International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 11 - Issue 07 || July 2025 || PP. 92-108

Cybersecurity and the Necessity of Its Regulation by the EU Law

Martin Janku
Czech University of Agriculture, Prague

Abstract: To ensure cybersecurity in all its complexity, the role of a legal framework setting out rights and obligations of responsible entities and providing for appropriate procedures and practices cannot be underestimated. It is increasingly frequent to refer to this area of legislation as the Cybersecurity Law. The paper opens with an overview of existing definition of cybersecurity and the role of its legal regulation. Then we focus to the role of the EU law in providing the legal framework of the cybersecurity and legal acts in this area represented by the EU secondary legislation. Attention is drawn on the two main acts in this area - the Cyber Security Act II (EU Regulation of 2019) and the Directive on measures for a high common level of cybersecurity across the Union (known as NIS2, 2022). Cybersecurity provides a perfect example of an area where corresponding legal rules need to be adopted bythe EU law and harmonized on the Member State state level.

Keywords: cybersecurity law; EU cybersecurity legislation; cybersecurity certification scheme; EU Cybersecurity Act

1. Introduction

The current global developments, marked in recent years by the long-term effects of the Covid-19 crisis, have shown beyond any doubt how deeply our economy and society as a wholedepend on digital technologies. In 2021, there have been in the EU 41.7 million people working in home office mode, which is twice as much as in 2019 [1]. This is likely to have lasting effects on everyday life and without digital networking, this would be unthinkable. However, digital technologies do not primarily connect human individuals: the number of connected devices already exceeds the number of people on the planet and is projected to increase to USD 25 billion by 2025 [2].

In our daily life, we see how many economic or service sectors, such as finance, healthcare, energy or transport, are totally dependent on access to telecommunications networks and the security of ICT infrastructure. Therefore, malicious attacks on individual components of critical infrastructure are also a major global threat.

Recent data clearly shows the vulnerability of the digital marketplace, which is constantly exposed to threats from cyber-attacks. As shown in the report 'Major Incidents in the EU and worldwide', prepared by the European Union Agency for Cyber Security (ENISA), the figures show the dimensions of the threat:

230,000 new malware strains are discovered every day;

It takes an average of 6 months to detect a data leak;

In 71% of organizations, there was malware activity that spread from one employee to another [3].

Cyber risks have become a significant threat to the financial system, among others. The International Monetary Fund has estimated the annual losses caused by cyber-attacks at 9% of the net profits of banks worldwide, or approximately USD 100 billion [4].

Malware attacks, ransomware, denial of service (DoS), phishing, social engineering, or insider threats are now common in this area [5, 6]. These types of security incidents or cybercrime can affect organizations and individuals, causing disruption and often significant financial losses.

Cybersecurity as a complex of measures designed to protect networks and information systems, users of these systems and other entities actually or potentially affected by cyber threats is becoming crucial for the development of computer technologies and their widest application in practice.

This role of the cybersecurity also highlights the need for adequate legal regulation of the measures leading to the cybersecurity and the responsibilities of the various actors involved in this process. This is why we can more and more encounter the area of legal regulation known as the cyber security law and, consequently, the efforts to define its role, objectives and scope of regulation. The problem of a proper determination of the role of law in the development of cybersecurity starts already with the difficulty of unification of the various views on the definition of cybersecurity as such and what should include.

2. Methodology and Objectives

Besides the technical and technological procedures and complex measures, forming the basis of the genuine cybersecurity in its entire width, the role of the legal definition of activities following the rights and

duties on the persons responsible and ensure appropriate procedures and secure the proper practices leading to cybersecurity cannot be underestimated as well.

From the legal perspective, the overwhelming part of activities leading to a violation or a threat to the cybersecurity constitute activities that, as a consequence, represent violation and/or limitation of the rights and freedoms aimed at protecting of the privacy of individuals. The content of these rights and freedoms, the scope of their protection, the means of securing them and the means of remedy for rights violated by cyberattacks are defined by legislative tools. Therefore, the law and the legal framework for the use of technical or technological means to combat threats to cybersecurity must constitute the criterion for assessing the availability and admissibility – i.e. the lawfulness of these means. In other words, the assessment of the admissibility of measures aimed at the granting of cybersecurity must - among other aspects - be based on their permissibility, especially in the case that their deployment - mostly for preventive reasons – should involve a certain degree of violation of the privacy of individuals. This means to balance the proportionality between the measures deployed for the cybersecurity protection and the extent of the invasion of privacy that may occur or is currently occurring due to such deployment. Examples include the deployment of visual devices monitoring premises with cameras and recording the movements of people - in conjunction with software enabling the identification of individual persons, and in particular the storage of video recordings made in this way and making them available for purposes other than the evaluation of cyber incidents. [7].

However important, useful or urgent the use of generally available technical means interfering more or less with the privacy of individualsmay appear, the relevance of the right to privacy as a fundamental human right must prevail over their extensive use or at least lead to the precise definition of the range of values, circumstances and interests that would justify such interference and deployment.The latter applies e.g. in cases like the use of information and recordings from the airport security camera system in the event of an intrusion into the air traffic information system and the threat of a breach of national airspace protection. In such a case, the interests of national security justify - to the extent necessary to identify the perpetrators or eliminate the actual threat - the use of these video recordings for purposes other than those for which they are intended, to monitor the movements of individual persons, including their identification (examples of such use include Entry Bio Access Software or the Azure AI Face service)[8]

Generally speaking, the rule " the end justify the means" cannot apply to the means for combating cyber security intruders, as these must always be kept *intra legem*. This is what the states are obliged to do when they adopt the legal framework for the cybersecurity, this is also expected from them by citizens. And this makes it all the more necessary to define the objectives and tools for ensuring cybersecurity and the limits of their applicability within the existing legal regulation, including not only the limits of permissibility but also the sanctions for non-compliance with obligations or prohibitions imposed by legal norms.

Based on the above premises, the first part of this paper focuses on the problemhow to define cybersecurity, taking into account the various and different outlines for such a definition. This effort motivated by a desire to understand the scope of this term as used in the strategy to strengthen cybersecurity and in documents dealing with the legal dimensions of the issue.

The second part of the paper examines both political and legal dimensions of the cybersecurity strategy and its regulation on the EU level.We open by characterizing the complexity of the whole EU cybersecurity scenario. In this connection we subsequentlycharacterize the EU's legislative activities in establishing the legal framework necessary for creation and strengthening the resilience to cyber threats, which, given the multiple levels of the environment, requires a broad-based approach in the EU-wide scale.

Using comparative methods, we observe how EU legislation addresses the requirements for security and privacy protection of individuals, the organizational procedures necessary for implementation of the EU rules by Member States.

The following part of the paper highlights the latest developments in legislation *de lege ferenda* at the level of EU legislative acts by characterizing the most recent documents entering into force or currently awaiting their approval.

In the last part, we formulate some conclusions that summarize the most important findings presented in this paper and outline some recommendations for the EU institutions in order to fill existing gaps in their cybersecurity strategy.

3. Definition of Cybersecurity and the Role of Legal Regulation

Following brief discussion attempts to provide an overview of how the cybersecurity is defined in the literature. It is a fact that more and more definitions appear along with the growing number of papers, studies and documents dealing with the issue. This is, firstly, due to the fact that various national legal systems operate in various ways (e.g. how to approach the method and scope of the regulation of cybersecurity in Civil Law countries and how in Common Law countries where the making and applying law is – *per definition em* -

different). Secondly, the cybersecurity is such a broad concept that an agreement upon a general definition is almost impossible. That´s why many authors create working definitions by themselves and use them in order to examine the issue. And thirdly, the cybersecurity is a fluid concept, not from a scientific point of view, but because the circumstances forming its content and scope change so fast that one has to come up with new and new solutions to keep the track.

