Casarosa Ultra Sintetizzato

Confidentiality: prevention of unauthorized disclosure of information
Integrity: guarantee that the message that is sent is the same as the message received and that the message is not altered in transit
Availability: guarantee that information will be available to the user in a timely and uninterrupted manner when it is needed regardless of the location of the user

The European Union (EU) operates under the principle of conferral, meaning it can act only within the limits of competences granted by Member States in the Treaties to achieve set objectives. Powers not conferred to the EU remain with the Member States. The Union must respect Member States' equality, national identities, and essential state functions, including territorial integrity, law and order, and national security, which remains their sole responsibility.

Legal basis for EU cybersecurity legislation:

- **Article 114 TFEU (Internal Market):** Enables harmonization of laws among Member States to ensure the proper functioning of the internal market by aligning regulations and removing trade and competition barriers.
- **Article 62 and 53(1) TFEU (Right of Establishment and Freedom of Service):** Provides for rules ensuring the freedom of establishment and services across the EU.
- **Articles 127(2) and 132(1) TFEU (Payment Systems):** Grants the European System of Central Banks (ESCB) and the European Central Bank (ECB) authority to support price stability, economic policies, and regulatory tasks.
- **Article 83(1) TFEU (Freedom, Security, and Justice):** Allows for establishing minimum rules on serious cross-border crimes, including cybercrime.

In non-exclusive EU competences, the **principle of subsidiarity** applies, requiring the Union to act only when objectives cannot be sufficiently achieved by Member States alone and are better addressed at the Union level. The **principle of proportionality** ensures that EU action is limited to what is necessary to achieve Treaty objectives. Both principles are governed by protocols and monitored by national parliaments.

The EU governance structure for cybersecurity is decentralized, allocating responsibilities across three key areas: network and information security, cybercrime, and cyber defense.

In **network and information security**, the European Union Agency for Cybersecurity (ENISA), established in 2004 and given a permanent mandate in 2019 by the Cybersecurity Act, plays a central role in improving resilience, raising awareness, and preparing European cybersecurity certification schemes. It works alongside CERT-EU, CSIRTs, and cooperation networks.

In **cybercrime**, the European Cybercrime Centre (EC3) provides operational support, training, and expertise to Member States for combating cybercriminal activities.

In **cyber defense**, entities like the European Defense Agency (EDA) and the EU Military Staff provide advisory functions, with Member States retaining operational control over defense activities.

The EU cybersecurity ecosystem is structured around four pillars: resilience, law enforcement, cyber defense, and cyber diplomacy. These pillars involve coordination between EU organizations and mechanisms to enhance security. The Joint Cyber Unit supports operational efforts such as creating capability inventories, producing situation reports, implementing crisis response plans, and mobilizing rapid reaction teams. Effective cybersecurity also relies on enhanced public-private information sharing to address increasingly complex cyberattacks.

Regulations vs. Directives:

Regulations, like the GDPR, are directly applicable across Member States, ensuring uniformity without requiring national transposition. Directives, such as NIS2, set objectives that Member States must achieve but allow flexibility in implementation, adapting to local contexts.

The **Cybersecurity Act (Regulation 2019/881)** emphasizes enhancing cybersecurity capabilities, fostering cooperation, and strengthening Union-level responses to large-scale incidents. ENISA is tasked with supporting public-private cooperation and critical infrastructure protection, including facilitating information sharing within sectors.

The **NIS2 Directive (2022/2555)** strengthens Member States' capabilities to handle cybersecurity incidents, requiring the establishment of well-resourced and capable CSIRTs. It highlights the need for effective information sharing on threats and vulnerabilities to improve prevention, containment, and recovery, despite existing barriers such as competition and liability concerns.

PPPs

Public-private partnerships (PPPs) in cybersecurity aim to enhance security through collaboration between governments and private entities. These partnerships address the reluctance of private actors to voluntarily share sensitive information with public authorities by creating structured cooperative models.

ENISA defines PPPs as contractual relationships where private and public entities share risks, responsibilities, and resources to achieve shared objectives, such as improving cybersecurity resilience. The level of interaction between public and private actors depends on the sector; for example, private entities providing consumer services often have a closer relationship with public authorities compared to those operating physical infrastructure.

Motivations and Benefits:

For private entities, PPPs provide access to public funding, regulatory insights, and opportunities to influence legislation and standards. For governments, they offer deeper understanding of industry needs, access to private resources, and alignment with international law and regulations. PPPs foster trust, promote information sharing, and enhance overall cybersecurity resilience.

Types of PPPs:

- **Institutional PPPs:** Established under legal frameworks for critical infrastructure protection, involving working groups and long-term communities.
- **Goal-Oriented PPPs:** Focus on building cybersecurity culture and exchanging knowledge.
- **Outsourcing Cybersecurity Services:** Governments and private sectors collaborate as third-party providers to meet industry needs while shaping policy.
- **Hybrid PPPs:** Often include CSIRTs tasked with nationwide cybersecurity services under government oversight.

Challenges:

PPPs face obstacles like a shortage of skilled professionals, limited public budgets, difficulties in fostering dialogue between sectors, and low SME awareness. Leadership gaps and unclear legal frameworks further hinder effective collaboration.

To address these challenges, ENISA's studies recommend fostering trust, enhancing knowledge sharing, and creating clear legal and organizational structures to support PPP development in Europe.

ECSO

The European Cyber Security Organization (ECSO) is a non-profit entity created in 2016 to act as the European Commission's counterpart in a public-private partnership under Horizon 2020. Its 250 members primarily include actors from the cybersecurity industry and research institutions, with some representation from the public sector and demand-side industries. ECSO focuses on community building, industrial development, and making recommendations on European cybersecurity programs.

