Department of Political Science
Master's degree in International Relations
Major in Security

Chair of Security Law and Constitutional Protection

The balance between security and fundamental rights in the era of cyberterrorism: a Euro-national analysis

Prof.ssa Elena Griglio
Supervisor

Prof. Giuseppe Pascale
Co-Supervisor

Sofia Nicolì
ID No. 649172
Candidate

Academic Year 2022/2023

«*Est modus in rebus sunt certi denique fines,*
quos ultra citraque nequit consistere rectum»

«Esiste una misura nelle cose; esistono determinati confini,
al di là e al di qua dei quali non può esservi il giusto»

(Orazio, Satire (I, 1, 106-107))

Table of Contents

Abstract 4

Introduction 5

Chapter I - The fight against cyberterrorism as a constitutional matter 9

1.1 Defining cyberterrorism: two approaches 9

1.2 The juridical dualism of public security and personal freedom 16

1.3 The Digital Rights Ireland Case 24

1.4 Conflict of interest in non-State actors 40

Chapter 2 – The European legal framework to counter cyberterrorism 50

2.1 From the Budapest Convention to NIS Directive 50

2.3 Evolving threat, evolving legislation: towards NIS 2 Directive 62

2.3 The role of ISPs in online terrorist content removal 74

Chapter 3 - The implementation of EU Directives at the Italian national level 83

3.1 Converging anti-terrorism and cybersecurity provisions 83

3.2 Privacy vs Security: the challenges of preventive interception 98

3.3 Criminal law and the problem of "anticipation of protection" vis-à-vis fundamental rights 109

Conclusions 120

Individual and collective protection: an unattainable combination? 120

Bibliography 129

Abstract

The development of cyberspace has emerged as a catalyst for significant innovation in modern society, bringing profound changes to the life of individuals but also of the States. The attractiveness of this new dimension, now officially defined as the fifth dimension, has made it desirable even for illegal and immoral purposes. When dealing with this issue, particular importance is given to terrorist groups that have extended and spread their activities also and especially in cyberspace.

From propaganda to recruitment and radicalization, to the organization and deployment of terrorist attacks, cyberspace currently represents the new frontier that the law shall incorporate in international, regional, and national legislation to structure an efficient network of prevention and fight against the phenomenon that threatens the stability of democratic States.

This research work explores the implications in the constitutional dimension of the fight against cyberterrorism, starting from the attempt to define the phenomenon and then deepening the legal framework set up by the European Union and then with a focus on the Italian legal system. The aim is to evaluate the possible legislative balance between ensuring and safeguarding public security and, at the same time, guaranteeing the respect of individuals in their fundamental rights and freedoms.

Keywords: Cyberterrorism, cyberspace, security, fundamental rights, privacy

Introduction

T*errorism, including jihadist terrorism, has original characteristics. Cooperation between States is indispensable at a time when terror would like to test the rule of law, which must emerge stronger. The commitment against terrorism must not mean giving a single millimeter of ground on the constitutional principles on which the tightly woven fabric of freedoms that inform our democracy depends*[1].

These are the words of the former Italian Minister of Justice, Hon. Andrea Orlando, who, on the occasion of the Guardasigilli's communications on the administration of justice in January 2016, before the Chamber of Deputies, reminded the audience. The choice of quoting this excerpt from the speech lies in the fact that it perfectly synthesizes the essence of this research. The "original characteristics of terrorism" are defined in the new phenomenon of cyberterrorism, while the constitutional principles in this research are public security and individual rights and freedom, analysed through the lenses of the legislator's endeavours to reach a balance.

Starting with the first element of the analysis, to define cyberterrorism a backwards analysis is necessary. The evolution of cyberspace has expanded throughout the last decades with an exponential increase in its diffusion and capacities. It is characterized by speed, anonymity, global diffusion, and cheapness. It has therefore become appealable not only to common people but also to terrorist and insurgent groups, who see in it a new means to spread their ideologies and produce internal and international destabilization. Terrorist groups have expanded their activities onto cyberspace, increasing the level of capillarization that they are able to reach and developing a new ad-hoc online structure for their propaganda, recruitment and radicalization processes, along with the use of cyberspace to deploy terrorist attacks. This phenomenon is defined as cyberterrorism, which, although it does not find a universal

[1] Original version in Italian language: "Il terrorismo, anche quello jihadista, ha caratteristiche originali. La cooperazione tra Stati è indispensabile in un periodo in cui il terrore vorrebbe mettere alla prova lo Stato di diritto, che invece deve uscirne più forte. L'impegno contro il terrorismo non deve significare cedere un so- lo millimetro sul terreno dei principi costituzionali da cui dipende il fitto tessuto di libertà che informano la nostra democrazia".

commonly accepted definition, it has been described in various aspects by the literature with the characteristics above mentioned being the lowest common denominator of the concerned phenomenon. With regard to Islamist terrorist groups, mainly Al-Qaeda and ISIS, they have had an increasing presence on online platforms mainly leveraging the fact that Internet is cheap and anonymous, in order to propagandize extremist ideology and recruit new would-be terrorists all over the world, especially in Europe and the United States. Since the late 1990s Al-Qaeda dedicated itself to increasing their online presence, to the extensive use of social networks such as Facebook and Youtube as well as creating online magazines and forums where to develop their activities and to create a strong and direct network with their members and supporters. There have also been cases of attempted cyber-attacks by individual radicalised so-called hacktivists. One of the first cases has as protagonist the Moroccan-born terrorist known as "Irhabi 007"[2], nickname of Younis Tsouli, who lived in the United Kingdom and deployed several terrorist activities via the Internet, from the setup of websites and forums to the diffusion of video-materials of propaganda and radicalization, to the support of actual Al-Qaeda's operations via the Internet[3]. The original element of terrorism is thus that of cyberspace, in which this phenomenon has expanded and then taken root, carrying out a multiplicity of activities that will be analysed in detail in the first section of chapter one.

The second element cited by the On. Orlando and chosen to introduce this research is the reference to the fundamental importance of constitutional principles, which in this analysis are declined in the balance between public security and fundamental rights, especially the right to privacy and the right to freedom of expression. In the fight against terrorism, and even more so in its new digital version, European and Italian legislation develop around the attempt to balance correctly, or in the most moderate and reconcilable way possible, the need to ensure public security, therefore adopting restrictive, emergency, or even ordinary but

[2] "Irhabi" is the Arab word for "terrorist".

[3] Jayakumar, S. (2020). *Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness With Three Case Studies on Estonia, Singapore, and the United States*. Handbook of Terrorism Prevention and Preparedness.

preventive measures that may consist in an invasion of the private sphere of the individual, and the need to respect the fundamental rights and freedoms of citizens.

An additional focal point cited by the On. Orlando in the opening quote is the necessity for a national but also international collaboration and cooperation in order to counter this phenomenon which is so far translational in its nature and expansion of influence. This concept of cooperation will be thoroughly discussed and explored several times in this research work, as it stands as one of the foundational principles of counter-terrorism legislative production both globally and domestically. This principle is articulated in several conventions, notably in the Budapest Convention, which will be explored in the first paragraph of the second chapter. Furthermore, it is reflected in the European production of directives and regulations which will be examined in depth in the second chapter, and also within the framework of the Italian legislation, to which the third chapter is dedicated.

This research wants to investigate how the antiterrorism regulation has evolved and developed adapting to the drift of the phenomenon in cyberspace, and how the combination of security and freedom is addressed at the legislative level. In this sense, a fundamental case of the European Court of Human Rights is dealt with in-depth in paragraph 3 of the first chapter, the Digital Rights Ireland case. its judgment, inserted in the European and global context of the immediate post-Snowden revelations, represents a key moment and a turning point for the jurisprudential line of the European court but also cascading, of the national courts which will refer to the 2014 judgment. The examination of this case opens the door also to an important novelty: the presence of private, non-State actors in the realm of public safety. From telecommunications companies to Internet Service Providers, to social networks such as Facebook under Meta, over the past decade, there has been an increasingly structured cooperation between the State and private actors in pursuit of an objective that until then, had been mainly the responsibility of the competent public authorities, which had ad-hoc tools but also training and a structured role specifically for a counter-terrorist activity. This research work, therefore, aims also to investigate how this double track between public and private entities, which goes in the same direction of public safety, is intertwined and has the potential for greater effectiveness in the protection of collective welfare, at the same time assessing the implications that it may have in a balanced analysis of constitutional principles.

The methodology used to develop this analysis consists first of identifying and circumscribing the concept of cyberterrorism, through the double lenses of the tool-oriented and the target-oriented approaches offered by the literature. To this, follows an investigation on the implications that counter-terrorism activities may have on the balance between public security and fundamental rights, firstly through a constitutional analysis and secondly with the analysis of the judgment Digital Rights Ireland as a benchmark for the subsequent legislative production. Then follows an in-depth examination of the European legislative instruments directed at addressing both counter-terrorism and cybersecurity, as there is not a single legislation addressing cyberterrorism but it is a threat addressed by multiple legislative measures and developed throughout the years since 2001.

In particular, EU Directive 2017/541 and Regulation 2021/784 represent two turning points in, respectively, the definition of the framework of terrorist offenses and in terrorist online content removal. After the supranational analysis, there follows an in-depth investigation of the Italian legislative framework, from the transposition at the national level of the European acts to the analysis of two specific measures, the intelligence preventive interception and the anticipation of criminal law protection. The *fils rouge* followed in this research is the evaluation of a possible legislative balance between collective security and individual protection, without encountering abuses neither in the expansion or strengthening of security measures nor in the individual sphere of fundamental rights and freedoms.

Chapter I - The fight against cyberterrorism as a constitutional matter

1.1 Defining cyberterrorism: two approaches

When discussing the threat of cyberterrorism, the first issue at stake is finding an unambiguous and commonly accepted definition of the terminology. In the academic literature, different efforts have been made to find a precise definition with greater semantic accuracy. Among these, two shall be taken into consideration for the clarity and development of this paper. The first definition is offered by the professor of computer science Dorothy Denning, the second one by the Nation Conference of State Legislatures.

According to Denning, during her testimony before the House Armed Services Committee in 2000, cyberterrorism shall be defined as the convergence of cyberspace and terrorism:

"*It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*"[4]

From this definition it appears clear the relation between terrorism, a long-lasting threat for State and public security, and the cyberspace, a relatively recent new venue where attacks by terrorists take place, leading to the neologism of cyberterrorism. What Denning highlights most is the use of computers to deploy acts of terrorism, conceiving cyberspace as a new means for terrorist attacks. The other definition of cyberterrorism offered by the National Conference of State Legislatures, an organization of legislators that supports policymakers mainly in homeland economy and security-related issues, is focused on a different perspective, describing the threat as:

[4] Denning, D. (2000). *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*. <Statement of Dorothy E. Denning | Georgetown University>.

"*The use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically*."[5]

These activities do not lead directly to significant financial repercussions or pose harm to individual's lives. Nonetheless, it is contended that embracing a broader conception of cyberterrorism enables a comprehensive exploration of the entire spectrum of legal concerns and corresponding responses from the legislator. This second definition considers, therefore, the use of cyberspace as an additional instrument in terrorist activity, using it to further the agenda, and conceiving it from a wider perspective vis-à-vis the internal organization of a terrorist group, and not merely as an additional place where to deploy attacks. This second definition will be taken as reference and examined in this research to delve into the legislative framework adopted within the European Union and subsequently incorporated and adapted at the Italian level in the fight against terrorism, specifically exploring terrorists' utilization of cyberspace and the manifestation of terrorism there.

To further investigate what cyberterrorism is, the academic literature has offered two main approaches through which the international threat has been analyzed and that are complementary to the two previous definitions examined. The two specular approaches are the target-oriented approach and the tool-oriented approach[6]. The target-oriented approach, used by the above-mentioned author Denning, is based on the conception of the network as the target, therefore it addresses all the attacks conducted physically or through other computers, with political motivation and against computers and networks, causing injuries, serious damage or fear. From this approach, it appears clear that the network is at the same time both the mean – the weapon - and the goal - the target -, but with the focus only on the deployment of an attack, the final part of the terrorist activity. With a substantial difference, the tool-oriented approach, instead, conceives cyberterrorism as the use of the network as an instrument and support, not only for the deployment of terrorist attacks, but for the entire

[5] National Conference of State Legislatures, <National Conference of State Legislature | Cyberterrorism>.
[6] Talihärm A. M., (2010). *Cyberterrorism: in Theory or in Practice?*, in Defence Against Terrorism Review, vol. 3, n. 2, pp. 63-64.

terrorist activity. Such an approach includes the use of the Internet for propaganda through terrorist websites (for instance alneda.com, almouhajiroun.com, jehad.net)[7], along with all the phases of the radicalization process, from the recruitment to the indoctrination and the final delivery of terrorist attacks. The tool-oriented approach considers also other types of actions that terrorists put in place through cyberspace, which are data mining, fundraising, and financing[8]. This approach is taken as reference by the author Gabriel Weimann to interpret the phenomenon, who explains in detail this wider interpretation of cyberterrorism investigating the use of the cyberspace in all the different phases of Islamist terrorist groups' agenda. From such a definition it appears clear the wider perspective from which the phenomenon is taken under analysis, considering cyberspace a tool, and not only the target of the terrorist groups.

Indeed, the tool-oriented approach is the one which mostly suits the scope of the analysis of this dissertation, investigating all the aspects of terrorist activity which include or make extensive use of cyberspace, not only considering it the place where to deliver terrorists attacks but also and mostly as the place where all the stages related to terrorism and the radicalization process take place, and therefore also the place where to address prevention and de-radicalization by the State authorities.

To better understand what cyberterrorism is, an objective-based analysis would be complementary to the previous approach-based analysis. As explained by a report of the US Army Training and Doctrine Command[9], the objectives of terrorist cyberattacks shall be differentiated into four main areas:

1. Loss of integrity, with the aim of improperly modifying information;
2. Loss of availability, with the aim of rendering unavailable mission-critical information systems to authorized users;
3. Loss of confidentiality, with the aim of critical information disclosure to unauthorized users;

---

[7] Weimann, G., (2004). *WWW.TERROR.NET: How Modern Terrorism Uses the Internet,* U.S. Institute for Peace, Washington DC.

[8] Weimann, G. (2015). *Terrorism in Cyberspace: The Next Generation*. Columbia University Press.

[9] U.S. Army Training and Doctrine Command (2005). *Cyber Operations and Cyber Terrorism*. Handbook No. 1.02, August 15, 2005, p. II-3. <US Army Training and Doctrine Commando | DCSINT>.

4. Physical destruction, with the aim of generating physical harm through commands that cause deliberate malfunctions to information systems.

It is worth mentioning here the reasons for the use of the Internet by terrorists. Such use has increased and expanded over the years and cyberspace has become an integral part of the agenda of such organisations. The literature has identified multiple reasons for terrorists to use the Internet as a preferential pathway, with the conclusion that its use is becoming essential for nowadays terrorist organizations[10] with the contribution of authors such as A. Kruglanski, M. D. Silber and A. Bhatt, who have investigated the correlation between the Internet and the radicalization process.

According to Silber and Bhatt's Model[11], who have investigated the use of the Internet by terrorists mainly in the Western world, the most common reasons identified are the fact that cyberspace is a cheaper tool than traditional in-person methods, it is easily available everywhere in the world and it simply needs an Internet connection to be used, and it can create and deliver computer viruses through smartphones or wireless connections, without the deployment of on-site units. Furthermore, it also guarantees high levels of anonymity, not only while carrying out the attack but also at the different levels of the radicalization journey, therefore representing a safer means for individuals approaching a terrorist organization for the first time. Indeed, staying behind a computer instead of being physically exposed, mainly using nicknames hiding the real identity, and especially maintaining anonymity when communicating virtually and exchanging information on terrorist ideology is perceived safer and therefore more captivating.

Further elements in favour of the use of the Internet by terrorist groups in the latest decades are highlighted by Ogun in a 2012 report on the subject[12]. What first emerges is the easiness of access to the Internet and, at the same time, the lack of strict regulation, censorship, and government control in general. This is accompanied by the fast flow of any type of

---

[10] Çeliksoy, E., Ouma, S. (2019). *Terrorist Use of the Internet*. *Bilişim Hukuku Dergisi*, *1*(2), 243-267. <Terrorist Use of the Internet>

[11] Silber, M. D., Bhatt, A., & Analysts, S. I. (2007). *Radicalization in the West: The homegrown threat* (pp. 1-90). New York: Police Department.

[12] Ogun, M. N., (2012). *Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes*. Journal of Applied Security Research, 7:2, 203-217.

information that circulates online characterized by a multimedia environment, which is an environment composed of the combination of texts, pictures, audio files, videos, and also the possibility of downloading files such as books, songs, movies, graphics. All these resources that the Internet makes available to its users become extremely useful and instrumental for the terrorist cause and activities.

In addition to all the reasons mentioned so far, it is also interesting to refer to another consideration highlighted in the literature on the subject. Indeed, Lachow and Richardson have identified five main points in favour of using the Internet[13]. Three of them correspond to the already-quoted easiness and quickness in communication, the low-cost essence of online activities, and the anonymity that the Internet guarantees. However, the other two additional reasons are novel. The first one identified by the two authors is the ubiquity of the Internet. What is meant by this definition is that even small terrorist groups may compete with much larger organizations in terms of global cyber presence. Besides being able to communicate with one another anywhere in the globe, terrorists may also be able to create a Website that can be reached and visited by millions of users and perhaps even be checked regularly for the news. The second new reason consists of the fact that the expansion of the bandwidth along with the creation of new software has facilitated unsophisticated users to produce and spread complex information via the Internet.

The use of the Internet by terrorist groups has become such an object of analysis in the scientific literature that a term has been coined to indicate the process of online propaganda, recruitment, and radicalization on dedicated forums: electronic jihad.

This term is well explanatory of the extent to which the use of cyberspace has not only entered the organisation of these groups but plays a role of great importance and prevalence in all their activities. With electronic jihad is intended to precisely represent the involvement of new followers in the fight against the Western World, although for the sake of accuracy, it is necessary to reflect on the not entirely correctness of this term. In fact, in this terminology appears the misuse of the term jihad, interpreting it as the holy war, perfectly in line with the terrorist re-interpretation of it but far from its original meaning. As written in the Quran jihad

[13] Lachow, I., Richardson, C., (2007). *Terrorist use of the Internet: The Real Story*. JFQ: Joint Force Quarterly, 45, 100-103.

denotes the internal "strive" of the single individual and his/her effort in the path of God, without any reference to an external war[14].

This parenthesis aside, the relevance of this electronic jihad has been seen in many cases of Internet use by single individuals who radicalise alone, at home, online, to the point of perpetrating terrorist attacks, many of them even without formally joining an organisation such as Al-Qaeda or ISIS, but simply having access to propaganda content disseminated by these organisations. In fact, as Weimann explains, the use of social media for this purpose is becoming more and more entrenched and widespread, and this phenomenon becomes, in fact, part of the interpretation of the term cyberterrorism. A case study may be cited as an illustrative instance, with the understanding that it represents merely one of numerous examples, potentially numbering in the hundreds or thousands. The case study taken as example has as protagonist Arid Uka, an Albanian Muslim residing in Germany, who on the evening of March 1, 2011, engaged in online activities, particularly viewing YouTube videos. In a pattern observed in many instances, he came across a jihadist video depicting the harrowing rape of a Muslim woman by US soldiers—a footage edited and disseminated on YouTube for the purposes of jihadist propaganda. After repeatedly watching the video, Arid Uka proceeded to board a bus at Frankfurt Airport, where he lethally shot two US servicemen and inflicted injuries upon two others using a handgun.

Upon his apprehension, investigators scrutinized Arid Uka's internet history. This examination, particularly evident in his Facebook profile, revealed a gradual interest in jihadist content, a subsequent process of self-radicalization, and ultimately, the viewing of the aforementioned video, which impelled him to partake in what he perceived as a war in defence of Muslims.

It is noteworthy that Arid Uka did not belong to any terrorist organization, nor had he visited notorious training camps for terrorists. His entire radicalization trajectory, spanning from an

[14] Campanini, M. (2014). *Oltre la democrazia: temi e problemi del pensiero politico islamico*. Oltre la democrazia, 1-166.

early attraction to jihadi preaching to the culmination in a fatal mission, transpired exclusively in the online domain[15].

This case, from which the undisputed power of online radicalisation appears evident, can be even better read in the light of a further statistical analysis on the "demand side" of online radicalization[16]. The concerned study examined the role played by social media in the trajectories of 51 Canadian Islamist extremists starting from 2012. Data pertaining to radicalization was accessible for 32 individuals, with online activities serving as a foundational element in the radicalization process for 21 cases. Consequently, the prevalence rate ranges between 41% and 66%, depending on the consideration of the overall group size as 51 or 32, respectively. It is imperative to note that, within this study, online activities were often concurrent with other radicalization mechanisms. Thus, the prevalence rate encompasses instances of mixed-mode radicalization as much as it does those influenced predominantly by online factors.

To wider analyse the relevance of online Islamist propaganda in the radicalization leading to attacks, the study of Gill, Horgan, and Deckert[17] offers an assessment of the extent of online engagement among lone-actor terrorists. Among 119 individuals, 35% were found to interact virtually with a broader network of political activists, and 46% acquired knowledge related to their attack methods through online sources. Comparative analyses employing inferential statistical methods revealed that lone-actors inspired by al-Qaeda were distinctly more inclined to learn through virtual sources compared to their right-wing–inspired counterparts (65% vs. 37%). Additionally, isolated dyads were notably more likely to engage in online interactions with co-ideologues than lone actors who carried out attacks independently.

[15] Weimann, G. (2014). *New Terrorism and New Media*. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars.

[16] Bastug, M. F., Douai, A., and Akca, D. (2020). *Exploring the "demand side" of online radicalization: evidence from the Canadian context. Stud. Conflict Terror.* 43, 616–637.

[17] Gill, P., Horgan, J., and Deckert, P. (2014). *Bombing alone: Tracing the motivations and antecedent behaviors of lone-actor terrorists*. Journal of Forensic Sciences, 59: 425– 435.

Building upon a similar set of inferential statistical techniques, Gill and Corner[18] conducted a comparison between the behaviours and characteristics of lone-actor terrorists who either acquired knowledge or engaged in interactions with co-ideologues online in respect to those who did not participate in either activity. Their findings indicated an emerging trend among lone actors to utilize the Internet. In essence, while the Internet did not lead to an increase in the overall number of lone-actor terrorists, it did reshape their pathways of radicalization and learning. Therefore, the Internet serves as a substitute for other forms of communication without necessarily acting as a facilitator of force.

To conclude these considerations, as the sociologist Marc Sageman wrote: "*Successful terrorism requires the transformation of interested outsiders into dedicated insiders*"[19], and in the digital Era the Internet has become the essential element in this process, facilitating the transformation into insiders and also the interactions needed after it, to maintain the required level of commitment to the cause, which before the advent of cyberspace were solely face-to-face interactions with the intrinsic limitations in the long-run.

1.2 The juridical dualism of public security and personal freedom

The foundational exploration of the concept of cyberterrorism and the use of the Internet by terrorist groups serves as both incipit and context for the subsequent legal analysis. This examination aims to scrutinize the legislative measures implemented by the European Union and Italy in response to this phenomenon. Specifically, it endeavors to assess the effectiveness of these instruments in safeguarding the security of the State and its citizens and, at the same time, the fundamental rights of individuals.

In fact, when discussing counter-terrorism activity and legislation there is an atavistic problem of juridical, political and social relevance to which no single solution has been found

[18] Gill, P., and Corner, E. (2015). *Lone-actor terrorist use of the Internet and behavioural correlates*. In (Lee Jarvis, Stuart Macdonald, and Thomas M. Chen, eds.), Terror- ism Online: Politics, Law, Technology and Unconventional Violence. London, U.K.: Routledge.

[19] Sageman, M., (2004). *Understanding Terror Networks*. Philadelphia, University of Pennsylvania Press, 158-161.

yet. This issue is characterized by a dualism that can be summarized as "security versus freedom", which entails striking a balance between public security and personal freedom.
The conflict between ensuring the right level of public security by guaranteeing the safeness of the citizens of a State, and at the same time safeguarding the individual freedom that each citizen in his/her own private life enjoys is open and represents the main argument that this dissertation aims at analyzing from a constitutional perspective, with an updated perspective considering the new means at disposal to fight terrorism: the most-advanced technological methods, from the use of cyberspace to the implementation of artificial intelligence, with their possibilities but also limits.
In order to unravel this thorny issue, it may be useful to start with a series of definitions of the topics constituting the main issue at stake, namely the meaning of *security* and the declination of the word *freedom* in this context.
The concept of security cannot be reduced to a single comprehensive definition as it has a wide range of interpretations, depending on the perspective from which the concept itself is conceived.
From an analysis of the etymology of the word, security derives from the Latin "se – curus", where "se" means "without" and "curus" means "uncomfort, concern". That is, originally security meant freedom from unease or a calm environment free from risks and threats.
In the context of this analysis, the concept of security shall be interpreted as National Security, referring to the security of the State, of its democratic government and of its citizens. In this sense, the definition of Arnold Wolfers has become a landmark in International Relations Theory: "National security objectively means the absence of threats to acquired values and, subjectively, the absence of fear that such values will be attacked"[20]. The absence of threats and fear is precisely what terrorist actions undermine and jeopardize by their very nature.
When discussing the concept of security, it is interesting also to underline the economic interpretation of it, which considers it a "public good". This perspective further corroborates

[20] Wolfers, A, (1962). *National Security as an Ambiguous Symbol*. Discord and Collaboration. Essays on International Politics John Hopkins University Press: Baltimore, pp. 147-165.

the idea of national security as strictly connected to the safeguarding of the citizens, of the public welfare, and of the possibility of exploiting and enjoying this public good.

To further elaborate on the concept of national security in this context, it would also be useful to refer to an EU regulatory source offering a commonly accepted definition of it. However, an answer to such a question is still pending from the European Parliament, as it has not been provided a final answer to the Parliamentary question E-006381/2014 yet[21]. However, the definition provided by the author Iain Cameron could cover other facets of the concept. The context in which he has developed the definition is the one of the global interdependence era, in which the conventional meaning of "national security" cannot be restricted to simply defending territorial integrity and political independence from external armed attack:

"*National security must also logically encompass espionage, economic or political, and covert (destabilizing) action by foreign powers. Moreover, notwithstanding a lack of foreign involvement, purely internal threats to change the existing political order of the state by force (e.i. revolutionary subversion and terrorism) must also be covered. Certainly these are regarded by most if not all governments as legitimate national security concerns*."[22].

With this definition, the author highlights the close link between the current globalization era and the increasing threat that this status of things brings with it, namely the easier and faster spread of sources of internal destabilization, as terrorism represents, with a political and social character, evolving from the mere threat of armed attack by conventional and non-conventional military apparatuses.

Analyzing the other concept protagonist of this discussion, that is the wide concept of freedom, in this research it shall be referred to considering the meaning provided by the articles 5, 8, 10, and 11 of the European Convention on Human Rights (hereinafter referred to as ECHR)[23].

---

[21] The concerned Parliamentary Question is the following: "Can the Commission clarify its definition of 'national security' when applied in relation to adopted or proposed EU legislation as a reason for the application of specific measures and provisions?". European Parliament. <Parliamentary Question E-006381/2014>.

[22] Cameron, I. (2021). *National security and the European convention on human rights*. BRILL.

[23] European Convention on Human Rights, Art. 5 on the right to liberty and security, Art. 8 on the right to respect for private and family life, Art. 10 on the freedom of expression, Art. 11 on the freedom of assembly and of association.

The relevance of each of the above-mentioned articles in the development of this analysis lies in their consequential connection to the crimes, or individuals suspected of crimes, related to terrorist activities and the punishment of such individuals. Indeed, when it comes to prosecuting crimes of a terrorist nature, the freedoms listed above are the ones most likely to be disregarded and violated, in the attempt to stop and punish the suspect individual as quickly as possible, eliminate a threat and act as a deterrent mechanism to others. More specifically, starting with Art. 5 ECHR, it proclaims the right to liberty referring to the physical liberty and security of the person in the cases of arrest and detention, in order to guarantee the acknowledgment by the person concerned of the crimes suspected of, and the lawful arrest and detention procedures along with the possibility of taking proceedings in case of breach of the provisions by the Article. The importance of these guarantees stems from past cases known for the abuse of power and the disregard of these rights, which have acquired international relevance influencing legislators even outside the borders. In fact, the first cases of application of restrictions on fundamental rights date to the famous Patriot Act in 2001 that the government of the United States enacted right after the 9/11 attacks. Following it, prominent examples of such cases are the multiple Guantanamo cases and the failure to respect the writ of habeas corpus, such as the case Boumediene v. Bush[24], or the famous case Salahi v. Obama[25], which from the Supreme Court of the United States have spread their recognized legislative relevance to the European Union, representing a benchmark for legislators in order to develop an increasing sensitivity towards the issue of respecting fundamental rights vis-à-vis prosecuting suspected terrorists.

Another perspective from which interpreting the concept of freedom is referred to Art. 8, right to respect for private and family life. This interpretation finds its raison d'être in the sphere that the article aims at safeguarding, that is the sphere of private life, family life, home, and correspondence. Stating that there shall be no interference with these rights and their exercise by a public authority in the context of a democratic society, except for specific cases

[24] Boumediene et al., petitioners, v. Bush, President of The United States, et al., respondents. 553 U.S. 723 (2008). Certiorari to the United States Court of Appeals for the District of Columbia Circuit.

[25] Mohamedou Ould Salahi, petitioner, v. Barack H. Obama, et al., respondents. Civil Action no. 05-0569 (RCL).

undermining national security, public safety or the economic well-being of the country, the cases of counter-terrorism enforcement activities have often been found crossing the border of what is considered to be an actual threat to national security justifying such interference. Several cases, indeed, have confronted the ECtHR with the assessment of whether it is actually necessary to override Art. 8 ECHR protections in order to meet the need to protect public safety against suspected terrorists. Such interference, especially nowadays, with the widespread use of advanced technologies, from the mere Internet to Artificial Intelligence, is less and less controllable and traceable within specific legally recognized, protected, and enforceable spheres of action. It should be emphasized how easily this right to privacy can be undermined since it is mainly a virtual privacy, i.e. that of all communications, exchanges, and accesses that take place in cyberspace, and which can therefore be monitored by the authorities without the suspected individual having any awareness of it. In fact, both target and bulk interception, which represent a fundamental instrument in the fight against terrorism, have been questioned in their legality before Courts, especially for their interference with Art. 8 ECHR.

The case of Zakharov v. Russia[26] of the ECtHR exemplifies the contentious interlacing and overlapping of privacy protection and preventive control actions, with an in abstracto examination by the court of the matter of targeted surveillance, with the conclusion that the mere existence of a law permitting surveillance in itself constitutes an interference with Art. 8. A further aspect of this controversial topic lies in the fact that for the very nature of the surveillance measures in themselves, applicants often struggle to demonstrate that they were under surveillance measures, not to mention first and foremost if they become aware of being under surveillance. The importance of the case mentioned resides in the fact that from it a new set of criteria to evaluate the admissibility of similar cases of surveillance measures interference in Art. 8 have been established, starting from assessing whether the case is admissible vis-à-vis the recognition of an interference with the right to privacy. The other criteria evaluate whether surveillance is in accordance with the law of the State concerned,

[26] Roman Zakharov v. Russia App. no. 47143/06 (ECtHR, 4 December 2015).

whether the surveillance follows a legitimate aim and whether the measure is necessary in a democratic society[27].

With regard to Art. 10 ECHR, namely freedom of expression, it provides for the safeguard of a range of freedoms, that are the freedom of opinion, to receive information and ideas and to impart information receive and ideas without interference of public authority and regardless of frontiers. The essence of this article is explained by the ECtHR in the ruling of the case Handyside v. The United Kingdom stating "freedom of expression constitutes one of the essential foundations of [democratic] society, one of the basic conditions for its progress and for the development of every man" [28]. The importance of this article has been underlined by the Court itself on different occasions in its case law, outlining States' positive obligations to protect the exercise of the right. In the case Zakharov v. Russia[29] the court held that statements made in private correspondence may fall within the scope of the article, despite the limited public nature of the statement[30].

The case of freedom of expression is of relevance in the present analysis because when it comes to combating terrorism and even more so when it comes to cyberterrorism, this guarantee may easily fail. The primary factors behind this situation stem from the crucial role of censorship in counterterrorism efforts. This involves the eradication of content, predominantly online but not limited to it, disseminated for proselytization purposes, and constituting actual propaganda. In the EU legal system, for instance, the Regulation 2021/784 which became effective on June 7, 2022, mandates Hosting Service Providers (HSPs) to expeditiously eliminate terrorist content from online platforms within one hour of receiving a takedown order issued by a competent national authority of an EU Member State. Additionally, the regulation incorporates various safeguards to uphold fundamental rights, with particular emphasis on the preservation of freedom of expression.

In the pursuit of balancing public safety and fundamental rights, concurrent considerations arise, especially in regard of the presence on social media platforms of materials of terrorist

[27] *Ivi*, paragraph 227.
[28] Handyside v. The United Kingdom App. no. 5493/72, paragraph 49 (ECtHR, 7 December 1976).
[29] Roman Zakharov v. Russia, *Op. Cit*., paragraph 23.
[30] European Court of Human Rights (31 August 2022*). Guide on Article 10 of the European Convention on Human Rights*. *Freedom of expression*.

nature. For instance, on YouTube circulate video tutorials providing instructions on the construction of Improvised Explosive Devices (IEDs), on Facebook circulate posts that serve as instructional tools for imparting knowledge on explosive usage, directing followers to websites with informative content, endorsing hacking techniques, and disseminating encryption programs. Postmodern terrorists even train in virtual online camps, leveraging the diverse array of contemporary social media platforms[31]. After considering all these factors, it is imperative to acknowledge the simultaneous presence of numerous other online products, such as Facebook and Twitter posts, forums, or comments beneath YouTube videos. These constitute expressions by individual users, at times lacking clear delineations to be identified explicitly as terrorist content. Nevertheless, from a preventive standpoint, they may be categorized within the group of content subject to censorship and be removed to comply with the Regulation abovementioned. In this instance, there is potential to construe this as a violation of freedom of expression, particularly in the absence of any intent on the part of the author to allude to an ongoing radicalization process and consequent threat to the security of the State. This issue will be addressed in detail in chap. 2, par. 2 and 3 and chap. 3, par. 1, based on an analysis of the legal sources at European Union level and at Italian level.

