Vilnius University Faculty of Law Department of Private Law

Victor Avisseau

2nd study year, LL.M International and EU Law programme Student

Master's Thesis: The Means of fighting against Cybercrime in the European Union

Supervisor: Victor Terekhov

Reviewer: Prof. G. Švedas

2019-2020 Vilnius

TABLE OF CONTENTS

INTRODUCTION

The relevance of the topic. On the 27th of April 2007 in Estonia, a series of cyberattacks targeted websites of Estonian organizations that lasted until the 18th May of 2007[1]. The attack was part of a political conflict between Estonia and Russia. Most of the malicious activities were located outside Estonia. This attack spread on many Russian speaking forums, which multiplied the number of offenders. This political-motivated attack led to a large denial of service for general public using several malicious processes such as spamming. This event, although not the first of this type, was one of the first large scale event related to cybercrime. At this time, legal instruments were already being prepared at the European level. But other serious cybercrime episodes followed during the next years, such as the WannaCry ransomware attack in May 2017. In fact, 10 years later after the Estonian episode, there was one of the biggest ransomwares attack the world has ever faced. Facing these attacks, Europe needs to react.

On the 29th of September 2017 at Talinn Digital Summit, Jean-Claude Juncker the president of the Commission declared: *'Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest link in this global threat'.* In fact, there is a matter of duty, according to which Europe needs to ensure security for all its citizens and needs to help Member States to reach this objective. Besides, there is a need for the European Union to be legitimate and counterfeit these threats, and especially towards new European Countries such as Estonia which joined the European Union in 2004. Furthermore, the European Union is also pushed by a competitivity motive in the cyber industry. However, cybercrime is a complex matter since it is a new threat that develops itself with the evolution of cyber technologies and telecommunication technologies. In fact, according to Mario Kunasek, Federal Minister for Defence of the Republic of Austria[2], the digital era brought many positive prospects and new possibilities. But *"very soon, challenges, risks and threats also developed in cyberspace. Viruses, worms and Trojans […] were targeting private as well as public*

[1] RAIN, O. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Talinn : Cooperative Cyber Defence Centre of Excellence, 2018
Available at :
<https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>

[2] REHRL, J. The Common Security and Defence Policy of the European Union. *European Handbook on Cybersecurity*, 2018. KUNASEK, M. <Forewords>

networks". We can see that cybercrime evolved together with the development of new technologies. Thus, it incarnates a new kind of threat, which is difficult to understand and defeat. Therefore, this topic appears to be interesting and relevant.

In that regard, the law theory of the European Union which is trying to harmonize the legal framework around the notions of cybercrime and cybersecurity, develops common definitions and bring up the standards of defence. In fact, a serious work is being performed by the European Institutions together with the Member States to stop cybercrime. But in practice, it appears to be much more difficult to apply. The development of a solid legal framework is long and complex. Thus, it will be relevant to always bear a critical point of view towards this notion that brings up many divergent points of views.

Aim. In our reflexion, a demonstration of the actual situation of the fight against cybercrime performed by the European Union will be performed. This situation is interesting since it covers many offences and thus, many objectives are to be reached. In order to get a global and accurate view of the situation, it will be relevant to cover a reflexion divided into three sections. The main question that will be answered, is how the European Union deals with the issue of cybercrime. It is a wide notion, that involves many kinds of crimes with different aspects. Thus, it is a complex topic that bears technical issues. However, it is important to focus on a legal analysis of the topic which means that few technical precisions regarding specific notions of cybercrime will be covered. In that regard, it will be important to define every notion, but the legal aspect will prevail. Furthermore, the notion of cooperation and the cross-border nature of cybercrime leads to an international analysis of this notion. In that regard, all the States of the world are concerned. Since the topic treats about the European Union only, the questions relating to the relations of the Union towards third countries and States candidates will be omitted. In fact, states candidate such as Turkey are trying to reach the same standards as European union in terms of cybersecurity. On that regard, the relation of the European Union towards other international institutions regarding cybercrime such as NATO or the United Nations will not be treated in this work. The objective is to focus on the action of the European Institutions and the Member States.

