CRITICAL INFRASTRUCTURES: EUROPEAN CONTEXT AND EVOLUTION OF THE LAW

Francesco TRINCHILLO

University of Rome Tor Vergata, Italy

This conceptual paper aims to investigate the European regulatory framework of topic "protection of critical infrastructures", starting from the genesis of the terminology up to the examination of the contents of the most recent European legislation. The normative study, initially, focuses on the contents of Directive 2008/114/EC - the first real European legislative reference - received in Italy with Legislative Decree 61 of 2011; the second part, instead, is dedicated to the analysis of the more recent Directive (EU) 2022/2557 which represents the current European regulatory instrument aimed to regulate a theme that has become increasingly central, also in light of the growing number of attacks against Member States. Directive (EU) 2022/2557, in addition to repeal the previous one, is proposed as a much broader and more complete rule capable of providing the elements to regulate a very complex topic. The paper shows how the European Union is making great efforts not only to regulate the matter, but also to clarify its boundaries and transversal aspects.

Key words: *privacy, behavior, challenges, regulation, solutions*

1. INTRODUCTION

The most developed countries are characterized, among other things, by having extensive and sometimes very complex infrastructure systems, which, as will be analyzed below, are defined as Critical Infrastructures, such as, for example, energy distribution networks and transport infrastructures. As specified in European legislation, a critical infrastructure is not necessarily constituted by a physical infrastructure but can also be represented by an immaterial system such as an IT system, which, even if it is not easily understood, makes the protection of these systems much more complex.

Critical Infrastructures can be subject first to malfunctions, linked to breakdowns or technological problems of various origins, but also to natural disasters and intentional attacks. The globalized society that is increasingly based on a complex system of interconnection both physical and digital, now present in all sectors, has determined that a very large amount of activity depends on the correct functioning of said systems, from this has derived a

growing attention towards security, in this perspective, the concern to protect critical infrastructures has always increased. The terrorist attacks of 11 September 2001 in the United States and those that hit the subway and railways in Madrid in 2004 and in 2005 in London, have further highlighted the problem especially regarding intentional attacks. In fact, right after these events - first the United States and then Europe - have concentrated on a precise regulation of the topic, it is reiterated, of certain interest but also very complex. The attention of the countries, initially, focused - almost exclusively - on intentional attacks, especially terrorist ones; subsequently, starting from the occurrence of Hurricane Katrina in 2005, which had devastating effects on the city of New Orleans and the states of Louisiana, Alabama and Mississippi, up to the terrible flood that hit Valencia and the surrounding areas on 29 October 2024, the regulatory approach was recalibrated, reasoning in a multi-risk vision that also extended to natural disasters and technological accidents such as massive fires, explosions and dispersions of chemical or biological agents.

The European Union, in fact, today takes into consideration the totality of the risks that may arise, even if in many Member States the attention is still focused on the threat posed by terrorism. It is also true that, today, terrorist threats constitute an important alert factor for industrialized countries because, generally, they concern places of passage of large masses, such as railway stations, airports, maritime stations. It is therefore essential to provide adequate and increasingly updated legislation for the protection of Critical Infrastructures to protect the health and safety of citizens, but also to avoid undermining the economy of the Member States themselves.

2. CRITICAL INFRASTRUCTURES: FROM THE ORIGIN OF THE TERM TO THE FIRST REGULATION IN EUROPE

The term Critical Infrastructure was born in America with the enactment of the USA Patriot Act (acronym of Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), federal law of the United States of America specifically approved on 26 October 2001 to fight terrorism following the attacks of 9 September 2001 that hit New York and Washington, causing approximately 3,000 victims. In the law (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 26 October 2001, s. 1016) , the first definition of Critical

Infrastructure is reported: "the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". In Europe, however, the concept began to be formalized on 20 October 2004 with the communication 702 from the Commission to the Council and the European Parliament to prepare a global strategy for the protection of Critical Infrastructures; the document presents a series of proposals to increase Member States' prevention, preparedness and response to terrorist attacks affecting critical infrastructures. In fact, similarly to the first definition of critical infrastructures born in the United States, the European Union, defining them as those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States (Communication from the Commission to the Council and the European Parliament of 20 October 2004). It is understood, therefore, that critical infrastructures are present in many sectors of the economy, including banking and finance, transportation and distribution, energy, services, healthcare, food supply and communications as well as essential public services. For some of these sectors, we cannot strictly speak of infrastructure, but they are still networks or distribution chains that provide a product or service of strategic importance.