The last article to analyze is Art. 11, which states that everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and join trade unions for the protection of one's interests. This article underscores the importance of citizens being able to convene peacefully and form associations without undue interference from government authorities. It plays a pivotal role in upholding democratic principles by facilitating the collective expression of views and interests through the acts of assembly and association. Nevertheless, akin to all rights, it is subject to lawful limitations essential in a democratic society, such as those mandated for national security or public safety considerations, in order to prevent disorders and crimes, to protect other's health, morals, rights and freedoms[32]. This right can be interpreted considering art 10, firstly because both are the foundations of a democratic society, secondly in the sense that the aim of the exercise

[31] Cfr. Weimann, G. (2014). *Op. Cit.,* p. 4.

[32] European Court of Human Rights (31 August 2022*). Guide on Article 11 of the European Convention on Human Rights. Freedom of assembly and association.*

of freedom of assembly is the expression of personal opinions[33], reinforcing the wider extension that the concept of freedom has in this case, and the complexity of its safeguard. As a matter of fact, the jurisprudence has been reluctant to accept claims that the applicants have suffered no "significant disadvantage" and to dismiss Art. 11 allegations based on Art. 35 para. 3 (b) of the Convention, which provides for the inadmissibility of any individual application if the applicant is considered not to have suffered a significant disadvantage[34].

After delving into the interpretative benchmarks of the concepts of security and freedom, the two develop on two parallel tracks. Indeed, the dualism between security and the protection of fundamental rights in the fight against terrorism has been of great importance from the outset, especially in constitutional matters. This dualism takes shape in the need to pursue the protection of both principles in parallel, but at the same time in the intrinsic difficulty that this objective presents, since the protection of one often causes the failure to protect the other, or its abuse. The traditional negative freedoms, beginning with personal freedom, are the first fundamental human rights that may be compromised by the increase of security protection measures, and this exemplifies the main difficulty of such dualism[35].

With the advent of cyberspace and social media in particular, this juridical issue has expanded and consolidated on a new different sphere, which is not regulated in detail yet and has uncovered black holes that need further examination, that this analysis aims at addressing.

To approach this challenging subject, it is best to begin with a series of questions that examine the different aspects of the issue at stake and ease the process of analysis. The first one evaluates whether it is necessary and justifiable to make an exception to the constitutional principles of fundamental rights and the rule of law to ensure the security of persons and the State. The second perspective entails an assessment on the extent to which a democratic State is entitled to deviate from its fundamental principles in order to guarantee the security of its citizens. The third and final question further expands the previous one in the case of a positive

[33] Ezelin v. France App. no. 11800/85, paragraph 37, (ECtHR, 26 April 1991).
[34] ECHR (31 August 2022*). Guide on Article 11 of the European Convention on Human Rights. Op. Cit.,* p. 6.
[35] Rubechi, M. (2016). *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*. Federalismi.it., 23, pp. 1-16.

answer, investigating the means that a constitutional democracy may legitimately use to pursue the objective of internal security.

In the attempt to balance these two parallel demands of public security and safeguard of personal freedom, a case that marked a crucial turning point in the European legal landscape of the trade-off between security measures and individual fundamental rights, in particular the right to privacy, is undoubtedly that of *Digital Rights Ireland*[36], about which will now follow a detailed examination.

1.3 The Digital Rights Ireland Case

In the European context, an historical and landmark case of first attempt to balance public security and protection of fundamental rights in the fight against terrorism is presented by the *Digital Rights Ireland* ruling of 8 April 2014[37]. The judgement responds to two claims together, C-293/12 and C-594/12, both on the validity of the so-called Data Retention Directive, namely the Directive 2006/24/EC[38], that constituted an innovative measure of bulk surveillance adopted by the European Parliament and the Council and that was declared invalid by the Court of Justice of the European Union (ECJ).

Starting from the beginning, the concerned piece of legislation adopted in 2006 provided for the implementation of data retention procedures, i.e. the generalized and undifferentiated retention of *metadata*, which are data on the sources, destinations, dates, times, and modes of communication, as well as location data related to mobile phone usage, that should have been carried out by telecommunication companies on their clients. This Directive has been adopted to replace the previous Directive 2002/58 on privacy and electronic communications to strengthen EU counter terrorism surveillance tools right after the terrorist attacks of the railway station in Madrid on the 11 March 2004 and the London Underground attack on 7

[36] Court of Justice of European Union (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (C-293/12). ECLI:EU:C:2014:238.

[37] *Ibidem.*

[38] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15.3.2006, L 105/54, 13.4.2006.

July 2005, and it is considered to be one of the major instruments to counter this threat in the European context. The primary aim of the directive is to harmonize the single Member State's legislation on the matter of publicly available electronic communication services and public communication networks' obligations towards the retention of the metadata that they generate and process[39]. This procedure follows the aim of guaranteeing that the data are retained for the purposes of investigation, detection and prosecution of serious crimes, in line of what each Member State defines in its national law.

The directive specifies that the retention period must begin on the date of the communication and end between six months to two years (Art. 6). The categories of data to be retained and their purpose is specified in Art. 5, according to which the retention of data shall allow the identification of a person, as source or as destination of a communication, and of the space position and time, be it deduced from the telephone number of the person, or his/her IP address, or the Cell ID. The peculiarity of data retention resides in the fact that it is a collection of bulk metadata, meaning that everyone's data are collected without any ex-ante targeting nor any required suspicion nor intercession of a judge - a requirement typically mandated in the context of data preservation[40]. The main difference between data retention and data preservation is that the latter is a measure directly controlled by the criminal justice system, therefore it operates within the borders of the two fundamental concepts of due process and fair trial, whereas data retention appears to have some grey zones of competences. On the one hand the preamble of the Directive refers to law enforcement authorities and declares the compliance of the act with the ECHR, while on the other hand Art. 4 of the Directive states that single Member States shall have access to data retained by

[39] Ojanen, T. (2014). *Privacy is more than just a seven-letter word: The Court of Justice of the European Union sets constitutional limits on mass surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, digital rights Ireland and Seitlinger and others*. European Constitutional Law Review, 10(3), 528-541.

[40] Data preservation requires a tribunal to order service providers to retain the data of specified individuals suspected of criminal activities from the date of the preservation order. Data preservation goes under the umbrella of targeted law enforcement measure that is managed by judicial authorities across the EU Member States and it represents a less intrusive alternative to data retention. The peculiarity lies in the fact that in this case a judge shall be convinced of the necessity of ordering a "quick freeze" of someone's data. See: Guild, E., Carrera, S. (2014). *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*. CEPS Liberty and Security in Europe Papers No. 65, p. 2.

whatever competent law enforcement agency chosen[41]: "*Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law* […]".

The reference to the general term "law enforcement authorities" to define the competence of access to retained data opens the question of who is specifically entitled to access it and under which conditions, as there is a lack of judicial intervention before the application of the Directive. Therefore, such ambiguity leaves space for concern over the conclusion that retention of data may be arbitrary and with unlimited access to it[42]. Indeed, the lacuna in this directive becomes evident in relation to the subsequent stages of the data retention process. While it delineates the conditions under which telecommunication companies are obligated to retain metadata, it remains silent on the procedures governing law enforcement agencies' access to such data. This regulatory gap allows individual Member States to defer to their domestic laws on this matter (Article 4). Furthermore, a notable deficiency exists in terms of regulatory provisions pertaining to the erasure of retained data subsequent to the expiration of the mandated two-year retention period.

Concluding from the examination of this piece of legislation, its core element is undoubtedly the concept of metadata and the implications of their retention for the safeguard of individual fundamental rights, within the framework of a legal discourse. Its distinctiveness lies in effecting a convergence between public security concerns and the role of private companies furthering this objective. It is important to underline that metadata do not include the content of the communication, as explained in Art. 5(2) of the Directive, therefore, although the right to privacy protects the actual content of communications, gathering metadata may be considered an ambiguous activity with excessive wide margins of appreciation but it does

[41] Directive 2006/24/EC. *Op. Cit.*

[42] Guild, E., Carrera, S. (2014). *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*. CEPS Liberty and Security in Europe Papers No. 65, p. 3.

not directly violate the EU Charter of Fundamental Rights[43], however it needs to be very precisely articulated in the regulation of its entire process, from the gathering to the elimination of such data. As it can be deduced from the analysis of the directive, such detailed regulation of all the steps of the data retention process appears no to be, leaving too many margins of appreciation to the single Member States and consequently becoming incoherent with the first intent of the directive, which is the harmonization of these procedures between all the European Union countries.

In this context of legislative ambiguity, several Member States questioned the directive and refused to adopt it in their national legal framework, making it one of the most controversial EU pieces of legislation on the fight against terrorism[44]. The first time the ECJ was requested to evaluate the legitimacy of the Data Retention Directive was in 2006 with the action taken by the Irish Government against the bodies that emanated the directive, the European Parliament and the Council[45]. According to the Irish government, the directive should not be implemented under the provisions relating to the internal market because its primary goal was law enforcement, not the completion of the latter, as instead had been done. The CJEU concluded that the directive governed actions that are separate from the application of any police and judicial cooperation in criminal cases. The Court affirmed that for it to be legitimately implemented as an internal market measure, it did not harmonize either the issue of data access by relevant national agencies or the issue of data usage and exchange between those authorities[46].

In Member States like Germany, Romania, and the Czech Republic, the domestic implementation of the directive into national law led to several constitutional issues. The German Constitutional Court, for instance, declared in 2010 that the internal adoption of the directive caused a "feeling of surveillance", neglecting to set adequate limits for the utilization of collected data[47]. Also Czech Republic[48] and Romania[49]'s Courts declared that

[43] Guild, E., Carrera, S. (2014). *Op. Cit.*, p. 1.
[44] Ojanen, T. (2014). *Op. Cit.*, p. 531.
[45] C-301/06, *Ireland v. the European Parliament*, 10 February 2009.
[46] Guild, E., Carrera, S. (2014). *Op. Cit.*, p. 4.
[47] German Const. Court (BVerfG), judgement of 3 March 2010, 1 BvR 256/08.
[48] Czech Const. Court, judgement of 22 March 2011, Pl. US 24/10.
[49] Romanian Const. Court, Decision No. 1258, 8 October 2009.

the implementation of the directive would be unconstitutional. Following the failure of national implementation of the directive by different Member States, the Commission brought actions against Sweden and Germany before the ECJ. In the case of Sweden, the Court sanctioned the country with an amount of EUR 3.000.000 for the failure of fulfilling directive's obligations[50]. In *European Commission v. Federal Republic of Germany*, following the judgement of the present discussion, the case was removed from the Court's register[51].

This background led to the ECJ ruling commonly known as Digital Rights Ireland case. Upon request of the High Court of Ireland[52] (C-293/12) and the Verfassungsgerichtshof of Austria[53] (C-594/12), the Court examined the validity of the Data Retention Directive in light of Artt. 7, 8 and 11 of the Charter of Fundamental Rights of the European Union, respectively on respect for private life and communications, protection of personal data, and respect for freedom of expression.

The first case (C-293/12) was brought before the court by the applicant Digital Rights Ireland Ltd, a company "dedicated to defending Civil, Human and Legal rights in a digital age"[54], against two minsters of the Irish government[55], the Commissioner of the Garda Sìochána and the Attorney General, with the request of annulment of the Data Retention Directive and of the Criminal Justice (Terrorist Offences) Act 2005[56] insofar as it required service providers to retain generalized traffic and location data, claiming that these two acts were in contrast

[50] Court of Justice of the European Union (Fourth Chamber), European *Commission v. Kingdom of Sweden*, 30 May 2013, case No. C-270/11.

[51] Ojanen, T. (2014). *Op. Cit.*, p. 532.

[52] The High Court of Ireland has original jurisdiction over all questions of law and fact, in civil and criminal matters. Moreover, it deals with matters on the validity of laws vi-à-vis the provisions of the Constitution, as in the present case. For more information: <High Court of Ireland>.

[53] The Verfassungsgerichtshof is the Austrian Constitutional Court (VfGH) and it is also responsible, among other functions, of verifying the legality of the statutes, ordinances and secondary laws. For more information: <Verfassungsgerichtshof>.

[54] This is the definition provided by the company itself on its website Digital Rights Ireland. During the appeal, Digital Rights Ireland declared that it was owner of a mobile phone registered a couple of years before the proceedings and in use from that date.

[55] The institutional figures involved in the case are, specifically, the Minister of Communications, Marine and Natural Resources, and the Minister for Justice, Equality and Law Reform.

[56] It is a domestic law legislation issued in June 2005 with the aim of amending specific provisions of criminal law. In the present case, the reference is to part 2 of the legislation, which is dedicated entirely to dismantling terrorist organizations. To access the text of the law: <Criminal Justice (Terrorist Offences) Act 2005>.

with the Irish Constitution and the ECHR. The High Court suspended the proceeding in view of a first ruling of the ECJ on the validity of the Directive 2006/24/EC.

The latter, in the first instance, was requested to verify whether the limitation of users' rights in the field of electronic communications resulting from the combined provisions of Articles 3, 4 and 6 of the directive[57] was compatible with Article 5(4) TEU, states that "Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties"[58] . Indeed, the generalized retention of data for a long period was considered not proportionate to the pursuit of the communitarian objectives, in this case specifically the detection and prosecution of serious crimes to ensure the proper functioning of the EU internal market.

In the second case (C-594/12) the applicants, Mr. Seitlinger and 11.000 other people, jointly presented a claim before the Verfassungsgerichtshof requesting the annulment of an internal piece of legislation, Art. 102-bis of the Austrian law (Telekommunikationgesetz 2003), created for the application of the Directive 2006/24/EC at national level, questioning its constitutionality. In this case the Austrian Court too suspended the proceeding requesting the intervention of the ECJ on the merit of the Directive.

The final judicial ruling was reached through an exceptionally participative process, as written observations were submitted by the Irish Human rights Commissioner, the Commission, the Council, the European Parliament and eight Member State governments. In addition, the European Data Protection Supervisor (EDPS) was consulted for an opinion by the CJEU, which also sent inquiries to the parties involved[59].

On 8 April 2014, the CJEU issues its ruling, concluding that "Directive 2006/24 was invalid". The Court held that it was invalid on the grounds that it disproportionately interfered with the fundamental rights to respect for private life and the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

---

[57] Art. 3 of the Directive 2006/24/EC is on the obligation to retain data, Art. 4 on the categories of data to be retained, Art. 6 on the periods of retention.

[58] Consolidated Version of the Treaty on European Union [2008] OJ C115/13. <Article 5(4) TEU>.

[59] Granger, M-P., & Irion, K. (2014). *The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection*. European Law Review, 39(6), 834-850.

In this landmark decision the Court established a rigorous scrutiny test for EU legislative acts that materially impair fundamental rights guaranteed by the Charter and the ECHR and applied a rigorous evaluation of the proportionality of the measure in light of the Charter. With this sentence the Court of Justice recognized that the legislator did not correctly evaluated the balance between security policies and the respect for private life of individuals when adopting the Data Retention Directive, as it imposed intrusive mandatory measures without guaranteeing sufficient protection of the fundamental rights to privacy and data protection[60]. With its ruling, the Court did not restrict the judgement's temporal impact, with a retroactive effect. Consequently, it can be presumed that the illegality of the directive began on the day it was put into operation in 2006.

Examining in detail the final judgement and the reasoning of the Court, it was rendered within the preliminary reference procedure under Article 267 Treaty on the Functioning of the European Union in these two cases, on the basis also of Art. 52(1) which lists the conditions for the restrictions of the rights protected by the Charter: "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*"[61].

When addressing the case, the Court initially observed that the traffic data stored according to Artt. 3,4 and 5 of the Directive 2006/24/EC enabled drawing precise conclusions about the daily routines, permanent or temporary residences, movements, activities, and social relationships of European citizens. Following this, the Court clarified that the obligation to retain such information affected the exercise of freedom of expression for the subscribers or users to whom the data pertains, as outlined in Art. 11 of the Charter[62]. Despite the directive

---

[60] Granger, M-P., & Irion, K. (2014). *The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection*. European Law Review, 39(6), 834-850, p. 835.

[61] Charter of Fundamental Rights of the European Union (2000/C 364/01). <Art. 52 – Scope and Interpretation>.

[62] Art. 11 of the Charter corresponds to Art. 10 of the ECHR, and states: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.".

not dealing with the content of conversations, it still had the potential to influence how individuals used electronic communication means and the methods they chose to transmit information, as for all practical purposes this case falls within the broader sphere of mass surveillance measures, which include a suite of tools available to the single Member States to counteract the threat of terrorism[63]. Moreover, the Court assessed that the activity of accessing and extracting data by competent authorities itself constituted an interference with the fundamental rights protected by Artt. 7 and 8 of the Charter. This occurred regardless of whether the information regarding private life had a "sensitive" character or not. The Court deemed that such interference should be regarded as particularly severe, given that it was - and still is- conducted without prior notification to the individuals concerned[64]. This could instill in European citizens the perception that their lives are subjected to continuous surveillance, as stated by the Advocate General Cruz Villalón in his opinion[65]: "[…] *The vague feeling of surveillance created raises very acutely the question of the data retention period*".

However, in the perspective of the CJEU, the level of interference is not of such magnitude as to completely nullify the essence of the right to privacy per se. This implies that the Data Retention Directive is not summarily invalidated as annihilating the core of privacy. Instead, what is imperative is that the interference be justified on a case-by-case basis. The justification entails a two-tier process, commonly referred to as the legality test. The initial stage involves ascertaining the existence of sufficient grounds for the interference. Subsequently, the second stage involves evaluating whether the justification is proportionate, considering its objective and the gravity of the intrusion into the fundamental right to privacy. Concerning the initial phase, any interference with an individual's private life, provided it does not eliminate the essence of the right, must be substantiated to attain legality. The EU institutions rationalized the Directive's interference focusing on its efficacy in combatting

[63] Cfr. Court of Justice of European Union (Grand Chamber), 8 April 2014. *Op. Cit.* para. 28.
[64] Guild, E., Carrera, S. (2014). *Op. Cit.*, p. 6.
[65] Opinion of Advocate General Cruz Villalón, Case C- 293/12, 12 December 2013, paragraph 72.

serious and organized crime as well as terrorism. The Court acknowledged these justifications as meeting the required criteria to pass the legality test[66].

The second stage of the test that the directive undergoes pertains to its proportionality in achieving the legitimate objective pursued, examining whether it surpasses the bounds of appropriateness and necessity for attaining said objective. The CJEU posits that due to the considerable and notably severe nature of the interference, the discretion of the EU legislature is diminished, warranting a stringent scrutiny of that discretion. However, acknowledging the potential value of retained data as a tool for criminal investigations, the Court deems the objective as fitting and appropriate[67].

The CJEU determined, though, that despite the significant importance of combating organized crime and terrorism for collective security, it does not serve as sufficient justification for the directive. The right to privacy necessitates a narrow interpretation of all exceptions, with the directive being inherently an exception to this right. At this juncture, the CJEU specifies that the obligation of data protection outlined in Article 8 of the EU Charter holds particular significance for the right to respect for private life as enshrined in Article 7 of the same source of legislation. Therefore, the primary right is the latter, that of respect for private life[68].

In order to identify which are the shortcomings of the Data Retention Directive and which aspects should be amended to comply with right to respect for private life (Art. 7 Charter), the CJEU has stipulated a set of ten criteria that must be met in order to pass the legality test[69]:

1. Clarity of Rules: The directive should establish clear and precise rules defining its scope and application.

[66] Court of Justice of European Union (Grand Chamber), 8 April 2014. *Op. Cit.* paragraph 41.
[67] *Ivi*, paragraph 48.
[68] *Ivi*, paragraph 53.
[69] Guild, E., Carrera, S. (2014). *Op. Cit.*, pp. 7-8.

2. Personal Data Safeguards: Minimum safeguards must be incorporated to protect personal data from misuse, accompanied by explicit measures against unlawful access.
3. Stricter Rules for Automated Processing: Rules governing personal data subjected to automated processing should be more stringent compared to non-automated processing.
4. Differentiation in Data: Distinctions between electronic communication and traffic data should align with the goal of combating serious crime.
5. Limits on Data Collection: Imposition of limits on personal data collection, specifying factors such as time duration, geographic scope, or specific individuals, with a rejection of blanket collection.
6. Objective Criteria for Limits: The set limits should be guided by objective criteria related to the purposes of prevention, detection, or prosecution of serious crimes, avoiding vague references to national law.
7. Enhanced Conditions for Access: The directive should establish substantive and procedural conditions for national authorities' access to data, with strict alignment to the purpose of the interference.
8. Objective Criteria for Authorization: Criteria determining who is authorized to access the data should be objectively defined and strictly necessary for achieving the specified objective.
9. Prior Review Process: Competent national authorities or an independent body should conduct a prior review before granting access to data, ensuring that it is strictly necessary for the identified legitimate objectives.
10. Differential Retention Periods: Different categories of data should be subject to distinct and clearly justified retention periods based on objective criteria, exclusively serving the legitimate aim.

The Court subsequently elaborated a second set of criteria[70] pertaining to data protection requirements outlined in Article 8 of the Charter. These requirements pertain to regulations governing the storage of data by private sector entities. To align with the EU Charter, a Data Retention Directive must also comply with the following four criteria:

2.1 Institute clear regulations for safeguarding retained data, considering volume and sensitivity;

2.1 Mandate providers to maintain a high level of security, encompassing technical and organizational measures;

2.1 Enforce irreversible destruction of data at the conclusion of the retention period;

2.1 Emphasize the exclusive retention of data within the EU to ensure effective protection, particularly in response to legal and political challenges like Snowden's PRISM revelations and issues associated with cloud computing.

Certainly, the enumeration of essential criteria and legal standards to be respected for potential revisions to the Data Directive poses several challenges for the EU institutions. Indeed, the judgment holds significant immediate implications for the intersection of privacy and surveillance. It serves as a landmark decision, representing a constitutional momentum that carefully balances fundamental rights and security in the digital era. Specifically, the judgment strongly condemns excessive data retention by private entities for law enforcement, unequivocally asserting that disproportionate infringement on the right to privacy and personal data protection is unacceptable, even for crucial objectives. This stands as a solid affirmation of privacy and data protection as inherent fundamental rights, countering the erosion observed in the context of counterterrorism and enhanced surveillance. In essence, the judgment underscores the imperative of upholding these rights while addressing terrorism and serious crime[71]. However, the reception of this judgement satisfied a small part of the audience. Amongst these, the European Data Protection Supervisor (EDPS) alone welcomed the ruling, considering it a landmark decision restricting indiscriminate surveillance of communication data by governments. The EDPS welcomed the CJEU's statement that the

[70] Guild, E., Carrera, S. (2014). *Op. Cit.*, p. 8.
[71] Ojanen, T. (2014). *Op. Cit.*, p. 539.

directive constitutes a serious and unjustified breach of the fundamental right to privacy enshrined in the EU Charter. In particular, the EDPS emphasized the importance of the judgment that states that retention of communication data must be explicitly specified and limited to specific contexts, with precisely defined and limited purposes, refusing to entrust this responsibility to the Member States. In a crucial remark, the EDPS pointed out that the judgment requires a firm position of the EU in negotiations with third countries, particularly the US, regarding access to and use of communication data belonging to EU residents - an observation that highlighted one of the most sensitive aspects of the judgment[72].

Simultaneously, the judgment may be seen as a letdown for those who have advocated for a distinct separation between privacy rights and the right to data protection, contending that Article 8 of the Charter independently safeguards the protection of personal data. The judgment acknowledges this distinction to a limited extent, as the Court's rationale primarily rests on the premise that the safeguarding of personal data is "especially important for the right to respect for private life enshrined in Article 7 of the Charter"[73]. Nevertheless, a positive aspect of this stance lies in its reinforcement of the substantive coherence between the Charter, the European Convention on Human Rights (ECHR), and other human rights treaties, such as the International Covenant on Civil and Political Rights (ICCPR). These treaties refer to the right to the protection of personal data as an integral facet of the broader right to the protection of private life under Article 8 of the ECHR and the right to privacy under Article 17 of the ICCPR[74]. It is crucial to underscore that the judgment does not categorically reject mandatory data retention. While it highlights the incompatibility of electronic mass surveillance, rooted in vaguely defined provisions, with the right to respect for private life and the protection of personal data, there is an implicit suggestion in the judgment that some form of mandatory data retention to address serious crime and terrorism might align with fundamental rights. It is noteworthy that the judgment distinctly outlines considerations that the EU legislature (or national legislatures operating within the EU law framework) should consider when constraining the legislative framework on data retention

[72] Guild, E., Carrera, S. (2014). *Op. Cit.*, p. 9.
[73] Court of Justice of European Union (Grand Chamber), 8 April 2014. *Op. Cit.*, paragraph 53.
[74] Ojanen, T. (2014). *Op. Cit.*, p. 540.

to what is deemed "strictly necessary"[75]. These principles can be derived primarily, if not exclusively, from the collective shortcomings of the Data Retention Directive that led to its invalidation. However, since the Court does not have the authority to establish the necessary legislative framework, there is now a positive obligation on the EU legislature and, consequently, on the authorities of the single Member States to formulate a legal regime for mandatory data retention that properly aligns with the Charter, as interpreted by the Court. The Court's ruling may be seen as a form of dialogue between the Court and legislators, in which the Court annuls a piece of legislation, and also suggests how legislators could enact valid legislation that achieves the primary objectives of the invalidated law. Although this can be a challenging task, it is essential to underline the positive obligations of legislators in providing an appropriate legislative framework for data retention, taking careful note of the CJEU's ruling. It is worth adding that this positive obligation extends to national legislators, considering that, within the broader framework of EU data protection, Member States are still perceived as operating under EU law and thus obliged to apply the Charter as construed by the Court in this milestone judgment[76].

Another aspect to consider about this ruling is that not only it has assigned to the EU a new responsibility to protect human rights, but it has also established a strict scrutiny test to apply to EU legislation to evaluate whether it interferes with human rights. Moreover, it has also defined a proportionality test that applies under the Charter's compliance. A further aspect to analyze concerns the clarification of the borders along which the concepts of privacy and data protection apply in the European Union, providing guidelines to the legislator for the definition of data retention schemes in respect with fundamental rights by private authorities and not only by the public ones[77].

With regard to the first aspect, the protection of human rights has gained importance in the Union in the latest two decades. The Court of Justice, traditionally cautious in its scrutiny of legislative acts, has shifted the responsibility to the EU legislators, urging them to include the necessary safeguards in laws that interfere with human rights. This change could lead to

[75] Ojanen, T. (2014). *Op. Cit.*, p. 541.
[76] *Ibidem*.
[77] Granger, M-P., & Irion, K. (2014). *Op. Cit.*, p. 844.

more human rights-focused EU legislation, expanding the Court's control over national measures. The increased legal weight of the Charter and the prospect of accession to the ECHR have influenced this change. The Snowden revelations, which exposed large-scale surveillance, and human rights concerns in some Member States have likely accelerated this change, positioning the Court as a key contributor to upholding EU principles and values[78].

With respect to the scrutiny test, the Court, while articulating the need for stringent measures to oversee EU legislative acts that potentially interfere with fundamental rights, has left certain aspect unaddressed entirely. Notably, questions persist regarding the application of the strict scrutiny test, including the criteria for assessing the seriousness of interference, the appropriate assessment method, the scope of rights to which the scrutiny test is applicable (whether all rights protected by the Charter or specific ones), the justification for serious interference with Charter's rights, the assessment method of such justifications, and the potential policy areas subject to the scrutiny test.

Primarily, the court refrains from defining the criteria that categorize an interference as serious. However, it endorses the rationale presented by the Advocate General concerning the extent and duration of the interference, the intrusion of privacy as a consequence of profiling and mapping, along with the outsourcing of such data to private companies as the providers of electronic communication services, and not public authorities. This reasoning also opens the question on the risk that these data may be transferred outside the territorial jurisdiction of European Member States, due to the lack of provisions in this merit in the Directive[79]. Secondly, with regard to the choice of rights to be included for the scrutiny test, although it is desirable that every right be considered of equal value, it is nevertheless noticeable that the Court has paid particular attention to certain rights, including the right to privacy. The third instance to be analyzed concerns the Court's evaluation of the proportionality of interference with the rights to privacy and data protection only in relation to "unofficial" security objectives of the Directive, which raised confusion. While choosing the security objective would have been tactically advantageous if the court intended to protect

[78] Granger, M-P., & Irion, K. (2014). *Op. Cit.*, p. 845.

[79] Opinion of Advocate General Cruz Villalòn in Joined Cases C-293/12 and C-594/12 (December 2013). Paragraph 70-80.

the Directive, the illogical aspect lies in the Court's willingness to annul the Directive despite relying on the security aim for evaluation. In this regard, one plausible interpretation offered by the authors Granger and Irion considers the option that faced with the imperative to uphold fundamental rights, the Court has generally shown a willingness to subject security measures, including anti-terrorist policies, to scrutiny based on human rights checks[80]. The Court has also developed a proportionality test to be applied in cases of interference with the right to privacy. Indeed, the development of such test in the concerned case has contributed to the definition of the Digital Rights Ireland as a landmark decision, providing a restrictive framework for the EU data protection reform, namely the Proposal for a Directive on data protection[81]. Furthermore, in line with Digital Rights Ireland, a comprehensive governance framework for public authorities is envisaged, incorporating specific safeguards and strict checks and balances throughout the data processing cycle. The judgement emphasizes the inadmissibility of indiscriminate data retention in law enforcement, calling for targeted approaches based on threat assessment, limited time periods, specific geographic areas or relevant groups. The "instruction to discriminate" approach supports the return to targeted data retention techniques. Furthermore, retained personal data should be subject to high levels of protection and security, supervised by an independent authority within the European Union. Retroactive access to retained data should be only allowed if strictly necessary to prevent, detect and prosecute certain serious crimes, and requests be subject to a reasoned review by a court or an independent body. Access and use should be restricted to a limited number of authorized persons, in line with specific requests, ensuring compliance with constitutional and legislative limits[82].

With regard to private sector organizations facilitating the collection and storage of data for law enforcement purposes, it is essential that strict rules are in place to ensure a high level of

[80] Granger, M-P., & Irion, K. (2014). *Op. Cit*., p. 847.

[81] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. COM/2012/010 final.

[82] Granger, M-P., & Irion, K. (2014). *Op. Cit*., p. 849.

protection. In particular, these rules should prohibit service providers from considering economic factors when determining security levels.

The EU judges demonstrate a deep understanding of contemporary global data flows and the potential for data storage in cloud services worldwide. The ruling, in paragraph 68, could be interpreted as prohibiting the transfer of data by private entities and, conceivably, by EU institutions and public authorities, outside the EU. This is because such a transfer would remove access and use from the supervision of an independent authority, contrary to the provisions of Article 8(3) of the Charter of Fundamental Rights[83].

However, winning against mandatory data retention may have symbolic weight, as metadata persist in the private sector for long periods. According to Article 6(1) of the ePrivacy Directive[84], network operators and providers of electronic communication services may retain metadata for as long as necessary for billing purposes or, with the user's consent, for the processing of data[85].

given the preceding analysis, it becomes evident why, as mentioned at the outset, the 2014 decision continues to be recognized as a milestone in European Union jurisprudence. First, it gives the EU legislator greater responsibility for safeguarding fundamental rights. Second, it introduces a new and strict test of judicial review. Third, it invalidates an EU framework law for violation of Charter rights. Fourth, it provides substantive guidelines for legislators at both European and national level, with the aim of ensuring adequate protection of privacy and data rights in a context of increasing securitization and exceptional circumstances. The ruling not only leverages Charter rights on privacy and data protection against blanket data retention, but also demonstrates a determined effort to curb the exceptional states and securitization tendencies prevalent in recent European anti-terrorism laws. The Digital Rights Ireland and Google Spain rulings affirm that strict privacy and data protection standards

---

[83] Court of Justice of European Union (Grand Chamber), 8 April 2014. *Op. Cit.* paragraph 68.

[84] "*Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1)*." Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[85] Granger, M-P., & Irion, K. (2014). *Op. Cit.*, p. 849.

apply to both the public and private sectors in the European Union's Big Data era. Legal challenges are emerging that seek to explore the broader implications of Europe's protective stance on other EU and national data measures. Moreover, the ruling changes the dynamic between the Court of Justice and the EU legislature from deference to mutual control. The Court's willingness to examine references for preliminary rulings challenging the validity of directives may transform this procedure into a constitutional review tool rather than a mere "integration tool". This redefinition of the constitutional context suggests a potential shift in which human rights take precedence over the internal market as the primary objective of the integration project. Lastly, as previously noted, this verdict delves into the potential involvement of private actors in the realm of data retention, thereby extending their role to the broader context of counterterrorism efforts.

Following to the comprehensive examination of these factors emerged from the case concerned, as elucidated in the case analysis, an additional distinct theme in the endeavor to combat online terrorism has surfaced: the involvement of private entities, including hosting service providers, in increasing anti-terrorist initiatives. Consequently, the subsequent section will scrutinize the extent of engagement by private actors in this domain.

1.4 Conflict of interest in non-State actors

As delineated in the initial pages of this research, terrorism has proliferated into the realm of cyberspace, utilizing the Internet, social media platforms, forums, and websites to advance its actions and objectives and to spread the communication of acts of violence across a multiplied audience through the network[86]. Additionally, terrorists exploit cyberspace as a platform to plan and execute real-world attacks. Consequently, the struggle against this evolving form of terrorism has extended into the digital domain, prompting the formulation and enactment of ad-hoc regulations governing counterterrorism efforts in the online domain, along with the actual sphere of influence of law enforcement agencies expanding there. Within this context terrorist groups extensively leverage social networks such as Facebook,

[86] Jenkins, B.M. (1974). *International Terrorism: A New Kind of Warfare*. Santa Monica, CA:RAND Corporation, p. 2.