3.1 Aspects and elements of the definition of cybersecurity

There are numerous and different definitions of the cybersecurity. When we compare them in more detail, we may separate three aspects and/ or elements on which the definitions of cybersecurity activities focus in a specific context:

3.1.1 The goal of cyber security is prevention as the protection of traffic occurring in cyberspace and averting potential threats:

Preventive measures to protect cyberspace [9]

Anticipating and eliminating threats to cyberspace [10]

Protection of computers, networks, programs and data [11]

Cyber security involves reducing the risk of malicious attacks against software, computers and networks [12].

Prevention is one of the basic duties related to activities aimed at ensuring cybersecurity. This process involves implementing of measures deterring potential attackers from accessing IT systems. To achieve this result, the investment in special infrastructure, including personnel, software and hardware, is often required. Protection can be achieved by putting physical barriers in place and controlling access to the network or the computer system. The implementation of some forms of geographic deterrence often leads to improved security outcomes by reducing the space for unauthorized entries. Improvements in hardware and software capabilities also have a major impact on the level of vulnerability of networks and the associated mitigation of the effect of potential attacks. Digital devices such as firewalls and antivirus examine potential vulnerabilities that can be misused by attackers and solve them.

3.1.2 Essence of cybersecurity lies in the ability to detect current threats or detected breaches in cyberspace in a timely manner

A set of tools, policies, security concepts, safeguards, guidelines, approaches to risk management[13]

Organization and the complex of resources, procedures and structures to enable the early detection of threats [14];

Cybersecurity consists mainly of defensive methods deployed to detect and defeat potential cyber intruders[15].

Detecting of breaches constitutes the critical element of cybersecurity that involves discovering and identifying potential threats. Isolating a threat is a part of its stopping or reducing its impact on the system in combination with appropriate measures to eliminate its negative effects. The detection is an integral part of the response to an incident that involves the alerting of the organization to potential and unauthorized entry or use. This process also protects the sensitive infrastructure and isolates part of the operations running within the **organization**in order to prevent more widespread intrusion. The entire system of security tools is being monitored for potential malicious activity that could compromise the network.

3.1.3 Cybersecurity as a set of measures aimed to efficient remedy of the previous cyberspace breach and to restore the initial status.

Achieving the status quo where users can safely operate and achieve their targets in the cyberspace after the breach has been remedied [16];

A set of technologies, processes, procedures and mitigation measures designed to protect networks, computers, programs and data from malicious consequences of an attack or unauthorized access [17].

Timely and effective response to an incident is the essential part of cybersecurity, which involves fundamental steps to mitigate the harmful effects of malicious activity in the computer system or network. Taking remedies constitutes a process involving specific actions that an organization must re-implement after the detection of aa attack. Threat response also includes analyzing the characteristics or behavior of the perpetrator of a malicious attack. It is often presumed that the elementary procedures will result in the containment and solution of the attack. The key activities may include the isolation of individual system parts and deployment of countermeasures for the threat dispersion.

3.2 Efforts for a comprehensive definition of cybersecurity in the EU context

As the European Union Agency for Cybersecurity (ENISA) states in the document "Defining Cybersecurity - Gaps and Overlaps in Standardization"(2016), it is not easy to define what cybersecurity is: The problem is that cybersecurity is an umbrella term and it is not possible to create a definition that covers the full scope of what cybersecurity addresses [18]. That's why it is also very difficult to adopt a definition of cybersecurity that encompasses the entire field of information technology and the vast scope of cyberspace under protection.

As the ENISA report continues, "even the correct spelling of the word 'cybersecurity' is disputed and varies. Some publications use the single word 'cybersecurity', others prefer a term composed of two words 'cyber security'[18].

In the light of the above considerations, ENISA proposed the following definition: "Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalized telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. Cybersecurity shall therefore encompass the CIA paradigm for relationships and objects within cyberspace" [18].

The "CIA paradigm" or also "CIA triad" is commonly mentioned by the cybersecurity professionals as covering three general categories of goals: (i) confidentiality, (ii) integrity and (iii) availability. *Confidentiality* refers to the prevention of unauthorized disclosure of information and is often associated with data breaches because attackers seek to obtain information without proper authorization.

Integrity refers to the guarantee that the message that is sent is the same as the message received and that the message is not altered in transit. It crucial importance follows from the fact that any alteration could cause internal chaos for the concerned entity and its operations.

Availability refers to the guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of the location of the user.

This definition has been proposed by ENISAon the basis of a "contextual definition". Such an approach has been chosen as the cybersecurity is perceived as a broad and evolving term. This leads to the conclusion that while choosing a specific definition may allow to maintain comprehensibility, affected parties and the drafters of relevant legislation should choose a definition that meets their specific needs in the particular context" [18].

3.3 Features and goals of the cybersecurity law

The cybersecurity threats that the international community, states and private persons are struggling with require the norm-builders to define adequate measures that would address these persistent dangers.

We can set out the features, scope and goals of cybersecurity law with the help of certain "boundaries" defining the default values and approaches that should be reflected in the content of legal rules focused on ensuring the cybersecurity. We will do that by answering the following questions:

What we secure (subject -matter of the regulation);
Whom we secure (scope of entities affected),
How we secure (forms and methods of legal regulation),
When we secure (timeframe of the cybersecurity measures to be taken),
Why we secure (reasons for the cybersecurity protection by the means of law) [19].

Ad **1**) First of all, it is necessary to determine what all should encompass the legal regulation. Based on the constant increase of significant and damaging cybersecurity incidents and the increased vulnerability due to the connection of everyday devices to the internet, cybersecurity law cannot be reduced only to data security and its protection but must also include the systems and networks of both public and private sector. Therefore, the cybersecurity law in general should aim to promote the complex scope of the CIA trial (as explained above) - confidentiality, integrity and availability of information, systems and networks. As Kosseff states:" A focus on integrity and availability is particularly important in the Internet of Things era, as everyday devices, ranging from medical devices to kitchen appliances to automobiles, are connected to the Internet. Attacks of these have only little to do with confidentiality of information, instead involve the mainly integrity and availability of systems and networks."[19]

Ad **2**) Answering this question means primarily defining the scope and structure of entities that may be affected by cyberspace attacks. Today, it is quite evident that threats of cybersecurity breaches are directed against entities in both the public and private sectors. It is equally clear the security of public infrastructure will face quite different legal requirements than the security of private infrastructure The public sector is partly under the influence of principles and rules forming part of the penal and the international (public) law of cybersecurity protection, although in this space, the states have already lost their monopoly on war-making, as well as the private persons are losing their monopoly on committing crime and terrorism[20]. Similarly, it is often difficult

to isolate in practice the target of an attack as exclusively private or exclusively public entity, just as it is often difficult to attribute an attack to a state or non-state actor. Therefore, cybersecurity legislation must consider the security of public and private infrastructure and information comprehensively and ensure that control operates across sectors such as finance, healthcare, energy or defense.