The European Commission identifies the types of critical infrastructures (Communication from the Commission to the Council and the European Parliament of 20 October 2004):

- Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system).
- Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet).
- Finance (e.g. banking, securities and investment).
- Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services).
- Food (e.g. safety, production means, wholesale distribution and food industry).

- Water (e.g. dams, storage, treatment and networks).
- Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems).
- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials).
- Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

The European Commission's communication 702 was followed first by the publication of communication 576 of 11.17.2005 - better called Green Paper - and then by the Communication 786 of 12 December 2006, which established the principles, objectives and contents of the European Programme for Critical Infrastructure Protection (EPCIP). Specifically, these new issues contain the following key principles that guide the implementation of the programme (Communication from the Commission of 12 December 2006):

- Subsidiarity - The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States Concerning National Critical Infrastructures.
- Complementarity - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.
- Confidentiality - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need to know basis. Information sharing regarding CI will take place in an environment of trust and security.
- Stakeholder Cooperation - All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated

as ECI as well as public authorities and other relevant bodies.

- Proportionality - measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.
- Sector-by-sector approach - Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

3. COUNCIL DIRECTIVE 2008/114/EC

The documents of 2004, 2005 and 2006 represent the theoretical basis that led to the approval of the Council Directive 2008/114/EC on 12.8.2008 "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" which in fact constitutes the first legislative reference in the European context on the theme of Critical Infrastructures. The directive, defines what is meant by Critical Infrastructure and European Critical Infrastructure (ECI): in the first case we are referring to: an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; by European Critical Infrastructures, instead, we mean: critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States (Council Directive 2008/114/EC of 8 December 2008, art.2). The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure.

The Council Directive 2008/114/EC is limited to considering only the Energy (Electricity, oil and gas) and Transport (Road, rail, maritime, air) sectors, although it is expressly stated that the list of ECI sectors in itself does not generate a generic obligation to designate an ECI in each sector (Council Directive 2008/114/EC of 8 December 2008, annex 1). This last clarification demonstrates how the Council itself recognizes that the issue of critical infrastructures is strongly complex and not easily circumscribed within a defined scope. The document provides

that each Member State identifies among its critical infrastructures those that can be designated as ECI in the sense that satisfy those cross-sectoral criteria and respond to the definitions reported above. The Council Directive does not limit to establish just this principle, but it indicates (Council Directive 2008/114/EC of 8 December 2008, annex 3) a procedure – essential but very effective - to allow each Member State to carry out an analysis with the aim of identifying only specific national critical infrastructures such as ECI; only the latter will be reported to the other Member States that may be significantly affected by such infrastructures.

According to the directive, the inter-sectoral criteria that in fact constitute the main parameter for the designation of an ECI are not generic, in fact, it is the directive itself that identifies them and groups them into the following three categories (Council Directive 2008/114/EC of 8 December 2008, art. 3), in this way as to allow the Member States have tangible and quantifiable indices:

a. casualties criterion (assessed in terms of the potential number of fatalities or injuries);
b. economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
c. public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services).

Moreover, the Council Directive defines which owners/operators of ECI "means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive" (Council Directive 2008/114/EC of 8 December 2008, art. 2) and always according to the dictates of the directive, the Member States are required to prepare an Operator Security Plan (OSP) aimed to identify the safety solutions to protect the designated ECI (Council Directive 2008/114/EC of 8 December 2008, art. 5); the contents of the OSP must comply with the following procedure (Council Directive 2008/114/EC of 8 December 2008, annex 2):

1. identification of important assets;
2. conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact;
3. identification, selection and prioritisation of countermeasures and procedures with a distinction between:

- permanent security measures, which identify indispensable security investments and means which are relevant to be always employed. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,
- graduated security measures, which can be activated according to varying risk and threat levels.

In addition to the preparation of OSP, each Member State is required to name, for each ECI identified, a Security Liasons Officer (SLO) (Council Directive 2008/114/EC of 8 December 2008, art. 6) who will act as a point of contact for safety issues between the owner/operator of the ECI and the competent authority of the Member State in order to allow maximum effectiveness for the exchange of useful information relating to the risks and threats identified.