Twitter, YouTube, and Google[87]. It follows that non-State actors, namely legitimate private entities, are directly implicated in both terrorist activities and the subsequent counterterrorism initiatives, both by their own initiatives and by law obligations.

In this regard, European Member States have chosen to address the issue of online terrorist content by enacting new legislation at the Union level, mainly with Regulation 2021/784[88].

This legislation places the burden on Hosting Service Providers (HSPs), comprising private entities such as online media outlets and social media platforms. These providers are tasked with preventing the so-called content providers, namely the users of these platforms, from disseminating content that may be perceived as terrorist-related. The complexity of this development lies in its significant impact on a fundamental right recognized by democratic States, namely the right to freedom of expression. This challenge is exacerbated by the absence of a straightforward answer to the question of what expressions precisely constitute terrorist content[89]. Despite the enduring tradition of voluntary collaboration between national governments and HSPs, a recent surge in global legislation compels the latter to assume extensive legal responsibilities in combatting the dissemination of terrorist content in the digital domain. As a result, there have been several EU efforts to regulate this field through supranational legislation, at the same time challenging fundamental human rights[90].

Starting from an analysis of the involvement of non-State actors in countering terrorism, the first consideration to be made regards the engagement of private entities in the broader sphere of security, which per se shall not be regarded as a brand-new phenomenon. Indeed, as per recent scholars works, the neoliberal restructuring of state power has accelerated the trend towards a "privatization of security"[91]. As a matter of fact, in the post-9/11 era a notable trend

---

[87] Bennett Clifford, *Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States*, (The George Washington University Program on Extremism, December 2021), pp. 14-18.
This argument has also been articulated by Weimann, G., *ivi note* 4 and 5.

[88] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (O.J. L 172, 17 March 2021). A detailed examination of the same will be provided in Chapter 3.

[89] Gherbaoui, T., & Scheinin, M. (2023). *A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it*. Journal Européen Des Droits De L'homme-European Journal of Human Rights, 1, pp. 3-29.

[90] *Ibidem.*

[91] Abrahamsen, R., Leander, A. (2016). *Routledge Handbook of Private Security Studies*. London; New York: Routledge, Taylor & Francis Group.

is the rise of "security assemblages", denoting transnational networks and structures wherein diverse players and normative frameworks engage, collaborate, and contend to generate newly established institutions, methodologies, and configurations of de-territorialized security governance[92]. In response to both transnational and domestic terrorism, governments are increasingly augmenting their robust counterterrorism (CT) strategies with softer measures aimed at countering violent extremism (CVE). These efforts involve a diverse array of participants, encompassing civil society in conjunction with law enforcement and the military[93]. Terrorism and violent extremisms are now governed through security assemblages, described as "*fluctuating arrangements of networks of state, corporate, and other voluntary actors*"[94]. As part of this shift towards a comprehensive approach, pivotal partners officially recognized are major social media corporations such as Google with Youtube, Facebook with Instagram, and Twitter. In this regard, the assumption underlying their recognition is that their services may contribute to cognitive and/or violent radicalization[95] of the would-be terrorists. The online presence of terrorist content is consequently deemed a priority by both public and private stakeholders due to its suspected real-world implications for physical safety and collective security of the citizens and of the State as a whole. According to the research conducted by Borelli[96], the private actors which

[92] Abrahamsen, R., Williams, MC. (2010). *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press, p. 90.

[93] Beutel, A., Weinberger, P. (2016). *Public-Private Partnerships to Counter Violent Extremism: Field Principles for Action.* Final Report to the U.S. Department of State. College Park, Maryland: START, p. 2.

[94] Tréguer, F. (2019). *Seeing like Big Tech: security assemblages, technology, and the future of state bureaucracy*. In: Bigo D., Isin E., and Ruppert E. Data Politics: Worlds, Subjects, Rights. Routledge Studies in International Political Sociology. London: Routledge, p. 148.

[95] Orsini, A. (2020). *What Everybody Should Know about Radicalization and the DRIA Model, Studies in Conflict & Terrorism*. Routledge Studies in Conflict and Terrorism. According to the DRIA Model, a crucial distinction lies between cognitive and violent radicalization. Cognitive radicalization pertains to an individual's interpretation of the world, which may enter into conflict with the mainstream interpretation. On the other hand, violent radicalization involves an additional dimension - the utilization of violence to enact the beliefs acquired through cognitive radicalism. These two forms are not inherently concurrent; frequently, individuals with extremist ideas may not exhibit violent behaviour.
In this regard, also Cfr. Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2020). *A field-wide systematic review and meta-analysis of putative risk and protective factors for radicalization outcomes*. Journal of quantitative criminology, 36, 407-447.

[96] Borelli, M. (2023). *Social media corporations as actors of counter-terrorism*. New Media & Society, 25(11), 2877-2897, pp. 2. The research investigation method is based on a qualitative inquiry conducted in the period

have become main players in the policy area of CT and CVE are the platforms of Google, Facebook and Twitter, consequently to their globally-recognized role as establishers and enforcers of a structured governance regime on terrorist communications. In this sense, since the wave of terror attacks from 2015 to 2017 carried out by the self-proclaimed Islamic State, there has been a notable increase in private and public-private online counterterrorism/countering violent extremism measures. This proliferation appears to be spearheaded by Google and Facebook, with Twitter playing a comparatively lesser role, and with YouTube, whose role has increased throughout the years.

In fact, the commencement of the effective utilization of the Internet by Islamists terrorist groups for recruitment and propaganda can be traced back to the year 2010, marked by the emergence of the magazine "Inspire" by Al Qaeda. The evolution of this realm has subsequently advanced toward prominent platforms such as the ones abovementioned which, by very of their inherent characteristics, now find themselves at the forefront of the ongoing conflict between terrorist organizations and governments striving to curb their activities[97].

In this regard, according to the analysis of Klonick[98], Google, Facebook, and Twitter can be considered as the "new governors" of online speech and democracy. Indeed, through their extensive content moderation mechanisms, these companies establish and enforce guidelines governing prohibited content and behaviors for their extensive user communities[99]. Although these legislative instruments are more flexible than those employed by states, their potential to reach global audience becomes particularly significant in combating a transnational phenomenon like terrorism occurring on a transnational medium, that is the Internet. Consequently, the distinctive positions occupied by the private companies of Google, Facebook, and Twitter permits them to contribute shaping the global governance framework

from May 2018 to March 2019 with different open sources that leverage corporate communications and it includes a series of interviews with European stakeholders.

[97] Jensen, M., James, P., LaFree, G., et al. (2018). *The Use of Social Media by United States Extremists*. College Park, Maryland: START.

[98] Klonick, K. (2018). *The New Governors: The People, Rules, and Processes Governing Online Speech*. Harvard Law Review (131): 1598–1670, p.1665.

[99] Gorwa, R., Binns, R., & Katzenbach, C. (2020). *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*. Big Data & Society, 7(1), p. 11.

in the matter of terrorist communications[100]. The way this governance regime is shaped by the concerned private actors is analyzed in depth by Borrelli, who provides a four-action-based analysis of the phenomenon, considering the spheres of policymaking, moderation, human resources and private multilateralism. In the context of the first action, namely policymaking, the author elucidates how these private entities leverage the absence of a clear and universally accepted definition of terrorism to maintain ambiguity. They strategically adopt a customized definition aligning with their counterterrorism/countering violent extremism activities. Evidences of their unwillingness emerged clear in their failure to respond when questioned by the Chairman of the US Senate hearing on online extremisms. The query pertained to whether company representatives had reached a consensus on a shared standard defining what qualifies as terrorist content[101]. In the interviews conducted by the author for his study, as previously explained, a relevant element emerged is that representatives from Facebook and Google acknowledged the contentious nature of the issue and, despite this awareness, they underscored the objectivity and non-political nature of their respective approaches. Of the three companies analyzed, it emerges that Facebook is the most active towards banning online terrorist contents, starting at the beginning of 2011 in the Community Standards of the social network the explicit prohibition of contents in support of violent organizations[102]. Twitter, initially aligning with its self-proclaimed identity as the "*free speech wing of the free speech party*"[103], demonstrated a slower response compared to its counterparts in incorporating measures against terrorism into its Terms of Service. Following a series of harassment incidents, the platform expanded its policy under "Abusive behavior" to include the prohibition of indirect threats of violence and their incitement, with the clear prohibition of "threatening or promoting terrorism". Concerning the YouTube platform, its guidelines are developed by the Public Policy branch of Google. Being it the venue where Al Qaeda and Iraq-war related contents were published, the company was forced to adopt policies on the merit, with the addition of a series of option at disposal of the users,

[100] Ganesh, B., Bright, J. (2020). *Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation*. Policy & Internet 12(1): 6–19, p. 9.
[101] C-SPAN, 17/01/18, in Borelli, M. (2023) *Op. Cit.* pp. 6.
[102] Facebook (2011). <Facebook Community Standards>.
[103] Jeong, S. (2016). *The History of Twitter's Rules*. <Vice Motherboard, 14 January>.

such as the option "promotes terrorism" to report videos[104], becoming YouTube the first case of a private actor engaging directly with a public concern and adopting own measures to countering a collective threat[105]. Currently, Google maintains the highest level of circumspection among the three companies with regard to adopting an official position on its conceptualization of terrorism, violent extremism or violent criminal organizations. Despite the use of these terms, the company has refrained from publicly outlining their definitions. Whether actively formulating definitions of terrorism, as in the case of Facebook, or adopting an ambiguous stance on the relationship between violent extremism and terrorism, as in the approaches of Twitter and Google, or exercising caution in proposing distinct definitions, as in the case of Google, the private political efforts of these social media companies collectively indicate a hesitation to directly confront the inherently political nature of the notion of terrorism. However, this reluctance inevitably emerges in the course of implementation.

With regard to content moderation and human resources, the analysis is deeply interconnected. In the cyber fight against terrorism, over the years, the reliance on humans, including both users and moderators, for the removal of unwanted content has faced increasing criticism for its inefficiency in dealing with the prevalence of terrorist content[106]. Consequently, social media companies are progressively improving the reporting system by incorporating active monitoring. This evolution is a direct result of massive investments in artificial intelligence (AI) aimed at filtering their platforms[107]. At present times, the implementation of the so-called algorithmic moderation, defined as a system that ranks user-generated content through matching or prediction, resulting in governance outcomes such as account removal or withdrawal, has become crucial for platforms such as Google, Facebook and Twitter. This approach is crucial to meet the growing demands for accountability from both the governments and the public opinion[108]. These platforms employ several

[104] YouTube (2009). <YouTube Community Guidelines>.
[105] Hughes, S. (2018). Whose Responsibility Is It to Confront Terrorism Online? <Lawfare>.
[106] Neumann, P.R. (2013). *Options and Strategies for Countering Online Radicalization in the United States*. Studies in Conflict & Terrorism 36(6): 431–459. DOI: 10.1080/1057610X.2013.784568.
[107] Gorwa, R., Binns, R., & Katzenbach, C. (2020). *Op. Cit.*, p. 3.
[108] *Ibidem*.

technologies, including content hashing/matching to prevent the re-uploading of previously removed content, prediction/classification systems to identify and alert moderators to terrorist content, and the profiling software used by Twitter to identify users based on their behavior. Facebook, in particular, only employs these technologies when they achieve a high success rate, given their potential impact on freedom of speech[109]. Recent data indicate that 99.7 per cent of terrorist content removed on Facebook and 98 per cent on YouTube in 2020 were detected before being reported. Similarly, Twitter's proprietary software was responsible for detecting 94% of accounts deleted for terrorism in 2020. Appears therefore evident how automation played a crucial role in deplatforming[110] efforts against ISIS[111]. The novelty and importance of this major step of algorithmic moderation lies in the fact that it overrides the direct requirements of the law, which by default exempt platforms from any form of liability in cases of the presence of terrorist content online, within the limits, in the case of EU, of asking the platforms concerned to remove the illegal contents[112]. The shift from human to technological-automated demonstrates in the first place an increasing normative and societal trend towards the implementation of cyberspace in more and more spheres of action. Secondly, this shift also testifies the ever-increasing discretion in the hands of the three platforms at stake, Google, Twitter and Facebook, which is made explicit in the ease with which individual users of the platforms may be excluded from global public interactions as a consequence of the application of CT policies; policies indeed developed and implemented by the companies themselves before being ordered by the government.

With regard to this discretion, the role assumed by non-State actors ends up being inconsistent in some cases, due to the ambiguous definition of terrorism and the consequent application of broad and unclear bans on the matter by companies. This consideration is further substantiated by the fact that the actions taken by the same companies against other

[109] Which goes under the wider prospectus of violations of the right to freedom of expression.

[110] The concept describes the process of denying access to a platform to voices unacceptable to the major tech companies, or also described as the attempt to boycott a group or individual by removing platforms used to share information or ideas. Cfr. Möller, J., (Oct. 11, 2022). *What Is Deplatformization And How Does It Work?*. Israel Public Policy Institute. <Digital Transformation>.

[111] Conway, M., (2020). *Routing the Extreme Right - Challenges for Social Media Platforms*. The RUSI Journal 165(1). Routledge: 108–113. DOI: 10.1080/03071847.2020.1727157.

[112] Borelli, M. (2023). *Op. Cit.*, p. 8.

extremist groups and ideologies remain veiled and less transparent in respect to the significant level of discretion of their policies towards prohibiting terrorism and violent extremism[113]. This approach further corroborates the fact that policies characterized by vague definitions with wide margins of appreciation permit these private actors to maintain a more flexible behavior with a short-time response to cases of online terrorist content removal on their platforms[114]. In this regard, it is interesting to underline that the shift to automated moderation led to an improvement of the manpower engagement in the organizational structure, as companies like Google, Facebook and Twitter have actually increased their human support in the deployment of CT/CVE technology, through actions such as public policy and government relations teams charged with formulating and disseminating CT/CVE initiatives globally, legal teams charged with examining the legality of government requests or corporate actions, and teams of moderators charged with enforcing established rules, with a double approach including qualitive and quantitative components[115]. Moving to the fourth dimension, that of private multilateralism, one of the most relevant efforts made by these non-State actors consists in the creation of the so called GIFCT, that states for Global Internet Forum to Counter Terrorism, founded in May 2017 by YouTube, Twitter, Facebook and Microsoft. It is a private multilateralism initiative rationalized by the challenge of terrorist migration, to be confronted by an industry-wide response[116]. It aims to facilitate negotiations with public authorities by offering a centralized platform for online terrorism discussions involving the private sector, with a core structure composed by a committee of senior representatives from the founding companies. The Forum allows other companies to seek membership, provided they meet six criteria outlined by the founding

[113] Evidences of this phenomenon became particularly conspicuous in the aftermath of the 2019 Christchurch attack, underscoring the platforms' lack of readiness in confronting the challenges posed by far-right terrorism. The concerned event disclosed the mismatch between general counter terrorism policies targeting terrorism and their implementation lacking in consistency. Moreover, this inconsistency appears to be intentionally overshadowed by corporate officials. Following the Christchurch event, Facebook declared to have expanded its hate speech policy to encompass white nationalism and separatism, resulting in favourable publicity. Common, M.F. (2020). *Fear the Reaper: how content moderation rules are enforced on social media*. International Review of Law, Computers & Technology 34(2). Routledge: 126–152. DOI: 10.1080/13600869.2020.1733762.

[114] Borelli, M. (2023). *Op. Cit.*, p. 11.

[115] *Ibidem*.

[116] Weimann, G. (2014). *Op. Cit.,* p. 14.

members, who retain discretion in admitting or rejecting applicants[117]. Moreover, the GIFCT comprises three key operational pillars, of which the technology pillar is the most relevant, with the "shared industry hash database" (SIHD) designed for terrorist content. It facilitates the assignment of a unique identifier, or hash, to terrorist content removed from member platforms. These hashes are incorporated into the shared database, allowing other participating companies to scan their respective services for such content, in a cooperative perspective[118]. The second pillar, focusing on "knowledge and information sharing", involves GIFCT initiatives aimed at disseminating best practices in content moderation to SMEs that may not have the resources or personnel to develop their own strategies against terrorist exploitation. This effort is implemented through a public-private partnership named Tech against Terrorism, created by the governments of Spain, Switzerland and South Korea in collaboration with GIFCT companies. Lastly, the third pillar is based on the objective of financing the Global Terrorism and Technology Research Network, which is a network guided by the Royal United Services Institute and comprising of eight partner institutions. The primary objective is to investigate in the field of policy-oriented studies focusing on the exploitation of the Internet by terrorists.

What emerges from these considerations is that private organizations are shifting from a responsive stance, influenced by concerns about potential damage to their reputation and anticipation of stringent regulations within the EU, to an increasingly proactive role as significant global players in counter-terrorism and countering violent extremism. They demonstrate a commitment to self-regulation and show inventive approaches in engaging in this area, exceeding the current legal requirements in both the EU and the US, at least for the time being. In fact, these private entities play a crucial role in the development and implementation of the burgeoning online CT/CVE regime, with a paradigm shift observed in the governance of these policies, wherein platform firms have emerged as a pivotal link in the so-called chain of security[119] through their implementation of self-regulation. This

[117] Cfr. GIFCT (2022). *GIFCT Working Group Principles and Guidelines*. <Principles and Guidelines of the GIFCT>.
[118] Gorwa, R., Binns, R., & Katzenbach, C. (2020). *Op. Cit.*, p. 4.
[119] De Goede, M. (2018). *The chain of security*. Review of International Studies, 44(1), 24-42, p. 28.

transformation aligns with the concept of global security assemblages, illustrating a new logic in the collaborative structures and networks shaping global security dynamics. Considering that the current framework for governing terrorist content originated in the aftermath of ISIS attacks, with limited public debate on the efficacy or desirability of involving social media companies in CT/CVE efforts, in recent the increased reliance on algorithmic moderation has increased and, consequently, opens the debate on risks to the safeguard of freedom of expression by essentializing political choices and introducing bias through inconsistent enforcement, masked as objectivity through technology[120]. The ambiguity surrounding content moderation, marked by vague rules, opacity, and inconsistent enforcement, also extends to terrorist content issues. In the realm of counterterrorism policy and CVE initiatives, renowned for civil liberties restrictions and discrimination, questions on the accountability are crucial in the analysis of the matter. In the following two chapters the evolution of the legislative framework of EU and Italy in countering terrorism activities on the cyberspace will be furtherly examined, in order to evaluate the balancing approach adopted by the Union and the Italian Nation to ensure collective security vis-à-vis the menace of terrorism and radicalization, and the safeguard level towards the respect of fundamental human rights, especially the right to freedom of expression and the right to privacy.

[120] Gorwa, R., Binns, R., & Katzenbach, C. (2020). *Op. Cit.*, p. 6.

Chapter 2 – The European legal framework to counter cyberterrorism

2.1 From the Budapest Convention to NIS Directive

Considering the analysis of the concept of cyberterrorism, it is a clear deduction the fact that terrorism has become a global phenomenon with the support and deployment of cyberspace, evident in the last two decades due to accelerating globalization, the spread of ICT and advanced information and communication systems, wide mobility, and the growth of Internet-based social networks. These factors have provided new opportunities for independent terrorists or groups operating in covert networks, while, at the same time, increasing the constant threat of terrorist incidents which has had a significant impact on state policies, societal perspectives, and legal structures. The present chapter seeks to explore the evolution of the legislative framework within the European Union addressing the threat of terrorism in cyberspace. The initial observation in this regard is that there is no dedicated legislation specifically addressing the comprehensive aspects of cyberterrorism, as elucidated in the previous chapter. This encompasses the use of Internet for purposes such as propaganda, recruitment and radicalization to the financing of terrorism and the execution of terrorist attacks with the support of cyberspace and on cyberspace itself. Nonetheless, there have been concurrent legislative endeavors aimed at delineating the threat and devising measures for the prevention, response and sanction of terrorist actions in cyberspace. These measures have evolved over the past two decades, driven by specific historical moments that have led to the immediate need to update existing regulations. Such moments include the events of 9/11 and the terrorist attacks of 2015-2017 that affected various member countries of the union. The Union, having encountered the repercussions of global terrorism and domestic sources of extremism, has been prompted to enact more robust legislation to address and counteract this threat. In the intersecting context of terrorism and cybersecurity, the first document to refer to as an attempt to draw up guidelines not globally in reacting to and

preventing the threats described above is the Budapest Convention[121] (hereinafter "The Convention") signed on 23 November 2001, a few months after the 9/11 attacks, by the Council of Europe. While being a document of international scope, it is noteworthy in the focused analysis of the European Union because it has served as a guiding framework for the subsequent implementation of community regulations. Additionally, as will be explored later, the Union stands out as the region with the most extensive reception and adoption of this international treaty. The Convention represents the first international treaty designated to combat crimes committed via the Internet and other computer networks and a benchmark for single States to draft national laws regarding cybercrime. Indeed, the Convention aims at harmonizing national laws, improving investigative techniques and strengthening international cooperation in the fight against computer crimes. It is interesting to highlight that the main objective of this Convention consists of the definition of offences related to computer systems, such as unauthorized access, illegal interception and data interference; the establishment of procedures for the investigation and prosecution of computer crimes and the facilitation of international cooperation between States in the areas of data retention and electronic evidence collection and extradition, providing the necessary means to justice authorities. The other main objective of the Convention consists in the promotion of the development of effective national legislation to tackle cybercrimes. The uniqueness of the Convention entails in its regional nature but its international application, as defined in Art. 37, which states that along with the Member States of the Council of Europe and those who participated in the draft of the peace of legislation, any other state is free to become a contracting party[122]. In fact, any state can be invited upon request of the Committee of Ministers to accede to the Convention following the unanimous consent of the contracting states[123], as explained in the aforementioned article. In this sense it is interesting to notice that by February 2020 38% of United Nations Member States were included in the

[121] Council of Europe (2001). *Convention on Cybercrime*. European Treaty Series, No. 185.
[122] Le Nguyen, C., Golman, W. (2021). *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "Law in action"*. Computer law & security Review, 40, 105521, p. 3.
[123] Council of Europe (2001), *Explanatory Report to the Convention on Cybercrime*. European Treaty Series, No. 185. Para 306.

Convention either by being Parties or Signatories or invited members, with a total of 74 States of which 46 from Europe, being members or observers in the Cybercrime Convention Committee (T-CY), evidence of the increasing consent and participation to the Convention especially within the European Region. Beyond its role in formal membership, the Convention currently seems to function as a framework or, at least, as a source inspiring the development of domestic legislation with 94% of UN Member States carrying out reforms or reforms being underway by January 2023[124]. The reasons for this increasing participation may be found in the fact that numerous additional states are deriving advantages from capacity-building initiatives considering that by February 2020 178 States had taken part to activities on cybercrime in the Council of Europe, of which, again, 48 States from Europe, representing the wide consent among countries from the Union, being the EU Member States all part of the Convention as signatory parties apart from Ireland which currently is an observer country. The importance of the Budapest Convention as a new source of legislation, the first in the field of criminal activities in cyberspace, is well explained by the following table:

		Use of Convention on Cybercrime as guideline or source							
	States	By January 2013		By January 2018		By February 2020		By January 2023	
All Africa	54	21	*39%*	33	*61%*	38	*70%*	42	78%
All Americas	35	22	*63%*	24	*69%*	26	*74%*	27	77%
All Asia	42	25	*60%*	27	*64%*	28	*67%*	30	71%
All Europe	48	46	*96%*	47	*98%*	47	*98%*	47	98%
All Oceania	14	10	*71%*	11	*79%*	14	*100%*	14	100%
All	**193**	**124**	***64%***	**142**	***74%***	**153**	***79%***	**160**	**83%**

Image 1. Use of Budapest Convention as guideline or source.

The Global State of Cybercrime Legislation 2013 – 2023: A Cursory Overview.

[124] Council of Europe (2022). *The Global State of Cybercrime Legislation 2013 – 2023: A Cursory Overview* (C-PROC, 2022), p. 3.

From these data appears evident the ever-growing trend of the relevance of the Convention in the development of domestic legislation, being it a guideline for the legislator, increasing from 64% to 83% in ten years, from January 2013 to February 2023[125].

Following these considerations, the widespread relevance and participation to the Budapest Convention has occurred concomitantly with the rise and spread of criminal activities deployed in cyberspace and/or with its auxilium. In this regard, its global nature, unparalleled growth, and the continuous technological advancements associated with it are indisputable aspects of this trend, which is consequently accompanied by an increase in the number of victims affected by such crimes, with a dominant role as protagonist played by the European Union, whose security is threatened by this phenomenon[126].

As early as 2015, the United Nations Office on Drugs and Crime (UNODC) projected that around 431 million individuals globally had fallen victim to cybercrime, with an increase to the first half of 2021 from 15% to 25% of victims operating in Europe. Furthermore, as per the most recent Cyber Security report from the Italian Postal Police, released on January 4, 2022, a total of 5,434 attacks targeted strategic structures throughout the year 2021 in Europe[127]. The high numbers of attacks and victims are the symptom of an upstream deficiency: the need for an international judicial cooperation which improves the effectiveness of both prevention and law enforcement actions. The transnational nature of cybercrimes is evident and indisputable, especially with regard to electronic evidence, which is one of the most relevant elements that competent authorities need to analyze. Electronic evidence has a specific location and storage, it originates most often from private sources, namely Internet Service Providers (ISPs), and is often located in a different jurisdiction than the one in which the crime is committed. Notwithstanding the translational nature of the criminal groups deploying such attacks, it therefore appears to be an imminent necessity to enhance the global legal structure, especially in terms of furnishing efficient tools for judicial collaboration and supranational coordination. The Convention represented the only

[125] *Ivi*, p. 6.
[126] Spiezia, F. (2022). *International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime*. In ERA Forum (Vol. 23, No. 1, pp. 101-108). Berlin/Heidelberg: Springer Berlin Heidelberg, p. 2.
[127] *Ibidem.*

instrument used by European states against cybercrime activities and to strengthen judicial collaboration in the beginning. In this sense, the development of the Additional Protocol[128] and the Second Additional Protocol[129] to the Convention confirmed its pivotal role in international cooperation procedures for investigating internet-related crimes and any other criminal activities requiring digital evidence acquisition. Indeed, the Second Protocol enhances specific positive aspects present in the original Convention, notably, it clarifies the relationships between digital service providers and the requesting authority[130], delineating the procedure to be followed by the designated authority in each Member State "to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control" upon order of the competent authorities in the cases when specific information of subscribers are required to conduct criminal investigations[131]. The overarching regulatory framework is refined, placing a strong emphasis on the cooperative dimension. Another dimension acknowledged by the Convention, but not extensively covered as it will be in subsequent provisions in the following years, pertains to the fundamental rights associated with the application of control measures in the sphere of cyberspace and information systems. It can be inferred that the Convention establishes an initial benchmark in considering the respect for individual rights, particularly referencing Article 8 of the European Convention on Human Rights on the right to privacy, as cited in Article 3 of the Convention regarding illegal interceptions. The latter article, in fact, is specifically focused on ensuring the privacy of data in communications. Further emphasis on the topic is given in Article 15 of the Convention, which obliges the Parties to establish conditions and safeguards that are sufficient for the protection of human rights and liberties. This provision allows national lawmakers the flexibility to incorporate variations in the legal safeguards for traffic data depending on its level of sensitivity[132]. This constitutes an initial assessment of the interplay

[128] Council of Europe (2003). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. European Treaty Series No. 189.
[129] Council of Europe (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. CETS No. 224.
[130] *Ivi*, Art. 6-7, Chap. II Sec. II.
[131] *Ivi*, Art. 7(1), Chap. II Sec. II.
[132] Council of Europe (2001). *Op. Cit.*, para 31.

between legislation aimed at countering online crimes and the fundamental rights of individuals, notably the right to privacy. Over the years and in subsequent legislative productions, there will be a continuous exploration and refinement of these intersections, particularly within the regulatory frameworks concerning counterterrorism and the fight against cybercrime. The impact of the Convention and the Protocols is, undoubtedly, noteworthy, particularly in terms of influence on EU regulatory processes aimed at enhancing the regulation of access to digital evidence for member countries. In fact, over the past decade, the EU has enacted significant legislative measures related to cyber-criminal matters. The first piece of legislation to consider is the Terrorism Situation and Trends Report (TE-SAT)[133] released by the Council and Europol in November 2002, addressing the threat of cyberterrorism for the first time. It was classified as a distinct form of terrorism together with other categories such as "anarchist terrorist movements", "bioterrorism" and "international terrorism". Despite the absence of reported cyberterrorism cases from EU Member States, it continued to be mentioned in the initial four TE-SAT reports. It was then excluded until 2012, when references to potential cyberterrorism threats to Member States began to surface more frequently in Europol reports. The perceived threat of cyberterrorism played a significant role in justifying the creation of a Framework Decision on Attacks against Information Systems[134], agreed upon in 2002. Conversely, the concept of cyberterrorism did not feature in the EU's inaugural Counter-Terrorism Strategy, released in December 2005[135]. During this period, the EU primarily concentrated on hindering terrorists' potential use of the internet for activities such as financing attacks, recruitment, and the dissemination of technical expertise related to terrorism[136]. Although initially overlooked in the original counter-terrorism strategy, cyberterrorism was identified as one of three main priorities in May 2006 as part of

[133] Council of the European Union (2002). *Non-confidential Report on the Terrorism Situation and Trends in Europe*. 20 November 14280/02.
[134] Council of the European Union (2002). *Proposal for a Council Framework Decision on attacks against information systems* (2002/C 203 E/16) COM(2002) 173 final — 2002/0086(CNS). OJEC C 203 E/109.
[135] Council of the European Union. *The European Union Counter Terrorism Strategy*. Brussels, 30 November 2005.
[136] *Ibidem*.

the revised EU Action Plan to Combat Terrorism[137]. The EU Working Party on Terrorism (WPT) placed particular emphasis on the concept of cyberterrorism in July 2011. As part of this initiative, the WPT recognized the necessity for a clearer definition of the concept and proposed that the EU develop a glossary of essential terms, potentially leading to the identification of legislative changes. The WPT underscored the absence of a clear definition of cyberterrorism in the EU and emphasized the need to establish a common understanding of the threat. It was suggested that a precise definition of cyberterrorism would facilitate a more effective response to the increasing prevalence of cyber-attacks in the EU[138]. The outcomes of this endeavor were released four months later in November 2011, where the TWP presented the previously mentioned glossary of terms related to cyber-attacks. The definition of cyberterrorism provided was described as "a terrorist offence as defined in the Council Framework Decision 2002/475/JHA committed in cyberspace"[139]. In this context, it was emphasized by the TWP that cyberterrorism is not clearly defined in any of the Member States, primarily because of the absence of a unified terminology at the EU level, leading to a deficiency in state resolutions for formulating strategies against cyberterrorism. Stepping forward to the Cyber Security Act, in Article 2 it enumerates twenty-two definitions of key terms; however, once again, a definition for the term cyberterrorism is not provided. The absence of a clear EU common definition adds complexity to the task of deducing the EU's understanding of cyberterrorism, making it more challenging. In fact, the EU's interpretation of cyberterrorism is multifaceted, encompassing several key dimensions. Firstly, it is classified as a hybrid security threat[140], among others, as highlighted in the European Agenda on Security. The agenda anticipates a rise in threats, including cyberterrorism and hybrid threats, in the future. EUROPOL emphasizes the merging of cyber and terrorism, stating that a cyber-attack has the potential to magnify the impact of a real-world attack, resulting in a hybrid attack that can disrupt essential public services[141].

---

[137] Council of the European Union. *Implementation of the Action Plan to Combat Terrorism*, Brussels, 11 June 2004.
[138] Baker-Beall, C., Mott, G. (2022). *Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis*. JCMS: Journal of Common Market Studies, 60(4), 1086-1105, p. 1093.
[139] *Ivi*, p. 1094.
[140] European Commission (2015). *The European Agenda on Security*. 28 April 2015.
[141] EUROPOL (2018). *TE-SAT: EU Terrorism Situation and Trends Report*. 20 July 2018.

Secondly, cyberterrorism is seen by the European Union as a dynamic, international threat that seriously jeopardizes democratic institutions. To lower the chance of being discovered, terrorists are increasingly using cyberterrorism, as highlighted by EUROPOL[142]. Thirdly, the EU calls for proactive steps in the current situation and describes cyberterrorism as a potential danger. The likelihood that future attacks will have a stronger cyber component is highlighted by Europol, which also highlights the flexibility of terrorists and their desire to further their technological know-how[143]. Lastly, there is a propensity within the EU to blend the concept of cyberterrorism with the broader phenomenon of terrorists leveraging the internet. Examples include references to terrorist propaganda sites and the internet's role in terrorism threats and radicalization. This conflation indicates a comprehensive interpretation of cyberterrorism within the broader framework of the internet's involvement in terrorism, which is the interpretation taken as a reference in the present analysis. Indeed, in addressing this issue, also the Council of the European Union has underlined that the internet and various network platforms play a central role in terrorism threats and radicalization[144].