Ad **3**) Whereas the definition of the subject matter of regulation (sub a) seems clear and obvious, it will be much more difficult to determine - especially in the context of the law-making procedure - how (i.e. by what means and to which consequences) we will cover the subject matter by legal rules. As a default presumption, we can consider the regulatory role of law as crucial especially in the areas of defining the harmful consequences that the legal rules seek to prevent.

a. the different types of damage caused by modern cyber-attacks
b. quantification, i.e. scaling the intensity of consequences
c. provision of corresponding legal remedies;

Defining duties and precautions on how to prevent or eliminate the harmful consequences of breaches;

Defining the control/monitoring powers of the bodies responsible for supervising the fulfilment of legal obligations by the persons concerned;

Defining the liability of these persons for causing harm due to their failure to comply with their legal duties;

Determining of penalties imposed by public bodies for violation of the legal obligations imposed by the law.

When adopting rules forming the content of cybersecurity law, the lawmaker has two options on how to approach the persons addressed by them - to base their efficiency on coercion (so-called regulatory deterrence)[19] or to base the latter on the incentives and will of the persons concerned to cooperate (the so-called cooperative approach). Since both these approaches represent to a certain degree extreme solutions granting only a limited success, cybersecurity law should consist rather in a mix of penalty-based regulatory deterrence along with cooperation and incentives.

Ad **4**) In determining the timeframe for the impact of legal rules aimed at cybersecurity, we need to consider whether the legislation is intended to cover events that have already occurred or should attempt to build resilience and defenses to prevent the attacks from occurring in the future. We must stress that the rules of cybersecurity law should be as forward-looking as possible. A set of obligations aimed at prevention should, if possible, prevent cyber incidents from occurring in the first place. If they do occur, the purpose of regulation is to minimize their scope and to enable, as quickly as possible, the remedy of harmful consequences caused by them (and thereby prevent future attacks or threats). The need for forward-looking cyber legislation is most evident when emphasizing the cyber resilience as the ability to withstand and recover rapidly from attacks, accidents or naturally occurring threats [21].

Ad5) The ultimate goal of a comprehensive regulation is undoubtedly to prevent and mitigate the harm caused. On the public level this includes initiation of mutual cooperation between states solving one and the same problem - the threat to their national security interests (beside threats to the state defense capability aimed at its critical infrastructure, it includes such values as a trustworthy democratic social system and/or the rule of law). On the level of individuals, the first reason is to prevent and mitigate the violation of their fundamental rights to privacy, on the level of legal persons then mainly to prevent the economic harm caused to intangible corporate assets such as goodwill or intellectual property rights.

4. European Policy and Legal Instruments for the Protection of Cybersecurity

Cybersecurity across the whole EU is essential for the citizens to have confidence in technological innovations, connectivity and automation, to benefit and desire to use them, while their fundamental rights and freedoms, in particular the right to privacy and data protection and freedom of expression and information, will be secured[22].

However, most academic work on EU cyber security strategy points out how difficult it is to map exactly the policy and legislative environment for cybersecurity. As stated in the briefing paper *Challenges to effective EU cybersecurity policy*:

"The EU's cyber ecosystem is complex and multi-layered, cuts across an array of internal policy areas, like justice and home affairs, the digital single market and research policies. In external policy, cybersecurity features in diplomacy, and is increasingly part of the EU's emerging defense policy. Bringing all its disparate components together is no small challenge."[23]

The legislative and policy environment in the field ensuring the cybersecurity is a complex one due to the numerous areas involved and is subject to frequent changes in relatively short intervals, mainly in view of the technological progress. Given this uneasy situation - and also due to the scope of our paper - it is not possible to

analyze every and all EU policy and legislative acts and documents. Therefore, the following chapters mention only the most important strategic policy and legislative acts in the field of EU cybersecurity.

4.1 EU Cyber Security Strategy and related policy documents

In 2013, the European Union institutions published a joint communication that can be seen as the cornerstone of the EU cybersecurity strategy. The joint communication begins by describing the links between cyberspace and our daily lives, highlighting the enormous benefits but also the vulnerabilities[24].

Any EU strategy must include all aspects of cyberspace to ensure a comprehensive approach to tackling the related and follow-up issues. This Strategy therefore first clarifies the principles that should guide cybersecurity policy in the EU and internationally to protect needs, values and human rights.

In developing the strategy, the Commission has defined several values and areas that fall under the concept of cyber security and its broader context:

1. **Protecting fundamental rights, freedom of expression, personal data and privacy;**

Access for all;

Democratic and efficient multi-stakeholder governance;

Shared responsibility to ensure security.

The view of the ENISA study, subsequently published on the issue of cyberspace, starts with the EU's core values of democracy and human rights and continues down to the basic needs of the protection of citizens [25].

Seven years after the publication of the first strategy, the EU Commission has taken a further step towards a more coherent and comprehensive strategy by publishing a new cybersecurity strategy document. [26]

The Communication states in its introduction:

"Cyber security is an integral part of the Europeans' security. Whether it is connected devices, electricity grids, or banks, aircraft, public administrations or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity. Cybersecurity is therefore essential for building a resilient, green and digital Europe."[26]

Following the progress achieved under the previous strategies, document contains concrete proposals for deploying three principal instruments –regulatory, investment and policy instruments – to address three areas of EU action:

1. **resilience, technological sovereignty and leadership,**

Building operational capacity to prevent, deter and respond; and **a**dvancing global and open cyberspace.

Within the EU Cyber Defense Policy Framework (CDPF) 2018 Update the EU designated cyberspace as an area of military operations. 'Military Vision and Strategy on Cyberspace as an Area of Operations', a document adopted in 2021, sets out the framework conditions and describes the objectives, modalities and means needed to exploit cyberspace as an area of operations in support of the EU's Common Security and Defense Policy.[27] Cyber defense and the exploitation of related capabilities across the full spectrum of military operations in cyberspace is a national competence of Member States, underpinned by a broader architecture including, inter alia, a strong industrial base supported by capability development at the level of the EU as a whole.

The Joint Communication on an EU Cyber Defense Policy adopted on 10 November 2022 announced an EU Cyber Solidarity Initiative with the following objectives:

Strengthening civilian detection and situational awareness capabilities developed for the protection of EU critical infrastructure in the form of Security Operations Centers (SOC),

support the gradual set-up of an EU-level cyber reserve with services from trusted private providers and testing of critical entities for potential vulnerabilities based on EU risk assessments [28]

Significant cybersecurity incidents can be too disruptive for a single or several affected Member States to handle alone. They can also form part of larger hybrid attacks carried out by third countries with the aim of destabilizing the economy and society, to weaken critical infrastructure needed to ensure the security of the EU or to undermine and harm the functioning of democracies, including through attacks on election infrastructures.

This is the *raisond'etre* of the EU's common cyber defense policy.

4.2 Role of the EU law in ensuring the cybersecurity and main legal acts in this area

It is evident from the above that in order to meet appropriately the EU's cybersecurity policy objectives through the measures taken by individual Member States, their goals, instruments and limits of permissibility must be defined by the rules of EU law. It is useful to recall the main reasons for the need to establish a legal

framework that would be applied uniformly by all Member States through their harmonized national legislation and the measures adopted by national executive and/or the judiciary bodies:

cross-border impact of the activities undertaken by national authorities of a State, affecting all entities under its jurisdiction. Due to the threats posed by attacks against the cybersecurity, these state activities form part of a national security policy with defined strategies and priorities in their implementation;

The interconnection of enterprises and other private entities operating within the internal (digital) market, where measures taken by the supranational management of a corporate structure (based in one Member State) have a domino effect of spreading to all its components in other Member States without any legal barriers imposed by their national laws;

The standards developed by standardization bodies for measures aimed at ensuring cybersecurity do not respect either the "national domain" of the state under which these bodies operate or the statutory provisions they must comply with;

The legal remedies used by private individuals in order to protect their rights and interests threatened or injured by cybersecurity attacks must be applicable and enforceable across the jurisdictions of all Member States in which the individual seeks redress for the harm suffered – whereas the concept of 'harm' must be understood in the broadest possible sense, i.e. including (i) harm caused by violations resulting from the conduct of perpetrators of cybersecurity attacks (ii) resulting from the failure to provide the protection guaranteed by the legal standards for the protection of their rights and legitimate interests, and (iii) harm that may arise from exceeding or misusing the powers of state authorities when protecting public values in the context of ensuring the cybersecurity.