Regulation (EU) 2021/887 established the European Cybersecurity Industrial, Technology, and Research Competence Center (ECCC) and a Network of National Coordination Centers (NNCCs). Located in Bucharest, the ECCC aims to develop a common agenda for cybersecurity technology development and deployment, focusing on areas of public interest and businesses, particularly SMEs. This initiative enhances European technological sovereignty by facilitating joint investments in strategic cybersecurity projects.

The ECCC focuses on coordination and facilitation, not operational cybersecurity tasks like incident handling. It supports ICT infrastructure development for industries, SMEs, and public sectors while collaborating with NNCCs to align efforts. The NNCCs consist of one center per Member State, recognized by the European Commission for their capacity to manage funds and execute cybersecurity objectives. These centers, typically public-sector entities, must possess expertise in cybersecurity and effectively engage with industry, research, and public sectors to achieve their mission.

The European Critical Infrastructure (ECI) Directive of 2008 focuses on energy and transport, identifying infrastructures whose disruption affects at least two Member States. It sets protection requirements for operators and authorities, though EU efforts now include broader sectoral and cross-sectoral actions like climate protection, civil defense, and cybersecurity. Member States apply varying national measures, and 94 ECIs have been designated, mainly in energy and Central/Eastern Europe.

Critical infrastructure policy has evolved to address modern risks, including natural hazards, hybrid threats, terrorism, pandemics, and new technologies like 5G. Increased interdependence among sectors means disruptions can have cascading effects across multiple countries. The scope now spans ten sectors, including energy, transport, health, finance, and space, with Member States identifying critical entities through national risk assessments.

The policy now emphasizes resilience over protection, incorporating both preventive and responsive measures while accepting that incidents will occur. It has shifted to a broader, bottom-up approach covering 11 critical sectors and addressing interdependencies between physical and digital systems.

Cybersecurity coordination aligns with the NIS 2 Directive, which strengthens resilience for essential and important entities. Authorities responsible for critical entities and NIS 2 will collaborate to address both cyber and non-cyber risks, integrating physical security into cybersecurity risk management for critical digital infrastructure.

NIS

The EU Directive 2016/1148 aims to establish a high level of common security for network and information systems across the Union to support the internal market. It mandates security measures for operators of essential services (OES) and digital service providers (DSP), with sector-specific legal acts taking precedence if they meet equivalent security obligations.

The Directive addresses cybersecurity challenges, such as insufficient capabilities, disparities in Member States' preparedness, and the lack of common security requirements for OES and DSPs. Its key objectives include enhancing Union-level cooperation through a Cooperation Group for strategic coordination and a CSIRTs network for operational collaboration.

Member States must adopt national strategies to define objectives, governance frameworks, and measures for preparedness, response, and recovery, alongside initiatives for education, awareness, and research. ENISA can assist in developing these strategies.

Each Member State must designate one or more CSIRTs to handle risks and incidents across critical sectors, ensuring adequate resources, resilient infrastructure, and effective cooperation within the CSIRT network. ENISA provides support for national CSIRTs, which must adhere to structured processes for incident management.

The Directive applies to OES and DSPs, which are required to comply with security and incident notification obligations to enhance cybersecurity resilience across the EU.

The Directive requires operators of essential services (OES) and digital service providers (DSP) to implement proportional technical and organizational measures to manage security risks to their network and information systems. These measures must align with the state of the art and ensure the continuity of essential services by minimizing the impact of incidents.

For incident notification, OES must inform the competent authority or CSIRT without undue delay about incidents significantly affecting service continuity. Notifications should enable an assessment of cross-border impacts without increasing liability. The significance of an incident is determined by parameters such as the number of users affected, duration, and geographical spread. Authorities are responsible for balancing the public interest in being informed with the operators' reputational and commercial risks.

DSPs must similarly implement measures to manage risks and ensure service continuity. They are required to notify significant incidents promptly, considering factors like user impact, duration, geographical spread, and societal disruption. Notification obligations only apply if the provider can adequately assess the incident's impact.

NIS2

The NIS 2 Directive (EU) 2022/2555 expands its scope to include more sectors critical to the economy and society, removing the distinction between operators of essential services (OES) and digital service providers (DSP). It strengthens security requirements with a risk management approach, ensuring entities implement appropriate measures to mitigate cybersecurity risks effectively. The Directive applies to entities providing critical services that, if disrupted, could significantly impact public safety, security, health, or the economy.

Security Requirements

Member States must ensure essential and important entities adopt technical, operational, and organizational measures proportionate to risks. These measures should include risk analysis, incident handling, business continuity (e.g., backups, crisis management), supply chain security, encryption policies, and secure authentication. An all-hazards approach must be used to protect systems and physical environments.

Incident Notification

Entities must notify CSIRTs or competent authorities of significant incidents promptly. Notifications should assess cross-border impacts and include early warnings (within 24 hours), incident notifications (within 72 hours), intermediate reports (if requested), and final reports (within one month). Entities must also inform service recipients about significant threats and mitigation measures.

Supervision and Enforcement

Essential entities are subject to proactive supervision, including audits, inspections, and security scans. Important entities are supervised ex post, with measures applied only after non-compliance evidence arises. Supervisory measures must be effective, proportionate, and dissuasive.

Sanctions

Administrative fines for non-compliance can reach up to €10 million or 2% of global turnover for essential entities and €7 million or 1.4% for important entities, depending on the severity of the violation.

Agenzia per l'Italia Digitale

Law No. 134/2012 established the "Agenzia per l'Italia Digitale" to coordinate innovation initiatives and promote ICT technologies in public administrations, aligning with the European Digital Agenda. The Prime Minister's Decree of January 24, 2013, centralized cybersecurity efforts across public administrations and the intelligence community.