Returning to the regulatory developments in the European Union in this field, after this consideration, the specific issue of cyberterrorism is no longer directly addressed in subsequent pieces of legislation. Instead, a distinction is observed between addressing cybersecurity, which also encompasses cases where terrorism utilizes cyberspace as a means or end, and, on the other hand, the issue of terrorist groups' use of the internet, with particular attention to the removal of terrorist online content. It is no longer a fusion but a division of threats and the ways to address them from the legislative approach. However, it is acknowledged that a clear boundary between the two cannot be drawn, and, in fact, over time, they tend to increasingly merge. Following the enactment of the Lisbon Treaty in 2009, cybercrime was explicitly incorporated into Article 83 TFEU[145] as a serious and transnational

[142] EUROPOL (2016). *TE-SAT: EU Terrorism Situation and Trends Report*. 20 July 216.
[143] Council of the European Union (2011). *Summary of Discussions. Working Party on Terrorism*. 25 July 2011. 13185/11.
[144] Council of the European Union (2013). *Letter from the LT Presidency to the Incoming EL Presidency on the Future Development of the JHA Area*. 13 December 2013, 17808/13.
[145] European Union (2007). *Consolidated version of the Treaty on the Functioning of the European Union - Part Three: Union Policies And Internal Actions - Title V: Area Of Freedom, Security And Justice – Chap. 4: Judicial cooperation in criminal matters – Art. 83 (ex Article 31 TEU)*.13 December 2007, 2008/C 115/01.

criminal phenomenon falling under the criminal jurisdiction of the EU. It is under the auspices of this article that directives such as Directive 2013/40/EU[146], adopted on 12 August 2013, addressing attacks against information systems, or Directive 2017/541[147] on combating terrorism, have been implemented. The significance of the Convention lies in its status as benchmark, being the initial international legislative framework that establishes the foundations for the development of communitarian and national legislation conforming to the principles and guidelines outlined therein, aiming to combat the proliferation of cybercrime, and establishing the groundwork for anti-terrorism regulations within the fifth domain[148]. In this regard, the European Union recognizes security as one of the focal points of anti-terrorism legislative production. Its security strategy outlines specific actions aimed at addressing strategic priorities in both the physical and digital realms, as well as in internal and external dimensions, in an integrated manner for the period 2021-2025[149]. It underscores the significance of security reports as tools to monitor progress and assess gaps and emerging threats. According to this report, the main points addressed by the EU's internal security strategy focus on enhancing the effectiveness of EU-wide alerts for criminal acts, optimizing the linkage of existing information through the implementation of interoperability in EU information systems, and fortifying the legal framework for cross-border police cooperation are key objectives[150]. This involves the augmentation of the acquis with provisions granting sufficient authority for cross-border surveillance and hot pursuit. Additionally, ensuring the responsible and transparent utilization of artificial intelligence technologies by law

[146] Directive 2013/40/EU establishes uniform regulations for criminalizing and imposing penalties on various offenses targeting information systems. It prohibits the use of botnets, malicious software intended for remote control of a network of computers. Additionally, it encourages EU countries to utilize the same contact points as the Council of Europe and the G8 for swift responses to threats involving advanced technology. The directive primarily addresses offenses such as attacks on information systems, encompassing denial of service attacks, data interception, and botnet attacks.

[147] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. OJEU L 88/6.

[148] Cfr. Martino, L. (2012). *La Quinta Dimensione Della Conflittualità. La Rilevanza Strategica Del Cyberspace E I Rischi Di Guerra Cibernetica*. Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Università degli Studi di Firenze.

[149] Council of the European Union (2020). *Council Conclusions on Internal Security and European Police Partnership.* Brussels, 24 November 2020.

[150] *Ivi*, pp. 2-3.

enforcement authorities is emphasized. Furthermore, efforts are directed towards augmenting the capabilities of law enforcement agencies to collaborate with international partners, encompassing both public and private entities globally. Lastly, the reinforcement of EU agencies, such as EUROPOL, FRONTEX and CEPOL, entitled to a more intensive work based on the sharing of information with public and private partners and third countries, especially granting access to all the necessary information to counter crimes of violent extremism and terrorism exploiting the internet[151]. This approach of wider margins of actions towards European agencies is integral to the comprehensive strategy aimed at fortifying the security infrastructure of the Union. Within this framework of EU's counter-terrorism strategy, the legislative production has focused on the matter largely, with three directives addressing the issue from different perspectives: Directive 2008/114[152], Directive 2016/1148[153], and Directive 2017/541[154]. In more recent times, also Regulation 2021/784[155] represents a piece of legislation particularly important on the matter.

The first directive in chronological order, 2008/114/EC, addresses the problem of the so-called "critical infrastructures". It is commonly recognized by the Union's bodies the necessity to safeguard European critical infrastructures from terrorist threats. Indeed, in June 2004, the European Council called for the development of a comprehensive strategy for the protection of critical infrastructure and in response, on October 20, 2004, the Commission issued a communication concerning the protection of critical infrastructure in the fight against terrorism. This communication outlined proposals to enhance prevention, preparedness, and response at the European level in the event of terrorist attacks involving critical infrastructures. In December 2005, the Council for Justice and Home Affairs urged the Commission to put forth a proposal for the European Programme for Critical Infrastructure Protection (EPCIP). It stipulated that this program should be based on a multi-

[151] *Ivi*, pp 5-6.

[152] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. OJEU L 345/75.

[153] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJEU L194/1.

[154] Directive (EU) 2017/541, *Op. Cit.*

[155] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. OJEU L 172/79.

risk approach with a primary focus on combating terrorism. Within this framework, the critical infrastructure protection process shall consider threats of both human and technological origin, as well as natural disasters, but with precedence to the terrorist threat. It is important to deepen the concept of critical infrastructure, which in this case is meant to identify an element, system, or part thereof located within the Member States that is crucial for sustaining the vital functions of society, health, safety, and the economic and social well-being of citizens. The damage or destruction of a European Critical Infrastructure (ECI) would exert a serious impact on a minimum of two Member States. Considering this, safeguarding sensitive information pertaining to the protection of ECI is imperative at an elevated level of safeguard as any unauthorized disclosure could be exploited for the strategic planning and execution of actions resulting in the harm or destruction of critical infrastructure installations[156], considering the fact that this type of infrastructures represent the optimal objective for terrorist groups. The reason for this stems from the modus operandi of terrorists, which is based on targeting objectives which, if struck, produce a consequent harm to the stability of the area hit and a widespread perception of insecurity within the society and/or to the symbol of the State as a whole. Indeed, the relevance of the terrorist menace and of the safeguard of sensitive information as drivers behind the development of this Directive testifies the need to improve the EU's efforts to enhance the resilience of critical infrastructure against potential threats, especially those related to terrorism. In this regard, it is important to highlight that the Directive sets a framework for cooperation and coordination - perfectly in line with the framework set by the Budapest Convention - among EU Member States, providing guidelines for the identification and protection of critical infrastructures while respecting the sovereignty of individual nations. Member States are expected to transpose the provisions of the Directive into their national legislation and take appropriate measures to ensure its effective implementation. Following this first legislative effort, due to the terrorist attacks that afflicted European Member States in the years 2015-2016[157], the

[156] Council Directive 2008/114/EC. *Op. Cit.*, p 3.

[157] Among the most infamous are Charlie Hebdo on 7 January 2015, the Bataclan on 13 November 2015, Brussels attacks on 22 March 2016 and the Nice attack on 14 July 2016. Cfr. Roy, O. (2018*). Secularism and Islam: The theological predicament.* Europe and Islam (pp. 15-29). Routledge.

Parliament and the Council jointly formulated Directive (EU) 2016/1148 and the year after Directive (EU) 2017/541. Directive (EU) 2016/1148 is considered to be the first comprehensive legislation at the European Union level addressing cybersecurity concerns and is known as the NIS Directive, addressing the security of network and information systems, officially adopted on July 6, 2016. The primary objective of this directive is to enhance and fortify the overall cybersecurity landscape within the EU and represents a critical step towards bolstering the resilience of critical infrastructure operators and digital service providers across Member States. The significance of the NIS Directive is underlined by its emphasis on promoting a proactive cybersecurity culture, requiring Operators of Essential Services (OES) and Digital Service Providers (DSPs) to implement appropriate security measures and report significant incidents to competent national authorities. These measures are crafted to proactively alleviate the consequences of incidents, thereby playing a role in safeguarding essential services and ensuring the security of personal data. In line with the NIS Directive, the EU cyber security strategy was reviewed at the end of 2017. Thereafter, in September 2017, the European Commission presented the Cybersecurity Act with the aim of giving the European Union Network and Information Security Agency (ENISA) the designation of EU cybersecurity agency. It also establishes a certification system for cyber-secure products at EU level, thus reinforcing the EU's commitment to rigorous cybersecurity practices and standards[158]. This proposal resulted in Regulation (EU) 2019/881[159], also known as the Cybersecurity Act, through which the ENISA has been granted a permanent mandate, enhancing its role, tasks, and responsibilities while allocating additional resources to effectively aid Member States in preventing and responding to cyber-attacks. In addition, this Regulation established the "European Cybersecurity Certification Framework", creating a unified system of technical regulations for certifying or assessing

[158] Andreeva, C. (2020). *The EU's counter-terrorism policy after 2015 - "Europe wasn't ready" - "but it has proven that it's adaptable"*. In Era Forum (Vol. 20, No. 3, pp. 343-370). Berlin/Heidelberg: Springer Berlin Heidelberg, p. 363.

[159] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJEU L 151/15.

ICT products, services, and processes, with the aim of enhancing the trust of citizens, organizations, and businesses in the European digital single market[160].

2.1 Evolving threat, evolving legislation: towards NIS 2 Directive

The following legislative development after the NIS Directive is constituted by Directive (EU) 2017/541, which concerns the fight against terrorism as the consequence of the escalating threat that foreign fighter and lone wolves, along with structured organizations such as Al-Qaeda and Daesh, represent. It has the dual objective of addressing existing protective gaps and of enhancing the Union legal framework establishing a common guideline for all Member States. The aim is to promote information exchange and cooperation among national authorities, and to facilitate the alignment of Communitarian law with international law, which had already expanded the scope of obligations for criminalization imposed on states to counter terrorism[161]. This Directive addresses three main fields of action. The first aims to address the gaps in the Framework Decision 2002/475/JHA[162] on combating terrorism, as amended by Framework Decision 2008/919/JHA[163], considering United Nations Security Council Resolution 2178(2014)[164] and the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism[165]. This is achieved through the introduction of four new obligations for criminalization: receiving training, undertaking travels for terrorist purposes, organizing or facilitating travels for terrorist purposes, and financing terrorism. The second field of action is the harmonization of the criminal and procedural-criminal legislation of the Member States

[160] Serini, F. (2022). *L'uso della normativa tecnica tra esigenze di mercato e di sicurezza delle reti e delle risorse informatiche*. GRUPPO DI PISA, (Quaderno 5, fasc. speciale monografico "Le fonti della crisi: prospettive di diritto comparato"), 747-759, p. 757.
[161] Santini, S. (2017). *L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541,* pp. 13-14.
[162] Council Framework Decision of 13 June 2002 on combating terrorism. OJEU L 164**.**
[163] Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism. OJEU L 330.
[164] United Nations Security Council (UNSC) Res 2178 (24 September 2014) UN Doc S/RES/2178.
[165] Council of Europe (2015). *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism*. CETS No. 217.

with the aim of creating a common legal framework that promotes cooperation among the states in all its forms. Also in this case, such as in the previous case of Directive 2008/114/EC and the NIS Directive, clear references to the Budapest Convention guideline framework are evident. The third line of action regards the victims of terrorism, whom the European legislator advocates for the adoption of specific protective, supportive, and assistance measures[166]. This directive broadens the scope of behaviors falling under the obligations of criminalization for the offense of terrorism, expanding and detailing the resulting sanctions, both in terms of criminal and procedural-criminal dimensions. Firstly, it is crucial to highlight that the concept of terrorism is updated here to encompass a dual nature, incorporating both objective and subjective elements. The objective element refers to intentionally enumerated acts that, by their nature, can cause harm to a country or an international organization. Meanwhile, the subjective element pertains to the intent to intimidate the population, coerce public authorities, and destabilize political, social, and constitutional structures[167]. Notably, this directive includes a first explicit significant reference to the use of cyberspace by terrorist groups. Initially it is recognized as one of the triggering reasons to focus on the punitive regulations concerning the misuse of the fifth domain for terrorist purposes. Subsequently, the need for a normative framework to take as a reference is emphasized, with an initial legislative step in this direction outlined in Article 5 of the Directive. In the preliminary considerations, found in *Whereas* (10), it is stated that the online dissemination of content (messages or images) related to terrorism and its victims, with the aim of garnering support for the terrorist cause and/or gravely intimidating the population, falls under offenses attributable to public provocation to commit acts of terrorism. These considerations are further elucidated in *Whereas* (22) and (23) from a perspective of countermeasures to address this threat. Indeed, it is emphasized how the removal of online terrorist content, constituting a public provocation to commit ideologically motivated and connected offenses, represents an effective means in this regard. However, contemplation is given to the role that individual Member States should or could play in this action. The necessity of cooperation with third countries is underscored to ensure the removal of online content comprehensively, extending

[166] Santini, S. (2017). *Op. Cit.*, p.14.
[167] Santini, S. (2017). *Op. Cit.*, p. 15.

to the servers of third parties located in the territories of third countries. This collaborative effort aims to make this counteroffensive measure fully effective. Additionally, it is specified that there is an intention to allow room for the private autonomy of industry actors, such as ISPs: "*[…] this Directive is without prejudice to voluntary action taken by the internet industry to prevent the misuse of its services or to any support for such action by Member States, such as detecting and flagging terrorist content*"[168]. Finally, emphasis is placed on the importance of respecting and protecting hosting providers, for whom no general obligation of surveillance over the information they transmit or store should be imposed. Moreover, there should be no requirement for them to actively seek facts or circumstances indicating the presence of illicit activities[169]. It is crucial to outline that, according to the provisions of the Directive, these entities should not be deemed responsible, except in cases where they are aware of the illegality of the activity or information[170]. From this analysis, three main points can be inferred:

1. the recognition of the need for joint and coordinated action at European Union level and also with third countries, thus potentially global, based on the timely exchange of information[171];
2. the identification of cyberspace as an increasingly critical focus in the fight against terrorism;
3. the imperative to complement the refinement of the sanctioning framework with a comprehensive program of prevention and response, not only on the procedural level

[168] Directive (EU) 2017/541. *Op. Cit.*, para. 22.
[169] *Ivi*, para. 23.
[170] *Ibidem*.
[171] On this point, particular attention is drawn to the *Whereas* (24): "To combat terrorism effectively, efficient exchange of information considered to be relevant by the competent authorities for the prevention, detection, investigation or prosecution of terrorist offences between competent authorities and Union agencies, is crucial. Member States should ensure that information is exchanged in an effective and timely manner in accordance with national law and the existing Union legal framework, such as Decision 2005/671/JHA, Council Decision 2007/533/JHA and Directive (EU) 2016/681 of the European Parliament and of the Council. When considering whether to exchange relevant information, national competent authorities should take into account the serious threat posed by terrorist offences." Additionally, the Whereas (25) states: "[…] Member States should ensure that relevant information gathered by their competent authorities in the framework of criminal proceedings, for example, law enforcement authorities, prosecutors or investigative judges, is made accessible to the respective competent authorities of another Member State to which they consider this information could be relevant.".

but also in practical terms, involving the removal of content. This action should be targeted and swift, contributing to a broader and effective prevention of the spread of radicalization.

This theme is underscored in *Whereas* (31) of the Directive, stating that "[…] prevention of radicalization and recruitment to terrorism, including radicalization online, requires a long-term, proactive and comprehensive approach". Accordingly, under Article 5, the Union mandates Member States to adopt necessary measures to implement these regulatory changes and pursue defined objectives, specifically making punishable "[…] the distribution, or otherwise making available by any means, whether online or offline, of a message to the public, with the intent to incite the commission of one of the offences listed in points (a) to (i) of Article 3(1), where such conduct, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences"[172]. However, it does not make any further mention of the specific methods that States should adopt internally, nor does it specify the constitutional limits within which the adoption of new rules to combat terrorism and its cyber aspects should be confined. This is particularly relevant given the involvement of private actors in this process and their increased autonomy in this regard. In fact, Article 5 creates a scenario of limitation on freedom of expression[173], although *Whereas* (40) believes it should not extend to include "[…] the expression of radical, polemic or controversial views in the public debate on sensitive political questions", along with the explanation that the content of the concerned piece of legislation shall not be intended to diminish or constrain the sharing of information for academic, scientific or reporting purposes[174]. These key issues, namely the removal of online content and the safeguarding of fundamental freedoms, are then addressed individually in Articles 21 and 23 respectively. Article 21, which focuses on measures to counter the problem of online terrorist content related to public provocation, not

[172] As for the interpretation of the terms "dissemination" and "otherwise making available", it may be useful to refer to the interpretation provided in the Explanatory Report of the Council of Europe Convention on the Prevention of Terrorism (§102). According to the report, distribution "refers to the active dissemination of a message advocating terrorism" while "otherwise making available" refers to "providing that message in a way that is easily accessible to the public, for instance, by placing it on the Internet or by creating or compiling hyperlinks in order to facilitate access to it.". Cfr. Santini, S. (2017). *Op. Cit.*, p. 5.

[173] A right consecrated by Art. 10 of the ECHR and Art. 11 of the European Charter of Fundamental Rights.

[174] Santini, S. (2017). *Op. Cit.*, p. 18.

only reiterates the obligation of content removal upon the single Member States and stresses the necessity to take measures congruent with the achievement of this objective, but also clarifies that such measures shall be established through transparent procedures. Furthermore, States must provide adequate safeguards to ensure that these measures are implemented in a manner that is limited to what is strictly necessary and proportionate, along with the respect of the publicist principle, specifically by publicly disclosing the reasons for implementing such measures to users. Regarding fundamental rights and freedoms, Article 23 clarifies that the concerned Directive does not prejudice the obligation to respect the fundamental rights and legal principles enshrined in Article 6 of the Treaty on European Union (TEU)[175]. Furthermore, it ensures that Member States may establish conditions in accordance with fundamental principles related to the freedom of the press and other means of communication. These conditions may encompass provisions regulating the rights and obligations of the press and other means of communication, as well as procedural safeguards associated with determining or restricting liability. A final interesting element of this Directive pertains to the principle of territoriality. Specifically, the general rule concerning the acknowledgement of jurisdiction within a State, as clarified in the accompanying report to the Directive proposal, remains anchored to the principle of territoriality[176]. Each Member State shall establish its jurisdiction for offenses covered by the Directive, committed wholly or partially within its territory. In the case of offenses related to a terrorist group or involving conspiracy, incitement, or attempted commission of said offenses, the jurisdiction applies "regardless of where the terrorist group is based or pursues its criminal activities"[177] provided that the offense is committed, entirely or partially, within its territory. It is interesting also the expansion to the extraterritoriality principle, insofar the State shall establish also its own extraterritorial jurisdiction in three scenarios[178]: if "the offender is one of its nationals or residents"; if "the offence is committed for the benefit of a legal person established in its

[175] Art. 6(1) TUE affirms that the Union recognizes the Charter of Fundamental Rights of the European Union, having the same legal status as the Treaties, and acknowledges the rights, freedoms, and principles outlined therein.
[176] Santini, S. (2017). *Op. Cit.*, p. 28.
[177] Directive (EU) 2017/541. *Op. Cit.*, Art. 19(5).
[178] Santini, S. (2017). *Op. Cit.*, p. 28.

territory"; if "the offence is committed against the institutions or people of the Member State in question or against an institution, body, office or agency of the Union based in that Member State"[179]. In this context, it is crucial to highlight the fundamental role that the assessment of jurisdiction and the principle of extraterritoriality plays in cyberspace-related terrorism crimes. Compared to classical crimes, cyberspace dynamics are characterized by an even greater margin of ambiguity and breadth in defining the boundaries of involvement of individual states. This complexity is accentuated by the possibility of exploiting remote networks and websites, introducing unique challenges in identifying competent jurisdictions and defining State responsibility in situations where criminal activities in cyberspace can easily cross traditional physical boundaries. In this perspective, Directive 2017/541 marks a fundamental first step in recognizing the growing importance of addressing emerging challenges in the regulatory environment. It focuses on identifying new regulations necessary to ensure public safety in the prevention of terrorism and radicalization. This initiative reflects the growing recognition that these threats have extended beyond the traditional terrestrial physical realm, increasingly penetrating the fifth domain, namely cyberspace. The Directive emphasizes the need to adapt and develop regulations that can effectively address the complex dynamics and unique challenges that emerge in this new context, thus helping to strengthen public protection and security in the era of increasing global digitization and interconnectedness.

The evolution of this Directive is represented by EU Regulation 2021/784, exclusively devoted to the formulation of a legislative framework for the removal of online terrorist content that represents a clear public incitement to commit crimes of a terrorist nature or to direct individuals towards terrorist ends. Differently from directives, which establish common objectives for all EU Member States to attain, a regulation is a legislative act that carries obligatory legal force. Indeed, by supplementing and expanding on the principles of Directive 2017/541, Regulation 2021/784 aims to consolidate the general obligation to cooperate among States and with third parties to remove online terrorist content hosted outside national borders by the platforms involved, upon a removal order from the designated

[179] Directive (EU) 2017/541. *Op. Cit.*, Art. 19(1, c-e).

competent authority[180]. By requiring Member States to share information on online activities, the Regulation promotes the establishment of national contact points to facilitate the exchange of information arising from criminal investigations of terrorist offences. Crucially, it should be noted that this piece of legislation not only focuses on preventing the online dissemination of material inciting terrorism, but also extends its scope to material used for recruitment or training, in accordance with Directive 2017/541. Differentiating from the latter, which does not impose surveillance obligations on natural or legal persons, the regulation introduces specific obligations also for Hosting Service Providers (HSPs), which perform "the storage of information provided by and at the request of a content provider"[181], clearly establishing responsibilities regarding the removal of terrorist content or the disabling of access to it. Moreover, as repeatedly emphasized by the text of Regulation 2021/784, it is imperative that the exchange of information regarding the potential dissemination of online content for terrorist purposes occurs with a preventive perspective, while respecting the system of fundamental rights related to the free expression of thought and information, as well as those linked to the processing of personal data[182]. Article 1(1) of the Regulation clarifies that the instructions for removal of terrorist content are subject to the HSPs' obligations of diligence and proportionality. The actual removal procedure, outlined in Article 3, requires each Member State to designate a competent authority with the power to issue the removal order to HSPs. In this context, timing is significant. Indeed, an obligation is imposed on HSPs to remove content within a maximum of 60 minutes from the receipt of the order by the competent authority, without prejudice. The specific situation of the removal order for cross-border content is also defined[183]. In this regulation, the legislator pays

[180] Signorato, S. (2021). *Combating terrorism on the internet to protect the right to life. The regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*. Yearbook: Human Rights Protection. Right to life, 403-408, p. 405.
[181] Regulation (EU) 2021/784. *Op. Cit.*, Art. 2(1).
[182] Villani, S. (2023). *La prevenzione di eventi CBRN di natura intenzionale: obblighi UE e attuazione in Italia*. Osservatorio Sulle Fonti, 1, 243-263, p. 19.
[183] Regulation (EU) 2021/784. *Op. Cit.*, Art. 4(1). In this case, the procedure for cross-border removal order starts from "where the hosting service provider does not have its main establishment or legal representative in the Member State of the competent authority that issued the removal order, that authority shall, simultaneously, submit a copy of the removal order to the competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established.".

particular attention to the principles that must guide the implementation of the procedure. The latter must be conducted with diligence, proportionality, non-discrimination and with respect for the fundamental rights of users[184]. In this context, the European legislator emphasizes the importance attached to freedom of expression and information in an open and democratic society. This principle is expressed repeatedly in the regulatory text, starting with the first Whereas[185]. This necessity, already stressed in Directive 2017/541, is further explained in Whereas 9 and 10 of the Regulation. The latter explicates that the aim is to preserve public security while providing adequate and robust protections to ensure the safeguard of fundamental rights, especially of the right to privacy, the protection of personal data, freedom of expression and the right to an effective judicial remedy. It also affirms that the designated competent authorities and HSPs shall only take measures that go under the umbrella of "necessity", "proportionate" and "appropriate" in a democratic open society. The approach considers the relevance attached to the freedom of expression and information, as well as to the freedom and pluralism of the media, which are fundamental to a democratic and pluralistic society, principles that are the foundations of the Union.

It is interesting to analyze the responsiveness to the regulation concerned, as it raised critical consideration. In Professor Martin Scheinin's analysis of Regulation 2021/784 within the framework of human rights law, the initial focus is on the challenges it presents regarding the permissibility of limitations, a crucial aspect of international human rights law that allows for flexibility, but within a well-defined framework for interpreting the boundaries of specific human rights. Although the Regulation states that its provisions apply "without prejudice to the fundamental principles relating to freedom of expression and information, including freedom and pluralism of the media", any removal order requires meticulous scrutiny of

[184] Regulation (EU) 2021/784. *Op. Cit*., Art. 5(1). "It shall do so in a diligent, proportionate and non-discriminatory manner, with due regard, in all circumstances, to the fundamental rights of the users and taking into account, in particular, the fundamental importance of the freedom of expression and information in an open and democratic society, with a view to avoiding the removal of material which is not terrorist content."

[185] The first Whereas states: "This Regulation aims to ensure the smooth functioning of the digital single market in an open and democratic society, by addressing the misuse of hosting services for terrorist purposes and contributing to public security across the Union.".

whether the measure implemented is necessary in a democratic society[186]. In this case, as explained by the author, a thorough assessment is required and with a double focus: on the one side on the identification of a legitimate aim, which in this case is related to counter terrorism, and on the other side on the benefits that the achievement of such aim would produce. This perspective aims to ensure that the reduction of human rights harm is appropriately minimized and remains proportionate in relation to the actual benefits obtained[187].

In this context, legal considerations in the field of human rights law open to complex questions as to whether specific content falls within the protected scope of freedom of expression, whether it is subject to exemptions during emergencies, or whether it is subject to limitations or exclusions permissible as an abuse of rights in normal times. These questions not only have legal implications, but also political ones, which is an aspect that derogates from the very nature that laws should have, being independent from the political sphere. EU Member States have different standards about the importance of freedom of expression and media pluralism, correspondent to the different nature of their political and governmental status. While international human rights law sets standards to which all treaty states must adhere, it also allows for interpretative flexibility, subject to international scrutiny, leaving space to adaptation to variations in societal norms regarding freedom of expression. Therefore, in cases of cross-border removal orders, the extraterritorial impact of an order from another state introduces the risk of imposing a more restrictive standard than the state in which the adverse human rights impact occurs might prefer[188].

The conflict between territorial jurisdiction in international human rights law and the extraterritorial impact of governmental expulsion orders is somewhat softened by the procedure provided for in Article 4(3)[189]. The latter allows the designated authority in the

---

[186] Gherbaoui, T., Scheinin, M. (2023). *A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it*. Journal européen des droits de l'homme-European Journal of Human Rights, 1, 3-29, p. 20.

[187] *Ibidem*.

[188] Gherbaoui, T., Scheinin, M. (2023). *Op. Cit*., p. 21.

[189] Regulation (EU) 2021/784. *Op. Cit.,* Art. 4(3): "The competent authority of the Member State where the hosting service provider has its main establishment or where its legal representative resides or is established may, on its own initiative, within 72 hours of receiving the copy of the removal order in accordance with

Member State where the HSP is located to carefully examine the expulsion order and determine whether it significantly or manifestly contravenes the provisions of this Regulation or the fundamental rights and freedoms protected by the Charter, leaving to the HSP the possibility to reintegrate the content ordered to be removed. What the author highlights in this reasoning is that what remains to be actually evaluated and confirmed by evidence and precedents is the effective making of these decisions on content reintegration[190].

A further regulatory development following Regulation 2021/784 is represented by the Directive (EU) 2022/2555, also known as the NIS 2 Directive[191]. It constitutes a major legislative effort in the field of cybersecurity, replacing the previous NIS Directive of 2016, in the effort to satisfy the need for new legislation in the face of the extremely fast development of the cyber front and its threats. Indeed, it aims to strengthen cybersecurity measures at the European level in a uniform and widespread manner. The Directive has thus enhanced and modernized the legal framework by broadening the scope of cybersecurity regulations to encompass novel sectors and entities, thereby improving not only the resilience capacity but also the incident response capacity of both competent authorities and public and private entities. Article 9 of the Directive delineates this enhancement, focusing on "National cyber crisis management frameworks"[192]. An initial examination reveals that this extension of applicability to new entities is configured through the joint fulfillment of three requirements, as defined in Article 2 of the Directive. The first requisite is that they operate in strategic sectors, such as energy, transport, banking, financial markets, drinking water, healthcare, and the digital infrastructures of e-commerce and cloud computing. The second requisite entails classification as medium-sized companies or exceeding the thresholds for

---

paragraph 1, scrutinise the removal order to determine whether it seriously or manifestly infringes this Regulation or the fundamental rights and freedoms guaranteed by the Charter. Where it finds an infringement, it shall, within the same period, adopt a reasoned decision to that effect.".

[190] Gherbaoui, T., Scheinin, M. (2023). *Op. Cit.*, p. 21.

[191] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[192] Art. 9(1): "Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management."

such enterprises. In this sense, the threshold used encompasses either a staff count of 250 or more, an annual turnover exceeding EUR 50 million, or an annual balance sheet surpassing EUR 43 million. The final requirement mandates the provision of services or conduct of activities within the jurisdiction of the European Union. Concenrning the objectives of the directive, they can be summarized in three main points. The first point aims to ensure an adequate level of preparedness of the Member States by requiring them to be adequately equipped, such as a structured security incident response team, the CSIRT[193], and a national Network and Information Systems authority (NIS)[194]. In particular, Art. 10 of the Directive refers to detection capabilities, Art. 11 to response and recovery and backup, while Art. 12 refers to backup policies and procedures, and recovery and restoration methods. The second objective is the development of a relationship between Member States based on cooperation (recital 5), both national (Art. 13) and International, the latter by establishing the International Union Cooperation Group (Art. 14) to support and facilitate strategic cooperation and intelligence sharing[195]. This objective is further detailed by the Directive in Art. 15 which refers to "further harmonization of ICT risk management tools, methods, processes and policies" to include detection capabilities, and in Art. 45 which refers to threat detection through "threat identification". The third objective concerns the development of a security culture in all sectors vital to the economy and society that depend on ICT, implemented through the adoption of the National Cybersecurity Strategy, as provided for in Art. 7 of the Directive[196]. With regard to the management of cybersecurity risks[197], particular attention is

[193] Directive (EU) 2022/2555, *Op. Cit.*, Arts. 10-12 on Computer security incident response teams (CSIRTs).
[194] Directive (EU) 2022/2555, *Op. Cit.*, Art. 8. on Competent Authorities and single points of contact, para. 1 "Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities)".
[195] Directive (EU) 2022/2555, *Op. Cit.*, Art. 13 on the Cooperation at National level, para. 1 "Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive" and Art. 14 on the Cooperation Group, para. 1 "In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established".
[196] Directive (EU) 2022/2555, *Op. Cit.*, Art. 7, para. 1 "Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity".
[197] Directive (EU) 2022/2555, *Op. Cit.*, Arts. 20-21, 24.

paid to the provisions of Article 17 on the "ICT-related incident management process", which refers to early warning detection, fundamental in order to reduce the risks and in line with the pre-emptive approach largely taken by the EU in its legislative approach to counter-terrorism and cyber threats. In addition, this securitization sphere is further regulated through the creation of channels for sharing cyber security information[198] as well as the submission to surveillance and enforcement measures[199]. It also establishes EU-CyCLONe, namely the European Network of Cyber Crisis Liaison Organisations[200]. From the analysis of the new directive, it emerges a new regulatory framework aimed at a homogeneous and coordinated strengthening of cybersecurity measures, with explicit attention to the creation of a fabric of resilience and prompt response to cyber-attacks both by public and private entities. However, it is important to underline how Directive NIS 2 has significantly complicated the regulatory framework regarding the security of critical infrastructures in terms of coordination, making the fulfillment of its requirements particularly burdensome for operators. In fact, following the delay in this normative production, several EU countries had already regulated, at least in an initial form, the cybersecurity framework internally. The issuance of the directive then represented a further burden on the actors, public and private, who shall now fulfill these obligations and provisions. Specifically, in cases where a good alignment between the European directive and national initiatives does not take place, many actors may face a burdening compliance cost while achieving, however, objectives already attained in practice. Therefore, the transposition of the NIS 2 Directive constitutes an opportunity for the national legal orders concerning the completion of a cybersecurity regulatory framework. Consequently, this effort of systematization shall be completed in consultation with EU member states to prevent the margins of discretion left to single States from creating differences in regulation and technology that could lessen or even completely negate the goals established by European legislation[201].

[198] Directive (EU) 2022/2555, *Op. Cit.*, Arts. 29-30.
[199] Directive (EU) 2022/2555, *Op. Cit.*, Arts. 32-33.
[200] Directive (EU) 2022/2555, *Op. Cit.*, Art. 16.
[201] Bavetta, F. (2023). *Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo*. <Media Laws>.

This analysis is crucial for deepening and interpreting in a broader perspective the legislation at stake, even from the point of view of its shortcoming. Although a new piece of legislation may represent significant progress and be at the forefront of regional legislation in some aspects, there remain other facets that require further attention and care, as illustrated in this concluding section of the analysis. It is evident that NIS 2 Directive, together with the other legal sources examined in this section, marks several improvements in recognizing regulatory gaps in the fight against terrorism and its manifestations in cyberspace. However, the role of institutional actors involves not only a punitive but also a preventive function, which requires cautious navigation between manoeuvres. Pursuing public safety while taking individual rights into account requires meticulous attention both in the legislative production process and in the subsequent monitoring of law enforcement in the practical and real sphere. Especially in a context like Europe, which is moving from a supranational entity to a state-level implementation of rules, meticulous attention and guidance in the implementation of new laws is indispensable.

2.3 The role of ISPs in online terrorist content removal

In the spectrum of the fight against cyberterrorism, particularly in its facet involving the prevention on the Internet (such as websites, forums, and social networks), the role played by Internet Service Providers, that are private entities, is of particular significance. These providers effectively function as private actors collaborating with the public sphere, undertaking responsibilities inherently associated with public authority, namely, online terrorist content removal. Their role, defined as global security actors in CT[202], aligns with the trend defined as the privatization of security[203], and deserves specific attention in the discourse concerning the analysis of the respect for fundamental rights of individuals, especially the right to privacy and the freedom of expression of online portal users. Simultaneously, the ability of ISPs, through their preventive and reactive actions, to ensure a

[202] Borelli, M. (2021). *Op. Cit.,* p. 13.
[203] Abrahamsen, R., Williams, MC. (2010). *Op. Cit.*

public security environment on the web is noteworthy. This environment is understood as one devoid of potential terrorist threats, in this case, defined as the mere presence of online content with a terrorist matrix, which may advocate violent religious radicalism and subversion, extending to actual participation in terrorist attacks. In this context different issues have emerged as subjects of the debate on the balance between legality and ethics, such as the role of private companies[204], the potential problem of censorship[205], the balance between ensuring a safe environment online and, at the same time, guaranteeing the respect of freedom of expression especially in the cases involving Social Media Platforms[206].