For the role he/she is invested with, this figure must have high relational and managerial skills in addition to adequate training and technical competence that is as transversal as possible due to the nature of the problems he/she finds. The risks that arise, indeed, can be very varied, not only on a case-by-case basis, but because, sometimes, even a danger that is the object of a specific assessment can generate a chain reaction of other emergencies that, although of a totally different nature, are activated by the initial triggering event. Despite the SLO role being so important, the directive does not provide any indication on the nature and type of his/her role, his/her responsibilities and specific competences; without a doubt, it is advisable that the profile is chosen internally to the infrastructure considered in order to guarantee greater knowledge of the internal processes, this will favor the methods for implementing the actions useful for managing the activities specific to the role to be performed.

Since 2008, each Member State has implemented the Council Directive 2008/114/EC in a different way, for example Italy has approved the Legislative Decree N. 61 of 11 April 2011, which, therefore, establishes - at a national level - the guidelines for the designation of European

Critical Infrastructures identifiable on Italian territory. Moreover, this law aims to introduce the Interministerial Situation and Planning Unit (defined with Italian acronym NISP) (Legislative Decree of President of Italian Republic N. 61 of 11 April 2011, art. 4), which, among other things, is assigned the tasks for the identification and designation of the ECI (Legislative Decree of President of Italian Republic N. 61 of 11 April 2011, art. 6). In general, the contents and provisions of the decree are therefore, overall, fully aligned with the 2008 European directive, thus Italy, as a Member State, has decided to apply to the letter what has already been indicated by the Council.

4. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

After 11 years, Europe - also in light of the Covid-19 pandemic and the increasingly frequent cyber-attacks perpetrated against various critical infrastructures - decides to update the legislation by issuing, on 14 December 2022, the Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities that repeals Council Directive 2008/114/EC. With the repealing of the previous directive, a modernization of the legislation is proposed and a several innovations are introduced with a new point of view by European Union; in fact, while before, the inspiring reason was the simpler concept of protection now, instead, we focus on that of resilience, that - wanting to use a single and concise definition - consists in a critical entity's ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 2).

The innovations introduced by the new Directive (EU) 2022/2557 are many and all of considerable interest: first of all, the directive abandons the designation of European Critical Infrastructures and consequently of their operators/owners and introduces what is defined as a "critical entity" that means a public or private entity which has been identified by a Member State in accordance with a specific procedure as belonging to one of the categories set out in the directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, annex). The list includes - obviously - the energy and transport sectors, but broadens the categories considered to 11, it returns to a broader and more widespread classification similar to that made in the communication 702 of 2004 according to which critical infrastructures had to be included in 9 different sectors (Communication

from the Commission to the Council and the European Parliament of 20 October 2004):

- Energy (Electricity, District heating and cooling, Oil, Gas, Hydrogen);
- Transport (Air, Rail, Water, Road, Public Transport);
- Banking;
- Financial market infrastructure;
- Health;
- Drinking water;
- Waste water;
- Digital infrastructure;
- Public administration;
- Space;
- Production, processing and distribution of food.

According to the provisions of the directive, by 17 July 2026 each Member State will be required to identify the critical entities for the sectors and subsectors listed in the directive. In general, the criteria to be followed for the designation of a critical entity are (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 6):

a) the entity provides one or more essential services;

b) the entity operates, and its critical infrastructure is located, on the territory of that Member State;

c) an incident would have significant disruptive effects, on the provision by the entity of one or more essential services or on the provision of other essential services in one or more of 11 the sectors that depend on that or those essential services.

It is necessary to specify that the importance of the disruptive effects is assessed according to some criteria, already indicated by the directive itself. Specifically, the criteria are related to the number of users relying on the essential service provided by the entity concerned; the extent to which other sectors and subsectors depend on the essential service in question; the impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population; the entity's market share in the market for the essential service; the geographic area that could be affected by an incident, including any cross-border impact and - at the end - the importance of the entity in maintaining a sufficient level of the essential service, considering the availability of alternative means for the provision of that essential service (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 7).

With reference to the provision of essential services, the directive specifies that a critical entity is qualified as a European critical entity if, in addition to being

preliminarily identified as a critical entity, it provides identical (or similar) essential services in six or more Member States; such entity will be given specific notification as indicated in the Directive (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art. 17).