It is therefore only logical that in order to create a framework for the EU cybersecurity law aimed at ensuring a harmonized approach by Member States to the issues falling within its concept, several regulations and directives have been adopted in the last decade, often in a relatively short time span. Let´s look at some of them in more detail.

4.2.1 EU Cyber Security Act I (Regulation 526/2013)

The goal of the Regulation (EU) No 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA)[29], called as the EU Cybersecurity Act I, was to ensure cyber resilience, trust and security within the society and/or for the users of information and communication technology products, services and processes (hereinafter "ICT" products) by creating a certification system that would prevent cyber-attacks or vulnerabilities, as well as strengthen the level of security of ICT products. In order to achieve this ambitious target, the ENISA Agency was empowered to promote the cyber-hygiene within the cybersecurity ecosystem, strengthen the cooperation between Member States and EU institutions, offices and agencies. ENISA shall also support the awareness, education and exchange of best practices between all these bodies.

The Agency is expected to play a key role in detecting, preventing and remedying the existing or potential vulnerabilities in order to reduce the risk of cybersecurity attacks. In order to accomplish this task, the Regulation contains rules for the implementation of a European cybersecurity framework, for the award of European cybersecurity certificates and declarations of conformity for ICT products that will be recognized and used in all Member States. At the same time, to grant the transparency and efficiency of the ENISA, the Agency equipped with autonomy and independence, including its own sufficient and autonomous budget.

In summary, the main purpose and scope of the EU Cybersecurity Act I was to establish European cybersecurity certification schemes that granting that ICT products certified under these schemes would meet specific requirements in accordance with the state of the art and be capable to prevent cyber threat attacks and/or risks during the life cycle of these products. All this shall be implemented at Union level and with the support of the Member States that shall designate their national cybersecurity certification authorities supervising the compliance of this Regulation.

The Regulation was repealed on 17.10.2024 and replaced by Regulation 881/2019 (see below sub 4.2.4)

4.2.2 Network and Cyber Security Directive (NIS 1 , Directive 1148/2016)

Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [30], also referred to by the acronym NIS 1 (Network Information Security) was adopted by the EU with the aim of ensuring an adequate level of security of information systems and networks. The main purpose of the Directive was to harmonize the EU Member States' legislation in the field of cyber security. The NIS Directive 1 came into force in 2016 and set out, in particular, the following requirements:

Adoption of national strategies - Member States were required to adopt a strategy for network and information systems security,

Establishment of a central authority at the Member State level - all states will establish national authorities to manage the cybersecurity agenda,

Establishing a Computer Security Incident Response Team (CSIRT), a capability set up for the purpose of assisting in responding to computer security-related incidents. Put in simple words, it is a group of IT professionals that provide organizations with services and support.

The Directive was repealed on 17.10.2024 and replaced by Directive 2022/2555, NIS 2 (see below sub 4.2.5).

4.2.3 Cybersecurity and ENISA Act II (Regulation 881/2019)

In line with the adopted policy on Cybersecurity Strategy, the EU has modernized and expanded the legal framework for protection of cybersecurity and adoptedthe EU Regulation 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification [31], called as the Cybersecurity Act II, replacing the previous Cybersecurity Act I of 2013(see above sub 4.2.1).

The main objective of this Regulation was to establish a uniform system for all 27 Member States to certify cybersecurity features of ICT products in order to eliminate the fragmentation of standards and procedures existing in the EU internal market. To achieve this objective, the Regulation entrusted the already existing Agency ENISA with the management and coordination role in the certification process.

According to the Regulation, it is very important that the European cybersecurity certification framework is implemented uniformly in all Member States to avoid "certificate trading" based on different levels of sophistication in different Member States.

The European cybersecurity certification schemes aim at ensuring that the ICT products certified thereunder meet specific requirements regarding the availability, authenticity, integrity and confidentiality of the data stored, transmitted or processed or related functions or services offered by or accessible through the ICT products during their entire life cycle.

The European Cybersecurity Candidate Certification Scheme (EUCC scheme) based on common criteria is also proposed by ENISA. It is based on the Common Criteria, the Common Methodology for Information Technology Security Assessment and the corresponding ISO/IEC 15408 and ISO/IEC 18045 standards respectively. This scheme is aimed at the ICT area in general. Certification under the Regulation is voluntary and the European Commission has been tasked with assessing whether a mandatory certification is necessary for certain categories of products and/or services.

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 is available for vendors since 27 February 2025. The scheme will apply EU-wide, on a voluntarybasis, and focuses on certifying the cybersecurity of ICT products in their lifecycle.

The effect of the certification should be the increase of trust in ICT products, which is essential for the European Digital Single Market. This is why, for example, the mandatory certification of the so-called internet of things (IoT) products is under consideration that fall at present under the ICT product category [32]. The national certification bodies called Conformity Assessment Bodies (CAB) shall facilitate the creation of risk-based certification schemes as a comprehensive set of rules, cybersecurity standards, technical requirements and procedures that reduce the risk of fragmentation of the single market, enable vendors to trade across the EU and support users in understanding product security features. The CAB will become an internationally recognized certification body for its fields of activity.

The EU Cybersecurity Act II emphasizes the categorization of products and services based on their uses and their cyber capabilities. Such categorization makes relatively straightforward the identifying of cybersecurity requirements, relevant standards, technical specifications, assessment methods and assurance levels. According to the Act, the self-assessment process for the basic assurance level reduces the requirements for certification of common products [33].

The EU-widely recognized certificate ideally falls into three levels of assurance that are appropriate to the levels of risk associated with the intended use of IoT products and reflect the market requirements (time, cost and performance). ENISA recommends the use of existing technical specifications and standards (European and international) as guidance to determine the levels of assurance, the EU Declaration of Conformity and the baseline for certification [34]. This allows for a non-discriminatory certification system with common standards promoting cooperation between certification bodies in different Member States.

4.2.4 Directive on measures for a high common level of cybersecurity across the Union (NIS2, Directive 2022/2555)

In view of, among other things, the dramatic increase of cyber-attacks and their impact on the functioning of enterprises and the society as a whole, the need for extended regulation around the cybersecurity became urgent. The EU responded by the adoption of Directive 2022/2555 of 14 December 2022on measures for a high common level of cybersecurity across the Union (abbreviated as "NIS 2 Directive") [35].The Directive brings a significant extension of the range of entities subject to the obligation - it now also applies to medium and large enterprises in the Member States falling within regulated sectors such as energy, transport, healthcare, selected IT services or manufacturing, including the automotive industry. The Directive also introduces new duties for the entities concerned, such as the obligation to manage risks, to control supply chains/relationships or to comply properly with the notification obligation.

