of electronic money.
DNS provider	An entity that provides publicly available recursive domain name resolution services for internet end-users; or authoritative domain name resolution services for third-party use, with the exception of root name servers.
domain name system / "DNS"	A hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources.
electronic money	Electronically, including magnetically, stored monetary values as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions.
entity	A natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations.
European Cybersecurity Certification Scheme (EUCC)	A comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.
hosting consortium	A consortium composed of participating Member States that have agreed to establish and to contribute to the acquisition of tools, infrastructure or services for, and the operation of, a Cross-Border Cyber Hub.
incident	An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.
information system	A device or group of interconnected or related devices, one or more of which,

	pursuant to a program, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.
internet exchange point	A network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic.
large-scale cybersecurity incident	Any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.
legal person	An entity having legal personality under the applicable law, except for states or public bodies in the exercise of state authority and for public international organisations.
managed security service provider	A managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.
managed service provider	An entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely.
near miss	An event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was

	successfully prevented from materialising or that did not materialise.
network and information system	An electronic communications network: • devices or groups of interconnected devices that automatically process digital data; or • digital data stored, received or transmitted by either of the above, for the purposes of their operation, use, protection and maintenance.
non-cash payment instrument	A non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange.
number-independent interpersonal communications service	An interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans.
online search engine	A digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.
pornographic performance	A live exhibition aimed at an audience, including by means of information and communication technology, of: - a child engaged in real or simulated sexually explicit conduct. - the sexual organs of a child for primarily sexual purposes.

protected device, object record	A device, object or record safeguarded against imitation or fraudulent use, for example, through design, coding or signature.
research organisation	An entity, the primary goal of which is to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.
risk	Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.
secure network and information systems	The ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.
service provider	Any public or private entity that provides the ability to communicate by means of a computer system to users of its service, and any other entity that processes or stores computer data on behalf of such communication services or users of such services.
significant cyber threat	A cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage.
social networking service platforms	A platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations.
technical specification	A document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process.

traffic data	Any computer data relating to a communication by means of a computer system, generated by a computer system, that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, data, size, duration, or type of underlying service.
trusted managed security service provider	Managed security service providers selected to be in the EU Cybersecurity Reserve.
virtual currency	A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically.
without right	Conduct including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.