Tasks and Objective. In order to get a coherent analysis of the issue, three axes will be covered.

(1) First, it is important to understand how the European Union fights against cybercrime on a textual basis. In fact, the European Institutions and mainly the Commission

can produce legal sources such as directives, which lead the Member States in their actions, and build a harmonized judicial system of the latter. In that regard, the notion of cooperation appears central. Computer related offences are bound to a cross-border nature, meaning that they can travel between States without being controlled at borders like any other product. Thus, it is important for the Member States to cooperate in order to fight these offences efficiently. Therefore, the action of the European Institutions is important since it will play the role of a leader which coordinates the action of the Member States and build a strong common policy and judicial system. Thus, it will be important to understand which texts regulate the fight against cybercrime and how. Also, it will be relevant to study the founding texts that legitimate the action of the European Union. However, it is necessary to bear in mind that the fight against cybercrime is still surrounded by many challenges and is therefore unperfect. Thus, it will be necessary through the analysis, to consider the reality of the facts behind the theory deployed in the legal texts.

(2) Secondly, the work will cover the judicial aspect of the fight against cybercrime. In fact, computer related crimes constitute criminal offences. Therefore, there is a need to sanction them, since punishing illegal actions are mandatory in a society of rights. Therefore, it is important to understand how the European Court of Justice behaves towards this notion. There is the question of its competence that is central in this topic, since the European Courts is not substituting to national Courts. Also, the judicial means of fighting against cybercrime covers the principle of mutual recognition which goes toward the logic of building a common legal framework around our notion of cybercrime. Furthermore, the issue of the evidence is an essential point that must be considered.

(3) Finally, in order to get a global overview of the means of fighting against cybercrime, the analysis of its organic aspect will be covered. In fact, there are many actors that are performing important actions regarding computer-related offences. Thus, it is important to analyse how these organs are trying to counterfeit these new threats. Therefore, we will dive into the action of European organs such as Europol or Eurojust and others, which are central actors of the fight against cybercrime. Also, it is important to study the specialised organs that have been developed by the European Union through its fight against cybercrime.

Methods. Various research methods were used in this work. A *technical method* of research was firstly performed, by reading articles on cyber technology in order to get a thorough conception of the notion of cybercrime, how it works and how it is perpetrated. Besides *data collection and data analysis methods* were used to search and study legal

European Union acts and articles relating to cybercrime law in order to find the stakes relating to cybercrime and what is the situation. Finally, since most of the sources used came from the European Union themselves, it was important to get different sources to compare point of views. On that regard, articles and books from different authors allowed a better understanding of the reality of the subject.

Originality. The first specificity of this topic stands in its modernity. Cybercrime consists in a new threat that is difficult to understand and is constantly evolving. Thus, a deep analysis of the means of fighting against cybercrime seems original. Furthermore, this analysis is divided into three main aspects, which define globally the landscape of this new issue. Thus, this work will give a global and accurate overview of the means developed to fight against cybercrime. Finally, the will to compare the theory and the practice gives this work an authenticity in terms of analyse of the results of the action of the European Union and the Member States around the notion of cybercrime.

Relevant Sources. In order to understand precisely the situation, the main sources used in this work come from the European Institutions. In fact, they are the most relevant sources since we study directly their action. Therefore, it is important to consider globally the European Sources, from the founding treaties, to polls and resolutions developed by the European Institutions. However, in order to compare the point of view and understand the practice, it is also important to implement doctrine from authors working in the field of law of new technologies, who provide more practical information regarding this notion. Thus, it will be relevant to balance these sources in order to analyse the reality of the situation. Between the authors cited, most of them work in the European territory. In fact, these authors are prioritized since we want to focus on the action of the European Union. For instance, central sources in the thesis were, the work of Dr. Peter Csonka, Head of Unit, Directorate-General Justice, Freedom and Security at the European Commission '*The council of europe's convention on cyber-crime and other European initiatives*' (2006) , Paul De Hert, Gloria González Fuster and Bert-Jaap Koops 'Fighting cybercrime in the two Europes' (2006). Moreover, the objective of the thesis focuses on a legal analysis of the topic. Cybercrime brings up many issues with ethic and political consequences. Therefore, many political sources treat of this subject. Although they are important to understand the context, it is important to stick to legal sources. Thus, the majority of the sources used come from European Institutions and European legal professors and experts.