Decreto Legislativo 65/2018 implemented EU Directive 2016/1148 to strengthen network and information security at the national and EU levels. Essential Service Operators (OES) and Digital Service Providers (DSP) must report significant incidents to the Italian CSIRT, with fines for non-compliance.

Decreto Legge 105/2019 expanded cybersecurity measures through the National Cybersecurity Perimeter (PSNC), including public and private entities critical to national security. DPCM 131/2020 defined the essential functions and services covered, such as government continuity, defense, public safety, infrastructure, and high-tech sectors, focusing on protecting systems whose disruption could threaten national security.

DPCM 81/2021 requires entities within the PSNC to prevent, report, and respond to incidents, maintaining updated inventories of networks, systems, and IT services. Risk assessments and mitigation measures must align with EU and international standards like the NIST framework. Incident severity determines reporting timelines to the Italian CSIRT, with penalties for non-compliance.

Presidential Decree 54/2021 mandates that entities in the PSNC notify the National Evaluation and Certification Center (CVCN) about outsourced ICT products or services. The CVCN conducts security assessments and issues guidelines for their use.

ACN

The Italian Cybersecurity Agency (ACN) is an autonomous body responsible for national cybersecurity efforts, operating independently while adhering to directives from the President of the Council and oversight by COPASIR to maintain political impartiality. Its objectives include safeguarding national cybersecurity, developing capabilities for prevention, monitoring, detection, and response to cyber threats. The ACN drafts the national cybersecurity strategy, coordinates public-private sector activities, enhances digital industry security, provides advisory opinions, and fosters international collaboration. It also enforces cybersecurity compliance within the National Cybersecurity Perimeter (PSNC) and serves as the national supervisory authority and contact for network security.

The Italian CSIRT monitors cybersecurity incidents, shares alerts and information, intervenes in incidents, conducts risk analysis, and participates in international collaboration through the CSIRT network with ENISA.

Legislative Decree No. 138 of September 4, 2024, implements EU Directive 2022/2555 (NIS 2), updating cybersecurity standards. The ACN will identify essential and important entities by April 2025, with specific security obligations based on risk exposure. Penalties for non-compliance include fines for essential and important entities, with additional fines for registration and communication failures. Repeated violations may lead to increased fines and suspension of certifications.

The EU Cybersecurity Act (Regulation 2019/881) establishes ENISA and aims for the EU to lead the global cybersecurity market, address gaps in responding to cyberattacks, and align with the EU's geopolitical strategy on the security of information systems and networks.

Cybersecurity Act

The Cybersecurity Act strengthens ENISA's role in enhancing cybersecurity across the EU. ENISA provides support, advice, and expertise to Member States, EU institutions, and stakeholders, aiming to reduce fragmentation in cybersecurity regulations and ensuring coordination with national efforts. It operates independently while fostering resource development to support cybersecurity duties, with a focus on capacity building, operational cooperation, and trusted solutions.

The EU Cybersecurity certification framework aims to create a unified system for certifying ICT products, services, and processes across the EU. This framework seeks to build trust, reduce conflicting national certifications, and lower business costs in the digital market. The certification process includes leveraging existing national and international schemes and establishing technical standards.

There are two main types of certification schemes: the European Cybersecurity Certification Scheme, defined at the EU level, and National Cybersecurity Certification Schemes, defined by individual Member States. Certification can involve self-assessment for low-risk products, with manufacturers declaring conformity. These certifications are recognized across EU Member States and can influence market access, liability, and compliance.

A centralised system involves one authority overseeing certifications, while a granular system uses multiple levels for tailored assessments. The EU's proposal to amend the Cybersecurity Act includes managed security services in certification schemes, focusing on security objectives such as ensuring qualified staff, maintaining internal procedures, protecting data, and ensuring service resilience and security

EUCC

Cybersecurity standards define procedures, guidelines, and specifications to ensure security, consistency, and reliability in products, services, and systems. In cybersecurity, these standards focus on security features, controls, processes, and guidelines that mitigate risks and prevent cyberattacks. Benefits of standards include time and cost savings, enhanced user awareness, business continuity, and compliance with best practices. They also enable international comparisons of security systems.

Cybersecurity standards provide specific methods for processes, while cybersecurity frameworks offer broader guidelines without detailing steps. Examples of cybersecurity standards include ISO 27000 series, NIST, and SOX.

The EUCC (European Cybersecurity Certification) scheme, proposed in 2020, aims to replace the SOG-IS Mutual Recognition Agreement and enhance ICT product security, particularly for products with built-in security functions like firewalls and encryption devices. It offers two levels of security assurance, "substantial" and "high," excluding basic levels and self-assessment. The EUCC scheme aims to harmonize security standards across EU Member States, boosting consumer trust in certified products. It follows the Common Criteria (CC) standard, which is recognized globally and used by national schemes in countries like France, Germany, and Italy.

To obtain an EUCC certificate, applicants must provide documentation about the product’s use and associated risks, which the certification body verifies. Technical domains for certification include AVA_VAN.4, for smart cards and devices relying on tailored hardware elements, and AVA_VAN.5, for hardware devices with physical protective enclosures, like payment terminals.

In cybersecurity, key values such as security, privacy, fairness, and accountability are essential for protecting information from unauthorized access, modification, destruction, and other threats.

Security refers to the protection from danger or harm, distinguishing itself from safety, which involves protecting from unintentional threats. Privacy concerns how personal information is shared or kept confidential, focusing on control over what data is disclosed. Fairness addresses equality, justice, and non-discrimination in the impact of cybersecurity measures, ensuring equitable treatment

for all individuals. Accountability relates to transparency and responsibility, ensuring that harms or imbalances in power are addressed.