The regulation of Terrorism Content Online (TCO) presents an interesting convergence of anti-terrorism laws and the management of private platforms. In this scenario, the application of anti-terrorism legislation is consistently viewed through the lens of securitization, while discussions within the realm of private platforms revolve around the potential politicization of an area that had, until that point, been predominantly private and autonomous from the state and political sphere[207]. The legislative trajectory of the TCO has been characterized by pronounced contention, prompting meticulous examination by diverse entities within the realms of digital rights and human rights. The initial implementation of Directive 2017/541 had already raised concerns among users and private actors. Subsequently, the adoption of Regulation 2021/784 confirmed the involvement of these actors in counterterrorism and the prevention of radicalization, placing them in a hybrid role between mere private entities and the typically state-performed functions, broadly understood to encompass all structures and entities constituting the state. Stakeholders undertook a rigorous scrutiny of the proposal of the Regulation and negotiations, actively engaging in lobbying efforts across all EU institutions to effect amendments to specific provisions, thereby ensuring the Regulation's alignment with fundamental rights. Facilitated by the European Parliament, civil society

[204] Cfr. Cohen-Almagor, R. (2017). *The role of internet intermediaries in tackling terrorism online*. Fordham L. Rev., 86, 425.
[205] Cfr. Citron, D. K. (2018). *Extremist speech, compelled conformity, and censorship creep*. Notre Dame L. Rev. 93, no. 3: 1035-1072.
[206] Cfr. Coche, E. (2018). *Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online*. Internet Policy Review, 7(4).
[207] Ahmed, R. (2023). *Negotiating Fundamental Rights: Civil Society and the EU Regulation on Addressing the Dissemination of Terrorist Content Online*. Studies in Conflict & Terrorism, p.1.

actors attained a measure of success in shaping pivotal facets of the Regulation's conclusive text. This achievement serves as a noteworthy challenge to the securitized underpinnings inherent in counterterrorism paradigms with the involvement of non-legislative actors[208].

The introduction of stringent measures initially targeted at websites and notably on social platforms such as YouTube[209] and Twitter, mandating the removal of content that contravenes guidelines and, specifically, is attributable to terrorist ideologies, sparked widespread protests and apprehensions regarding a potential resurgence of censorship activities by institutions[210]. However, this time such actions would be executed comprehensively through the mediation of private actors, ISPs[211]. Therefore, accordingly to this legislative framework, private entities not only execute the removal action, but also establish, enforce and assume the role of mediators in the management of conflicting rights and freedoms, a function traditionally associated with the public domain. This marks a substantial shift in the dynamics between the public and private spheres, with significant implications not only for public policy, but also for private entities and the individuals affected by their decisions. Importantly, the existing legal framework fails to adequately capture or govern these emerging power dynamics. An example of this transformation is precisely the area of online content moderation within the framework of countering terrorism, where service providers play the key role in monitoring and removing such material, as explained. This responsibility is progressively subject to legislative and regulatory oversight; nevertheless, scrutinizing this

---

[208] *Ivi*, p. 2.

[209] See e.g.: Albadi, N., Kurdi, M., & Mishra, S. (2022). *Deradicalizing YouTube: Characterization, Detection, and Personalization of Religiously Intolerant Arabic Videos*. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1-25, and: Conway, M., & McInerney, L. (2008). *Jihadi video and auto-radicalisation: Evidence from an exploratory YouTube study*. Intelligence and Security Informatics: First European Conference, EuroISI 2008, Esbjerg, Denmark, December 3-5, 2008. Proceedings (pp. 108-118). Springer Berlin Heidelberg.

[210] Rojszczak, M. (2022). *Online content filtering in EU law–A coherent framework or jigsaw puzzle?* Computer Law & Security Review, 47, 105739, p. 2. See e.g.: *The EU Will Be The End Of Free Speech Online*, Forbes (6 July 2019), <End of Free Speech>.

[211] In a broad analysis, with regard to the regulation of publications, including online content, two main types of control can be identified: preventive (ex-ante) and reactive (ex-post). Reactive control involves judicial or competent authority intervention after content has been published, while preventive control aims to prevent potential infringements before publication. Reactive control is seen as a more proportionate interference with free speech and information rights, as it addresses already published content. In contrast, preventive control, often defined as censorship and connected to institutional action, seeks to avoid infringements by requiring prior approval from a designated public authority before publication. Rojszczak, M. (2022). *Op. Cit.*, p. 2.

approach is not without controversy, especially when ISPs are compelled to negotiate the delicate equilibrium between freedom of expression and other rights, not always convergent, traditionally within the purview of the State[212].

The responsibility of providers comes into play once the rules are agreed, requiring enforcement. As the process unfolds, providers are entitled to specifically address potential conflicts between freedom of expression or of speech and further connected fundamental rights. In this regard, private actors take on functions akin to public actors at various stages, engaging in rulemaking, enforcement, and adjudication. The essential element to recognize in this moment of the analysis is that this broadening of the scope of competence and responsibility for private actors arises directly from a legislative imposition, therefore from the law.

Nevertheless, platforms also proactively assume roles within this regulatory, adjudicative, and enforcement framework, as well exemplified by the Facebook Oversight Board case[213].

It can be indeed highlighted that, while legislation may impose certain duties, it doesn't always offer sufficient guidelines on resolving the above-mentioned conflicts. This creates room for private actors to perform public functions, and it becomes evident in the case of the European Union legislative efforts to counter online terrorist content with respectively Directive 2017/541 and Regulation 2021/487 which grant more margin of actions to private actors, with the aim of creating a sort of collaborative framework in which public actors not only cooperate with private ones, but more accurately, they benefit of the wider autonomy of

[212] Tosza, S. (2021). *Internet service providers as law enforcers and adjudicators. A public role of private actors.* Computer Law & Security Review, 43, 105614, p. 2.

[213] In May 2020, Facebook introduced its Oversight Board (FOB), composed of 20 members, among which prominent members such as Helle Thorning-Schmidt, former Prime Minister of Denmark, and Nobel Peace Prize winner Tawakkol Karman. The initiative was a response to requests from civil society organisations and the UN Special Rapporteur for an accountability mechanism to independently review content removal decisions. The FOB, which functions independently of Facebook, is funded by an irrevocable $130 million fund. The scholars analysed the expectations and limitations of the FOB, highlighting the broader need for private actors to participate in law enforcement and demonstrate proactivity and judicial power. Digital technologies, in particular Facebook, create a vital digital public space with both positive and negative consequences. Addressing regulatory challenges involves finding a balance between free speech and other values, managing both legal and harmful content, and navigating differences in laws around the world. This underlines the difficulty of finding the right balance in this context of multipolarity. Tosza, S. (2021). *Op. Cit.* and Cfr. Douek, E. (2019). *Facebook's oversight board: Move fast with stable infrastructure and humility*. North Carolina Journal of Law & Technology, vol. 21(1).

action upon ISPs, to the point of delegating them not only the action per se but also the responsibility of the balancing between security and freedom, without however weighting enough the lack of specific competences upon private actors on the merit of public and constitutional law, which is a competence of the State, or at least it has been so until this new legislative framework.

In this legislative context another element of relevant importance is the first attempt to regulate the cases of liability of ISPs vis-à-vis the publication on their platforms of illegal content and their obligations to provide for the prompt removal of such content. The first attempt in EU legislation is represented by the E-Commerce Directive[214] which provided for a set of essential and interconnected provisions, that, when are collectively satisfied, they ensure the exemption of the provider from liability for the content made available. These three provisions are related to mere conduit (Art. 12); caching (Art. 13); and hosting (Art. 14), with no obligation to monitor communications[215] (Art. 15). However, this legal framework quickly revealed its weaknesses, as the evolution from 2000 to today in the use of cyberspace and the platforms active on it has changed exponentially, rendering the provisions of such regulations outdated. It is interesting to note, however, that from the outset, the legislator had paid particular attention to the case of ISPs' liability, which needed careful evaluation[216].

The most recent and, so far, most extensive attempt to regulate the liability of service providers in the handling of illegal content can be found in the Regulation on a Single Market for Digital Services, known as the Digital Services Act[217], presented by the European Commission on 15 December 2020 and officially published on 27 October 2022. The Digital

[214] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") OJEU L 178/1.

[215] *Ivi*, Art. 15(1): "to monitor the information which they transmit or store, or to actively [...] seek facts or circumstances indicating illegal activity".

[216] Cfr. Rojszczak, M. (2022) *Op. Cit.*, pp. 6-7. "The E-Commerce Directive was adopted at a time when the global digital services known today – in particular social networks or media sharing services - did not exist. The development of electronic communications services has not only made it easier for millions of users to communicate freely but also made it possible for each of them to become an author publishing content of their choice and gaining an audience comparable to traditional media".

[217] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC. OJEU L277/1.

Services Act (DSA) preserves the liability exemptions of the e-Commerce Directive and maintains the prohibition of general monitoring obligations[218]. It systematically outlines the notification and action procedures applicable to all hosting and intermediary service providers, specifying the rules on how this mechanism should be provided to users, the components of a notification and the procedure for its processing[219]. Online platforms are obliged to implement an effective internal system for handling complaints related to decisions to remove content, restrict access, or suspend/terminate a user's account or provision of services. This obligation applies when these actions are taken due to a user's provision of content that is illegal or violates the platform's terms and conditions. For larger online platforms, a further significant obligation is to conduct a platform-specific systemic risk analysis[220]. These systemic risks include: the dissemination of illegal content and negative effects "for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child", as explained in Art. 26(1) of the DSA.

According to the EU Commission proposal on e-evidence[221], and the Council's General Approach, the ISPs may have role, however limited, in invoking grounds for refusal. The ISP may contest the order based on grounds related to the issuance conditions, if the order was not issued or validated by the competent authority, issued for offenses to which it does not apply, or if the service is not within the scope of the Regulation. Additionally, the ISP may challenge the order on the basis of manifest errors or factual impossibility, either *de facto* impossibility or if the order does not pertain to data stored by or on behalf of the service provider at the time of receiving the order[222]. The original proposal, which allowed Internet Service Providers to raise concerns about fundamental rights in cases of manifest violations of the Charter or evident abuse, is denied in the General Approach. In contrast to enforcing authorities, ISPs are not granted the ability to invoke fundamental interests of the enforcing

[218] *Ivi*, Art. 3-5 and 7.
[219] *Ivi*, Art. 14-15.
[220] Tosza, S. (2021). *Op. Cit.*, p. 7.
[221] European Commission (2018). *Proposal for a Regulation of The European Parliament and of The Council on European Production and Preservation Orders for electronic evidence in criminal matters*. COM/2018/225.
[222] *Ivi*, Whereas 45.

state, reasons connected to privileges and immunities, or considerations related to freedom of the press or freedom of expression[223]. In the event of non-compliance, sanctions will be determined by individual Member States[224].

What becomes evident is that service providers, as private actors, actively engage in enforcement and are obligated to conduct a proactive balancing of rights and values. This compels them to assume tasks that resemble the adjudicative role typically carried out by public actors.

The concept of involving private actors in regulation and enforcement is not a novel one. Over the years, there has been a noticeable trend wherein private actors have played an increasingly active role in regulation and enforcement. This involvement may manifest in various forms, including co-regulation, self-regulation, or purely private regulation and enforcement. The monopoly of regulation and enforcement by the state has ceased to be the exclusive norm for some time, with this phenomenon aligning with theories such as responsive regulation or smart regulation[225]. Moreover, private players assess competing rights against one another and make value judgments. In severe circumstances this may even include defying governmental commands and giving the safeguarding of certain values priority over other considerations. Such activities, even in cases where they are permitted, are exceptions that require legal explanations, highlighting the fact that public officials bear a basic obligation to balance fundamental rights.

In this evolving landscape, private entities may find themselves compelled to navigate the delicate balance of potentially conflicting rights, including freedom of expression, the right to privacy, freedom to conduct business, rights of the child, rights to the protection of intellectual property, and the right to non-discrimination. However, the inherent nature of private actors, primarily profit-driven entities, poses a fundamental challenge to undertaking this function. While they may act in the pursuit of a greater good or assume a benevolent

[223] *Ivi, Whereas* 45, 51-52.
[224] Tosza, S. (2021). *Op. Cit.*, p. 11.
[225] *Ivi*, p. 12. Cfr. Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press, USA.

stance, public policy cannot solely rely on such behavior, as private actors are inclined to act in ways that are beneficial to their interests[226].

The case of delegation of counter-terrorist powers to public-private partnerships by supranational public actors has also been analyzed by the author mentioned in the previous paragraph Scheinin from the standpoint of international human rights law. Such delegation, provided for in Regulation 2021/784, according to his analysis, raises profound questions about the potential human rights implications inherent in such private outsourcing arrangements[227]. The need for meticulous examination and evaluation is extensive, as the involvement of public-private partnerships in the enforcement and adjudication of counter-terrorist powers introduces a complex interplay between security measures and individual rights. The assignment of such powers should ideally be vested in impartial bodies that guarantee fairness and independence in their decision-making processes. This perspective advocates for the involvement of entities such as courts or independent bodies, emphasizing the importance of ensuring a judicious balance between security imperatives and the protection of individual human rights within the framework of counterterrorism measures[228]. Furthermore, an analysis of the remedy procedure outlined in Article 9 of the Regulation[229] reveals potential shortcomings. The lack of specificity within this provision poses a challenge to ensuring an effective remedy, especially in cases where the content provider is a national of the state. This becomes particularly problematic considering the fast-paced nature of digital content dissemination, requiring remedies that are, along with effective, also rapid. The existing framework may be insufficient in addressing this urgency, and the reliance on *ex post facto* reintegration of incriminated content via an infringement decision by the

[226] *Ivi*, p. 13. Cfr. Klonick, K. (2017). *The new governors: The people, rules, and processes governing online speech*. Harv. L. Rev., 131, 1598.

[227] Gherbaoui, T., Scheinin, M. (2023). *Op. Cit.*, p. 22.

[228] European Union Agency for Fundamental Rights (2019). *Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications - Opinion of the European Union Agency for Fundamental Rights* (FRA Opinion – 2/2019, Vienna, 12 February 2019), p. 25-26.

[229] Regulation (EU) 2021/784. *Op. Cit.*, Art. 9(1): "Hosting service providers that have received a removal order […], shall have a right to an effective remedy. That right shall include the right to challenge such a removal order before the courts of the Member State of the competent authority that issued the removal order and the right to challenge the decision […] before the courts of the Member State of the competent authority that took the decision.".

competent authority in the service provider's state could prove untimely for the timely dissemination of content in the digital dimension, contradicting the underlying principles of the one-hour rule. As explained by the author, this highlights the need for a more nuanced and responsive approach to remedy procedures within the regulatory framework.

Moreover, the establishment of a transnational public-private "duopoly" by the Regulation places the content provider, the actual rights-holder, in a precarious position from the legal point of view. This complex scenario introduces the concept of "positive obligations" within the framework of human rights law, which may be considered as a double-edged weapon in the context of public-private partnerships outlined by the Regulation. The issuance of governmental removal orders to combat terrorist content presents a complex interplay between public and private powers and such collaboration, while well-intentioned in its proactive approach to prevent online content dissemination and protect the human rights of potential terrorism victims, especially the right to life, has implications under international human rights law. This legal framework imposes responsibilities on states to safeguard human rights against actions by private entities, including hosting service providers restricting freedom of expression. Consequently, the Regulation assigns states the task of fulfilling their positive human rights obligations, akin to traditional diplomatic protection, by designating an authority in the Member State where the service provider is based to scrutinize removal orders issued by authorities of other countries. However, this protective role faces practical challenges and, in more concerning scenarios, is formally nonexistent in Member States lacking a designated competent authority. This intricate interplay further underscores the need for a thorough examination and potential refinement of the regulatory framework to ensure effective protection of human rights in the evolving digital landscape[230].

[230] Gherbaoui, T., Scheinin, M. (2023). *Op. Cit.*, p. 23.

Chapter 3 - The implementation of EU Directives at the Italian national level

3.1 Converging anti-terrorism and cybersecurity provisions

After a thorough examination of the European regulations addressing the fight against cyberterrorism, an approach has emerged that tackles this threat by simultaneously addressing its dual nature. On one hand terrorism, that is addressed as an international transborder phenomenon threatening political, economic, and social stability. On the other hand, cybersecurity, which is a more recent and cutting-edge phenomenon with a hybrid and almost immaterial nature, occurring in cyberspace. In this chapter, the focus will be on the case of Italian legislation which, as a member of the European Union, has confronted the same threat by incorporating the directives and regulations mentioned within the Union into its legal framework. From this analysis, it is evident how the Italian legislation proposes a series of measures that, collectively, present a comprehensive and unified approach to the aforementioned threat. This involves establishing a regulatory framework that encompasses both preventive and punitive actions specifically designed to counter cyberterrorism. The legislative path concerning terrorism in Italy has gone through different phases over the years. Initially, in the 1970s, the figure of the internal terrorist emerged, leading to the establishment of Italy's first legislation on terrorism. This phase resulted in the introduction of significant articles such as 270-bis, 280, and 289-bis of the Penal Code (c.p.) into the Italian legal system. Subsequently, starting from 2001, a second phase unfolded where emphasis was given to the figure of the international terrorist. The increasing globalization of threats necessitated an adequate legislative response to address terrorism on an international scale. Another development occurred in 2014 with the adoption of UN Security Council Resolution No. 2178. This resolution marked the beginning of the criminal consideration and the introduction of measures specifically aimed at countering the new figure of the mobile terrorist, known as the foreign fighter. The latter represents a particularly complex element, requiring specific legislative attention to address the dynamics of individuals moving across national borders to engage in terrorist activities. There it can be concluded that anti-terrorism regulations are

modified and adapted in response to the evolving needs of the context. In this regard, commencing the examination of the Italian counter-terrorism legislation, the foundational reference to this offense is delineated in Article 270-bis c.p., amended in 2001 through Law No. 438/2001. This legislative measure reformulates the statutory provision outlined in the article, specifying "Association with the Purpose of Terrorism, Including International Terrorism, or Subversion of the Democratic Order" [231]. With this normative update, the presumption of financing terrorism is also introduced as one of the motives subject to sanction. Additionally, there is a clear expansion towards the internationalization of the terrorist phenomenon, explicitly articulated in the third paragraph, which stipulates that "For the purposes of criminal law, the purpose of terrorism also exists when acts of violence are directed against a foreign State, an international institution, or organization" [232]. However, following the update of this article multiple doubts have arisen regarding the terminological vagueness characterizing the provision in question, and with respect to the lack of coordination with the international legal framework, which has caused numerous challenges in its practical application[233]. In 2018 was then added in the penal code the new article 270-bis.1, inserted by art. 5 of D. Lgs. 01/03/2018, n. 21, which provides for the regulation of a series of special circumstances, aggravating and mitigating, regarding crimes committed for the purpose of terrorism or subversion of the democratic order[234].

[231] Viganò F. (2006). *Terrorismo, guerra e sistema penale*, Rivista italiana di diritto e procedura penale, Vol.49(2), p. 648.

[232] De Ruvo, L. (2022). *L'importanza dell'art. 270-bis del Codice Penale nel contrasto al terrorismo internazionale*. In <Diritto.it>.

[233] *Ibidem*. In this regard the intervention of the jurisprudence of the Court of Cassation has provided clarification on the matter. With the judgments n. 24994/2006 and n. 24995/2006, regarding the incriminating offense outlined in Article 270-bis c.p., it was established that "in the presence of an organized structure, even if rudimentary, in which the suspect participates, it is sufficient to constitute the crime in question that ideological adherence materializes in serious criminal intentions aimed at achieving one of the specified purposes, even without their initial material execution, exceeding the typical limit of presumed danger".

[234] Art. 5 of Legislative Decree March 1, 2018, n. 21, concerning provisions implementing the principle of delegation of the code reserve in criminal matters pursuant to Article 1, paragraph 85, letter q), of Law No. 103 of 23 June 2017, with effect from 06/04/2018.

The second legislative implementation derives from the Budapest Convention of 2001, ratified into the national legal framework by Law No. 48 of March 18, 2008[235]. It extends its application not only to cybercrimes in the strict sense but also to all offenses for which the collection of computer data is necessary, as per Article 14 of the Convention[236]. Indeed, on one side, it has expanded the specific scenarios[237] ensuring appealability without modifying the original formulation of other regulations, preserving the criminalization of actions not addressed by supranational and European authorities[238]. On the other side, it has impacted the configuration of individual instances by introducing novel elements[239]. Around the same period, from 2006 to 2015, other two provisions have been implemented in the Italian legislative framework: art. 270-quarter and art. 270-quinquies c.p., to address the specific need for the criminalization of preparatory conduct related to acts of terrorism, thereby significantly lowering the threshold for punishability. The two articles have been drafted following Law n. 155/2005[240], which extends the area criminally punishable with the provision of new circumstances affecting the activities of recruitment and training, and updated accordingly to Law n. 43/2015[241] known as the "Counter-terrorism Decree", which

[235] L. March 18, 2008, n. 48. *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, G.U. n. 80, 4 aprile 2008.

[236] Vigneri, A. F. (2018) *Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto*, p. 19. Budapest Convention, Art. 14: "Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a) the criminal offences established in accordance with Articles 2 through 11 of this Convention; b) other criminal offences committed by means of a computer system; and c) the collection of evidence in electronic form of a criminal offence".

[237] Examples of this are offenses related to computer damage under Articles 635-bis, 635-ter, 635-quater, 635-quinquies c.p., as well as the new provisions concerning the electronic signature certifier under Articles 495-bis and 640-quinquies c.p.

[238] This is the case, for example, with Article 615-ter c.p., which penalizes, in addition to unauthorized access, the unauthorized persistence in a computer system, where the latter conduct is not envisaged by supranational and European sources.

[239] An example of new elements is represented by Article 615-quinquies c.p. and the new specific intent. In the previous formulation, indeed, the "purpose" of causing damage was objectively linked to the nature of the program and not to the subjective intent of the perpetrator. Cfr. Vigneri, A. F. (2018) *Op. Cit*., p. 19-21.

[240] The article was introduced with D.L. 27 July 2005, n. 144, converted with modifications in Law 31 July 2005 n. 155.

[241] Amended by Art. 1, paragraph 3, Lett. a), D.L. 18 February 2015, n. 7, converted, with amendments, from L. 17 April 2015, n. 43. The last paragraph was added by art. 1, paragraph 3, Lett. b), D.L. 18 February 2015,

provides for the extension of the punishability to the figure of the self-training, with the addition of new circumstance of organization of travels with the purpose of terrorism, as defined by art. 270-quarter.1[242]. In a preventive perspective, the legislator, through the paragraphs 2, 3, and 4 of the concerned law, mandated the establishment of the so-called black lists of websites used for terrorist proselytism. Service providers are required to obscure the webpage reported by the Attorney General, prohibit access to it, and, following a prosecutor's directive, remove illicit content accessible to the public that is potentially related to the purpose of terrorist propaganda[243]. What is demanded from law enforcement operators, to enable the site's obscuration through a streamlined and rapid procedure, is an assessment that is "discretionary and devoid of any judicial oversight on the impact and persuasiveness of the content, potentially capable of generating a certain degree of interest and of agreement"[244]. It is interesting to highlight also that, according to Law 43/2015, articles 170-quarter, 270-quarter 1, and 270-quinquies c.p. introduce an increase of the punishment in case of conviction for the crimes described in these articles, precisely providing for the ancillary penalty of the loss of parental authority where a child is involved. Such regulations aim to tackle the terrorist phenomenon at its core, providing for serious sanctions for acts such as recruitment, training, organizing transfers, and financing activities with the purpose of terrorism. The amendments introduced by Articles 9 and 10 of Law 43/2015 represent a significant element, highlighting the clear objective of the legislator to strengthen the investigative activity through more effective coordination between the new district anti-terrorism prosecutors. These changes give the National Counter-Terrorism Prosecutor

n. 7, converted, with modifications, from L. 17 April 2015, n. 43. Pursuant to art. 1, paragraph 3-bis, D.L. 18 February 2015, n. 7, converted, with amendments, from L. 17 April 2015, n. 43, the penalty provided for the offence referred to in this article entails the accessory penalty of the loss of parental responsibility in case of involvement of a minor.

[242] Art. 270-quarter 1 c.p.: "Fuori dai casi di cui agli articoli 270-bis e 270-quater, chiunque organizza, finanzia o propaganda viaggi in territorio estero finalizzati al compimento delle condotte con finalità di terrorismo di cui all'articolo 270-sexies, è punito con la reclusione da cinque a otto anni." That is "Apart from the cases referred to in Articles 270-bis and 270-quater, any person who organises, finances or propaganda trips abroad for the purpose of carrying out the acts of terrorism referred to in Article 270-sexies shall be punished by imprisonment for five to eight years.".

[243] Nocerino, W. (2016). *Le norme italiane di contrasto al terrorismo: repressione e prevenzione tra diritto interno ed internazionale*. Diritto pubblico comparato ed europeo, Fascicolo 4, ottobre-dicembre 2016, p. 1222.

[244] C. cass., sez. I, sent. n. 47489, 6 October 2015.

stronger powers. In particular, with a merely nominal correction but with organizational impact, Article 9, paragraph 3, amends Article 117 of the Code of Criminal Procedure (c.p.p.), giving the National Anti-mafia and Counter-terrorism Prosecutor the power to access the register of criminal reports[245], as well as all other registers related to criminal proceedings and prevention measures, including those present in the databases dedicated to the district prosecutors and developed within the shared database of the National Directorate for Anti-mafia and Counter-Terrorism[246]. Moreover, paragraphs 1, 2 and 4 of Article 9 of Law 43/2015 extend part of the discipline on organized crime to terrorist crimes, thus consolidating the regulatory framework for a more effective and coordinated response in the field of investigation[247]. In addition to these provisions, Article 270-sexies c.p. is of major importance. It was introduced by Decree-Law 144/2005[248], which does not prescribe any type of conduct but rather defines the concept of conduct with the purpose of terrorism. In this manner, the gaps in the definition that originally characterized the post-2001 legislation are partially filled[249]. The year 2016 is of particular significance concerning the evolution of the counter terrorism legislation in Italy. Indeed, the enactment of Law 153/2016[250] ratifies

[245] Art. 117, para 2-bis c.p.p.: "Il procuratore nazionale antimafia e antiterrorismo, nell'ambito delle funzioni previste dall'articolo 371-bis accede al registro delle notizie di reato, al registro di cui all'articolo 81 del codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n. 159, nonché a tutti gli altri registri relativi al procedimento penale e al procedimento per l'applicazione delle misure di prevenzione. Il procuratore nazionale antimafia e antiterrorismo accede, altresì, alle banche di dati logiche dedicate alle procure distrettuali e realizzate nell'ambito della banca di dati condivisa della Direzione nazionale antimafia e antiterrorismo".

[246] The ratio for the regulatory intervention appears clear: the trend towards the centralization of the management of databases eases the filling of data and, consequently, the familiarity of the National Counter-Terrorism Prosecutor (PNA) with them, ultimately contributing to its coordination activity.
Cfr. Nocerino, W. (2016). *Op. Cit*., p. 1223 and Cortesi, M.F. (2015). *Il decreto antiterrorismo – i riflessi sul sistema processuale, penitenziario e di prevenzione*, Dir. pen. proc., 919.

[247] Nocerino, W. (2016). *Op. Cit*., p. 1223.

[248] Law Decree 27 July 2005, n. 144 "Misure urgenti per il contrasto del terrorismo internazionale", converted, with amendments, to Law 31 July 2005, n. 155 (in G.U. 01/08/2005, n.177).

[249] Cfr. Licciardello, S. (2016). *Nuove Norme antiterrorismo in Italia*. <Sistema di informazione per la sicurezza della Repubblica> sez. Il mondo dell'intelligence, 9 September 2016.

[250] Law 28 July 2016, n. 153. "Norme per il contrasto al terrorismo, nonché ratifica ed esecuzione: a) della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatta a Varsavia il 16 maggio 2005; b) della Convenzione internazionale per la soppressione di atti di terrorismo nucleare, fatta a New York il 14 settembre 2005; c) del Protocollo di Emendamento alla Convenzione europea per la repressione del terrorismo, fatto a Strasburgo il 15 maggio 2003; d) della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, fatta a Varsavia il 16 maggio

five different international acts, all aimed at preventing and combating terrorism. These are the Council of Europe Convention for the Prevention of Terrorism and its Additional Protocol, the UN Convention for the Suppression of Acts of Nuclear Terrorism, the Protocol of Amendment to the European Convention for the Suppression of Terrorism, and the Council of Europe Convention on Money Laundering, Research, Seizure and Confiscation of the Proceeds of Crime. Furthermore, to adapt our internal legal system, the law inserts in the penal code three new crimes: financing of conduct for terrorism (Art. 270-quinquies 1 c.p.); theft of goods or money subjected to seizure (Art. 270-quinquies 2 c.p.) and acts of nuclear terrorism (Art. 280-ter c.p.). This legislative reform expanded the legal framework, providing specific legal tools to address critical issues related to the financing of terrorist activities and the risk of nuclear terrorism. The year 2016 represents a pivotal moment in the development of counter-terrorism regulations, both at Communitarian and national level. In fact, following the serious attacks that hit Europe between 2015 and 2016, the imminent need to take new regulatory measures to combat the threat and, above all, prevent it, has arisen. In fact, in Europe, it can be asserted that a new historical phase in the fight against international terrorism is underway, grounded in the prioritization of European cooperation for the exchange of information among the intelligence services present in the various countries of the Union. This approach is particularly necessary given the impossibility, at least in the short term, of creating a unified network of European secret services[251]. In this perspective a relevant Italian legislative moment is represented by the Council of Ministers approving, on 25 March 2016, the regulation concerning the creation, functioning, and organization of the DNA database and of its central database laboratory[252]. In particular, this Regulation represents the integration at national level of the decisions of the Council of the European

2005; e) del Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatto a Riga il 22 ottobre 2015.".

[251] Nocerino, W. (2016). *Op. Cit.,* p. 1225.

[252] *Ibidem*. The creation of these institutions was foreseen by Law No. 85 of 30 June 2009: "Adesione della Repubblica italiana al Trattato concluso il 27 maggio 2005 [...], relativo all'approfondimento della cooperazione transfrontaliera, in particolare allo scopo di contrastare il terrorismo, la criminalità transfrontaliera e la migrazione illegale".

Union No. 2008/615/JHA[253] and No. 2008/616/JHA[254] on the strengthening of cross-border cooperation with specific attention to the fight against terrorism and cross-border crime and for international police cooperation. Also to strengthen the investigative activity against terrorism, recognized as a transnational phenomenon, the Legislative Decree n. 34/2016[255] introduced joint investigation teams, withdrawing, more than 15 years later, Framework Decision 2002/465/JHA. The novelty of this legislative integration is reflected in allowing each prosecutor to request the formation of an investigative team for crimes specified in the legislative text or for crimes punishable by life imprisonment or a sentence exceeding 5 years, and in cases involving particularly complex investigations in several Member States[256]. A further step taken by the Italian legislation to adapt to European guidelines is represented by the Legislative Decree n. 53/2018[257] implementing Directive (EU) 2016/681 on the use of Reservation Code (PNR) data for the purposes of prevention, investigation, and prosecution of terrorist offences and serious crimes. In particular, the Directive deals with the collection and processing of data relating to persons travelling by airplanes to countries outside the European Union, implementing various safeguards for data protection. By pursuing the objective of adapting the Directive to the principle of proportionality and including security measures for data protection, some predictions are made. Prominent ones are a limited list of serious offenses justifying the use of PNR data, the appointment of data protection officers in each Passenger Information Unit (UIP), the strengthening of the monitoring powers of data protection authorities, and strict conditions for access to PNR data retained beyond six

[253] Council of the European Union, Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. OJEU L 210/1.
[254] Council of the European Union, Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. OJEU L 210/12.
[255] Legislative Decree 15 February 2016, n. 34, entered into force on 25 March 2016, "Norme di attuazione della decisione quadro 2002/465/GAI del Consiglio, del 13 giugno 2002, relativa alle squadre investigative comuni.".
[256] Nocerino, W. (2016). *Op. Cit.,* p. 1225.
[257] Legislative Decree of 21 May 2018, n. 53 "Attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004.".

months. These provisions are then incorporated into the Italian regulatory system representing one of the most important methods adopted in the prevention of the terrorist threat and, at the same time, with a particular safeguard on the so-called sensitive data of the passengers, that are those data that reveal racial origin, religion, political opinion, health, and sexual orientation. Indeed, Art. 22(3)[258] of the Decree explicitly prohibits the retention of such data, in a perspective of safeguarding the right to privacy and non-discrimination of the passengers[259].

In addition to provisions specifically geared towards counterterrorism, the Italian legislative framework, in alignment with European guidelines, has developed a set of regulations addressing cybersecurity. These regulations seamlessly fit into the context of the threats posed by cyberterrorism.

The Italian legal framework on cybersecurity includes several legislative provisions and European directives. Initially, Art. 7-bis of the Decree-Law 144/2005 introduced urgent measures to combat international terrorism, focusing on electronic security "for the prevention and suppression of terrorist activities or facilitation of terrorism carried out by electronic means". With a step forward, the following main legislative act addressing another aspect of cybersecurity vis-à-vis the threat of terrorism is represented by the NIS Directive, namely addressing the security of Networks and Information Systems in the European Union which established a minimum requirement for operators of essential services and digital service providers. It was adopted on 6 July 2016 and transposed in Italy with the Legislative Decree n. 65 of 18 May 2018[260]. The latter imposes new security obligations on operators and providers of digital services, requiring the adoption of security measures and especially the notification of incidents. It introduces the creation of the Computer Security Incident Response Team (CSIRT) in case of an incident, promoting collaboration and the exchange of

[258] Legislative Decree n. 53/2018, *Op. Cit.*, Art. 22, para 3: "È vietato il trattamento dei dati PNR idoneo a rivelare l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, lo stato di salute, la vita o l'orientamento sessuale dell'interessato".