I – The Legal Aspect of the fight against cybercrime

Cybercrime developed itself following the exponential evolution of new technologies during the past thirty years. This fast growth created a dark threat which has been difficult to handle for public authorities and led to major attacks such as the attack in Estonia in 2007, or the massive ransomware in 2017 by Wannacry. The Organisation for Economic Co-operation and Development (OECD), already warned about the potential dangers of such new technologies[3]. Later, the studies of the OECD inspired the works of the European Institutions in the fight against cybercrime. Following this, the European Union, together with the Member States, had to find legal solutions. Thus, the fight against cybercrime operated by the European Union's Institutions and the Member States, is governed by a plurality of legal texts. In that regard, it is important to develop the concept of cybercrime which led the European Union and especially the European Commission to enact a European strategy (A) which points out the different objectives that need to be reached in order to fight cybercrime in an efficient way. Furthermore, this action is framed by the founding texts of the European Union. Thus, it seems relevant to analyse the European's primary and secondary law (B) that concerns the fight against cybercrime. Finally, since most of the acts perpetrated by cybercriminals are criminal acts, the notion is directly linked to criminal law, which is a sensitive question in the European Union's competences. Thus, the question of criminal law inside European Union (C) will be covered.

A. The concept of cybercrime and the European Strategy

In order to establish a clear and thorough analysis of this strategy, it is important to give an explanation of the concept of Cybercrime (1). Facing this threat, the European Union built a strategy (2), and set objectives which coordinate the actions of the Member States and the European institutions.

1. The concept of Cybercrime

Since cyber activity is a new stake in our society, it was necessary to define it. The main legal instrument in that regard is the Cybercrime Convention (a). Besides, the telecommunication technologies brought many illegal activities. Therefore, the European

[3] OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 23 September 1980.

institutions, mainly the European commission, gave a large definition of cybercrime, which led to a classification of these crimes (b). Finally, a crucial aspect of cybercrime stands in its cross-border nature (c), which must be explained in order to understand all the stakes around this notion.

a. The Cybercrime Convention

The Convention on Cybercrime was created on the impulse of the Council of Europe in Budapest in 2001[4]. It entered into force in 2004 on 18th March 2004 after the Republic of Lithuania ratified this International Convention on cybercrime. Its entry into force required 5 ratifications with at least 3 member states of the Council of Europe. Since it entered into force, many third countries to the European Union ratified this Convention such as Turkey, which means it is an international Convention that falls out of the scope of purely European treaty.

On that regard, the European Court of Justice doesn't refer to this Convention when it judges cases. For example, the judgement of the Court in Grand Chamber called eDate Advertising GmbH against Martinez[5], the Court makes no reference to the Convention. It seems this convention doesn't have influence on European law.

In the details of the Convention, the Council of Europe argues that the main objective of the Convention is to "*pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation*". Thus, it could be inferred that this Convention doesn't act like a binding legal text. In fact, the Council of Europe isn't mandated to produce such texts since the Commission is the only Institution with a power of initiation. However, it plays a role in establishing a common definition of cybercrime at a time where there are none, in order to build an efficient cooperation between Member States of the Council of Europe. Besides, the European Parliament mentions the Convention when it makes resolutions about cybercrime[6].

This definition by the Convention has inspired the European Institutions, and especially the European Commission, who brought it inside the European legal framework.