The relationship between security and privacy is complex, as achieving one often impacts the other. Security is necessary for privacy, but achieving privacy may require sacrifices in security, and both contribute to each other's effectiveness.

GDPR

The General Data Protection Regulation (GDPR) outlines legal standards for protecting personal data and ensuring privacy for individuals within the European Union. It applies to personal data processed both within and outside the EU, provided the processing concerns the offering of goods or services to EU data subjects or monitoring their behavior.

Personal data includes any information that can identify or make identifiable an individual, such as details about their health, lifestyle, or economic situation. Sensitive data, such as health-related or judicial data, are subject to additional protections.

Key actors in data processing include the data subject, whose personal data is processed, the data controller, who determines the purposes and means of processing, and the data processor, who processes data on behalf of the controller.

The GDPR grants data subjects several rights, including the right to access their data, request rectification, erasure, or restriction of processing, and to object to processing, particularly for direct marketing. The right to be forgotten ensures that individuals can have their data erased, with controllers required to inform others who have received that data of the erasure request.

Data processing must comply with principles like lawfulness, purpose limitation, data minimization, accuracy, and storage limitation. Processing must be secure, with personal data kept only for as long as necessary. It also requires a lawful basis, which can include consent, contractual obligations, or public interest. Consent must be freely given, informed, and specific for each purpose, and data subjects must be provided with clear, transparent information about how their data will be processed.

The GDPR emphasizes accountability and transparency, ensuring that individuals are well-informed about how their data is used and giving them control over their data.

The GDPR regulates the transfer of personal data to countries outside the EU, allowing it only when the receiving country has been deemed adequate by the European Commission, or when appropriate safeguards or exceptions apply.

Data protection supervisory authorities, including national bodies like the Italian Data Protection Authority, oversee compliance. They have powers to monitor, advise, investigate, handle complaints, and impose corrective actions. Complaints may lead to administrative sanctions, with fines based on the severity of the violation.

The principle of accountability requires data controllers and processors to ensure compliance with GDPR and be able to prove it. Measures for this include maintaining records of processing activities, implementing security measures, and conducting data protection impact assessments (DPIAs).

GDPR also establishes the right to compensation for individuals harmed by non-compliance. Data controllers and processors can be held liable for damages, although they may be exempt if they can prove they are not responsible for the violation.

Risk assessments are key in GDPR, with controllers required to implement appropriate security measures based on the nature, scope, and risks of processing. This includes data protection by design and by default, and measures like encryption and pseudonymization to protect data. If processing is likely to result in high risks to individuals' rights, DPIAs are required before processing begins.

Risks in data processing can lead to significant consequences, such as discrimination, fraud, loss of reputation, or damage to privacy. The GDPR considers risks related to sensitive data categories and large-scale data processing, particularly when vulnerable individuals, like children, are involved.

The effects of data processing can lead to significant negative consequences for individuals, such as damage to reputation, discrimination, identity theft, financial loss, and physical or psychological harm. Individuals may also lose control over their personal data or face difficulties in exercising their rights, accessing services, or taking advantage of opportunities due to improper processing.

Risk assessment involves identifying and controlling risks within an organization. Key elements include evaluating the origin, nature, severity, likelihood, and impact of risks on individuals' rights and freedoms. The severity of risks is categorized into four levels: low, medium, high, and very high, with consequences ranging from minor inconveniences to irreversible damage.

A Data Protection Impact Assessment (DPIA) is required only when processing is likely to result in a high risk to individuals' rights and freedoms. Even if a DPIA is not mandatory, controllers must still assess risks and implement appropriate measures to manage them, ensuring that risks to data subjects' rights are minimized.

A **DPIA** (Data Protection Impact Assessment) is a tool under GDPR used to evaluate the risks of personal data processing operations and ensure compliance. Its purpose is to identify potential risks to individuals' rights and freedoms, assess the necessity and proportionality of processing activities, and define safeguards to mitigate those risks.

When is a DPIA required?

It is mandatory for processing operations likely to result in high risks, such as:

- Automated decision-making or profiling with significant effects on individuals.
- Large-scale processing of sensitive data or criminal records.

- Systematic monitoring of publicly accessible areas on a large scale.

DPIAs are not required when processing poses no significant risk, similar processing has already been assessed, or it is regulated by specific laws where a DPIA was already performed.

Who conducts a DPIA?

The data controller is responsible for ensuring a DPIA is carried out, though it can delegate the task internally or externally. Data processors must assist in providing relevant information. Data Protection Officers (DPOs) must be consulted, and where appropriate, the views of data subjects should be sought.

How to conduct a DPIA?

The process begins before the data processing operation starts and should be updated throughout the lifecycle. It includes:

1. Describing processing operations and purposes.
2. Assessing risks to individuals' rights and freedoms.
3. Evaluating the necessity and proportionality of the processing.
4. Identifying technical and organizational measures to mitigate risks.

Consequences of non-compliance:

Failure to conduct or improperly execute a DPIA can result in fines of up to 10 million euros or 2% of annual worldwide turnover.

Data breaches and GDPR:

A personal data breach involves unauthorized access, loss, or disclosure of personal data. Not all security incidents are data breaches; only those that impact personal data confidentiality, integrity, or availability qualify.

Breach management:

- **Prevent**: Minimize data collection, secure devices, use encryption, and regularly update systems.
- **Detect**: Use logging, monitoring, and forensic tools to identify breaches promptly.
- **Evaluate**: Determine the breach's impact on personal data and individuals' rights. Notify authorities within 72 hours if there is a risk to individuals.
- **Communicate**: Inform affected individuals if the breach poses a high risk, unless protective measures (like encryption) mitigate that risk.