[259] Nocerino, W. (2016). *Op. Cit.*, p. 1225. Cfr., A Soro. (2014*). Non siamo contrari a tracciare i passeggeri in Europa, privacy e sicurezza non sono in contraddizione*, <Huffington Post>.

[260] Legislative Decree n. 65 of 18 May 2018 "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione".

information among EU member states[261]. Specifically, Article 4 focuses on the identification of operators of essential services, assigning this task to the competent NIS Authority. The central body of the Ministry of the Interior is designated as the supervisory authority for the security and regularity of telecommunications services. It also requires the formulation of a national strategic plan for cybersecurity, as defined in Art. 6. The decree establishes specific entities to manage the matter, instituting a single point of contact responsible at the national level for coordination and cooperation with the European Union. Moreover, at the presidency of the Council of Ministers, the Italian CSIRT[262] is created with the task of ensuring compliance with EU regulations and defining procedures for the prevention and management of cyber incidents. Finally, the decree envisions collaboration between the competent NIS authorities, the single point of contact, and the CSIRT through the establishment of a Technical Coordination Committee[263], composed of representatives from competent state authorities and autonomous Regions and Provinces, to fulfill obligations for the protection of network and information systems security[264].

As regards the obligations of essential services operators, the Decree obliges them to adopt appropriate technical and organizational measures to manage the risks related to the security of the network and information systems, as provided for in Article 12. In the event of significant incidents affecting the continuity of essential services, operators shall notify the CSIRT and the NIS authority thereof[265]. The CSIRT then sends the notifications to the Department of Security Information. Notifications shall include information allowing the CSIRT to assess the transboundary impact of the accident, taking into account the number of users affected, the duration, and the geographical spread. According to Art. 13 of the Decree, operators shall also provide information on the security of their network, demonstrate the

[261] Muià, P.P. (2021). *Il decreto legislativo n. 65 del 2018 in materia di cybersicurezza*. <Diritto.it>.
[262] Legislative Decree n. 65/2018. *Op. Cit.*, art. 8: "È istituito, presso la Presidenza del Consiglio dei ministri, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale […]".
[263] *Ivi*, art. 9.
[264] *Ivi*, artt. 10-11.
[265] *Ivi*, art. 12 para 5: "Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti".

implementation of security policies, and make the results available. Compliance with these obligations by operators is subject to verification by the NIS competent authorities, which are also responsible for assessing their effects on network and information system security[266]. It is interesting to also highlight the section of the decree that concerns the obligations imposed on digital service providers. Specifically, it is stipulated that these suppliers must identify and implement appropriate technical and organizational proportionate measures to manage network security risks, considering system and facility security, incident handling, operational management, and compliance with international standards (Art. 14). In addition, suppliers shall take precautions to prevent and minimize the impact of incidents on network security while ensuring the continuity of services. It is mandatory for providers to notify the Italian CSIRT and the NIS authority of incidents affecting the provision of digital services (Art. 14, para 4). Such notifications must contain relevant information, considering the number of users involved, the duration of the accident, its geographical spread, the extent of the disturbance, and the impact on economic and social activities. The significance of the notification requirement lies in the fact that it compels the competent authorities to recognize the necessity of imposing an obligation on those who have experienced attacks to inform them. Without a clear understanding of the extent of the phenomenon, it would be challenging to effectively counteract it. The following legislative relevant step taken towards an improvement of the national framework to counter cyberterrorism is represented by the implementation of the EU Regulation 2021/784 with the Legislative Decree n. 107/2023[267] on combating the spread of terrorist content online. The main instrument of contrast is the issue of removal orders (o.d.r.) as provided for in Article 12, paragraph 1, letters a) and b) of Regulation (EU) 2021/784. The competent authorities of each Member State can issue removal orders, obliging service providers to eliminate or disable access to terrorist content in all Member States. To allow hosting providers to act promptly before the adoption of the order, authorities shall provide information on the applicable procedures and timescales at

[266] Muià, P.P. (2021). *Op. Cit.*

[267] Legislative Decree of 24 July 2023, n. 107 "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici on-line".

least 12 hours in advance. Hosting providers are required to remove terrorist content or to disable access to it in all Member States as soon as possible and in any case within one hour of receiving the order. After the order has been placed, the hosting provider shall immediately inform the competent authority about the removal or disabling of terrorist content in all Member States, indicating the date and time of the action. This communication is also required if the supplier cannot execute the order for reasons of force majeure or impossibility not attributable to him, including the technical or operational reasons objectively justifiable. The EU Regulation mandates that the removal order be transmitted via the SIENA channel[268], a collaborative channel with Europol. This process is also implemented in Italy trough the adoption of this Legislative Decree. However, it is crucial to emphasize possible gaps in the piece of legislation under analysis. Indeed, article 3 of the Legislative Decree contains a specification which may give rise to uncertainty. The removal order may be adopted when terrorist content, as defined in Article 2, point 7) of the Regulation, is linked to a terrorist offence[269]. This wording contains a double reference clause to national legislation and criminal law, the use of which could be complex. In particular, Article 2, para 7 of Regulation 2021/784 outlines an extensive description of terrorist content, including materials inciting the commission of terrorist offenses; urging a person or group of persons to commit or contribute to one of the offenses; encouraging participation in the activities of terrorist groups; provide instructions for the manufacture of explosives or weapons, or constitute a threat of commission of terrorist offenses. The broad scope of this definition could pose challenges in implementing the dual reference clause within national legislation. The issue revolves around the fact that, while in certain cases, specifically letters a) to d), national

[268] EUROPOL has three main channels for the exchange of information with Member States, third countries and other independent bodies. These channels are Europol Information System (EIS), Secure Information Exchange Network Application (SIENA), and the Europol Platform for Expert (EPE). They are key tools in the fight against international crime, providing crucial access to data and investigative evidence and respecting specific management rules. The SIENA channel is the information exchange platform used by Europol for communications of operational interest to national law enforcement agencies. The communications are characterized by an identification protocol that identifies the investigative case (SIENA case), followed by the progressive specific request (ID request) and another progressive representative of the number of messages exchanged for each request (ID flow).

[269] Legislative Decree n. 107/2023, art. 3(1): "quando i contenuti terroristici di cui all'articolo 2, punto 7) del regolamento sono riconducibili a un delitto con finalità di terrorismo".

legislation explicitly outlines instances of criminal offenses, the concept of a "threat of commission" in letter e) alludes to something much broader than the preparatory acts under Article 56 c.p., thereby positioning itself within a perimeter of extreme vagueness and breadth. While the matter may be of neutral importance for other countries, in Italy, the involvement of the judicial authority in applying such a broad category, within the constraints of public security powers, presents significant challenges. The reservation of jurisdiction functions as an external limit, preventing the judiciary from being assigned tasks outside its control that could potentially entangle it in security responsibilities, not within its purview[270]. In the same year of Regulation 2021/784, the necessity to unify all cybersecurity activities and enhance the state security apparatus has led to the establishment of the Agenzia per la Cybersicurezza Nazionale (ACN) initially with the Law Decree n. 82 of 14 June 2021 and then converted into Law n. 109 on the 4 august 2021[271]. The provisions of Law Decree n. 82/2021 represent the synthesis of two previous pieces of legislation, Regulation 2016/1148 (the NIS Directive) aimed at achieving a "high common level of network and information systems security in the Union in order to improve the functioning of the internal market"[272] and Law Decree n. 105 of 21 September 2019[273], with which Italy established the National Cybernetic Security Perimeter (PSNC)[274] to develop a national discipline integrating that of the European Union through the involvement in the PSNC of both all public and private operators[275]. The Law Decree n. 82/2021, pioneering in the context of the Italian legal system, introduces for the first time the definition of the term cybersecurity. This is outlined as "the set of activities, in compliance with the powers established by Law August 3, 2007, n. 124, and obligations arising from international treaties, necessary to protect networks, information

[270] Cisterna, A. (2023). *In G.U. il D.Lgs. 107/2023: le nuove norme per il contrasto alla diffusione di materiali terroristici sulla rete*. <Altalex>.
[271] Law Decree 14 June 2021, n. 82 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", converted with amendments from Law 4 august 2021, n. 109.
[272] Directive 2016/1148/EC, Art. 1., implemented in Italy by Legislative Decree no. 65 of 18 May 2018.
[273] Law Decree of 21 September 2019, No. 105, "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", converted with amendments by Law 18 November 2019, No. 133.
[274] *Ivi*, art. 1.
[275] Serini, F. (2022). *La nuova architettura di cybersicurezza nazionale. Note a prima lettura del decreto-legge n. 82 del 2021*. Federalismi. it, (12), 241-272, p. 243.

systems, IT services, and electronic communications from cyber threats. This protection aims to ensure its availability, confidentiality, and integrity, while ensuring resilience, also with the aim of preserving national security and national interest in cyberspace"[276]. This definition is the result of a multidisciplinary composition process and is characterized by the inclusion of various aspects constituting the matter. First, the object deserving of protection includes the "availability, confidentiality and integrity", in addition to the "resilience"[277] of networks, information systems, IT services, and electronic communications. These elements are associated, respectively, with the dimensions of computer security and information, regulated in the corresponding industry technical regulations. Resilience, however, refers to the organizational capacity of the national system to anticipate and prevent cybersecurity incidents that can cause serious crises to the country, as well as mitigate them in case they occur[278]. The conversion of the Law Decree into Law introduced an additional dimension pertaining to the objectives of the previously mentioned activities, specifically in safeguarding national security and interests within the realm of cyberspace[279]. Deepening the analysis of Law 109/2021, it also modifies the organization and internal structure, which previously consisted of three levels[280] and focused on the Information System for the Security of the Republic. It now establishes a separate organizational model specialized in the specific sector of cyberspace security. This is evidenced by the introduction of two ad hoc bodies, namely, the Interministerial Committee for Cybersecurity (CIC) and the establishment of the National Cybersecurity Agency (ACN). Additionally, there is an absence of confirmation of

[276] Law Decree n. 82/2021, art. 1, co. 1, lett. a). This definition aligns with that formulated in Regulation (EU) 2019/881, also known as the Cybersecurity Act, where Article 2, No. 1, defines the term cybersecurity as "[...]the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".

[277] *Ibidem*.

[278] Serini, F. (2022). *Op. Cit*., p. 269.

[279] *Ibidem*.

[280] The architecture previously developed on three levels foresaw the first level, the political one, with the President of the Council of Ministers supported by the Interministerial Committee for the Security of the Republic (CISR). The second operational and administrative level involved the Cyber Security Unit (NSC), established within the Office of the Military Adviser to the Presidency of the Council of Ministers, with the task of assisting the President in the security of the cyberspace for prevention, crisis preparation and activation of alert procedures. The third level included Security Intelligence Agencies, responsible for information research, analysis, threat assessment and information transmission to the Cyber Security Core and other public and private entities, interested in acquiring information. Serini, F. (2022). *Op. Cit*. pp. 244-245.

the Security Information Organizations among the constituent actors of the new National System for Cybersecurity (SNSC). From the point of view of the effective role of ACN within the overall national security structure, the need for close cooperation with the Italian Data Protection Authority clearly emerges. Such cooperation is essential in order to ensure the protection of the fundamental rights and freedoms of persons whose data processing falls within the competence of the Agency[281]. In addition, the ACN is subject to the supervisory power of the Authority, which is responsible for the correct application of the relevant directives. It should be stressed that, in exercising this power, the Authority has the power to conduct investigations, access personal data processed, issue warnings, impose restrictions on processing, promote the reporting of violations and report any crimes committed. This interaction reflects an important monitoring and regulatory mechanism, which is essential to ensure compliance and the safeguarding of individual interests in the context of ACN activities[282]. However, it is essential to clarify that this provision must be interpreted by carefully considering the two limits imposed by the legislation in question. The first limitation concerns the exclusion of the Authority's power of control over data processing carried out by the judicial authority in the exercise of its judicial functions, as well as the judicial activities of the public prosecutor. The second limit concerns the exclusion of data processing from the Directive "carried out in the course of activities relating to national security or falling within the scope of Title V, Chapter 2 of the Treaty on European Union and for all activities falling outside the scope of European Union law"[283]. On this point, doubt inevitably arises about the application of this discipline to the functions performed by the Agency, especially considering that the definition of cybersecurity provided by the Law Decree explicitly orients the activities of protection of networks and computer resources also for the protection of national security and national interest in the cyberspace. Ultimately, considering the structure of the ACN, the internal supervision profiles assigned to the Board

[281] Serini, F. (2022). *Op. Cit*. p. 264.
[282] Cfr. Art. 37 of the Legislative Decree of 18 May 2018, n. 51. "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio".
[283] Legislative Decree n. 51/2018, art. 1, para. 3, lett. a), b).

of Auditors and the Independent Assessment Body can be outlined. The Board of Auditors shall examine the acts of financial management, making relevant comments, as well as carrying out audits on cash and balance sheet. In parallel, the Independent Evaluation Body of performance plays a key role in the analysis and evaluation of processes and performance, thus contributing to ensuring a complete and effective internal oversight within the Agency[284].

In conclusion, the ACN structure, with its comprehensive multidisciplinary analysis and internal supervisory mechanisms, is a key pillar in the context of national cybersecurity. However, it is crucial to take into account the evolving regulatory landscape. The latest update, represented by Directive (EU) 2022/2555 (NIS 2)[285], introduces measures to ensure a high common level of cybersecurity in the European Union, requiring changes to pre-existing regulations. Entered into force on 17 January 2023, the Directive requires transposition to national legislation by Member States by 17 October 2024. This Directive, which aims to strengthen the preparation of Member States, promotes cooperation between them to facilitate the exchange of strategic information and establishes a regulatory framework for IT security at European level, requiring the presence of a Cybersecurity Incident Response Team (CSIRT) and a National Network and Information Systems Competent Authority (NIS). In addition, it aims to establish a security culture in sectors crucial to the economy and society, closely linked to information and communication technologies[286]. In this context, Italy will be called upon to transpose and implement the provisions of NIS 2, adapting its structure and practices to respond to new needs and effectively contribute to European cybersecurity[287].

In conclusion to this discussion, it is crucial to emphasize the significant role of two Italian entities within the realm of intelligence tools dedicated to addressing the emerging challenges associated with the evolving threat of cyberterrorism. The National Anti-Crime Computer

[284] Serini, F. (2022). *Op. Cit*. p. 265.
[285] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[286] Cfr. Vandezande, N. (2024). *Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor*. Computer Law & Security Review, 52, 105890.
[287] Singh, D.D. (2023). *Cibersicurezza, la Direttiva NIS 2*. <Altalex>.

Center for the Protection of Critical Infrastructures (CNAIPIC) and the Observatory for Security against Discriminatory Acts (OSCAD) are particularly relevant as they not only actively contribute to national security but also represent a direct point of contact with the population. CNAIPIC, entrusted to the Postal and Communications Police Service, stands out for its use of advanced technologies and highly qualified personnel. Among its main functions, the operations room serves as a unique contact point, operational 24/7, for the exchange of information. It analyzes the gathered data, compiles reports on cyber threats and vulnerabilities, and engages in operational investigations in collaboration with foreign and international law enforcement bodies, including Interpol, Europol, and the G8 High Tech Crime Subgroup. The CNAIPIC also functions as the national contact point for the Budapest Convention on Cybercrime and serves as the contact point for the G8 Network 24/7 High Tech Crime - Rome-Lyon Group - during computer emergencies[288]. On the other hand, OSCAD operates under the Public Security Department to provide support to victims of discriminatory crimes, facilitate the filing of complaints, and promote the prevention of such crimes. It plays a crucial role in mediating between victims and law enforcement, contributing to the effective counteraction of hate crimes[289]. The concerted endeavors of these entities collectively constitute a foundational component in safeguarding national security and furnishing immediate assistance to the community, especially in a preventive approach.

3.2 Privacy vs Security: the challenges of preventive interception

In Italy, the ongoing battle against cyberterrorism is fortified by a suite of intelligence tools that have undergone continuous refinement and enhancement over the years, aligning with the evolving needs arising from the ever-changing threat landscape confronted by national security. Noteworthy among these tools, alongside the previously mentioned CNAIPIC and

[288] Ministero Dell'Interno, *Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche,* <CNAIPIC>.
[289] Ministero Dell'Interno, *Osservatorio per la sicurezza contro gli atti discriminatori,* <OSCAD>.

OSCAD, is the pivotal role played by preventive interception. This imperative to bolster counterterrorism endeavors has spurred the call for regulatory measures, frequently dictated by the urgency to equip law enforcement with tools apt for unforeseen emergencies. In this context, the regulatory landscape has sought to address the dynamic nature of the threats, emphasizing the importance of tools like preventive interception in fortifying the nation's security apparatus. The most legislative incisive interventions focused on the phase of preliminary investigations, including the extension of the functions of the national anti-mafia prosecutor to crimes committed with terrorist purposes, as provided by art. 371-bis c.p.p., the inclusion in the catalogue of offenses subject to arrest in flagrant cases so-called "sentinel" related to terrorist events (art. 497-bis c.p. and art. 12, paragraphs 1 and 3, d.lgs. n. 286/1998), and the incorporation of terrorist crimes among those that allow the use of tools such as interviews, as defined in art. 18-bis ord. penit., and interceptions for investigative purposes, disciplined in art. 226 disp. att. c.p.p.)[290]. This paragraph will focus on a specific type of interception, that is preventive interception carried out by the Security Intelligence Services also defined as Intelligence preventive interception[291], introduced into Italian law in 2005 with Article of the Decree Law 144/2005[292], to counter international terrorism. As such, it quickly became the subject of heated debate in doctrine. Used with preventive purposes to minimize the possible realization of certain offences, it arouses reflections about its potential interference in the individual sphere of the intercepted, as well as the specificity of its scope and its possible procedural relevance. Limiting therefore the scope of the analysis to the field of interception, it is essential to note that the Italian Code of Criminal Procedure considers interception as a means of gathering evidence, the use of which is subject to the presence of serious indications about the existence of specific categories of crimes, an absolute necessity for the continuation of the investigation and with the authorisation of the judicial authority

[290] Agostini, B. (2017). *La disciplina delle intercettazioni preventive nel sistema antiterrorismo*. Diritto penale contemporaneo, p. 142.
[291] Intelligence preventive interception have been introduced in the Italian legal framework by art. 4 of the d.l. 27 July 2005, n. 144, converted, with amendments, in l. 31 July 2005, n. 155. The discipline concerned has been modified for the first time in 2007 (Law 3 August 2007, n. 124) and then, lastly, in 2012 (Law 7 August 2012, n. 133).
[292] Law Decree 27 July 2005, n. 144. *Misure urgenti per il contrasto del terrorismo internazionale*.

(art. 266 et seq. c.p.p.)[293]. The tool of interception as a preventive measure against crimes, that is, *ante delictum* to neutralize future criminal behavior, has been vividly characterized by scholars as a "dusty tool"[294]. In fact, it was initially opposed with the advent of the current new Code of Criminal Procedure.[295]. This instrument, conceived during the terrorist emergency of the 1970s with the aim of preventing serious political crimes, provided, pursuant to Article 226-sexies of the then existing Code of Criminal Procedure, that the interception of communications or telephone conversations can be authorized by the public prosecutor of the designated location. This authorization may be requested by the Minister of the Interior or delegated by them, or through the competent prefect, the police chief, the commander of the carabinieri group, or the commander of the financial guard group. Authorization is granted when it is necessary for investigations related to the crimes specified in the first paragraph of article 165-ter[296]. Subsequently, the possibility of using the tool of preventive interception has been extended also to activities of organized crime, including among the bodies authorized to request it from the prosecutor the then High Commissioner for the fight against the mafia. The discontentment and criticism surrounding the instrument under consideration since its introduction had led the Parliamentary Commission to highlight, in its final report to the Code, its contradiction with the same reasons underlying the new procedural system[297]. Despite this, the Mafia-related events in the summer of 1992 prompted the legislator to resort to this instrument again, introducing a new form of preventive interception. This was foreseen at the request of the police authorities, including the newborn Directorate of Anti-mafia Investigation, and subject to the situations in which they considered such activity necessary for the prevention and information in relation to the crimes covered

---

[293] Art. 266 c.p.p. on the Limits of Admissibility, art. 266-bis on Interception of computer or telematic communications: "Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi".

[294] De Leo,F. (1998). *L'irrisolto presente e un possibile futuro delle intercettazioni preventive*, in Cass. pen., p. 1862.

[295] For an analysis on the matter, cfr. Mengoni, *Commento all'art. 4 del d.l. 2005*, in <www.csm.it/circolari/050727_T.pdf>: "Con l'avvento del c.p.p. vigente, la disciplina delle intercettazioni preventive appariva cancellata dal sistema, perché ritenuta tanto di dubbia legittimità costituzionale, quanto -e soprattutto- ampiamente superata dalle regole del nuovo codice e dalle sue più profonde ragioni ispiratrici".

[296] Agostini, B. (2017). Op. Cit., p. 143.

[297] *Ibidem*.

by art. 51, paragraph 3-bis c.p.p.[298]. However, as underlined, this new provision, included in art. 25-ter of Legislative Decree No. 306/1992[299], did not include any criterion of coordination with the discipline of art. 226 c.p.p. Following the /911 attacks, which represented a further boost resulting from a terrorist-related emergency, the legislature directly intervened in the regulation of interception, repealing the previously mentioned Article 25-ter and reforming Article 226 c.p.p. The new system, which is currently in force, stipulates that the Minister of the Interior or the heads of the central services, upon his delegation, may request authorization for preventive interception from the Public Prosecutor's Office at the court of the capital of the district in which the person to be monitored is located, whenever they deem it necessary to acquire information related to the prevention of crimes specified in Articles 407, paragraph 2(a) and 51, paragraph 3-bis c.p.p. It is stipulated that a summary record of the operations, together with the media used, must be prepared and filed with the secretary of the prosecutor who authorized the interception for evaluation of compliance and subsequent destruction. It is expressly stated that the elements acquired may not be used in a criminal trial, except for investigative purposes[300]. Recently, interception regulations underwent further amendments through Legislative Decree No.

[298] Art. 51, co. 3-bis c.p.p.: "Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 416, sesto e settimo comma, 416, realizzato allo scopo di commettere taluno dei delitti di cui agli articoli 12, commi 1, 3 e 3-ter, e 12 bis del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 600, 601, 602, 416 bis, 416 ter, 452 quaterdecies e 630 del codice penale, per i delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416 bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti previsti dall'articolo 74 del testo unico approvato con decreto del Presidente della Repubblica 9 ottobre 1990 n. 309 [190 bis, 295, 371 bis, 406 c.p.p.], e dall'articolo 291 quater del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, [e dall'art. 260 del decreto legislativo 3 aprile 2006 n. 152, le funzioni indicate nel comma 1 lettera a) sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente".

[299] Law Decree 8 June 1992, n. 306 "Modifiche urgenti al nuovo codice di procedura penale e provvedimenti di contrasto alla criminalità mafiosa" converted in Law n. 356/1992. Art. 25-ter: "[..] il procuratore della Repubblica presso il tribunale del capoluogo del distretto ove le operazioni devono essere eseguite può autorizzare con decreto dell'intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione (ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici), nonché l'intercettazione di comunicazioni tra presenti anche se queste avvengono nei luoghi indicati dall'articolo 614 del codice penale, quando le intercettazioni medesime siano necessarie per l' attività di prevenzione e di informazione in ordine ai delitti indicati nell'articolo 51, comma 3-bis, del codice di procedura penale[…]".

[300] Agostini, B. (2017). *Op. Cit*., p.144.

7/2015, which again amended Article 226 c.p.p. This amendment included attempted or consummated crimes with the purpose of terrorism, committed through the use of computer or telematic technologies, as defined in Article 51, paragraph 3-quater c.p.p. This provision reflects the legislature's goal of addressing the phenomenon of lone wolves. Although the limitation to situations involving the use of cyber tools has been criticized by the doctrine, which calls for a broader formulation, it seems to be welcomed, especially considering the need to respect the principle of proportionality in the limitations of constitutionally protected rights, such as the confidentiality of communications. A relevant new feature is the new paragraph 3-bis, which introduces an exception to the obligation of immediate destruction of the acquired data (with the exception of the content of communications), upon the authorization of the competent prosecutor, if they are indispensable for the continuation of the investigation, with a maximum duration of twenty-four months[301]. An additional as well as the most recent regulatory development on interception occurred in 2023 with the approval of Law Decree No. 105/2023[302]. The complex and extensive financial maneuver of 2023 in fact introduced a reform of preventive interception carried out by the Security Intelligence Services, defined as "intelligence preventive interception". This reform was implemented to address the interpretative ambiguity arising from Article 13 of Legislative Decree 152/1991, which reserves a special regime for the use of this tool in the investigation of organized crime offenses. The need to clarify the scope arose from a potential interpretive conflict that emerged after a ruling of legitimacy. Preventive wiretaps are technical activities carried out prior to the crime and absolutely unusable in criminal proceedings, directed "to gather information useful for the prevention of serious crimes and not for the acquisition of elements aimed at ascertaining responsibility for individual criminal acts"[303]. Basically, they consist of eavesdropping on conversations or communications (telephone, environmental, home or telematic) and monitoring activities on communications, which can be carried out even in the

[301] Berrutti, L. V. (2016). *Una nuova formulazione delle intercettazioni preventive al servizio della lotta contro il terrorismo*, in Commento al d.l. 7/2015, art. 2.
[302] Law Decree 10 august 2023, n. 105 "Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione".
[303] Cantone, R. & D'Angelo, L.A. (2006). *Una nuova ipotesi di intercettazione preventiva*, in Aa. Vv., *Le nuove norme di contrasto al terrorismo*, a cura di A.A. Dalia, Giuffrè, p. 54.

absence of criminal proceedings, "regardless of the existence of a *notitia criminis* and the objective of gathering evidence that can be used in court"[304]. In other words, these fall neither into the category of judicial interception, regulated by the Code of Criminal Procedure in Articles 266 et seq. nor preventive police interception regulated by Article 226 of the Implementing Provisions of the Code of Criminal Procedure. Rather, it is a third type, that is, interception conducted by the Intelligence Services in the context of their security and intelligence activities[305]. Changes to this institution have long been called for, both because of the increasingly evident increase in its use in investigations and because of the often crucial importance that information gleaned from such interception has assumed in initiating criminal proceedings and contributing to the evidence presented to the court. Over the years, this has generated some confusion, as such interception have acted as an articulation to the evidentiary rules common to other means of evidence-seeking, mixing up roles, functions and safeguards[306]. The reform was enacted to address the interpretative ambiguity arising from Article 13 of Legislative Decree 152/1991, which reserves a special regime for the use of this tool in investigations of "organized crime" offenses. The need to clarify the scope arose from a potential interpretative conflict that emerged following a ruling of legitimacy. Rather than wait for a jurisprudential resolution, the legislature opted for a direct solution. The rules remain unchanged, consolidating the solution of the 2016 United Sections Scurato, which also extends the derogatory regime to specific crimes such as those provided for in Articles 452-quaterdecies and 630 c.p., as well as those committed for the purpose of terrorism or by availing oneself of the conditions of Article 416-bis, or in order to facilitate the activity of the associations provided for in the same article. The conversion law, however, introduces innovations of a general scope, not limited exclusively to interception for organized crime crimes. The first relevant change introduced by the reform regards the fact that preventive interception undergoes a significant cost reduction with a radical change. The legislation shifts the financial burden from the Justice sector to the Security sector, detailing

[304] Illuminati, G. (1983). *La disciplina processuale delle intercettazioni*, Giuffrè, p. 171 ss.
[305] Nocerino, W. (2023) La riforma delle intercettazioni preventive d'intelligence. <Sistema Penale>.
[306] Cfr. Nocerino, W. (2018). *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio,* Cedam, p. 458.

the costs of interceptions to the expenditure program related to the Intelligence System for the Security of the Republic, included in the budget of the Ministry of Economy and Finance (Article 1, paragraph 684, Law 197/2022[307]). This shift in economic responsibility, however, has a far more significant impact than the initial cause, namely the high costs of the justice system. The financial separation of the security sector in the management of preventive interception aims to guarantee and strengthen the secrecy of the sensitive information acquired, while ensuring the distinction of the data from the investigative dynamics of criminal trials[308]. The recent legislative amendment focuses on two crucial aspects. First, it aims to ensure greater secrecy of information obtained through preventive interception, particularly prior to the crime. This goal not only preserves the confidentiality of those involved in the operations, but also acts as a safeguard against possible undue contamination with the evidentiary process, while also helping to maintain a clear separation between the security and justice sectors. Second, the decision to shift financial responsibility from the Ministry of Justice to the expenditure program of the Intelligence System for the Security of the Republic goes beyond a mere matter of managing economic resources. This strategic change intervenes in the management of acquired information, preventing the transfer and storage of data by external bodies. This measure is essential to prevent the circulation outside the intelligence sector of sensitive documents, thus preserving the confidentiality of operations conducted by the Intelligence Services[309]. Deepening the analysis, one of the most innovative aspects pertains to the introduction of Article 4-bis in Decree Law 144/2005, dedicated to "Provisions on preventive interception by security intelligence services", bringing changes mainly of a formal nature, on the way interception is carried out. While some features of the previous legislation remain unchanged, such as the maximum duration of interception [310] and the form of authorization[311], systematic innovations emerge. Among

[307] Law 29 December 2022, n. 197. "Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025".
[308] Nordio, C. (2022). *Intervento alla Camera, 7 dicembre 2022*, Sist. pen., 8 dicembre 2022.
[309] Nocerino, W. (2023). *Op. Cit.*
[310] The term of duration remains 40 days extendable for successive periods of 20 days, according to Article 4a, paragraph 1, first sentence, d.l. 144/2005.
[311] The required form of the measure is the authorizing decree, according to the second sentence of paragraph 1 of Article 4a, d.l. 144/2005.

the new features is the obligation to hand over, which also extends to the content of the interception[312], and the deadlines for such fulfillment are reshaped, raised from 5 to 30 days after the conclusion of the operations, with provision for deferral of the deadline for a period not exceeding 6 months upon reasoned request of the Directors of the Intelligence Services[313]. Another change concerns the expansion of the destruction obligations concerning the entire material handed over, including intercepted contents and copies thereof, whether total or partial, in paper or computer format, in order to ensure greater consistency to this provision. Moreover, a requirement is introduced for the prosecutor to dispose of the documentation held by him, with the exception of decrees containing requests for authorization of interception operations, which must also include a summary of the wiretaps[314]. The change also affects the timing of the disposal of the results of control activities that go beyond wiretapping intended in *stricto sensu*, namely "controls"[315]. Filling a previous regulatory gap, the reform stipulates that these data must be destroyed within 6 months of their acquisition. In addition, related records must be sent to the attorney general. However, there is provision for the attorney general to authorize an extension of the retention of such data for up to 24 months[316]. Another relevant change is made with Paragraph 2-bis of Article 1, which intervenes in the regulation of interception by means of a computer interceptor, amending Paragraph 1 of Article 267 c.p.p. With it, a strengthening of judicial control is highlighted, as it requires that the authorization decree issued by the judge for preliminary investigations (GIP) include an independent assessment of the reasons justifying the use of this tool, emphasizing that this assessment must be carried out "in concrete terms"[317]. In addition, paragraph 2-ter of Article 1 intervenes in the regulation of the

[312] Art. 4 *bis,* paragraph 2, d.l. 144/2005.
[313] Nocerino, W. (2023). *Op. Cit.*
[314] The prosecutor shall proceed with the destruction after the deadline for the fulfillment of reporting obligations by the President of the Council of Ministers to the Parliamentary Committee for the Security of the Republic, i.e. 30 days from the conclusion of the operations. Cfr. Nocerino, W. (2023). *Op. Cit.*
[315]That is, the tracking of telephone and telematic communications, the acquisition of external data relating to the telephone and telematic communications that have taken place, and the acquisition of any other useful information in the possession of telecommunications operators.
[316] Nocerino, W. (2023). *Op. Cit.*
[317] Law 9 October 2023, n. 137. "Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi

transcript of interception, making amendments to paragraphs 2 and 2-bis of Article 268 c.p.p. These amendments provide for a more detailed transcript, limited to the "content of the intercepted communications relevant to the investigation", with the aim of avoiding the inclusion of irrelevant material in the records of the proceedings[318]. The provision extends to the prosecutor, tasking him or her with overseeing compliance with the prohibition against transcribing "irrelevant" communications. It also replaces the reference to sensitive data with a broader reference to "facts and circumstances pertaining to the private life of the interlocutors", aiming to strengthen the effectiveness of this provision[319]. Furthermore, another important modification is represented by paragraph 2-quarter[320], which intervenes in the regulation of the usability of interception in proceedings other than those in which they were authorized. Paragraph 1 of Article 270 c.p. undergoes an amendment, causing the segment added by the legislature with Law Decree No. 161/2019 to fall[321]. The latter generally permitted the use of interception if it was essential to ascertain crimes under Article 266, Paragraph 1 c.p.p. The amendment is clearly restrictive, reestablishing the regulatory framework prior to the *Cavallo* ruling of the Joint Sections[322]. The principles enunciated in that ruling may now be reevaluated in their the validity, considering that the 2019 interpolation, set to be removed, had been a significant argument used by some doctrine and jurisprudence to criticize the Court's conclusion. The latter stipulated that the usability of interception in the "same proceedings" was allowed only if they were aimed at ascertaining related crimes according to Article 12 c.p.p. and simultaneously falling under Article 266,

boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonchè in materia di personale della magistratura e della pubblica amministrazione".

[318] *Ibidem*.

[319] Lazzeri, F. (2023). *Convertito in legge, con modificazioni, il d.l. 105/23: novità in materia di intercettazioni, incendio boschivo, ambiente e 231*. <Sistema Penale>.

[320] Applicable only to future proceedings according to paragraph 2-quinquies.

[321] Law Decree No. 161/2019 had added a part to Paragraph 1 of Article 270, allowing the general use of interception if they were essential for investigating crimes stipulated in Article 266, Paragraph 1 c.p.p. Now, with the new amendment, this addition is removed, making it necessary for interception to be used only if they are strictly necessary to investigate crimes requiring arrest in flagrante delicto, as stipulated in Article 266, Paragraph 1 c.p.p.