[4] Convention on Cybercrime. *Council of Europe Portal*, 23 November 2001. ETS No. 185
[5] CJEU. 25 October 2011. Decision *eDate Advertising v. Martinez*, Joined Cases C-509/09 and C-161/10
[6] 3 October 2017. European Parliament resolution (2017/2068(INI)) on the fight against cybercrime. *OJ C 346, 27.9.2018, p. 29-43*

Cybercrime englobes many different crimes, which led to a large definition of it and a classification of the crimes.

b. The large definition of Cybercrime and the classification of crimes

The rapidly growing society of telecommunication led to malicious usage of these new technologies. These deviant behaviours were labelled as being part of Cybercrime. According to the European Commission[7], cybercrime encompasses "all the criminal acts that are committed online by using electronic communications and information systems". It must be noted that this definition is general and large. In fact, the element of using cyber technologies and committing crimes with them, is enough to put the so-called crime under the umbrella of cybercrime, which includes many kinds of crimes. The definition seems to rely on a criterion of a use of cyber technology related to a crime.

Therefore, legislating on cybercrime seems difficult because it means creating laws on a large panel of criminal acts, with different forms. This difficulty is reinforced due to the untraceable nature of cyberattacks. Thus, a large definition of the notion enables the possibility of linking the acts with cybercrime.

In order to clarify and distinguish different crimes, the notion has been divided into several categories by European law. The European Commission distinguishes between three different types of crimes.

The first category concerns the crimes "*specific to the internet*". It refers to the attacks directed against information systems or phishing. It regroups all the actions of identity theft. Phishing occurs when a communication, such as an email or a text message, is sent to a recipient, and tries to convince him to reveal sensitive personal information. These scams are usually concealed by disguising the communication into an official message.

The second category described refers to "*Online fraud and forgery*", which is usually a large-scale identity theft, phishing, spam and malicious code.

Finally, the third category indicates "*Illegal online content*". It means every content that would lead to encourage behaviours that are totally forbidden in real life, such as child sexual abuse, incitement to racial hatred or terrorist acts, racism and xenophobia.

[7][online] *Cybercrime*. What is Cybercrime ?. Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

The convention on cybercrime from 2001[8], adds a fourth category which includes the offences related to infringement of copyright and related rights. In fact, the usurpation of copyrights is frequent in cyber illegal activity. It is a major stake in the fight against cybercrime.

Beyond the large number of crimes included in the concept of cybercrime which makes it hard to legislate on, it is the cross-border nature of this matter that forces the European institutions and the Member States to adapt their strategy.

c. The cross-border nature of cyber activity

A very important aspect of crimes committed online, through electronic communications and information systems, stands in their border-less nature. According to Dr Peter Csonka, head of Unit in charge Criminal Justice at the European Commission[9], when users connect to communication and information services, it creates a "*cyber-space*", which gathers all the data and interactions between the latter. One of the specificities of this space, is its trans-border character, which doesn't fit with the concept of national borders. Although the cyber-space bears legitimate usages, it also brings misuses, which corresponds to cyber-offences, and cybercrime.

This trans-border aspect of cyber-offences enters in conflict with the principle of territoriality of national law enforcement authorities, since data and communications are immaterial and are not respecting the border controls, like any other product or person. This point is essential, since it will lead the European Institutions and the Member States to adapt their action towards these crimes, by following the path of cooperation, more than national law enforcement.

Cybercrime incarnates a new kind of threat which followed the development of new telecommunications and technologies. It encompasses a large number of crimes, and incorporates a cross-border nature, which makes it a different phenomenon that differs from the other crimes. Facing this new threat, the European Union developed a strategy in order to build a strong defence against Cybercrime.