Transparency is essential for trust and organizational accountability. Data controllers must document breaches and demonstrate compliance to supervisory authorities, while public communication may be required for significant breaches.

The European Data Strategy emphasizes creating a unified data space within the EU that promotes free data flow, adherence to European laws, and fair access to data while ensuring robust governance and maintaining European values. It recognizes the value of data reuse in public and private sectors, highlighting challenges like market imbalances, interoperability, and governance to maximize data's utility, particularly in AI

The **Data Act** aims to harmonize rules on accessing and sharing data, covering manufacturers, service providers, and public institutions in the EU. It ensures fair data usage, safeguards against unauthorized access, facilitates switching between data services, and develops interoperability standards. The regulation applies broadly, including manufacturers, users, public institutions, and data processors.

In cases of exceptional need, such as public emergencies or critical public interest tasks, the Act requires data holders to provide data to public authorities, including the European Commission and the European Central Bank, if no alternatives are available. Such requests must be precise, justified, proportionate, and respect data protection principles, with safeguards like pseudonymization or anonymization where personal data is involved.

The Act also addresses cybersecurity concerns, particularly in emergencies like ransomware attacks, asserting that public interest in accessing data can outweigh a data holder's control. It sets conditions for data sharing, ensuring protection of trade secrets and compliance with legal frameworks, while mandating transparency and accountability in the request process.

Autonomous Driving Vehicles

Autonomous driving vehicles (AVs) rely heavily on connectivity to function effectively, utilizing systems like Vehicle-to-Network (V2N), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Infrastructure-to-Vehicle (I2V), Vehicle-to-Person (V2P), and broader Vehicle-to-Everything (V2X) communication. While current AV features primarily assist drivers with warnings or limited control, future advancements aim to integrate these functions fully into the driving process, replacing the driver altogether.

AI plays a critical role in enabling autonomous vehicles, with core capabilities like sensing, localizing, scene representation, planning, and controlling. Key AI technologies include object recognition, segmentation (classifying image regions into categories), vehicle localization (estimating position over time), and tracking the dynamics of moving objects.

However, cybersecurity remains a significant concern. Intentional threats involve exploiting AI vulnerabilities to cause harm, while unintentional threats arise from limitations in the trustworthiness, robustness, and safety of current AI and machine learning methods. Both types of risks underscore the need for robust safeguards in AV systems.

Cybersecurity threats in autonomous vehicles include remote hacking, which compromises vehicle systems, sensor manipulation that disrupts critical functions like obstacle detection, data breaches exposing sensitive information, and DoS attacks that degrade performance or immobilize vehicles.

Countermeasures involve intrusion detection systems to monitor for threats, encryption to protect data integrity, regular updates to fix vulnerabilities, and authentication protocols to prevent unauthorized access. Together, these measures enhance safety and security.

European and international regulations have focused on enabling cooperative, connected, and automated mobility while ensuring safety and cybersecurity. The European Union has introduced several strategies, platforms, and regulations, including the 2016 Cooperative Intelligent Transport Systems strategy, the C-Roads platform for deployment activities, and the 2019 Vehicle General Safety Regulation, which mandates advanced driver assistance systems and sets a legal framework for automated and driverless vehicles.

The UN has established Regulation No. 155, requiring a cybersecurity management system for vehicles to identify, mitigate, and prevent risks of unauthorized access, and Regulation No. 156, which ensures proper procedures for software updates, including compatibility checks and secure delivery. These measures aim to safeguard vehicles against cyberattacks and maintain system integrity.

EU legislation emphasizes harmonized rules for software modifications, addressing unauthorized remote access, and providing diagnostic data for maintenance. It also sets technical requirements for automated vehicles, including driver control systems, real-time monitoring, safety information, and event data recorders, ensuring safe and reliable operation on public roads.

Internet of Things

The Internet of Things (IoT) is broadly understood as a network of interconnected physical and virtual objects that communicate with each other and the environment using sensors and advanced information and communication technologies. It enables autonomous interaction without human intervention, creating a system that bridges the physical and digital worlds. IoT systems are structured into three layers: the **perception layer**, which collects data through sensors; the **processing layer**, where data is analyzed and decisions are made; and the **application layer**, where services and user functionalities are delivered.

IoT poses several **security risks** across different levels. At the **information level**, there are concerns about data integrity, privacy, and confidentiality. At the **access level**, issues revolve around authentication, authorization, and access control. At the **functional level**, challenges include resilience to failures or attacks and the system's ability to self-organize and adapt to threats.

Data protection in IoT is complex due to the large volume and diversity of data collected. Challenges include ensuring transparency, obtaining valid user consent, and avoiding excessive or unintended data processing. Privacy risks are compounded by difficulties in controlling data use and the involvement of multiple, often unknown actors. European regulations, such as **Regulation 1807/2018**, ensure the free flow of data while protecting privacy through principles like purpose limitation, storage limits, and compliance in data transfers.

The **Cyber Resilience Act** mandates that products with digital elements meet cybersecurity standards throughout their lifecycle. Manufacturers must assess risks during design, production, and maintenance, focusing on the confidentiality, integrity, and availability (CIA) of data. Security requirements include data minimization, resilience to attacks, secure design principles, and free updates for vulnerability management. Additionally, manufacturers must maintain records of internal activities and share security information with third-party component providers to minimize risks.

Privacy by design and security by design involve embedding security and privacy measures into the development process from the outset. These approaches ensure that products are designed to protect users' data and privacy, using strong security protocols and ensuring timely updates, vulnerability reporting, and transparency about security policies.