The Directive with transposition deadline for Member States by October 2024, replaces the previous NIS1 Directive (although only six years old, see above sub 4.2.2.). As regards main provisions, the Directive extends its scope of regulation and deepens the duties of both public and private sector entities in the field of cybersecurity. The principial goals remain to ensure the high level of cybersecurity, toimprove the resilience ofboth public and private sectors and ensure responsiveness to security threats and attacks. We can sum up the main changes brought by NIS 2 as follows:

setting up the European Cyber Crises Liaison Organization Network to deal with cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on the sectors covered by the directive, more detailed regulation of remedies and sanctions to ensure enforcement of the directive.

updating the list of sectors and activities covered by the Directive,

Size limitation rule - medium and large organizations that are included in the lists of sectors and activities will now be subject to the Directive,

a higher level of risk management,

Simplifying mandatory reporting of cyber incidents to the national CSIRT,

compliance with DORA and CER legislation (see further chapters 4.2.5 and 4.2.6)).

The Directive came into force as of October 17, 2024.

4.2.5 Critical Entity Resilience Directive (CER, Directive 2022/2557)

Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities is also known as the CER Directive.[36]It refers to a set of European Union directives and recommendations that aim to reduce the vulnerability and strengthen the physical resilience of critical entities to various threats. This Directive is an update and replacement of the previous European Critical Infrastructure Directive 2008/114/EC, which addressed to selected sectors provisions on only certain aspects of resilience. The rules of CER Directive aim to strengthen the resilience of critical entities to various threats, including cyber- incidents that may be caused by, among other things, natural disasters or human-made threats.

In the context of these objectives, EU Member States must adopt and implement a national strategy for increasing the resilience of critical entities, whereby the affected bodies will be required to carry out risk assessments at least once every four years - they will be responsible for identifying relevant risks that may significantly undermine the delivery of their services, as well as taking appropriate action to ensure a higher level of their own resilience. Each Member State must ensure that its national authorities have the powers, resources and means to carry out their supervisory tasks, including conducting on-site inspections of critical entities and introducing penalties for non-compliance as part of an enforcement mechanism. Specific sanctions are to be defined by Member States legislation within two years of the entry into force of the Directive.

The Directive came into force as of October 18, 2024.

4.2.6 Regulation on digital operational resilience in the financial sector (DORA, Directive 2022/2554)

Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector [37] is also known as the as DORA Directive. The aim of this comprehensive regulation is to increase the cybersecurity, address, respond to and recover from any disruption or threat related to information and communication technologies (ICT) and improve digital operational resilience in the European financial market.

Banks, credit institutions, insurance companies, securities dealers, investment firms and funds, and service providers for account information, crypto assets, data reporting, crowdfunding and ICT third parties are required to comply with the directive provisions.

DORA establishes a strict regulatory framework aimed at preventing cyber threats and disruptions, detecting impending attacks and responding to actual attacks. The main duties and responsibilities under the regulation include:

Focus on ICT risk management: the DORA requires the implementation of a comprehensive ICT risk management framework that includes vulnerability assessments, mitigation strategies and ongoing monitoring.

Selection of third parties: due to the interconnectedness of the financial system, DORA also focuses on managing third-party risk as an integral component of their overall ICT risk. Financial institutions must conduct thorough due diligence on them and, where possible, use only DORA-compliant third parties as service providers in order to strengthen the overall security level of the financial sector's operations.

Digital operational resilience testing: the DORA imposes an obligation to regularly test digital operational resilience capabilities and requires management systems to be in place to monitor and report all significant ICT incidents to the relevant authorities.

The implementation of the Regulation is expected to bring substantial benefits, not only for individual institutions but for the entire financial sector, especially:

Improvement of consumer protection: increased digital resilience means a safer financial environment, protection of sensitive customer data and boosting consumer confidence.

Reduction of systemic risk: DORA strengthens the overall resilience of the financial sector and minimizes the impact of cyber-attacks and disruption on the wider economy.

The Directive came into force as of January 17, 2025

4.2.7 Regulation on adoption of the European common criteria-based cybersecurity certification scheme (Implementing Regulation 2024/482)

Regulation 2024/482on adoption of the European common criteria-based cybersecurity certification scheme is implementing regulation setting out rules for applying Regulation 2019/881 (see above sub 4.2.3) for the European common criteria-based cybersecurity certification scheme (EUCC) [38]. The EUCC is a framework for the assessment and certification of cybersecurity of products and ICT protection profiles. It aims to ensure that ICT products meet the strict security standards through an organized process that seeks to enhance cybersecurity, achieve uniformity across the European Union (EU) and provide a reliable certification. The EUCC is based on the Senior Officials Group on Information Systems Security ("SOG-IS") Mutual Recognition Agreement on Information Technology Security Certificates.

Ensuring cybersecurity at different levels, in different areas, with different scopes of protection and with different goals has over time become the subject of highly sophisticated services provided by entities that have practical experience in this field, have developed the know-how and, moreover, have the necessary technological equipment. In this context, we often encounter the term *managed security services* (in more detail, see Chapter 6.1 below). The managed security services are services that provide aid in performing activities related to the management of cybersecurity risks of the entities requesting these services. With the increasing complexity of security measures, the technological complexity of the process and the constant need to update the procedures, these services are becoming increasingly important not only in preventing intrusions but in mitigating the consequences of cybersecurity incidents.

Within 12 months of the entry into force of the Regulation, national cybersecurity certification schemes must adapt to the EUCC and terminate their existing procedures. National certification procedures launched during this period must be terminated within 24 months after the entry into force of the Regulation.

The Implementing Regulation is applicable from February 27, 2025.

4.3 Further EU legislation related to cybersecurity law

The EU Cybersecurity Act II is at present one of the cornerstones of the EU cybersecurity law aiming to improve the data security. These efforts fall within the broader legislative concept of the Digital Single Market (DSM) which started already by the adoption of the NIS1 Directive, since 2016 the first set of EU-wide legal rules on the network and information security (see above sub 4.2.2). The Directive put the basis for the notification duty and security requirements for the providers of essential services and digital service providers, including the cloud service providers.

The Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, better-known General Data Protection Regulation (GDPR) [39], came into force in May 2018. It aims to protect the personal data and privacy of EU citizens and simplifies the regulatory process for international organizations. It requires the data administrators and processors to follow certain protocols and put measures in place to ensure that the data cannot become publicly available without providing explicit and informed consent.

Similarly, the proposal of a regulation concerning the respect for private life and the protection of personal data in electronic communications was drafted. It was intended to replace the existing Directive 2002/58/ECconcerning the processing of personal data and the protection of privacy in the electronic communications sector[40] with the aim of harmonizing and strengthening citizens' rights and defining the

practices permitted for participants in the European digital market. It focused on the regulation of electronic communications within the EU and dealt with online communications, internet tracking technologies, and electronic direct marketing. In February 2025, however, the European Commission announced in its 2025 work program that it would withdraw the proposal for this new regulation.

The adoption of the EU Cybersecurity Act II has not affected some of the existing sectoral certification schemes. These include ISO 27001, Germany's BSI C5 and France's SecNumCloud, and PCI - DSS, CSA Cloud Control Matrix, NIST 800-53, SOC 2 Trust Services Criteria, However, it can be assumed that many of these previously established systems will be designed and subsequently approved as EUCC (see above sub 4.2.7)[41].

4.4 Legal tools for ensuring of cybersecurity in EU Member States

If we consider the rule of law as the principle that any democratic society is obliged to develop and protect, the means for the safeguarding of cybersecurity that are designed, enabled and/or tolerated by the State must be limited by the commitment to the protection of the individual's right to privacy. This premise cannot be affected by the bare fact that cybersecurity intruders, particularly the perpetrators of cybersecurity crimes, do not otherwise feel restrained by these legal boundaries.