[8] DE HERT, P.; GONZÁLEZ FUSTER, G.; and KOOPS, B. *Fighting cybercrime in the two Europes*, Revue Internationale de droit pénal 2006/3-4 -Vol.77, p.503

[9] CSONKA, P. *The council of europe's convention on cyber-crime and other European initiatives*. Revue Internationale de droit penal, 2006/"-4 (Vol.77), p.473

2. The European strategy

Internet does not exist in the same territorial boundaries as other domains, and the cyber-space appears to be totally immaterial. Therefore, it seems delicate to build strong rules to defeat the missuses of such a technological improvement which transformed our society. In that regard, the European Union decided to face the problem by leading the action of its institutions and the Member States, by publishing its strategy regarding cybercrime. The European Union started leading the fight with recommendations (a) very soon. But more recently, the European Union launched a new strategy (b) which set new objectives. However, the objectives are still unperfect, and many challenges are still to be reached (c).

a. The Recommendations of the Council of Europe

In the context of a new immaterial threat rising, the Council of Europe gave its opinions to the member States. One of the main texts, is the Recommendation R (89) 9 of the Council of Europe of the Committee of Ministers to Member States on Computer-Related Crime[10]. This recommendation shows that, the Council of Europe was aware of the potential dangers of the criminal usage of computers. On the one hand, the recommendation asks Member States of the Council of Europe to take into consideration the link between criminality related to computers when legislating or revising their legal system. On the other hand, the Council requires the member States to produce a report to the Secretary General in 1993, on the evolution of their legislation and their judicial practice as well as their experiences in international judicial international related to cybercrime.

These requirements show how the will of harmonizing and considering the problem of cybercrime, and therefore, encouraging international cooperation. Thus, the recommendation supports the fight against cybercrime in the European Union. Besides, the recommendation R (95) 13 related to problems of criminal procedural law connected with information technology[11], helped the Member States to coordinate their criminal system.

The Council of Europe, through these recommendations, stressed the issue of cybercrime, at a time when it wasn't popular enough to be a State priority. Afterwards, the

[10] 13 September 1989. Committee of ministers to Member States, Recommendation R (89) 9 on Computer-Related Crimes.

[11] 11 September 1995. Committee of ministers to member States, Recommendation R (95) 13 concerning problems of criminal procedural law connected with information technology

European Institutions, mainly the Commission, inspired them self from these recommendations to build a strong strategy to fight against cybercrime.

b. The European Cybercrime strategy

Willing to develop the security of cyber space within European's borders, the European Institutions decided on a cybersecurity strategy in 2013 [12]. According to this communication, "*Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain reliability and interoperability of the Internet*". This sums up the main objectives of the document which also refers to the responsibility of the "*private sector* [which] *owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role*". Therefore, the European institutions are also stressing the responsibility of the private entities which are running the Internet industry.

The tile 2 of this communication entitled "Strategic priorities and actions", lists the objectives on which the actors must focus in order to reach the highest possible freedom and security for the benefit of everyone.

The first objective deals with the achievement of cyber resilience. In order to achieve it, it is required for the public and private sectors to cooperate and develop capabilities to fight cybercrime. Thus, the Commission developed a policy on Network and Information Security (NIS). Besides, the European Network and Information Security Agency (ENSIA), must be modernised.

The second concern goes to reducing cybercrime. The text brings up the increasing sophistication of cybercrime networks. Thus, the European Institutions encourage a strong and effective legislation, and enhanced operational capability to combat cybercrime.

Furthermore, it is supported the idea of developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP). It is remembered that threats are multifaceted. Thus, a significant support should be provided to Member States' defence and national security interests. Besides, cooperation with third countries or entities such as NATO, should be encouraged.

[12] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace /* JOIN/2013/01 final /*

The fourth objective relies on developing industrial and technological resources for cybersecurity. The issue that most of the main ICT leaders are located outside the European Union, brings the idea that the latter could, at some point, be dependent on these ICT producers. Thus, the promotion of a Single Market for cybersecurity products is widely encouraged and supported by the European Institutions, for the European Union to become competitive in this sector of activity. Besides, a support will be given to Research and Development investments and innovation on cybersecurity products.

Finally, a major issue relies on building a coherent international policy for the European Union and promote its values. In fact, since the European Union has to face the challenge of securing cyberspace with its border-less nature, it recalls the necessity of having a consistent policy and legislation regarding cybercrime. This coherent policy is relevant for Member States together, but also regarding third countries. Thus, there is a need to mainstream cyberspace issues into the European Union's external relations and Common Foreign and Security Policy (CFSP).