[322] Cass., Sez. un., 28 novembre 2019 n. 50. After this amendment, it will always be necessary, in order to use authorized interception in a different proceeding, for that proceeding to concern "crimes for which arrest in flagrante delicto is mandatory". Cfr. Illuminati, G. (2020). *Utilizzazione delle intercettazioni in procedimenti diversi: le Sezioni unite ristabiliscono la legalità costituzionale*. <Sistema Penale>.

Paragraph 1 c.p.p. This limitation, considered unreasonable by several parties, is restored in light of the rule introduced by Law Decree No. 161/2019, which, ironically, allowed usability even in "different proceedings"[323]. During the conversion phase, Article 2-bis was added to strengthen tools against cybercrime and promote online security[324]. The provisions, detailed in the article, touch on several aspects, including strengthening the tasks of the National Cybersecurity Agency, establishing an information flow with the National Anti-Mafia and Counterterrorism Prosecutor, and specific amendments to the Code of Criminal Procedure (Articles 54-ter, 371-bis, 724 and 727). These amendments extend the powers of the National Anti-Mafia Prosecutor, already operating in the crimes referred to in Article 51, paragraphs 3-bis and 3-quater c.p.p, to some relevant computer crimes, listed in the new paragraph 4-bis of Article 371-bis[325]. In addition, it is also important to mention the objective and subjective expansion, with reference to the cyber sphere, of the perimeter of undercover operations regulated by Article 9 of Law 146/2006. This update is indicated in paragraph 4 of Article 2-bis of the decree.

The 2023 reform on preventive interception thus reflects a growing awareness of the importance and frequency of use of such tools in daily investigative activity. The legislature, aware of the risks associated with the possible inclusion of acquired data in criminal proceedings, decided to intervene with a specific discipline for preventive intelligence wiretapping, aiming to strengthen the secrecy of information. The change of "economic competence" from the Ministry of Justice to the Security branch is a significant step in preserving the confidentiality of information by preventing the external circulation of acquired data. Other formal changes, such as enhanced filing requirements and destruction extended to the prosecutor, also contribute to this goal by containing exceptions to the evidentiary unusability of captured data. The reform is distinguished by an effective methodological approach, overcoming critical previous interpretative issues and introducing an autonomous discipline for preventive intelligence interception. However, in terms of

[323] Lazzeri, F. (2023). *Op. Cit.*

[324] Law Decree n. 105/2023. Art. 2-bis "Disposizioni urgenti in materia di contrasto della criminalità informatica e di cybersicurezza".

[325] The cases referred to are the ones defined in arts. 615-ter, 635-ter, 635-quinquies, 617-quater, 617-quinquies e 617-sexies c.p.

content, the reform does not have the desired effects, and the result that is achieved is certainly less valuable than the intent behind the maneuver. In fact, despite the attempt to eliminate the mechanism of regulatory referral, the reform largely replicates the discipline of Art. 226 disp. att. c.p.p., resulting in a proposal that does not fully meet expectations, maintaining all the critical issues already encountered in relation to those provisions and extending them also to the newly introduced provisions of Articles 4 and 4 bis, d.l. 144/2005[326]. In light of this analysis, the delicate balance between state security and individual privacy rights emerges as a clear topic of discussion, and there arises the need to reflect on how to address the challenges of the current historical context. The increasingly widespread use of sophisticated investigative tools, essential as it may be to confront current threats, raises questions about safeguarding citizens' privacy. As stated by the German Constitutional Court and applied also in many other constitutions: "the Constitution excludes the pursuit of the goal of absolute security at the price of the nullification of freedom"[327]. However, the discussion on this balance cannot ignore a broader perspective that views privacy not as an obstacle to security but as a crucial value in itself for the defense of democracies[328]. As stated by jurist Soro[329], privacy represents the best synthesis between freedom and security, as data protection serves as a bulwark against cyber threats and the recruitment of terrorist followers through the internet, affirming that "the defense of privacy is the only real effective strategy to protect us from cyber threats and a terrorism that increasingly feeds off the network to recruit new followers, promote fundamentalism and intolerance, and move from cyber espionage to the very real, concrete violence of massacres and attacks"[330]. The fight against terrorism, therefore, plays a fundamental role in preserving democratic identity[331]. In this context, the importance of cooperation in criminal justice, enshrined in the Lisbon Treaty, is crucial to address transnational crime. Legislative innovations, the result of decades of collaboration among the judicial bodies of member

[326] Nocerino, W. (2023). *Op. Cit.*
[327] BVerfG, 1 BvR 518/02. Commented by Vedaschi, A. (2010). Has the balancing of rights given way to a hierarchy of values. *Comp. L. Rev.*, *1*, 1.
[328] Vedaschi, A. (2010). *Op. Cit.*
[329] A Soro. (2014*). Op. Cit.*
[330] *Ibidem*.
[331] Cfr. Trabelsi v. Italia, App. No. 50163/08 (ECtHR, 13 April, 2010).

states, reflect an awareness of the absence of boundaries for crime in a globalized world. Furthermore, it is emphasized that the recent reform aims to consolidate security through an active data-sharing system, respecting the right to privacy and promoting close cooperation in the field. This approach represents a vital resource to efficiently address the terrorist threat, balancing societal protection with respect for the fundamental rights of citizens. Hence, the most effective resource against the growing terrorist threat can only be achieved through an active data-sharing system, supported by a continuous exchange of information, and respecting the value our legal system places on the right to privacy. This is further strengthened by a close cooperation "on the field"[332].

3.3 Criminal law and the problem of "anticipation of protection" vis-à-vis fundamental rights

In the process of delving into the Italian legislation concerning the crime of cyberterrorism, it is crucial to highlight a specific aspect of the criminal legislation in this realm. In fact, it is pertinent to scrutinize specific articles of the penal code, already mentioned in the previous paraphs, that address various offenses falling under the broad umbrella of cyberterrorism. This explicates the peculiarity of Italian criminal law, characterized by multiple provisions that may be applicable to this type of crime, with the aim of encompassing the majority of facets that constitute it. Each provision addresses a different aspect that the offense may encompass, collectively shaping a regulatory framework that tends toward completeness. An example is in the case of a cyber-attack aimed at damaging, deleting, or altering information used by the State or for public purposes; it would constitute an offense under Article 635-ter c.p. Similarly, an analogous act aimed at destroying even just a part of an information system of public utility falls under Article 635-quinquies c.p.[333]. Another example is that, in the case of preparatory activities, such as the delivery or provision of malicious software with the aim of unlawfully damaging computer systems, data, or information, or the unlawful interception of computer or telematic communications between systems to acquire strategic data on the

[332] Nocerino, W. (2016). *Op. Cit*. p. 1226.
[333] Vigneri, A. F. (2018) *Op. Cit.*, p. 19.

configuration of target logical infrastructures, or even the installation of applications designed to intercept such communications, the respective Articles to find application would be 615-quinquies, 617-quater, and 617-quinquies c.p. If the unlawful interception or installation of devices for interception had as target communications between individuals, also the so-called "common" computer crimes would be applicable, under Articles 615-bis, 617, and 617-bis c.p. [334]. Hence, there appear to be no specific or serious gaps in the Italian legal system, at least in the realm of cybercrime, as it currently possesses some basic tools for preventing and countering activities that can be categorized under the phenomenon of cyberterrorism. A potential legislative intervention could possibly address the sanctioning framework concerning particularly serious acts carried out with "terrorist purposes". A case worth considering is that of unauthorized access to computer systems, particularly in aggravated instances involving computer systems of military interest or those related to public order and security. This offense is punishable by imprisonment, ranging from one to five years and three to eight years, respectively. However, it is essential to emphasize that given the nature of activities endangering sensitive and critical State systems, crucial in the information society and strategic assets for the maintenance of social stability, and in comparison to other offenses and their corresponding penalties, the contemplated offense might be increased not only to punish but also to serve as a deterrent factor if presented with a higher penalty. The lack of rationality in the penalties becomes particularly evident when juxtaposing this regulatory framework with those stipulated, for instance, for individuals enlisted (according to Article 270-quater c.p.) or in cases of self-training (as outlined in Article 270-quinquies c.p.)[335]. According to Art. 270-quater, in cases of recruitment, the recruiter is subject to imprisonment ranging from seven to ten years, while the recruited faces imprisonment from five to eight years. Conversely, as provided for by article 270-quinquies c.p., in instances involving training or the mere provision of instructional materials for

[334] *Ivi,* p. 20.

[335] *Ivi,* p. 21. On the analysis of the introduction of Articles 270-quater and 270-quinquies, attributed to procedural rather than substantive needs, with the aim to provide investigative and law enforcement authorities with more tools to easily conduct inquiries and prevent the commission of offenses related to Islamic terrorism, cfr. Presotto, A. (2017). *Le modifiche agli artt. 270-quater e quinquies del codice penale per il contrasto al terrorismo*. Dir. pen. cont.—Riv. Trim, 1.

learning, for instance, how to create Improvised Explosive Devices (IEDs) for terrorist activities, the penalty is imprisonment from five to ten years. The same penalty applies to the trained individual and the person who independently trains themselves by obtaining such information from the web, with a specific provision that if the training activities are conducted online and/or through computer tools, the penalty is increased. Even with many hermeneutic difficulties, the internal discipline of counter-terrorism, particularly regarding the regulatory interventions of the years 2015-2016, can be applied to facts attributed to cyberterrorism. Starting from the new disposition of art. 270-quinquies c.p., as reported by Law No. 43 of 17 April 2015, it can be noted that the penalty treatment is addressed both to those who train and to the trained person, article 270-sexies. Furthermore, the penalties mentioned in this Article will be raised if the trainer or instructor is responsible for using computer or telematic means[336]. The situation can be abstractly applied both to those who, with the intention of carrying out terrorist acts, provide information through the Net and its infinite potential (think of the tutorials sent by the trainer to the trainer containing instructions on how to access the dark web to buy weapons), both to those who, through research on the Net or the dark web, acquires know-how (think of the information concerning the construction of self-produced explosives, known as home-made explosives), if it implements behaviors clearly aimed at the commission of the conduct provided for in Article 270-sexies[337]. In this context, a crucial aspect of the doctrine is highlighted, which is the potential contradiction between the clause that could exclude punishability for activities solely focused on obtaining information and the legislator's intention to allow self-administration[338]. This ambiguity is manifested in the punishment of conduct for the purpose of terrorism, where the

[336] The rule in question provides for a double specific intent because, in addition to the purpose of terrorism, the purpose of committing acts of violence or sabotage is also required. The rationale for the increased punishment inserted in the last paragraph and intended for those who train or instruct by means of the Internet, is related to the aspatial nature of cyberspace, which allows for easier retrieval of information and instructions, as well as for the terrorist message to be much more easily conveyed, which can potentially be directed to an indefinite audience of users. Vigneri, A. F. (2018). *Op. Cit.*, p. 22.

[337] Vigneri, A. F. (2018). *Op. Cit.*, p. 22.

[338] Pelissero, M. (2016). *Contrasto al terrorismo internazionale e il diritto penale al limite*. Questione Giustizia, 99-112, p. 99.

finding of instructions would represent a background[339]. The wide and indeterminate definition of "purpose of terrorism" in 270-sexies c.p. extends the scope of punishment to include finding information through the web, raising the issue of excessive repression[340]. Further critical issues emerge in the evaluation of neutral conduct, such as travel propaganda online or through online organizations, which only become criminal if it is directed towards terrorist acts. Specific challenges arise when a legislator sanctions facts outside of the specific cases indicated in art. 270-bis or in combination with arts. 270-bis and 270-quater, leading to the need for a concrete assessment[341]. The legislator's choice to penalize the act of acquisition raises further questions, categorizing the situation as "improper computer crimes"[342]. The interpretation of this conduct should adapt to the technological context but also consider the possibility of obtaining "dangerous" information through manuals and specialized magazines. Finally, the analysis concludes that the mere possession or storage of information in a computer does not assume criminal relevance unless such information is used for conduct explicitly aimed at committing the acts referred to in Article 270-sexies[343].

As illustrated, cyberterrorism emerges as a hybrid phenomenon in Italy, falling both under the legislation on cybercrimes and anti-terrorism. The latter takes a preventive approach, lowering the threshold of criminal relevance and penalizing actions considered prospective. In this context, the contribution of the scientific analysis by Flor, points out that the Italian legislation on cyberterrorism seems to tend to stigmatize the network and computer tools, which could result in a significant decrease in the constitutionally guaranteed individual freedoms. The protection of individual rights and freedoms and the exercise of State sanction powers are forming a delicate balance in political and criminal decisions. Criminal law, while

---

[339] Flor R., (2017) *Cyber-terrorismo e diritto pnale in Italia, in Diritto Penale e Modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali, Atti del convegno Trento 2 e 3 ottobre 2015*, Università degli Studi di Trento, Quaderni della facoltà di Giurisprudenza, Fornasari G., Wenin R. (a cura di), Trento, 2017, p. 342.

[340] Cavaliere A., *Considerazioni critiche intorno al D.l. antiterrorismo n. 7 del 18 febbraio 2015*, Diritto Penale Contemporaneo, fasc. 2, 2015, p. 226.

[341] Flor R., (2017). *Op. Cit*., p. 343.

[342] *Ibidem*.

[343] Vigneri, A. F. (2018). *Op. Cit.,* p. 24. Cfr. Cavaliere, A. (2017) Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali. In Wenin, R. & Fornasari, G. (2017) *Diritto Penale e Modernità, Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*.

on the one hand it protects assets worthy of protection, on the other it acts on such assets, highlighting a double-edged nature and raising questions about the legitimacy of the punitive power itself[344]. The analysis of the regulatory provisions relating to the system of sanctions against the cyberterrorist threat is a fundamental starting point to fully understand a trend that has increasingly taken root in the Italian judicial system in recent years: the anticipation of protection from a preventive perspective. This analysis aims to outline the regulatory framework that depicts the criminal response to the cyberterrorist threat, drawing attention to the legislative dynamics and ways in which the legal apparatus addresses the emerging challenges in the context of cybersecurity. Through this legislative overview, it emerges clearly the subsequent reflection on the growing propensity of the Italian judicial system towards early action to preserve national security. The debate on the need to anticipate criminal protection in relation to preparatory acts, often cited as a distinctive feature of criminal law linked to organized crime, focuses on the issue of the alleged a priori illegality of the indictments of preparatory acts in the light of the constitutional principle of offensive conduct[345]. The critical perspective is that a penal system limited to the incrimination only of the executive acts of terrorist attacks may be insufficient to guarantee an effective social defense. In response, there may be a need for a system of preventive detention measures directly managed by the executive, although this approach is considered potentially more dangerous for the fundamental rights of individuals than a judicial system that holds, under judicial control, the perpetrators of preparatory actions. The real dilemma, therefore, lies in carrying out a thorough examination of the suitability and strict necessity of anticipating criminal protection in relation to the objectives of social protection. This implies avoiding excessively wide-ranging incriminations, which could indiscriminately affect both truly dangerous behaviour for legal goods and acts of mere ideological dissent or affinity with the perpetrators of crimes. At the same time, it is essential to ensure that sanctions remain within the limits of reasonable proportionality to the actual degree of insult of the act committed[346].

---

[344] *Ivi*, p. 26.
[345] *Ibidem*. Cfr. Flor R., (2017). *Op. Cit.*
[346] Viganò, F. (2007). *Sul contrasto al terrorismo di matrice islamica tramite il sistema penale tra "diritto penale del nemico" e legittimi bilanciamenti*. Studi Urbinati, A-Scienze giuridiche, politiche ed economiche, 58(4), 329-348, p. 344.

The current regulatory framework against terrorism in Italian criminal law aligns with the tradition of political criminal law, highlighting a progressive protection approach. This system enhances the techniques of early protection, intervening before the stage typed in crimes of attack. This choice responds to the new modes of action of international terrorism, which operate through networks rather than within hierarchically structured organizations[347]. At the same time, these provisions respond to the need to combat lone wolves and foreign fighters, as provided for in Law n. 433/2015. Partial recognition has been given to the so-called self-training, but only when it follows behaviors clearly aimed at the implementation of the actions provided for by Article 270-sexies c.p. This solution, while avoiding punishing the mere acquisition of information, which in itself could be considered neutral, seems inconsistent with the legislator's intention to sanction self-training. In fact, it punishes "the accomplishment of actions with terrorist purposes, in which the search for instructions is a preliminary step"[348]. In addition, Article 270-quater, paragraph 2 c.p., sanctions those who enlist for acts of violence or sabotage of public services for terrorist purposes, even if training or participation in an associative crime does not occur. Furthermore, criminal relevance is recognized to those who organize, finance, or promote trips abroad with the intention of carrying out terrorist acts (Article 270-quarter 1 c.p.)[349]. These situations respond to a procedural need as they allow for the punishment of behaviors without requiring proof of the individual's participation in an associative offense, as it is no coincidence that all these situations include a reservation clause regarding the offense specified in Article 270-bis c.p. The increasing emphasis on cases with a highly anticipated structure in criminal law shows a gradual approach to the borders of the delegitimization of the latter. While criminal liability remains tied to the charge of an associative offense, actions of participation or external competition require broader and more robust evidentiary support[350]. However, when preparatory actions are punished outside the cases referred to in art. 270-bis, simplifies the

[347] Cfr. Fasani F., (2016). *Terrorismo islamico e diritto penale*, Cedam, Milano.

[348] Wenin, R. (2015). L'addestramento per finalità di terrorismo alla luce delle novità introdotte dal D.L. 7/2015, Diritto Penale Contemporaneo, p.16.

[349] Pelissero, M. (2016). *Contrasto al terrorismo internazionale e il diritto penale al limite*. Questione Giustizia, 99-112, p. 109.

[350] Cfr. Viganò, F. (2007). Il contrasto al terrorismo di matrice islamico-fondamentalistica: il diritto penale sostanziale. In *Terrorismo internazionale e diritto penale.*

evidentiary framework necessary to support the prosecution. This poses the risk that, even if formally it does not seem to restrict the freedom of expression, such situations can quickly result in a violation of this freedom. It is therefore the task of the magistrate, charged with interpreting the norm and evaluating the evidence, to ensure compliance with the border of legitimacy of the criminal control[351]. In this context, two fitting examples can be provided - one illustrating an overstepping of the boundary of legitimate interpretation of the criminal rule, and another representing what is known as positive jurisprudence, acting as a barrier to the expansive potential of penal control. The first one is represented by the judgement n. 40699[352], which establishes the configurability of the form attempted for the crime of enlistment (art. 270-quater cp). The judgement does not prevent the application of the general rule of art. 56 cp, since the crime is of a nature of danger. The Supreme Court, through a thorough investigation, identifies the act of enlistment as the conclusion of a serious agreement between the parties, where the seriousness derives from the authority of the proposer, with effective ability to integrate the aspirant in the organizational structure, and firm determination of the recruiter. The Supreme Court faces the challenge of defining the boundary between a "serious" verbal commitment and a simple consensus to commit terrorist acts, noting the difficulty of admitting the attempted form in an agreement-based crime[353]. While formally accepting the configurability of the attempted form, the Court stresses the obvious need to distinguish between the punished attempt and the activities of proselytism or free manifestation of thought. The Court acknowledges the complexity of drawing such a boundary, especially in relation to crimes that already punish preparatory conduct, pointing out that the attempt itself seems to remain outside the possibilities of prosecution[354]. On the other side, a crucial ruling that serves as a positive example of restrictive jurisprudence against the expansion of criminal control has emerged from the Court of Cassation concerning the offense of training outlined in Article 270-quinquies c.p.[355]. In this particular

[351] Pelissero, M. (2016). *Op. Cit.*, p. 110.
[352] Cass., Sez. I, 9 settembre 2015, n. 40699.
[353] Cfr. Cavaliere, A. (2015). *Considerazioni critiche intorno al dl antiterrorismo, n. 7 del 18 febbraio 2015*. Diritto penale contemporaneo, 2, 226-235.
[354] Pelissero, M. (2016). *Op. Cit.*, p. 111.
[355] Cass., Sez. I, 6 novembre 2013, n. 4433.

case, the issuance of a protective order was based, among other factors, on the subject's ideological context, deduced from his Facebook and Twitter profiles, as well as online searches encompassing videos on explosives assembly and military training footage. The Supreme Court has elucidated that, for the offense of training to be established, the military notions provided or acquired must be "suitable to constitute in those who receive them a technical baggage sufficient to prepare or use weapons and anything else, not only […] to arouse or increase their own or others' interest in this field"[356]. Furthermore, the judgment unequivocally asserted that self-training and hetero-training are criminal offenses, while information and proselytism fall within the realm of constitutionally protected individual freedoms[357]. The reduction of the threshold of punishability and the encroachment into the repression of forms of thought expression pose the risk of transforming criminal law from a law of facts to a copyright criminal law, where subjective dangerousness becomes the criterion for the interpretation of the evidentiary framework[358]. In doctrinal terms, there is indeed a systematic recourse to the maximum "subjectification" of regulatory cases. In this context, the focus of the disvalue and the very raison d'être of the indictment center on the element of the end pursued by the agent, as specified by the legislator with reference to the definition contained in Article 270-sexies c.p.[359]. On the contrary, the conduct or the underlying act, objectively described in terms of concrete material realization, often appear intrinsically neutral or otherwise lawful, and remain significantly distant from the actual achievement of the intended purpose. This is in contrast to the absence of any explicit requirement for objective suitability or unequivocal direction, as prescribed by the general framework of attempt concerning consumption. These criteria have been interpretatively extended to the various forms of attack outlined in our legal code, with some explicitly incorporated by the amendment introduced by Law No. 85 of 24 February 2006[360].

---

[356] *Ibidem*.
[357] Cfr. Continiello, A. (2017). *Terrorismo e indottrinamento. Anatomia della fattispecie alla luce di una recente pronuncia della Suprema Corte di Cassazione*. Giurisprudenza Penale.
[358] Pelissero, M. (2016). *Op. Cit.*, p. 111.
[359] Picotti, L. (2017). *Terrorismo e sistema penale: realtà, prospettive, limiti*. Diritto Penale Contemporaneo, (1), 249-263, p. 255.
[360] *Ibidem*.

The Legislative Decree n. 7/2015, which introduced provisions making both the actions of the trained and transfers abroad for terrorist purposes punishable, has expanded the scope of application of preventive measures. In this context, the clue itself becomes evidence of the "preparatory acts, objectively relevant, directed... to take part in a conflict in foreign territory in support of an organization that pursues the terrorist aims as defined in Article 270-sexies c.p."[361].

In the analysis of the doctrine, which appears to be largely in favor of the anticipation of protection against terrorism offenses, two main arguments in support and justification thereof emerge prominently. The first argument is grounded in the preventive function, emphasizing the need to steer criminal law towards the prevention of criminal conduct by intervening promptly, even before such actions materialize[362]. However, this approach raises concerns about its coherence with constitutional principles of offensiveness and extrema ratio, tied to a perspective on the relationship between the individual and criminal law-oriented toward social integration, rather than excessively neutralizing state intervention, risking evolving into forms of extremely invasive control. The paramount consideration for the individual, according to the Italian Constitution, suggests that the intervention of criminal law should be limited to situations where there is a concrete and current danger to the legal rights of others, allowing for a period of extrajudicial prevention with less invasive measures. However, the criminalization of remote preparatory acts, such as the interception of extremist speeches or visits to fundamentalist websites, or the acquisition of elements like concentrated hydrogen peroxide or enrollment in martial arts courses, effectively transforms criminal law into a primary means of control for the police or security services, making even investigative elements punishable and justifying, in some cases, pre-trial detention. This approach, defined as "panpenalism", suggests that even in the face of the earliest, most remote signs of potential terrorist activity, the prevailing response should be incarceration, raising critical questions

[361] Legislative Decree 6 September 2011, n. 159 "Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136". Article 4, paragraph 1, letter d): "[…] nonché alla commissione dei reati con finalità di terrorismo anche internazionale ovvero a prendere parte ad un conflitto in territorio estero a sostegno di un'organizzazione che persegue le finalità terroristiche di cui all'articolo 270-sexies del codice penale".

[362] Hassemer, W. (2006), *Sicurezza mediante il diritto penale*, in *Crit. dir.*, n. 1-2/2008, 35-36.

about proportionality and consistency with the fundamental principles of the Italian legal system[363]. The second argument, widely embraced in doctrinal discourse and endorsed by the Constitutional Court[364], proposes that the principle of proportionality justifies the anticipation of legal protection concerning remote acts in relation to the defense of fundamental goods[365]. While it aligns with proportionality to anticipate legal protection of such goods before an actual and concrete danger manifests, a fundamental concern arises. The critical issue pertains to the possibility that these primary goods may be protected even in the face of non-offensive conduct or mere criminal intentions, calling into question the principle of offensiveness as a barrier against excessive prevention. Paradoxically, the assertion that proportionality allows for derogation from necessary offensiveness in the context of safeguarding fundamental goods reveals an apparent contradiction: if proportionality can be invoked to justify such derogation, it could also be applied to derogate from the personality of criminal responsibility or strict legality. This surreptitious emptying of the principle of offensiveness raises critical questions about the coherence and durability of the fundamental principles guiding the legal system[366][367].

To conclude this analysis, it may be asserted that the new approaches shall be interpreted in light of traditional criminal law needs, respecting essential limits of proportionality and clarity in legal provisions, even if oriented primarily toward the purpose of incrimination. Remaining anchored in these principles is crucial to identifying and preserving both substantive and procedural safeguards, even in the face of the serious threat of jihadist terrorism, which may elude conventional models of understanding and prevention. Suspending rights is not an acceptable response. Even preventive actions, such as

[363] Cavaliere, A. (2017). *Op. Cit*., p. 23.

[364] Corte cost., sent. 10-11 luglio 1991, n. 333, in Riv. it. dir. proc. pen., 1992, 295- 296.

[365] With regard to the anticipated legitimacy of offenses, falling below the threshold of attempted acts, for the protection of the personality of the State, cfr. Marinucci, G., & Dolcini, E. (1995) *Corso di diritto penale, 1. Nozione, struttura e sistematica del reato*, Milano, p. 149 ss.

[366] Cavaliere, A. (2017). *Op. Cit*., p. 24.

[367] In this context, it might be insightful to explore the aspect of specific intent in a case selected by the legislator to define terrorist crimes. This case differs from crimes of attempted offenses and common attempts because it doesn't inherently require suitability for achieving the end. Unlike events tied to the basic action through a (potential) causal relationship or objective univocity of direction, specific intent focuses on the agent's purpose rather than the action itself. The moment of consummation is precisely determined with the accomplishment of the agent's purpose or the basic fact. See: Picotti, L. (2017). *Op. Cit*., pp. 254-257.

wiretapping and investigative measures, must respect fundamental guarantees of legality, proportionality, and judicial review, even if they are not used in the criminal process. The judicial guarantee is essential to control legislative choices and ensure respect for constitutional principles and fundamental rights. In conclusion, the protection of the rule of law must rely on the law itself, strengthening the means of protection and guarantee rather than seeking emergency shortcuts that weaken these principles.

Conclusions

Individual and collective protection: an unattainable combination?

Having come to this point in the legal analysis, it is now appropriate to examine the *fils rouge* of this study and draw the necessary conclusions. However, this is not an entirely straightforward process, considering that the concept of cyberterrorism remains at the centre of an ever-evolving debate without finding a single definition, along with the possible legislative instruments to counter it, which are considered to be many and varied in nature. This intricate legislative scenario with a constitutional character, given the convergence of public safety and individual fundamental rights, undoubtedly contributes to making this topic a fascinating object of study. In fact, the absence of an internationally commonly accepted definition for cyberterrorism, as for the case of terrorism, has been recognized as a significant challenge. In the present analysis, the choice of adopting a definition that reflects European and Italian regulatory schemes, framing the phenomenon through the joint lens of terrorism and cybersecurity related to the use of cyberspace in a broad sense, has permitted to embrace the multiplicity of facets that characterize this threat. Particular attention has been paid to the preventive context, where the legal framework aims to prevent cyberterrorism, however with possible constitutional implications. For the examination of the intricate phenomenon of cyberterrorism and its legal implications, examining the legislative responses of the European Union and Italy has brought to light the central theme of the attempt to balance public security and the protection of individual freedoms, summarized in the dichotomy of *security versus freedom*. This research set out to analyze this conflict from a constitutional perspective, delving into the evolving nature of terrorism in cyberspace and the consequent legislative and constitutional challenges posed by methods of countering this threat, including online content removal, intelligence preventive interception and the anticipation of criminal protection to mere suspicion before the offensive act. The concept of security is in itself very broad and can have many facets. It encompasses not only traditional defense against external armed attacks, but also internal and, to date, intangible threats, such as cyber-attacks on critical infrastructure and Islamist radicalization propaganda circulating on the web. National

security, in the globalized era, extends beyond territorial integrity to include a security that becomes intangible but is, in fact, in the everyday life of each individual and, more broadly, of the State[368]. In fact, this research also seeks to emphasize the interconnection of the current geopolitical landscape with the growing risk of internal and external destabilization, which in the face of a phenomenon such as the one in question, which is transnational in nature, requires a further effort to create a defensive and, above all, preventive structure. The analysis emphasizes the critical moment when counter-terrorism efforts collide with individual rights, raising fundamental questions about the balance between security imperatives and the preservation of democratic values. The need arises to examine the legal convenience of considering security as an individual right or to characterize it as a collective interest. The discussion on security in relation to fundamental rights can be outlined by considering the perspective of defining it as a collective interest or as a fundamental right[369]. In the Italian case, examined in chapter three, the consideration that must be made when attempting to untangle this complex concept of security is that the Italian Constitution does not explicitly contemplate a right to security and does not pose public order as a possible limit to the rights of liberty, thus giving rise to the need to investigate the legal expediency of treating security as an individual right or of configuring it as a collective interest. This diversification of the concept, which can also expand into further binomials such as external/internal and material/ideal security, complicates the theoretical analysis, especially considering the new challenges related to information technology[370]. In the current European judicial framework, the security structure of democratic systems reveals the individualistic profile of security, implicit in the very characterization of these systems as democratic and liberal, as outdated. This makes it possible to focus on the collective interest in which security is embodied, strengthening, and evolving it without replacing the individual profile. By adopting a restrictive definition of security, limited to its traditional preventive and repressive role, as a guarantee of public order, it can be agreed that it is not confined to a specific sphere of

[368] Rubechi, M. (2016). *Op. Cit.*, pp. 5-6.
[369] Giupponi, T. F. (2008). *La sicurezza e le sue dimensioni costituzionali*. Diritti umani: trasformazioni e reazioni, 275 – 301.
[370] Rubechi, M. (2016). *Op. Cit.*, p. 5.

guaranteed activities. On the contrary, it is configured as a purpose justifying restrictive measures of freedoms, representing a reason to limit recognized rights[371]. The definition of the relationship between security and fundamental rights is thus oriented towards the proportionality and balance of the limits introduced in pursuit of the purposes, making it essential to assess the quantum and quomodo of this operation of limitation in order to ensure the overall resilience of the rule of law.

The examination of the concept of security and its application in the fight against cyberterrorism has highlighted the importance of balancing public safety, the maintenance of democratic order and social stability with, at the same time, guaranteeing the protection of the fundamental rights of the individual. In this context, the question of the balance between preventive measures and the fundamental rights has emerged as a central issue, delineating a legal dualism. This dualism, as outlined in this analysis, manifests itself in particular in the areas of fundamental rights of the right to liberty and security (Art. 5 ECHR), the right to respect for private and family life (Art. 8 ECHR), freedom of expression (Art. 10 ECHR) and the right to assembly and association (Art. 11 ECHR). The analysis highlighted a general trend in the European Union and also in the Italian legislation towards the use of preventive measures, such as the supervision of online activities, the removal of terrorist content and even preventive interception. However, such measures, if not meticulously created upstream and then rigorously applied, may lead to an abuse of powers in favour of public security at the expense of individuals, in their privacy protection and/or in their freedom of expression. Especially in cyberspace, the potential restriction or abuse of freedom of expression, again related to measures to prevent the dissemination of terrorist propaganda online, is a real and far-reaching case. In this regard, the European Regulation 2021/784 has represented an important legislative contribution in the field of countering online terrorist activities. The legislation establishes a clear and harmonized legal framework and defines the responsibilities of Member States and the obligations of hosting service providers on the removal on online terrorist content, being one of the most accurate pieces of legislation which directly addressing the repercussions that such removals may have on individual freedom of

[371] Ruotolo, M. (2014). *Costituzione e sicurezza tra diritto e società*. In A. Torre, *Costituzioni e sicurezza dello Stato*, Rimini, 2014, 588.

expression. The regulatory text repeatedly emphasizes the imperative for Member States to adopt this rule internally, based on a delicate balance with the individual sphere of web users. It thus shall be considered a piece of legislation marking a crucial moment for European Union improvement of the balance between security and fundamental rights in the fight against terrorism. In this regard, the Digital Rights Ireland case, analyzed in detail in section 1.3, was not chosen by chance. Indeed, it is of significant importance when it comes to balancing public security and the protection of individual rights, representing the first episode in which the Court annulled in its entirety an act of secondary legislation in conflict with the provisions of the Charter of Fundamental Rights, and it undoubtedly represents the basis for the future development of pieces of legislation such as the Regulation abovementioned. The Court, having found the limitation of the right to data protection in the name of internal and international security disproportionate to the pursued objectives of preventing and countering terrorism, constituted a pivotal moment in the jurisprudence, affirming the need for a comprehensive and nuanced approach to address the challenges posed by cyberterrorism with respect to the delicate balance with individual fundamental rights[372]. The incessant evolution of technology and its interaction with legal frameworks therefore requires constant scrutiny and adaptation to ensure the effectiveness of security measures without compromising the fundamental principles of a democratic society. In this context, it is also important to emphasize the role played by private actors, such as HSPs and ISPs, which following the NIS directive and Regulation 2021/784 are officially charged with contributing to the prevention of terrorism and the protection of public safety - actions historically the responsibility of public law enforcement authorities - by removing terrorist content online. Their role, much debated, is configured in the grey space that could be part of the so-called participatory security, where the prevention and contrast ground is also extended to non-canonical and non-public actors. Within the framework of European regulatory analysis, which provided for the creation of standards and guidelines to be followed at the national level, another text has been of particular importance. The European Directive 2017/541 has provided for a wider definition of terrorist offences, representing a benchmark for Member States in their

[372] Cfr. Rubechi, M. (2016). *Op. Cit.*, pp. 18-20.

transposition and interpretation of the provisions at national level, with an explicit trend towards preventive measures and anticipation of criminal law protection, where the disvalue of the offense ends up residing almost exclusively in the element of specific intent, emphasizing the regression towards a criminal law of mere suspicion of the perpetrator[373]. Therefore, it is in the face of another intervention on the subject of terrorism which legitimizes the introduction of rules that set backwards the threshold of criminal relevance, that inevitably it raises the question as to the tolerability of this trend of massive anticipation of criminal protection, incriminating acts which are increasingly distant, chronologically speaking, from the injury to legal assets which are realized through the crime with scope, raising also unavoidable tension with the principle of offensiveness[374].