In other words, the principle of "the end justifies the means" cannot apply to measures taken by state authorities against cybersecurity intruders, as these measures must always be kept *intra legem*. This is a fundamental obligation of States expected by all citizens to be fulfilled. It does not mean that the State and its authorities will always remain one step behind the cybersecurity intruders, but the requirement of legal certainty must simply at any time prevail when deciding about the ways and means of dealing with the cybersecurity threats.

Similarly, the above-mentioned principle of the rule of law is binding for the ways and measures through which the EU law is implemented to the national legal environment of the Member States. Therefore, the latter also concerns the deployment of the objectives, tools and how they can be used to ensure cybersecurity on the basis of existing EU legislation. It is a fundamental requirement for the national law of the EU Member States that the goals, instruments and forms defined by the national law must be derived from the rules of EU law. As in all areas with defined EU competences, the directly effective Union legislative acts related to the cybersecurity replace the national rules with EU rules uniformly applicable by all Member States. In the case of indirectly effective EU law, i.e. the EU directives, States are obliged to modify or amend their existing national law accordingly within the respective transposition period. The transposition period is the deadline for incorporating the EU legislation into the national law in a way that ensures, on the one hand, that the EU-harmonized rules shall have uniform effects in all 27 Member States ,and, on the other hand, that specific national features and the practice of their implementation by national authorities and other institutions may be taken into account.

Among the reasons and circumstances determining the above relationship between the EU law and national laws we can stress in particular the fact that the measures of the national state authorities relating to its citizens and other entities underlying its jurisdiction must have cross-border effects, due, inter alia, to the free movement of persons within the EU. Depending on the nature of the threats caused by the cybersecurity breaches and attacks, the above measures form part of the national security policy of each of the member States. These policies, accordingly, have to be coordinated in terms of the definition of their strategies, priorities and the means used for their implementation.

Further reasons of the need to establish a legal framework applicable uniformly by all Member States when adopting their harmonized national legislation are linked with the arguments already stated above in Chapter 4.2.

5. Quo Vadiseu Cybersecurity Law?

Recently, the legal framework for the protection of cyber-security under EU law has been further developed due to the adoption of several legal acts responding to the technology progress in the field of ICT. In the following part of the paper, we try to characterize briefly these acts and the principial changes of the EU cybersecurity law resulting there from.

5.1 Amendment to Regulation 2019/881 (Cybersecurity Act II) of December 2024

The existing core source of EU cybersecurity law has been extended by the EU Regulation 2025/37 of 19 December 2024 amending the Cybersecurity Act II by including the issue of managed security services within the scope of mandatory regulation implemented by national legislation(as provided by the Implementing EU Regulation on Cybersecurity Certification Scheme, see chapter 4.2.8 above)

The purpose of the extension to the legal regulation is to empower the EU Commission to adopt, through Commission implementing acts, the EU cybersecurity certification schemes for the managed security services,

in addition to the ICT products, services and procedures already covered by the Cybersecurity Act II. The reason for the regulation extension is that the managed security services play an increasingly important role in preventing cybersecurity incidents and mitigating their impact.

Certification of the managed security services is important not only for the selection process for the EU cyber security reserve established by Regulation No. 2025/38 (see Chapter 5.3 below) but serves also as an essential quality indicator for private and public entities intending to purchase these services. Given the critical nature of managed security services and the sensitivity of the data processed, their certification could provide important clues and assurances to potential customers concerning the credibility of these services. The aim of the European cybersecurity certification schemes for the managed security services is to avoid fragmentation of the EU internal market. Thus, we can identify as the aim of this Regulation therefore aims to support and develop the internal market operation.

Providers of the managed security service are considered essential and important entities belonging to the sectors of high criticality within the meaning of NIS 2 Directive (see chapter 4.2.4 above). They have a particularly important role in assisting public and private entities in their efforts to prevent, detect, respond to or recover from incidents in areas such as incident response, penetration testing (authorized simulated cyberattack on a computer system, performed to evaluate the security of the system) [42], security audits and consultancy.

European cybersecurity certification schemes for managed security services should contribute to the availability of secure and high-quality services that guarantee a safe digital transformation and to the achievement of the objectives as defined by the Digital Decade Policy Program 2030 [43]. Some EU Member States have already started to adopt certification schemes for managed security services. Therefore, the risk of fragmentation of the internal market for managed security services is increasing due to the lack of uniformity of these schemes within the Union. By creating European cybersecurity certification schemes for these services, the Regulation EU 37/2025 prevents further in this respect.

The aim of the amendment is also to improve the quality of managed security services and increase their comparability. The amendment shall thus allow the essential and critical entities to exercise greater care in the selection of their managed security services provider as required by the NIS 2 Directive.

5.2 Commission Implementing Regulation to NIS2 Directive (Regulation 2024/2690)

As required by NIS2 (see above sub 4.2.4), the Commission Implementing Regulation (EU) 2024/2690 was published in order to set out "technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers" [44]

One of the key elements of the new Regulation is the enhanced technical and methodological requirements. The Regulation specifies specific standards that Member States and critical infrastructure entities must meet to ensure an adequate level of cyber security. These requirements cover:

Implementation of technical measures to protect systems from cyber-attacks, including firewalls, anti-virus programs and data encryption.

Introduction of measures to protect sensitive and personal data, including rules for storage, transmission and processing.

Implementing of procedures for regular evaluation and improvement of security measures, including staff training and security audits.

The Implementing Regulation is divided into two parts:

1. The first part (Articles 3-13) specifies the notion of "significant incidents" regarding each of the reference sector (DNS service providers, TLD name registries, etc.). These rules are very important as they specify the thresholds for reporting incidents to the authorities,

The second part (Annex) specifies in more detail the security measures listed by the Article 21 of the NIS 2 Directive.

As regards the definitions of "significant incidents", the organizations included by NIS2 will have to update their incident management procedures accordingly. They need to have an incident management phase to assess whether an incident falls within the thresholds indicated and, if so, must be notified to the national authority.[45]

As a result, this Implementing Regulation represents a significant step forward in strengthening cybersecurity in the EU. The enhanced technical requirements, new certification procedures, stricter sanctions

and enhanced cooperation between Member States aim to raise the overall level of cybersecurity and ensure that all actors are better prepared to face cyber threats.

5.3 Act on Cybersecurity Solidarity (Regulation 2025/38)

The Regulation 2025/38 of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (*Cyber Solidarity Act*) [46] constitutes the result of Europe's efforts to strengthen its institutional framework for cybersecurity activities and measures.

With the adopted Regulation, The EU responds to the calls from Member States to strengthen the EU's cyber resilience and fulfilling its commitment to prepare an EU Cyber Solidarity Initiative, as expressed in the 2022 Joint Communication on Cyber-defense. The EU Cyber Solidarity Act aims to strengthen the EU's capacity to detect, prepare for and respond to major cyber security threats and attacks. The Act includes two important elements:

European Cybersecurity Alert System consisting of security operations centers linked across the EU and comprehensive mechanism for cybersecurity emergencies to improve the EU's cyber resilience.

The Cyber security alert system improves the cyber threat detection, analysis and response. This system consists of national and cross-border security operations centers across the EU These are the entities entrusted by sharing information and tasked with detecting and acting on cyber threats.

Furthermore, an EU Cybersecurity Reserve is established to assist designated users (Member States' cyber crisis management authorities as well as authorities of third countries associated with the Digital Europe Program for cyber crisis management), upon request, in responding to or providing support in responding to and initiating recovery from major cyber security incidents, large-scale cyber security incidents and incidents similar to large-scale cyber security incidents.[47]

The Cyber Solidarity Act, together with the Cyber Resilience Act and the NIS Directive2, is one of the cornerstones of the EU Cybersecurity Strategy.