In 2013, these objectives were set, developing a coherent and solid framework around the threats that rise with new technologies. The European Union seems to have understood the issue. But the fight against cybercrime as depicted in this strategy, isn't simple, and takes time to solve. Therefore, 6 years after the European strategy, the legal tools are still progressing.

c. The challenges of the fight against cybercrime

On the 18th of October 2018, the General Secretariat of the Council[13], stressed the necessity to combat cyber-enabled illegal and malicious activities by building strong cybersecurity. Thus, negotiations are being concluded. It shows that, nowadays, the fight against cybercrime isn't accomplished. Therefore, new tools are being elaborated, such as the cyber diplomacy toolbox[14], which would help improve cooperation and prevent conflicts.

[13] 18 Ocotber 2018. European Council conclusions, point 9. Available at: https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/

[14] Council of Europe, *Cyber-attacks : EU ready to respond with a range of measures, including sanctions*, 19 June 2017. Available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

The High Representative also issued a declaration on behalf of the EU[15], in April 2019, in which the actors (private or public) are urged to stop undertaking malicious cyber activities, and encouraging an international cooperation between States and private actors to build a strong security and stability of cyberspace.

The European Parliament, through a resolution in October 2017[16] stresses that an increasing amount of unauthorised impairment of computer systems significantly impacts the security of individuals. In its resolution, the European Parliament requires more harmonized definitions of cybercrime. Besides, the fight against cybercrime *"should be first and foremost about safeguarding and hardening critical infrastructures and other networked devices, and not only pursuing repressive measures*". It is important to realise that the European Parliament intends to privilege higher standards regarding cybersecurity over stricter sanctions.

These recent reports from the highest representatives of the European Institutions, show that the situation regarding cyber activity is hard to handle, and is still subject to many frauds. However, the European Union seems to be determined to keep cyberspace open and stable, without over controlling it.

It is observed that the notion of cybercrime a complex, which brings up many different threats with a cross-border nature. Facing this situation, the European Union deployed objectives in order to fight against these malicious usages of the telecommunication and new technologies. In order to understand how this fight is led by the European Institutions, we need to dive into the founding treaties referred to as primary law, as well as the legal acts enacted by the Institutions called secondary law.

B. The European primary law and fundamental rights and secondary law around the notion of cybercrime

The European Institutions are bound by their founding texts, which edict their range of action and objectives. According to the European Commission "*every action taken by the EU is founded on the treaties*"[17]. In fact, the founding treaties of the European Union direct

[15] Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/

[16] *Idem:* 3 October 2017. European Parliament resolution (2017/2068(INI)) on the fight against cybercrime. *OJ C 346, 27.9.2018, p. 29-43*

[17] European Commission, *Primary versus secondary law*, Types of EU law. Available at: https://ec.europa.eu/info/law/law-making-process/types-eu-law_en

the action of the Institutions to create security for its citizens[18], and thus protect effectively the rights infringed by cybercrime (1). The protection of these rights legitimates the action of the European Institutions that's why it is important to analyse them. Furthermore, the action of the European Institutions is mainly identified through secondary law (2).

1. The rights conferred by European Union's Primary law

Primary law of the European Union gathers all the values shared by the Member States and the Union itself. Inside these values, several rights and especially fundamental freedoms are ensured by the Treaty on European Union (TEU), and the Treaty on the Functioning of the European Union (TFEU) (a). Furthermore, since 2009, the Charter of Fundamental Rights of the European Union[19] became legally binding and "*shall have the same legal value as the Treaties*"[20]. Thus, fundamental rights contained in this Charter are also being defended by the European Institutions in their fight against cybercrime (b).

a. The freedoms granted by the founding Treaties: TEU and TFEU

The Article 3(2) TEU sets an objective of the Union to offer its citizens an area of security. Cyberspace can be considered to fall under the scope of this definition, since it is directly related to the users who are commonly users inside the territory of the European Union. On that ground, it is a European Union's duty to fight cybercrime, and not only through the Member States action, but directly from the top institutions. The TFEU, in its Article 67 also recalls the necessity to constitute an area of freedom, security and justice. Thus, the European Union's duty to ensure cybersecurity is justified by the founding texts, which will legitimate the legislation of the European Union, to stop malicious activities.