Deepening the comparative analysis between European Union and Italian legislation, this trend of anticipation of criminal law protection appears to be evident and even stronger at the Italian legislative level than at the European Union one. In fact, it can be traced a remarkable progression emerged in the national context, as Italian legislation has not limited itself to transposing European measures, but has embarked on a more advanced path, outlining a regulatory framework that aims to meet a wider range of needs for safeguarding security. This innovative approach is evident in the preventive intelligence interception measures established by Decree Law No. 105/2023 and, as mentioned, in the anticipation of protection. The model of countering Islamic terrorism adopted is configured as hybrid, escaping homologation to the American war paradigm and presenting significant deviations from the traditional ways of countering common crime. While maintaining a guarantor-like imprint, the national legislation reflects the response of an order to a contingent situation, although only marginally involved in the logistics and self-financing of radical Islamic groups[375]. The strategy to counter the terrorist threat is distinguished by the attempt to remain within the system of guarantees supported by the principles of the Constitutional Charter, unlike in the United States, where repressive interventions with dejurisdiction are envisaged, thus safeguarding the foundations of the liberal-democratic legal tradition. However, in order to

[373] Cfr. Cavaliere, A. (2015). *Op. Cit.*
[374] Santini, S. (2017). *Op. Cit.,* p. 43.
[375] Viganò, F. (2006). *Op. Cit.*, p. 648.

acquire useful information, the Italian system contemplates incisive methods of investigation and interception, exceptions to official secrecy and other instruments of autonomous intervention by the police forces. While meeting the needs of investigation and security, these instruments introduce significant limitations on fundamental rights, addressing constitutional challenges in the domestic legal system, although provided for by international conventions[376].

A final important aspect to be highlighted with regard to the Italian legal system and which fits well into the conclusions of this long analysis is the assumption on which Italian criminal procedural law is based: the principle of non-guilt. The Italian criminal process in based on this fundamental assumption, which shall be reminded also and especially when discussing about counter terrorism legislation and measures which tend to the anticipation of protection. This principle is guaranteed by Article 27(2) of the Italian Constitution, which states that "the defendant shall not be considered guilty until finally sentenced". The scope of this constitutional provision has been the subject of interpretation by both doctrine and jurisprudence, resulting ambiguous at times. In relation to the measures analyzed in this research, from data retention to online content removal, to preventive interception, what clearly emerges as crucial is the necessity to delineate the boundaries of an increasingly invasive investigative activity favored by new technological tools, balancing the need to fight cybercrime with respect for individual rights and freedoms and, at the trial stage, the preservation of the presumption of innocence, which may undergo threats with the entrenchment of the anticipation of protection.

Drawing conclusions after this long and in-depth analysis of the dichotomy between national security interests and the protection of human rights, it may be emphasized how the topic is often approached as an irreconcilable balancing act. It is, however, revealed to be more nuanced and complex by taking into account the divergent interpretations of the doctrine offered by civil liberties advocates on the one hand and by supporters of stricter security measures on the other. A deeper analysis reveals how these two aspects are constantly intertwined, both in the production of legislation and in the procedural and sanctioning

[376] Pace, A. (2003). *Problematica delle libertà costituzionali*. Parte generale, Padova, Ce dam, III ed., p. 337.

phases. At the legislative level, the European acts and the Budapest Convention show that when defining an anti-terrorism framework, legislation takes due account of respect for and protection of individual rights, with an increasing trend throughout the years and the judgements. On the procedural and sanctioning front, it is evident that in cases of abuse of counter-terrorism instruments, citizens resort to higher courts, such as the European Court of Human Rights, to obtain ex-post protection of their violated rights. These courts have shown increasing attention and sensitivity to the need to balance State security with respect for individual rights, marking out a legislative guideline for individual national governments to follow. Cyberterrorism, then, presents further challenges, requiring regulatory and enforcement interventions also in cyberspace. In this immaterial and too often anonymous dimension, security measures must be stringent, but it is crucial to respect the privacy and freedom of expression of platform users. Maintaining a strong State structure, with a cohesive and firm social fabric, is essential in the fight against terrorism. The threat of cyberterrorism calls for tougher security measures, but they shall be accompanied by greater attention to the delicate line between preventing cyberthreats and respecting the personal sphere of users. From this point of view, the determination of both the Union and Italy to go down this road emerges, providing themselves with all the regulatory tools they need to pursue this objective. Returning to the debate on the security-personal freedom binomial, despite the divergences on the weight to be attributed to these interests and on the conditions of this balancing act, the debate on counter-terrorism legislation starts from the assumption that the needs of national security and the protection of human rights are in conflict. However, what this research aims to highlight is the need to overcome this dichotomous view and adopt a more nuanced, balanced, and inclusive approach. The starting question of the research investigates the possible balance between public safety and respect for fundamental rights in the fight against cyberterrorism. In this context, the complexity of managing the emerging threat in cyberspace without compromising democratic principles emerges, while emphasizing the crucial importance of developing legislative and enforcement strategies that are able to protect public safety without unduly sacrificing fundamental rights. A holistic and adaptive approach is essential to address the evolving challenges while ensuring a secure society that respects democratic values. Moreover, dealing with the threat of cyberterrorism requires

increasingly robust security measures, but these must be accompanied by an ever-increasing focus on the delicate line between preventing cyber threats and respecting the personal sphere of online users, which is nothing more than the virtual version of the individual's personal sphere, traceable to the "right to respect for private and family life". From the analysis of the legislation produced in the last decades, it appears clear that this issue is on the tables of legislators and, with a slow but effective process, the balance between ensuring public security and safeguarding fundamental rights seems not to be unattainable, as the intentions and the efforts are evident both at European and Italian level, however, it seems to be a slow process in continuous change and adaptation to new requirements of the protection of both the State and the single individuals. What is particularly noteworthy in these conclusions is the recognition that a crucial catalyst for change has been sparked: the recognition of the imperative to sustain this balance and to constantly maintain it as a guiding principle in legislative initiatives.

Bibliography

Book Chapters and Academic Papers

Abrahamsen, R., Leander, A. *"*Routledge *Handbook of Private Security Studies"*. London; New York: Routledge, Taylor & Francis Group (2016).

Abrahamsen, R., Williams, MC. *"Security Beyond the State: Private Security in International Politics"*. Cambridge: Cambridge University Press (2010).

Ahmed, R. *"Negotiating Fundamental Rights: Civil Society and the EU Regulation on Addressing the Dissemination of Terrorist Content Online"*. Studies in Conflict & Terrorism (2023).

Agostini, B. *La disciplina delle intercettazioni preventive nel sistema antiterrorismo*. Diritto penale contemporaneo, (2017).

Albadi, N., Kurdi, M., & Mishra, S. *"Deradicalizing YouTube: Characterization, Detection, and Personalization of Religiously Intolerant Arabic Videos"*. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), 1-25 (2022).

Andreeva, C. *"The EU's counter-terrorism policy after 2015 - "Europe wasn't ready" - "but it has proven that it's adaptable"*. In Era Forum (Vol. 20, No. 3, pp. 343-370). Berlin/Heidelberg: Springer Berlin Heidelberg (2020).

Ayres, I., & Braithwaite, J. *"Responsive regulation: Transcending the deregulation debate"*. Oxford University Press, USA. (1992).

Baker-Beall, C., Mott, G. *"Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis"*. JCMS: Journal of Common Market Studies, 60(4), 1086-1105, (2022).

Berrutti, L. V. *"Una nuova formulazione delle intercettazioni preventive al servizio della lotta contro il terrorismo"*, in Commento al d.l. 7/2015, art. 2, (2016).

Borelli, M. *"Social media corporations as actors of counter-terrorism"*. New Media & Society, 25(11), 2877-2897. (2023).

Cameron, I. *"National security and the European convention on human rights*". BRILL (2021).

Campanini, M. *"Oltre la democrazia: temi e problemi del pensiero politico islamico*". Oltre la democrazia. (2014).
Cavaliere A., *"Considerazioni critiche intorno al D.L. antiterrorismo n. 7 del 18 febbraio 2015"*, in Diritto Penale Contemporaneo, fasc. 2, (2015).

Cantone, R. & D'Angelo, L.A. *"Una nuova ipotesi di intercettazione preventiva*, in Aa. Vv., *Le nuove norme di contrasto al terrorismo"* a cura di A.A. Dalia, Giuffrè (2006).

Cavaliere, A. *"Le nuove emergenze terroristiche: il difficile rapporto tra esigenze di tutela e garanzie individuali".* In Wenin, R. & Fornasari, G. *"Diritto Penale e Modernità, Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali"* (2017).

Citron, D. K. *"Extremist speech, compelled conformity, and censorship creep"*. Notre Dame L. Rev. 93, no. 3: 1035-1072 (2018).

Clifford, B. *"Moderating extremism: the state of online terrorist content removal policy in the United States*.". Program on Extremism. The George Washington University (December 2021).

Coche, E. *"Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online"*. Internet Policy Review, 7(4) (2018).
Cohen-Almagor, R. *"The role of internet intermediaries in tackling terrorism online"*. Fordham L. Rev., 86, 425 (2017).

Common, M.F. *"Fear the Reaper: how content moderation rules are enforced on social media"*. International Review of Law, Computers & Technology 34(2). Routledge: 126–152. (2020).

Continiello, A. *"Terrorismo e indottrinamento. Anatomia della fattispecie alla luce di una recente pronuncia della Suprema Corte di Cassazione"*. Giurisprudenza Penale (2017).

Conway, M. *"Routing the Extreme Right - Challenges for Social Media Platforms"*. The RUSI Journal 165(1). Routledge: 108–113. (2020).

Conway, M., & McInerney, L. *"Jihadi video and auto-radicalisation: Evidence from an exploratory YouTube study"*. Intelligence and Security Informatics: First European Conference, EuroISI 2008, Esbjerg, Denmark, December 3-5, 2008. Proceedings (pp. 108-118). Springer Berlin Heidelberg. (2008).

Cortesi, M.F. *"Il decreto antiterrorismo – i riflessi sul sistema processuale, penitenziario e di prevenzione"*, Dir. pen. proc., 919, (2015).

De Goede, M. *"The chain of security*". Review of International Studies, *44*(1), 24-42 (2018).

De Leo, F. *"L'irrisolto presente e un possibile futuro delle intercettazioni preventive",* in Cass. pen., p. 1862. (1998).

Douek, E. *"Facebook's oversight board: Move fast with stable infrastructure and humility"*. North Carolina Journal of Law & Technology, vol. 21(1) (2019).

Fasani, F., *"Terrorismo islamico e diritto penale"*, Cedam, Milano (2016).

Flor, R. *"Cyber-terrorismo e diritto pnale in Italia, in Diritto Penale e Modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali, Atti del convegno Trento 2 e 3 ottobre 2015"*, Università degli Studi di Trento, Quaderni della facoltà di Giurisprudenza, Fornasari G., Wenin R. (a cura di), Trento (2017).

Gherbaoui, T., & Scheinin, M. *"A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it*". Journal Européen Des Droits De L'homme-European Journal of Human Rights, 1, 3-29 (2023).

Giupponi, T. F. *"La sicurezza e le sue dimensioni costituzionali".* Diritti umani: trasformazioni e reazioni, 275 – 301 (2008).

Gorwa, R., Binns, R., & Katzenbach, C. *"Algorithmic content moderation: Technical and political challenges in the automation of platform governance"*. Big Data & Society, 7(1) (2020).

Granger, M-P., & Irion, K. *"The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection"*. European Law Review, 39(6), 834-850 (2014).

Hassemer, W. *"Sicurezza mediante il diritto penale"*, in Crit. dir., n. 1-2/2008, 35-36, (2006).

Illuminati, G. *"La disciplina processuale delle intercettazioni"*, Giuffrè, (1983).

Jayakumar, S. *"Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness With Three Case Studies on Estonia, Singapore, and the United States"*. Handbook of Terrorism Prevention and Preparedness, (2020).

Jenkins, B.M. *"International Terrorism: A New Kind of Warfare"*. Santa Monica, CA: RAND Corporation (1974).

Jensen, M., James, P., LaFree, G., et al. *"The Use of Social Media by United States Extremists"*. College Park, Maryland: START (2018).

Klonick, K. *"The New Governors: The People, Rules, and Processes Governing Online Speech"*. Harvard Law Review (131): 1598–1670 (2018).

Le Nguyen, C., Golman, W. *"Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "Law in action"*. Computer law & security Review, 40, 105521 (2021).

Marinucci, G., & Dolcini, E. *"Corso di diritto penale, 1. Nozione, struttura e sistematica del reato"*, Milano (1995).

Martino, L. *"La Quinta Dimensione Della Conflittualità. La Rilevanza Strategica Del Cyberspace E I Rischi Di Guerra Cibernetica"*. Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Università degli Studi di Firenze. (2012).

Neumann, P.R. *"Options and Strategies for Countering Online Radicalization in the United States"*. Studies in Conflict & Terrorism 36(6): 431–459. DOI: 10.1080/1057610X.2013.784568. (2013).

Nocerino, W. *"Le norme italiane di contrasto al terrorismo: repressione e prevenzione tra diritto interno ed internazionale"*. Diritto pubblico comparato ed europeo, Fascicolo 4, ottobre-dicembre 2016, (2016).

Nocerino, W. *"Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio",* Cedam (2018).

Ojanen, T. *"Privacy is more than just a seven-letter word: The Court of Justice of the European Union sets constitutional limits on mass surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, digital rights Ireland and Seitlinger and others"*. European Constitutional Law Review, 10(3), 528-541. (2014).

Orsini, A. *"What Everybody Should Know about Radicalization and the DRIA Model, Studies in Conflict & Terrorism"*. Routledge Studies in Conflict and Terrorism. DOI: 10.1080/1057610X.2020.1738669 (2020).

Pace, A. *"Problematica delle libertà costituzionali".* Parte generale, Padova, Ce dam, III ed., (2003).

Pelissero, M. *"Contrasto al terrorismo internazionale e il diritto penale al limite"*. Questione Giustizia, 99-112 (2016).

Picotti, L. *"Terrorismo e sistema penale: realtà, prospettive, limiti"*. Diritto Penale Contemporaneo, (1), 249-263 (2017).

Presotto, A. *"Le modifiche agli artt. 270-quater e quinquies del codice penale per il contrasto al terrorismo"*. Dir. pen. cont.—Riv. Trim, 1, (2017).

Rojszczak, M. *"Online content filtering in EU law–A coherent framework or jigsaw puzzle?"* Computer Law & Security Review, 47, 105739 (2022).

Roy, O. *"Secularism and Islam: The theological predicament*". Europe and Islam. Routledge (2018).

Ruotolo, M. *"Costituzione e sicurezza tra diritto e società"*. In A. Torre, *"Costituzioni e sicurezza dello Stato"*, Rimini, 2014, 588, (2014).

Santini, S. *"L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541"* (2017).

Serini, F. *"La nuova architettura di cybersicurezza nazionale. Note a prima lettura del decreto-legge n. 82 del 2021"*. Federalismi.it, (12), 241-272 (2022).

Serini, F. *"L'uso della normativa tecnica tra esigenze di mercato e di sicurezza delle reti e delle risorse informatiche"*. GRUPPO DI PISA, (Quaderno 5, fasc. speciale monografico "Le fonti della crisi: prospettive di diritto comparato"), 747-759 (2022).

Signorato, S. *"Combating terrorism on the internet to protect the right to life. The regulation (EU) 2021/784 on addressing the dissemination of terrorist content online"*. Yearbook: Human Rights Protection. Right to life, 403-408. (2021).

Silber, M. D., Bhatt, A., & Analysts, S. I., *"Radicalization in the West: The homegrown threat"*. New York: Police Department (2007).

Spiezia, F. *"International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime".* In ERA Forum (Vol. 23, No. 1, pp. 101-108). Berlin/Heidelberg: Springer Berlin Heidelberg (2022).

Talihärm A. M., *"Cyberterrorism: in Theory or in Practice?"*, in Defence Against Terrorism Review, vol. 3, n. 2. (2010).

Tosza, S. *"Internet service providers as law enforcers and adjudicators. A public role of private actors".* Computer Law & Security Review, 43, 105614 (2021).

Tréguer, F. *"Seeing like Big Tech: security assemblages, technology, and the future of state bureaucracy"*. In: Bigo D., Isin E., and Ruppert E. Data Politics: Worlds, Subjects, Rights. Routledge Studies in International Political Sociology. London: Routledge. (2019).

Vandezande, N. *"Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor"*. Computer Law & Security Review, 52, 105890 (2024).

Vedaschi, A. *"Has the balancing of rights given way to a hierarchy of values".* Comp. L. Rev., 1, 1. (2010).

Viganò F. *"Terrorismo, guerra e sistema penale"*, Rivista italiana di diritto e procedura penale, Vol.49(2), (2006).

Viganò, F. *"Il contrasto al terrorismo di matrice islamico-fondamentalistica: il diritto penale sostanziale"*. In Terrorismo internazionale e diritto penale. (2007).

Viganò, F. *"Sul contrasto al terrorismo di matrice islamica tramite il sistema penale tra "diritto penale del nemico" e legittimi bilanciamenti"*. Studi Urbinati, A-Scienze giuridiche, politiche ed economiche, 58(4), 329-348, (2007).

Vigneri, A. F. *"Cyberterrorismo: realtà o finzione? Profili problematici di definizione e contrasto"*. Opinion Juris, (2018).

Villani, S. *"La prevenzione di eventi CBRN di natura intenzionale: obblighi UE e attuazione in Italia"*. Osservatorio Sulle Fonti, 1, 243-263 (2023).

Weimann, G. *"New Terrorism and New Media"*. Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars (2014).

Weimann, G. *"Terrorism in Cyberspace: The Next Generation"*. Columbia University Press. (2015).

Weimann, G. *"WWW.TERROR.NET: How Modern Terrorism Uses the Internet"*. U.S. Institute for Peace, Washington DC (2004).

Wolfers, A. *"National Security as an Ambiguous Symbol"*. Discord and Collaboration. Essays on International Politics John Hopkins University Press: Baltimore (1962).

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. *"A field-wide systematic review and meta-analysis of putative risk and protective factors for radicalization outcomes"*. Journal of quantitative criminology, 36, 407-447. (2020).

Official Documents and Legislation

Beutel, A., Weinberger, P. *"Public-Private Partnerships to Counter Violent Extremism: Field Principles for Action"*. Final Report to the U.S. Department of State. College Park, Maryland: START. (2016).

Council of Europe. *Explanatory Report of the Council of Europe Convention on the Prevention of Terrorism*. Council of Europe Treaty Series No. 196. Warsaw (May 16, 2005)

Council of Europe. *Explanatory Report to the Convention on Cybercrime*. European Treaty Series, No. 185. (November 23, 2001).

Council of Europe. *The Global State of Cybercrime Legislation 2013 – 2023: A Cursory Overview.* (C-PROC, December 31, 2022).

Council of the European Union. *Council Conclusions on Internal Security and European Police Partnership.* (Brussels November 24, 2020).

Council of the European Union. *COUNCIL FRAMEWORK DECISION 2002/475/JHA of 13 June 2002 on combating terrorism*. (2002) OJEU L 164**.**

Council of the European Union. *COUNCIL FRAMEWORK DECISION 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*. (2008) OJEU L 330.

Council of the European Union, Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. OJEU L 210/12. (June 23, 2008).

Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. OJEU L 210/1. (June 23, 2008).

Council of the European Union. *Implementation of the Action Plan to Combat Terrorism*. (Brussels, June 11, 2004).

Council of the European Union. *Letter from the LT Presidency to the Incoming EL Presidency on the Future Development of the JHA Area*. 17808/13 (December 13, 2013).

Council of the European Union, *Non-confidential Report on the Terrorism Situation and Trends in Europe*. 14280/02. (November 20, 2002).

Council of the European Union. *Proposal for a Council Framework Decision on attacks against information systems* (2002/C 203 E/16) COM(2002) 173 final — 2002/0086(CNS). OJEC C 203 E/109. (April 19, 2002).

Council of the European Union. *Summary of Discussions. Working Party on Terrorism*. 13185/11 (July 25, 2011).

Council of the European Union. *The European Union Counter Terrorism Strategy*. (Brussels November 30, 2005)

Decreto Legislativo 1 marzo 2018, n. 21. *Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103.*

Decreto Legislativo 15 febbraio 2016, n. 34. *Norme di attuazione della decisione quadro 2002/465/GAI del Consiglio, del 13 giugno 2002, relativa alle squadre investigative comuni.*

Decreto Legislativo 18 maggio 2018, n. 65. *Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.*

Decreto Legislativo 18 maggio 2018, n. 51. *Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*

Decreto Legislativo 21 maggio 2018, n. 53. *Attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004.*

Decreto Legislativo 24 luglio 2023. *Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici on-line.*

Decreto Legislativo 6 settembre 2011, n. 159. *Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136*.

Decreto-Legge 13 maggio 1991, n. 152. *Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*.

Decreto-Legge 8 giugno 1992, n. 306. *Modifiche urgenti al nuovo codice di procedura penale e provvedimenti di contrasto alla criminalità mafiosa*.

Decreto-Legge 14 giugno 2021, n. 82. *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.*

Decreto-Legge 21 settembre 2019, No. 105. *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*, convertito con modificazioni dalla legge 18 novembre 2019, No. 133.

Decreto-Legge 27 luglio 2005, n. 144. *Misure urgenti per il contrasto del terrorismo internazionale*.

Decreto-Legge 30 dicembre 2019, n. 161. *Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*.

Decreto-Legge 10 agosto 2023, n. 105. *Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonche' in materia di personale della magistratura e della pubblica amministrazione.*

European Commission, *Proposal for a Regulation of The European Parliament and of The Council on European Production and Preservation Orders for electronic evidence in criminal matters*. COM/2018/225. (Strasbourg, April 17, 2018)

European Commission. *The European Agenda on Security*. (April 28, 2015).
European Council, *Directive No 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (2008) OJEU L 345/75.

European Parliament and Council, *Directive (EU) No 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union* (2016) OJEU L194/1.

European Parliament and Council, *Directive No 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")* (2000) OJEU L 178/1.

European Parliament and Council, *Directive No 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* (2002) L 201.

European Parliament and Council, *Directive No 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* (2006) OJEU L 105/54.

European Parliament and Council, *Directive No 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA* (2013) OJEU L 218/8.

European Parliament and Council, *Directive No 2017/541/EU on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA* (2017) OJEU L 88/6.

European Parliament and Council, *Directive No 2022/2555/EU on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

European Parliament and Council, *Regulation (EU) No 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC* (2022) OJEU L277/1.

European Parliament and of the Council, *Regulation (EU) N. 2021/784 on addressing the dissemination of terrorist content online* (2021) OJEU L 172.

European Parliament and of the Council, *Regulation (EU) No 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. (2019) OJEU L 151/15.

European Union Agency for Fundamental Rights. *Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications - Opinion of the European Union Agency for Fundamental Rights* (FRA Opinion – 2/2019, Vienna, February 12 2019),

European Union. *Consolidated version of the Treaty on the Functioning of the European Union - Part Three: Union Policies And Internal Actions - Title V: Area Of Freedom, Security And Justice – Chap. 4: Judicial cooperation in criminal matters – Art. 83 (ex Article 31 TEU)*. 2008/C 115/01. (December 13, 2007).

EUROPOL. *TE-SAT: EU Terrorism Situation and Trends Report*. (July 20, 2016).

EUROPOL. *TE-SAT: EU Terrorism Situation and Trends Report*. (July 20, 2018).
Trends in Europe. 14280/02. (November 20, 2002).

Legge 18 marzo 2008, n. 48. *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*.

Legge 4 agosto 2021, n. 109. *Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*.

Legge 28 luglio 2016, n. 153. *Norme per il contrasto al terrorismo, nonché ratifica ed esecuzione: a) della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatta a Varsavia il 16 maggio 2005; b) della Convenzione internazionale per la soppressione di atti di terrorismo nucleare, fatta a New York il 14 settembre 2005; c) del Protocollo di Emendamento alla Convenzione europea per la repressione del terrorismo, fatto a*

Strasburgo il 15 maggio 2003; d) della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, fatta a Varsavia il 16 maggio 2005; e) del Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatto a Riga il 22 ottobre 2015.

Legge 9 ottobre 2023, n. 137. *Conversione in legge, con modificazioni, del decreto-legge 10 agosto 2023, n. 105, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione*.

Nordio, C. *Intervento alla Camera, 7 dicembre 2022*, Sist. pen., 8 dicembre 2022.

International Treaties, Charters and Conventions

Council of Europe, *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism*. CETS 217. (Riga, 22 October, 2015).

Council of Europe. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. European Treaty Series No. 189. (Strasbourg, January 28, 2003).

Council of Europe. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. CETS No. 224. (Strasbourg, May 12, 2022).

Council of Europe. *Convention on Cybercrime*. European Treaty Series, No. 185 (November 23, 2001).

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms and Protocol* (opened to signature 4 November 1950, entered into force 3 September 1953) 67075 CoE.

Council of Europe, *Convention on the Prevention of Terrorism* (opened to signature 5 May 2005) CoEUTS 196.

Council of the European Union, *Charter of Fundamental Rights of the European Union* (2000) OJEU C 364/01.

European Court of Human Rights, Rules of Court (Strasbourg, last update 3 June 2022).

European Union, *Treaty on Functioning of the European Union* (Treaty of Lisbon), (signed 13 December 2007, entered into force 1 December 2009).

United Nations Security Council (UNSC) Res 2178 UN Doc S/RES/2178 (September 24, 2014)

Case Law

Boumediene et al., petitioners, v. Bush, President of The United States, et al., respondents. 553 U.S. 723 (2008). Certiorari to the United States Court of Appeals for the District of Columbia Circuit.

Cass. Pen., Sez. I, 6 Ottobre 2015, n. 47489.

Cass., Sez. I, 9 settembre 2015, n. 40699.

Cass., Sez. I, 6 novembre 2013, n. 4433.

Cass., Sez. un., 28 novembre 2019 n. 50.

Corte cost., sent. 10-11 luglio 1991, n. 333.

Court of Justice of European Union (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (C-293/12).

Court of Justice of the European Union (Fourth Chamber), European *Commission v. Kingdom of Sweden*, 30 May 2013, case No. C-270/11.

Czech Constitutional Court, judgement of 22 March 2011, Pl. US 24/10.

Ezelin v. France App. no. 11800/85, paragraph 37, (ECtHR, 26 April 1991).

German Constitutional Court (BVerfG), judgement of 3 March 2010, 1 BvR 256/08.

Handyside v. The United Kingdom App. no. 5493/72, paragraph 49 (ECtHR, 7 December 1976).

Mohamedou Ould Salahi, petitioner, v. Barack H. Obama, et al., respondents. Civil Action no. 05-0569 (RCL).

Opinion of Advocate General Cruz Villalón on the joined cases *Digital Rights Ireland Ltd* (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others (12 December 2013).

Roman Zakharov v. Russia App. no. 47143/06 (ECtHR, 4 December 2015).

Romanian Constitutional Court, Decision No. 1258, 8 October 2009.

Trabelsi v. Italia, App. No. 50163/08 (ECtHR, 13 April, 2010).

Web Sources

Bavetta, F. (2023). *"Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo*. In Media Laws. Available at: <https://www.medialaws.eu/rivista/direttiva-nis-2-verso-un-innalzamento-dei-livelli-di-cybersicurezza-a-livello-europeo/>.

Çeliksoy, E., Ouma, S. "*Terrorist Use of the Internet"*. Bilişim Hukuku Dergisi, 1(2), 243-267 (2019). Available at: <https://dergipark.org.tr/en/download/article-file/952271>.

Cian C. Murphy. "*Opinion of AG Villalón In Case 293/12 Digital Rights Ireland Ltd and Case 594/12 Seitlinger & Others"*. 12 December 2013, King's Law Journal, 25:1, 1-4, (2014). Available at:
< https://www.tandfonline.com/doi/pdf/10.5235/09615768.25.1.1?needAccess=true>.

Cisterna, A. *"In G.U. il D.Lgs. 107/2023: le nuove norme per il contrasto alla diffusione di materiali terroristici sulla rete"*. Altalex, Penale (September 5, 2023). Available at: https://www.altalex.com/documents/2023/09/05/g-u-d-lgs-107-2023-nuove-norme-contrasto-diffusione-materiali-terroristici-rete.

Denning D., "*Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services', U.S. House of Representatives"* (May 23, 2000). Available at: <https://irp.fas.org/congress/2000_hr/00-05-23denning.htm>.

De Ruvo, L. *"L'importanza dell'art. 270-bis del Codice Penale nel contrasto al terrorismo internazionale"*. Diritto.it (2022). Available at: <https://www.diritto.it/limportanza-dellarticolo-270-bis-del-codice-penale-nel-contrasto-al-terrorismo-internazionale/>.

Facebook (2011). Facebook Community Standards. Available at: <https://web.archive.org/web/20110127224041/https://www.facebook.com/communitystandards/>.

Forbes, *"The EU Will Be The End Of Free Speech Online"*. (6 July 2019), Available at: <https://www.forbes.com/sites/kalevleetaru/2019/06/06/the-eu-will-be-the-end-of-free-speech-online/>.

Ganesh, B., Bright, J. "*Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation"*. Policy & Internet 12(1): 6–19. Available at: <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.236>.

GIFCT (2022). "*GIFCT Working Group Principles and Guidelines*. Available at: <https://gifct.org/wp-content/uploads/2023/03/GIFCT-Working-Groups-Principles-and-Guidelines-3.pdf>.

Guild, E., Carrera, S. "*The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive"*. CEPS Liberty and Security in Europe Papers No. 65, (May 29, 2014). Available at: <https://ssrn.com/abstract=2445901>.

Hughes, S. "*Whose Responsibility Is It to Confront Terrorism Online?*" In: Lawfare (2018). Available at: <https://www.lawfareblog.com/whose-responsibility-it-confront-terrorism-online>.

Illuminati, G. (2020). *"Utilizzazione delle intercettazioni in procedimenti diversi: le Sezioni unite ristabiliscono la legalità costituzionale"*. In Sistema Penale. Available at:

<https://sistemapenale.it/it/opinioni/utilizzazione-intercettazioni-procedimenti-diversi-sezioni-unite-ristabiliscono-legalita-costituzionale>.

Jeong, S. "*The History of Twitter's Rules*". Vice Motherboard (14 January 2016). Available at: <https://www.vice.com/en/article/z43xw3/the-history-of-twitters-rules>.

Lazzeri, F. *"Convertito in legge, con modificazioni, il d.l. 105/23: novità in materia di intercettazioni, incendio boschivo, ambiente e 231*". In Sistema Penale, 5 Ottobre 2023. Available at: <https://www.sistemapenale.it/it/documenti/legge-conversione-decreto-legge-2023-105-intercettazioni-incendi-ambiente>.

Licciardello, S. (2016). *"Nuove Norme antiterrorismo in Italia. Sistema di informazione per la sicurezza della Repubblica"*, sez. Il mondo dell'intelligence (9 Settembre 2016). Available at: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/09/Norme-antiterrorismo-Italia-Licciardello.pdf>.

Ministero Dell'Interno, *"Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche"*. Available at: <https://www.interno.gov.it/it/temi/sicurezza/crimine-informatico/centro-nazionale-anticrimine-informatico-protezione-infrastrutture-critiche-cnaipic>.

Ministero Dell'Interno, *"Osservatorio per la sicurezza contro gli atti discriminatori"*, Available at: <https://www.interno.gov.it/it/ministero/osservatori-commissioni-e-centri-coordinamento/osservatorio-sicurezza-contro-atti-discriminatori-oscad>.

Möller, J. "*What Is Deplatformization And How Does It Work?"*. Israel Public Policy Institute (Oct. 11, 2022). Available at: <https://www.ippi.org.il/what-is-deplatformization-and-how-does-it-work/>.

Muià, P.P. *"Il decreto legislativo n. 65 del 2018 in materia di cybersicurezza"*. Diritto.it (2021). Available at: <https://www.diritto.it/il-decreto-legislativo-n-65-del-2018-in-materia-di-cybersicurezza/>.

National Conference of State Legislatures, *"U.S. Army Training and Doctrine Command. Cyber Operations and Cyber Terrorism"*. Handbook No. 1.02, (August 15, 2005). Available at: <https://nsarchive.gwu.edu/sites/default/files/documents/4065692/US-Army-Training-and-Doctrine-Command-DCSINT.pdf>.

Nocerino, W. *"La riforma delle intercettazioni preventive d'intelligence"*. In Sistema Penale (2023). Available at: <https://www.sistemapenale.it/it/scheda/nocerino-riforma-intercettazioni-preventive-intelligence#_ftnref34>.

Singh, D.D. (2023). *"Cibersicurezza, la Direttiva NIS 2"*. Altalex. Available at: <https://www.altalex.com/documents/news/2023/01/24/cibersicurezza-direttiva-nis-2>.

YouTube (2009). YouTube Community Guidelines. Available at: <https://web.archive.org/web/20090403124358/http://www.youtube.com/t/community_guidelines>.