6. Final Remarks

In conclusion of the present paper, we consider it appropriate to formulate some summary remarks and recommendations for the future, which arise from our previous discussion and concern the state and future needs of the EU cybersecurity law.

1. **Legal regulation of cybersecurity will continue to keep its importance in view of the potential implications for the fundamental human rights.**

This conclusion follows from the arguments presented in the opening part of our paper. The importance of cybersecurity is beyond doubt, and its legal regulation is necessary in view of the potential consequences of cyber incidents in terms of restricting individuals' fundamental rights to privacy and personal data protection, as well as freedom of expression and information. This is also emphasized by the already quoted 2020 EU Recommendation:

"Improving cybersecurity rules is essential to enable people to trust, use and benefit from innovation, connectivity and automation, and to protect fundamental rights and freedoms, including the right to privacy and the protection of personal data and freedom of expression and information." [48]

The rules of cybersecurity law should combine a coercive approach (regulatory deterrence) and cooperative approach when regulating the behavior of entities (persons) obliged

The rules of cybersecurity law must exploit both approaches to the entities (persons) under regulation - approach where the effect of regulation is based on coercion (threat of sanctions) and approach where the effect is based on encouraging the willingness and/or readiness to cooperate (cooperative approach) of the entities obliged. It would be wrong to overestimate coercion as a method of regulation, as there is enough space for stimulation of the cooperative attitude as concerns the cybersecurity, particularly in view of a principal unity of interests of all the entities addressed by legal rules. The legal systems of the EU and its Member States are expected to continue imposing sanctions on constituting a breach of the entities' duties and undermine thereby the cybersecurity in sector under regulations. However, the cybersecurity law should ultimately aim to encourage private entities (enterprises) to invest in cybersecurity preventive measures.

The European Union plays a crucial role in strengthening cybersecurity of all Member States.

The measures adopted by the European Union appear to be adequate and proportionate with the view to the cross-border nature of cyber-attacks and, in accordance with competence to adopt delegated acts, underline the fact that protection cannot be efficiently secured by rules adopted at the level of individual Member States, either at central, regional or local levels. On the contrary, the level of Union legal rules is better suited for the

achievement of these goals. Therefore, the recent legal acts of the EU are directed at promoting the harmonization of the single market for cybersecurity products and services as necessary measures. As the ultimate goal remains the introduction and implementation of a single European cybersecurity certification and standards as a common basis for all Member States.

The development of cybersecurity standards and certification at the EU level will "promote the development of a 'made in Europe' cybersecurity industry in the EU [...] to enhance the security of digital systems and guarantee the fundamental rights of EU citizens, while increasing job creation and Europe's competitiveness in the global market." [49]

As regards the last decade, the EU institutions have undertaken substantial efforts in the legislative field to fill the existing gaps and space for improvement. They have extensively worked on preparation and submitting drafts for new EU legislation. As the best example of the success of these efforts may serve the Network and Information Security Directive (NIS 2) and the Cyber Security Act II, setting up the new institution ENISA entrusted with the task to build a strong and secure digital environment.

Although the ensuring of cybersecurity is essentially a technological issue, the importance of a robust legal framework (effectiveness of legal norms) is equally important

The NIS 2 Directive includes a definition of cyber security as: "the ability of network and information systems to withstand, at a given level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services offered by or accessible through those network and information systems".

Given the close link between measures adopted to ensure cybersecurity and the potential restriction of fundamental human rights, the EU legal framework for which is de-rived from the Charter of Fundamental Rights of the European Union, it is essential to regulate legal safeguards for the protection of fundamental rights as part of the rules on cybersecurity. These safeguards constitute a coherent system of orders, prohibitions and restrictions with accompanying legal sanctions as a consequence of non-compliance. There is therefore a unifying framework for national laws of the Member States, essential for both the organizational (institutional) and regulatory functions of law in this dynamically developing area of social and economic relations.

The use of standards is crucial for an optimal approach to the ensuring of cybersecurity

The importance of unified standards and certifications ensuring a procedural framework for the implementation of technical and organizational measures for cybersecurity cannot be underestimated. There is no doubt that the implementation of EU standards in the field of cybersecurity will lead to the harmonization of assessment criteria and corrective measures in all EU Member States in accordance with the harmonized cybersecurity requirements. The synchronized transposition of EU regulations by national legislation EU Member States as consistently as possible remains the most reliable guarantee of the effectiveness of the cybersecurity law both for the protection of national security of states and the protection of fundamental human rights against potential or actual cyber threats.

7. Conclusion

In the very conclusion we should note that in the real terms, however, the adoption and implementation of measures for the strengthening of cybersecurity faces the same problems that exist in many other EU policy areas, in particular the still insufficient harmonization time plan and/or delays in complying with transposition deadlines established thereto. The consequence is a fragmented approach across Member States and lagging behind with the creation of the necessary vertical coherence at EU and national level.

In this context, it should also be noted that the application of international standardization rules, such as those of the US National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), cannot provide an adequate response, as these standards do not take into account the specific characteristics and interests of the European internal market. In this sense, the EU Cybersecurity Strategy emphasizes the importance of ETSI, CEN CENELEC, and ENISA, stressing that the EU Commission will support the development of the security standards. This work should build on the ongoing standardization efforts of European standardization organizations (CEN, CENELEC, and ETSI), the Cyber Security Coordination Group (CSCG), as well as the expertise of ENISA and other relevant actors [50].

For various reasons, the Member States show significantly diverse levels of preparedness to cope with the EU legislative frameworkdue to its continuous developments. This results, on the other side, in varying levels of protection of consumers and enterprises and undermines the overall security efforts of network and information systems security in the Union as a whole. The lack of common requirements for essential service operators and digital service providers in turn prevents the establishment of a comprehensive and resistant cooperation mechanism at the Union level [56].

Cyber security offers a striking exampleof an area where different policy sectors need to be integrated (calling for horizontal coherence) and where corresponding legal rules need to be adopted at both EU and Member State levels (calling for vertical coherence). The Member States should not lag behind in taking measures to harmonize EU and national cybersecurity law which represents an important marker in the further development of the Digital Single Market.