Liability for damages in the Internet of Things (IoT) is addressed by the GDPR, which holds parties accountable for data processing, and the Product Liability Directive, which provides compensation for damages caused by defective products. The Proposal for an AI Liability Directive establishes uniform rules for civil liability related to damages caused by AI systems. This directive aims to ensure that victims of AI-related harm are protected and that businesses face reduced legal uncertainty, while introducing a presumption of causality to simplify claims.

Internet of Health Things

The Internet of Things (IoT) ecosystem includes devices connected to networks through sensors, interacting with the physical world and exchanging information autonomously. The ecosystem is structured into three layers: the perception layer (including wearable and implanted devices and hospitals), the processing layer (involving middleware services), and the application layer (providing high-level services).

Health data processing, as defined by the GDPR, includes personal data related to an individual’s physical or mental health. Processing of special categories of data requires a specific legal basis, such as consent, protection of vital interests, or public health purposes. Security measures must be implemented to protect personal data from unauthorized processing or loss, as outlined in Article 32 of the GDPR.

In case of non-compliance, the French Data Protection Authority imposed a fine on a company for failing to secure medical data, highlighting breaches in areas like encryption, data migration, and server security. The Medical Device Regulation (MDR) defines medical devices as products used for diagnosis, treatment, or prevention of diseases. It includes software that is intended for medical purposes, whether stand-alone or connected to other devices.

IoT devices with a medical purpose fall under MDR, while those without such a purpose are not regulated by it, even though they may collect health-related data. The MDR requires certification and adherence to safety standards, and manufacturers must report serious incidents, with specific timelines for reporting based on the severity of the incident. Corrective actions, such as recalls or software updates, must be taken, and users must be informed through safety notices.

Medical IoT devices must comply with both the GDPR and MDR. The interplay between these regulations raises questions about whether national bodies responsible for MDR compliance also verify GDPR compliance, particularly in terms of the security measures required by both frameworks.

The Cyber Resilience Act (CRA) applies to products with digital elements, including software and hardware, but excludes those already defined as medical devices under the MDR. Products subject to the MDR must meet security and safety standards, while products under the CRA must meet cybersecurity requirements. The CRA mandates that products with digital elements be designed and manufactured to ensure an appropriate level of cybersecurity before being placed on the market. They must be delivered without known exploitable vulnerabilities and deployed with secure default configurations.

Manufacturers must notify relevant authorities, such as CSIRT and ENISA, about actively exploited vulnerabilities. Notifications must be made within strict timelines, including an early warning within 24 hours, a vulnerability notification within 72 hours, and a final report within 14 days after corrective measures are available.

Open issues related to the CRA include the coordination between general and sector-specific legislation, particularly in distinguishing medical and health devices, and addressing generic standards. There is also concern about notification overload, with overlapping timelines, different authorities, and varying requirements for notifications.

Cloud Computing

According to the National Institute of Standards and Technology (NIST), a cloud service is defined by five characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Cloud services are categorized into different models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). There are also different types of cloud environments: private, community, public, and hybrid clouds. Cloud services operate at multiple levels: data, application, network, and host levels, each of which involves different resources, including data storage, network elements, applications, and virtualization components.

Cybersecurity in cloud services faces challenges, such as mismatches between the demand and supply sides regarding cybersecurity functions. These gaps are often linked to unclear responsibilities for implementing and maintaining security measures. The cybersecurity market involves stakeholders such as cloud service providers, end users, researchers, and regulatory bodies. The relationship between cybersecurity and cloud computing is multi-dimensional, covering security from, for, and within the cloud.

Cloud contracts include specific technical features, such as the shift of data storage from the user's physical servers to the provider's systems, the use of shared infrastructure (multi-tenant model), and the reliance on the internet for service access. Cloud services are typically offered on a pay-as-you-go basis, allowing flexible scaling to meet changing needs, such as additional storage or computing power.

The processing operation involves handling various types of personal data, including contact details, medical information, and administrative or financial data. The purpose of this data processing is to provide healthcare services, such as diagnosis, treatment, hospitalization, and billing, with the data subjects being patients, their relatives, doctors, and nurses. The recipients of this data are doctors, nurses, administrative and accounting departments, public health systems, and patients themselves. An IaaS cloud service provider acts as the data processor in this context.

In terms of data protection challenges, techniques like privacy by design, effective data management, deletion, and portability are key considerations. Cybersecurity challenges involve a wide range of issues such as access control, audit, authorization, availability, and ensuring compliance. Other areas of concern include maintaining confidentiality, securing the chain of trust and responsibility, managing cybersecurity incidents, and safeguarding network security, privacy, and storage, all while ensuring transparency and visibility, as well as preventing repudiation

Cybersecurity architecture in cloud computing

- **Access Control**: This involves mechanisms like authentication and authorization to regulate who can access data and systems.
- **Encryption**: This process turns data into a coded format, ensuring it's secure both when stored (at rest) and while being transmitted (in transit).
- **Data Backup & Recovery**: These strategies make sure that data can be restored in case of a breach or system failure. Backups can be stored separately in cloud services or on-premise data centers.
- **Network Security**: This includes protections such as firewalls, intrusion detection/prevention systems (IDS/IPS), and virtual private networks (VPNs) to guard against cyber attacks and unauthorized access.
- **Compliance**: Adherence to regulations like GDPR and standards like PCI DSS is crucial for maintaining robust cybersecurity.