A further innovation concerns the risk assessment which becomes more complex and is now divided into two levels: a first risk analysis is carried out directly by the Member State and subsequently the critical entity carries out one for its critical infrastructure(s). Specifically (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.12), the Member State's risk assessment takes into account all the relevant natural and man-made risks which could lead to an incident, including those of a cross-sectoral or cross border nature, accidents, natural disasters, public health emergencies and hybrid threats and other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541.

Critical entities shall, within nine months of receiving notification of identification as such, be required to assess, and based on Member States' risk analysis and other relevant sources of information, all relevant risks that could disrupt the provision of their essential services. This evaluation shall be repeated when necessary and at least every four years, without prejudice to the cessation of the designation of critical entity. Critical entities have the obligation to prepare and then apply a resilience plan in which the adequate and proportionate technical, security and organisational measures to guarantee their resilience are described, therefore the OSP (Operator

Security Plan) provided for by the previous directive disappears and the resilience plan of the critical entity is born in which specific measures are included (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.13).

However, the critical entity remains required to appoint its own liaison officer to act as a point of contact with the competent authority of the Member State. In this regard, it should be noted (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.9) that each Member State is required to designate one or more competent authorities responsible for the correct application of this Directive at national level and that, therefore, they will be the ones to interface and receive communications from critical entities exclusively through the single point of contact already appointed by them. Critical entities - unless they are operationally unable to do so - shall make an initial notification of the occurrence within 24 hours of becoming aware

of the incident, this communication shall then be followed, if deemed appropriate, by a detailed final report at the latest after one month (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.15).

A final innovation introduced is the establishment of the group for the resilience of critical entities which has the task of supporting the Commission and facilitating cooperation between Member States and the exchange of information on issues relating to the themes of the directive itself (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.19). The group is composed of representatives of the Member States and is chaired by the representative of the European Commission. By 17 January 2025 - and every two years thereafter - the Critical Resilience Group is required to draw up a work program on the actions to be undertaken to achieve its objectives.

A very important aspect of the directive is that it does not apply to matters covered by Directive (EU) 2022/2555 (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.1), without prejudice to the provisions of the same for Critical entities in the banking, financial market infrastructure and digital infrastructure sectors (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.8).

Considering the relationship between the physical security and cyber-security of critical entities, Member States shall ensure that this Directive and Directive (EU) 2022/2555 are implemented in a coordinated manner. This shows, first of all, that the issue of cyber security has now become so central as to dedicate an entire regulation to the matter and, furthermore, that cyber-attacks can have strong repercussions on the entire system of critical infrastructures and therefore cannot be considered isolated attacks and must be treated in all respects as incidents that can significantly disrupt the provision of essential services of a Member State (Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022, art.1).

5. CONCLUSIONS

The identification and consequently the protection of critical infrastructures is a relatively recent topic, in fact, in Europe, it has been regulated for less than twenty years. It is a theme in continuous change and updating, also due to the application of not only physical but also digital technologies that are increasingly sophisticated and aggressive, capable of significantly disrupting the functioning of one or more systems of a Member State of the European Union.

The European legislation was updated in 2022 with Directive (EU) 2022/2557 which proposes important innovations on the topic, drawing attention to the resilience of critical entities, i.e. the capacity to resist, adapt and restore their operational functions. Each Member State of the Union is aligning its legislation with European directives, for example Italy, will certainly adapt to the provisions of Directive (EU) 2022/2557 and therefore it is very likely that - already in the next few months - there will be an update of the Italian legislation which, currently, with the validity of Legislative Decree No. 61 of 11 April 2011 remains anchored to the previous Council Directive 2008/114/EC.

REFERENCES

[1] Communication from the Commission to the Council and the European Parliament of 20 October 2004. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (Accessed: 18 September 2024).

[2] Communication from the Commission of 12 December 2006. Available at: https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786 (Accessed: 18 September 2024).

[3] Council Directive 2008/114/EC of 8 December 2008. Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32008L0114 (Accessed: 23 September 2024).

[4] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541. (Accessed: 25 September 2024).

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557 (Accessed: 23 September 2024).

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (Accessed: 25 September 2024).

[7] Green Paper on a European Programme for Critical Infrastructure Protection of 17 November 2005. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576 (Accessed: 18 September 2024).

[8] Legislative Decree of President of Italian Republic N. 61 of 11 April 2011. Available at: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2011-05-04&atto.codiceRedazionale=011G0101&elenco30giorni=false (Accessed: 23 September 2024).

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 26 October 2001, s. 1016. Available at: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm (Accessed: 16 September 2024).