References

[1]. EU: *Working conditions and sustainable work*.. Eurofound, Updated 01/2023. Available online at https://www.eurofound.europa.eu/cs/publications/2022/rozsireni-prace-na-dalku-dopad-na-pracovni-podminky-predpisy
[2]. GSMA.2022. Estimate published in a document by the Telecommunications Trade Association. Available online at https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2022.pdf
[3]. ENISA. *Main Incidents in the EU and worldwide*. 2020. ENISA. Online at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents
[4]. Lagarde, C. *Estimating cyber risk for the financial sector*, IMF, 2022. Available online at https://blogs.imf.org/2022/06/22/estimating-cyber-risk-for-the-financial-sector/
[5]. Gřivna, T. et al. *Kyberkriminalita a právo* [Cybercrime and law]. 1st ed. Prague : Auditorium, 2008
[6]. Smejkal, V. *Kybernetickákriminalita* [Cybercrime]. Plzeň: Aleš Čeněk, 2015. 636 p.
[7]. Dalal, A. Cybersecurity and Privacy: Balancing Security And Individual Rights In*The Digital Age* (December 05, 2020). Available online at http://dx.doi.org/10.2139/ssrn.5171893
[8]. Enerstvedt, O.M. Protection of Privacy and Data Protection in Aviation Security. In: *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*. Springer Cham, vol. 37, 2017, pp. 25 – 29. Avaiable online at https://doi.org/10.1007/978-3-319-58139-2
[9]. Shalin Hai-Jew, Beware! A Multimodal Analysis of Cautionary Tales in Strategic Cybersecurity Messaging. In: *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, Fields, Z ed.). IGI Global, Pensylvania, 2018, pp.27-64. Available online https://www.igi-global.com/viewtitlesample.aspx?id=206779&ptid=185479&t=Safe%20Distances:%20Online%20and%20RL%20Hyper-Personal%20Relationships%20as%20Potential%20Attack%20Surfaces&isxn=9781522547631
[10]. Lukings M.; Lashkari A. H. *Understanding Cybersecurity Law and Digital Privacy*. 2021 Springer Publishing,(pp. 59 et. seq. ISBN 978-30-3088-703-2
[11]. Shafali, A.: Preserving Information Security Using Fractal-Based Cryptosystem. In: *Handbook of Research on Cyber Crime and Information Privacy*; Cruz-Cunha M. M.; Mateus-Coelho, N.:(eds.), IGI Global, 2020, Chapter 26, p. 540
[12]. Amoroso, E. *Cyber Security*, Silicon Press: New Jersey. 2006. p. 5 et seq. Available online https://dumitrudumbrava.wordpress.com/wp-content/uploads/2012/01/cyber-security.pdf
[13]. Tchiangxin, C.: The Significance of STEM Education for National Security. In *Intelligence and Law Enforcement in the 21st Century*, De Silva, E., Abeyagoonesekera, A. Security and Forensic Books, 2021, Chap. 10, p. 189
[14]. Stevens, T.: What is Cybersecurity for ?, In *Proceedings 25th International Conference on Software Engineering*," 25th International Conference on Software Engineering, 2003. Proceedings., Portland, OR, USA, 2003, p. 36 et seq.
[15]. Kemmerer R.A., Cybersecurity. In *Proceedings 25th International Conference on Software Engineering*," 25th International Conference on Software Engineering, 2003. Proceedings., Portland, OR, USA, 2003, pp.705-715.
[16]. Lere Thuto, D.: The Increased Need for Cybersecurity in Developing Countries: COVID-19 and the Adverse Cybercrime Risks Imposed In Cybersecurity Capabilities in *Developing Nations and Its Impact on Global Security*, Dawson M.; Tabona O.; Maupong,T. ; Hershley, (eds). IGI Global: Pensylvania, February, 2022, p. 218
[17]. Emergency Management Vocabulary, "*Terminology Bulletin*" 2014, no. 281,Available online http://www.bt-tb.tpsgcpwgsc.gc.ca/publications/documents/urgence-emergency.pdf
[18]. European Union Agency for Cybersecurity (ENISA).): *Definition of Cybersecurity - Gaps and overlaps in standardisation*. Heraklion, Greece: ENISA.01 July 201.5 DOI 10.2824/4069
[19]. Kosseff, J.: Defining Cybersecurity Law, (March 1, 2018). *Iowa Law Review*, Vol. 103, No. 985, 2018, p. 999et seq. Available at SSRN: https://ssrn.com/abstract=3225691

[20]. Brenner, S. W. Cyber-Threats and the Limits of Bureaucratic Control. *Minnesota Law Journal*, 2013, vol. 14, issue 1, p.150.
[21]. Dobrygowski, D.: Cyber Resilience: Everything You Need to Know, *WORLD ECON. FORUM* (July 8, 2016), https://www.weforum.org/agenda/2016/07/cyber-resilience-what-toknow
[22]. Joint Communication to the European Parliament and the Council: *An EU Cybersecurity Strategy for the Digital Decade*. 2019.,p. 4JOIN(2020)18 , OJ 52020JC0018
[23]. European Court of Auditors: *Challenges to effective EU cybersecurity policy*. Briefing Paper, 2019, p.12 Available online at https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf
[24]. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Cyber Security Strategy for the European Union: Open, Safe and Secure Cyberspace* / JOIN/2013/01 final, p.9 et seq.
[25]. Sciacca, G.: *Cybersecurity in the EU: An introduction*. 2022. UNED, available online at https://blogs.uned.es/digitaleconomy/wp-content/uploads/sites/253/2022/01/Cybersecurity-in-the-EU-an-introduction.pdf
[26]. European Commission. The *EU's Cybersecurity Strategy for the Digital Decade.* Brusels, 2020. Available online at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga
[27]. European Union: Military *Vision and Strategy on Cyberspace as a Domain of Operations.* Official document of the European External Action Service , EEAS (2021) 706 REV4
[28]. Joint Communication to the European Parliament and the Council, *EU Cyber Defense Policy* / JOIN/2022/49 final
[29]. Regulation (EU) 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA). Online https://eur-lex.europa.eu/eli/reg/2013/526/oj/eng
[30]. EU Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, online https://eur-lex.europa.eu/legal-content/CS/LSU/?uri=CELEX:32016L1148
[31]. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. Online https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
[32]. Cirne A., Sousa P. R., Resende J. S., Antunes L.: IoT security certifications: challenges and potential approaches. *Computer& Security*, May 2022, vol. 116, Art. no. 102669
[33]. European Union Agency for Cybersecurity (ENISA): *Standardisation in Support of the Cybersecurity Certification*. (Feb. 2020). Online at https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i
[34]. European Union Agency for Cybersecurity (ENISA) EU *Cybersecurity and Standardisation.* (March 2023). Online at https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20of%20AI%20and%20Standardisation.pdf
[35]. EU Directive 2022/2555 of 14 December 2022on 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 (abbreviated as "NIS 2 Directive") online https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
[36]. EU Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Online https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng
[37]. Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector. Available online https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
[38]. Implementing EU Regulation 2024/482. Available online https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=OJ:L_202400482
[39]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[40]. EU Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Online at https://eur-2lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[41]. Vostoupal, J. *Certifikacekyberbezpečnostníchtechnologií* [Certification of cyber security technologies] 2018/2019, Diploma Thesis, Brno: PrF MUNI. Brno, 2019,p.48
[42]. Henry, K.M. Penetration Testing: Protecting Networks and Systems. IT Governance Publishing , 2012
[43]. Decision (EU) 2022/2481 oftheEuropeanParliament and oftheCouncilof 14 December 2022 establishingthe Digital DecadePolicyProgramme 2030. Available online at https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng
[44]. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers Available online at https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
[45]. Gallotti, C. *NIS2: EU Commission Implementing Regulation 2690/2024*. Available online at https://www.linkedin.com/pulse/nis2-eu-commission-implementing-regulation-26902024-cesare-gallotti-12usf/
[46]. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). Online https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng
[47]. Villani, S.: The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System, *European Journal of Risk Regulation*, 2025. DOI: 10.1017/err.2025.24. Available online at https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/cyber-solidarity-act-framework-and-perspectives-for-the-new-euwide-cybersecurity-solidarity-mechanism-under-the-eu-legal-system/46B9B28588DE644A2EE10EBBAD90FA51
[48]. European Union Agency for Cybersecurity (ENISA): Best Practices for Cyber Crisis management. (2024). Available online at https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management
[49]. European Union Agency for Cybersecurity (ENISA): Guidance and gaps analysis for European standardisation. (2019). Available online at https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for european-standardisation
[50]. Herrmann, D.; Pridöhl, H. Basic Concepts and Models of Cybersecurity.in the Ethics of Cybersecurity. Loi, M. C. (Ed.), (2020) Springer Open. DOI: 10.1007/978-3-030-29053-5_2.