Cybersecurity challenges often involve using tools such as firewalls, IDS/IPS, and VPNs to protect data. In a cloud environment, digital forensics processes include several stages. Acquisition focuses on collecting large, distributed, and elastic data linked to an incident or allegation. Preservation ensures that digital artifacts remain intact through techniques like imaging, hashing, and duplication. The examination phase involves reviewing the collected forensic data to inform further analysis. Analysis entails a thorough examination, including data fusion and correlation, to draw conclusions. Finally, reporting involves presenting and documenting the results of the forensic analysis.

DSA

The E-Commerce Directive (Directive 2000/31/EC) applies to all information society services (ISS) within the EU, including online intermediaries, and aims to ensure the proper functioning of the internal market. It operates under the country of origin principle, allowing limited exceptions only based on specific reasons and procedural requirements. Intermediaries are exempt from liability, though this does not affect court orders. The Digital Services Act (DSA), which replaced the E-Commerce Directive's liability exemptions, focuses on enhancing online safety, limiting illegal content, promoting transparency, and protecting freedom of speech and minors. It applies to all online intermediaries and illegal content, defining illegality by national or EU law. The DSA establishes due diligence obligations for intermediaries while ensuring that they are not held liable for content, provided they comply with regulatory requirements.

The Digital Services Act (DSA) builds on the E-Commerce Directive, specifically through Articles 4, 5, and 6, which correspond to Articles 12, 13, and 14 of the Directive. These articles distinguish between different types of online service providers, such as mere conduits, caching, and hosting services, with liability arising from any illegal content, regardless of its nature or origin. The DSA introduces new provisions, including Article 6(3), which addresses liability under consumer protection law and establishes exceptions linked to due diligence obligations.

The Court of Justice of the European Union (CJEU) emphasizes that Internet Service Providers (ISPs) should remain neutral and avoid taking an active role in content that would give them knowledge or control over it. The Good Samaritan clause in Article 7 of the DSA still allows exemptions from liability when voluntary measures are taken to address illegal content.

In terms of governance, the design of platforms must prioritize societal risks, with a dynamic approach for identifying and addressing these risks through systems like terms and conditions and algorithmic choices. Oversight is crucial, involving independent audits, regulatory supervision, and public scrutiny through transparency reports, data access for researchers, and consultations on guidelines.

At the national level, the Digital Services Coordinator (DSC) is responsible for ensuring compliance and coordinating with other authorities, while the European Commission has direct enforcement powers over Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). Public communication about breaches is not mandatory unless there's a high risk to individuals' rights, and in such cases, it may be used. Data breach transparency plays a significant role in building trust, protecting an organization's reputation, and enhancing its value, especially in situations like mergers or takeovers.

EU Artificial Intelligence Act

The EU Artificial Intelligence Act (AI Act) aims to improve the internal market and foster the use of trustworthy, human-centric AI while ensuring protection for health, safety, fundamental rights, and the environment. The regulation applies horizontally across all sectors in the EU and is directly applicable in member states. It defines AI as a machine-based system designed to operate autonomously with varying levels of adaptability, inferring outputs such as predictions or decisions from received inputs.

The Act addresses several concerns, including subliminal techniques, biometric categorization, and predictive policing, with specific regulations for high-risk AI systems that could impact public health, safety, or fundamental rights. These high-risk systems are listed in annexes, and their scope can be modified by the EU Commission. Obligations for these systems include risk management, data governance, technical documentation, transparency, human oversight, and cybersecurity measures.

The AI Act also covers general-purpose AI models (GPAI) such as ChatGPT or GPT-3, with obligations including transparency, documentation, and risk management. Models with systemic risks, typically those with significant reach or potential to affect society on a large scale, face additional requirements such as model evaluation and cybersecurity testing.

The AI Act addresses various types of attacks on AI systems, including poisoning attacks, where data is altered during training to shift the model's decision boundary; adversarial attacks, where inputs are manipulated to push decisions inappropriately; model stealing, which involves replicating the model by observing its inputs and outputs; and privacy theft, where training data and parameters are extracted.

Article 15 of the AI Act emphasizes robustness and cybersecurity for high-risk AI systems. These systems must be resilient to errors, faults, or inconsistencies, and organizations must implement appropriate technical and organizational measures to reduce risks such as biased outputs or feedback loops. The Act also requires high-risk AI systems to be protected against unauthorized manipulation by third parties, including measures to address vulnerabilities like data poisoning, adversarial examples, and model flaws.

Challenges include ensuring organizational measures for cybersecurity, aligning cybersecurity and robustness requirements, and balancing these with the specific needs of general-purpose AI models (GPAI). The Act acknowledges that achieving perfect accuracy, robustness, privacy, and fairness is technically impossible, and it emphasizes the need for risk management strategies to balance these conflicting requirements. The technical documentation for AI systems must account for any trade-offs made when implementing solutions to comply with the Act’s standards.

Products security

The European Commission has focused on improving the cybersecurity of connected devices by incorporating minimum cybersecurity requirements into product safety legislation, particularly under the New Legislative Framework (NLF). Starting around 2019, the Commission began revising directives like the Radio Equipment Directive (RED) and other product safety regulations to include essential cybersecurity requirements. This is part of a broader effort to address vulnerabilities in connected products, such as wearables, and ensure ongoing cybersecurity across their lifecycle.

The Commission also initiated the revision of the General Product Safety Directive and the Machinery Directive, proposing new regulations to include cybersecurity requirements. The core problem stems from the widespread vulnerabilities in products with digital elements, inadequate security patching, and insufficient access to cybersecurity information by users. Cyberattacks increasingly threaten hardware and software products, posing risks to organizations and supply chains.

The proposed Cyber Resilience Act (CRA) aims to address these issues by ensuring that manufacturers enhance the security of products with digital elements from the design phase onward. It seeks to establish a coherent cybersecurity framework, improve transparency around product security, and enable secure usage for both businesses and consumers. The CRA applies to products with digital elements that are connected to networks or devices but excludes certain categories, such as medical devices, national security products, and spare parts.

Manufacturers under the CRA will have ongoing obligations to handle vulnerabilities, report exploited vulnerabilities to Computer Security Incident Response Teams (CSIRTs) and the European Union Agency for Cybersecurity (ENISA), and address any severe incidents impacting product security. The regulation emphasizes a proactive approach to cybersecurity, ensuring that products remain secure throughout their lifecycle.

Manufacturers are required to assess and document cybersecurity risks for products with digital elements, including considering their intended and foreseeable use. This process should be updated throughout the product's lifecycle. Products must be designed to meet cybersecurity standards, including secure configurations, protection from unauthorized access, and encryption of personal or sensitive data. Vulnerabilities must be identified, addressed through updates, and publicly disclosed after the fixes are made. Manufacturers must provide technical documentation for 10 years after the product enters the market and must inform users of vulnerabilities and corrective actions.

In the maintenance phase, manufacturers must report incidents and vulnerabilities, with specified deadlines for notifications and updates. If a manufacturer does not notify users within the required timeframe, the Computer Security Incident Response Teams (CSIRTs) may step in. Manufacturers must also inform the component providers about vulnerabilities in integrated parts, including open-source components.

Market surveillance authorities (MSAs) ensure compliance with the Cyber Resilience Act (CRA), collaborating with entities like ENISA and other national authorities. If a product does not comply, the MSA can require corrective actions or recall the product. Penalties for non-compliance can be substantial, up to €15 million or 2.5% of the manufacturer's total global turnover.

Recent Developments in Cybercrime Legislation

The UN's 2019 General Assembly Resolution highlights the dual nature of information and communication technologies (ICTs), which, while beneficial for development, also create opportunities for criminal activities, particularly in cyberspace. The rise in cybercrimes threatens critical infrastructure, businesses, and individuals. To combat this, the resolution calls for international cooperation and proposes creating a committee to develop a global convention to address the criminal misuse of ICTs. The draft convention aims to improve the prevention and prosecution of cybercrime, enhance international cooperation, and support capacity-building, especially in developing countries.

Key aspects of this initiative include the increasing use of ICTs, the responsibility of governments to protect society, and the challenges of obtaining and managing electronic evidence across jurisdictions. It also emphasizes the need for cooperation between states and the private sector, as well as improvements in legal procedures for disclosing stored data and handling emergency mutual assistance.

The European Parliament's 2017 resolution further stresses the social and economic damage caused by cybercrime, particularly through encryption and ransomware, and highlights the threats to fundamental rights and democratic stability. It calls for clearer definitions of cybercrime-related terms and increased liability for service providers, while focusing on better cooperation between law enforcement agencies, particularly in managing electronic evidence.

The "E-Evidence Package" (Regulation 2023/1543 and Directive 2023/1544) introduces measures to help law enforcement effectively obtain and preserve electronic evidence, aiming to combat cybercrime. The package focuses on adapting the procedural framework to the internet age, with service providers playing a key role in supporting investigations and prosecutions. Legal tools such as the EU Production Order and EU Preservation Order are introduced, requiring service providers to produce or preserve electronic evidence. Additionally, the package ensures the protection of fundamental rights by requiring providers to designate legal representatives in the EU.

Italy's Law 90/2024 addresses both cybersecurity and cybercrime, with a traditional approach to cybercrime but increased penalties and expanded procedures to address growing concerns, such as ransomware. The law also introduces corporate liability for cybercrimes and redefines certain offences. The law's provisions reflect broader EU efforts, including the 2022 EUNIS2 Directive, which highlights the need for Member States to report cybercrimes like ransomware and stresses coordination among authorities.

The law strengthens penalties for ransomware, criminalizing it and extending special procedural regimes for cybercrimes targeting critical infrastructure.

Ransomware attacks have become increasingly frequent and severe, involving diverse attack methods, ransom demands, and the use of technologies like cryptocurrencies. The EU and global frameworks emphasize the need for better legal responses to these crimes, with the Oxford Process advocating for human rights protections and the criminalization of ransomware. Italy's law criminalizes ransomware and cyberextortion, imposing prison sentences and fines. It also addresses reporting obligations related to data breaches and ransomware incidents, alongside international legislative efforts like the US Bill on ransomware payments.

Internet of Things and Liability

The interplay between IoT, AI, and liability reveals significant technical and legal challenges. IoT systems are versatile but often centralized and cloud-dependent, with limited peripheral computational power, hindering encryption and protection measures. Issues like internet traffic congestion, data deluge, and technology-induced pollution compound these problems.

Liability in IoT systems spans multiple scenarios, from pre-contractual obligations to contractual and non-contractual responsibilities. EU directives (2019/770 and 2019/771) have introduced rules for goods incorporating digital elements, such as IoT devices, including conformity obligations, burden-of-proof reversal, and remedies for non-compliance.

The AI Act introduces a broad definition of AI, categorizing systems as prohibited, high-risk, or general-purpose. High-risk AI systems face strict obligations, including transparency, oversight, and certification. However, the overlap between AI regulations and IoT product liability remains unclear, especially for integrated systems like medical tools.

The revised EU product liability directive includes software and AI, emphasizing standards for safety and product conformity. New rules address evidence disclosure and introduce rebuttable presumptions of causation for AI-related damages, with stricter requirements for high-risk systems. Future regulatory adaptations will aim to bridge technological and legal gaps, ensuring harmonization with frameworks like GDPR and cybersecurity laws. Regulatory proposals are still evolving, with a focus on hybridizing IoT with AI, blockchain, and digital twins.