Together with the article 39 TEU, the article 16(1) TFEU ensures a right to protection of personal data to everyone. According to these articles, the legislative institutions of the European Union are mandated to rule on the protection of individuals, without harming the free movement of the data. This data protection right granted by the treaties can be linked to the first objective set in the European Strategy, according to which the European Institutions and the Member States must prevent offences against the confidentiality, integrity and availability of computer data and systems mentioned above.

[18] Consolidated version of the Treaty on European Union, Article 3(2) and Article 5
[19] Charter of Fundamental Rights of the European Union 2012/C 326/02
[20] Consolidated version of the Treaty on European Union, Article 6(1)

Mention must be made of the value of the fundamental rights contained in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Although the content of this instrument doesn't affect the competences of the European Union's Institutions, it still affects them by constituting general principles of law, as depicted in the Article 6 of the TEU[21]. These general principles fall into the scope of supplementary sources of law together with the case-law of the CJEU, the International law. It designates the unwritten sources of EU law. Thus, it is not directly mentioned, but these fundamental rights are influencing the European's action regarding cybercrime. In fact, several rights can be linked to the objectives set in the European Strategy to fight against cybercrime.

For instance, the Article 5 of the ECHR concerns the right to security, which has been developed already in the Treaties, and to the objective of fighting computer fraud and computer-related offences. Furthermore, the right to private life (Article 8 ECHR), can be linked to the objectives of data protection, since personal data will be kept in the private sphere of the individuals. Also the Article 14 concerning the prohibition of discrimination, leads to the objective of prohibiting content-related offences which also covers the propagation of racist, xenophobic ideas, also the Article 2 concerns right to life to the fight against dissemination and possession of child pornography.

It is evident that the fight against cybercrime finds its legitimacy in the founding treaties, which means that its at the core of the action of the European Institutions. Thus, the reference to the founding treaties incarnates a powerful legal mean in legislating on this issue since European law prevails on any other law of the Member States. Furthermore, the reference to the fundamental rights isn't only depicted in the supplementary law of the European Union, since the Charter of Fundamental Rights of the European Union plays a significant role.

b. The Charter of Fundamental Rights of the European Union

With the entry into force of the Treaty of Lisbon in December 2009, the Charter of Fundamental Rights became legally binding. In fact, it was added to the primary law corpus which has the highest value in the hierarchy of norms of the EU. In that regard, the article

[21]Article 6(3), Consolidated version of the Treaty on European Union: "*fundamental rights, as guaranteed by the European Convention for the protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law*".

6(1) TEU recognises the rights, freedoms and principles defended by the Charter, and grants them the same legal value as the Treaties[22]. Although this provision does not "*extend in any way the competences of the Union as defined in the Treaties*", there is a strong intention to introduce fundamental rights and to defend them, by granting a direct effect to this Charter.

Thus, the Charter allows the European Institutions, and especially the European Court of Justice, to invoke them in order to sanction computer-related crimes. In the case *Google Spain v. Agencia Española de Protección de Datos* [23], the Court compared the articles 7 and 8 of the Charter of Fundamental Rights of the European Union, with the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Thus, it allows the Courts to implement European Human Rights into their decision.

The rights contained in the Charter are consistent with the ECHR's rights, but also include 'third generation' fundamental rights such as guarantees on bioethics, transparent administration, and especially, data protection[24]. Thus, it makes it an even more important legal mean of fighting against cybercrime.

Fundamental rights appear to be central in the fight against cybercrime. In fact, the European Parliament requested the FRA (European Union Agency for Fundamental Rights) to develop a handbook with guidelines to ensure compliance with fundamental rights while countering cybercrime[25]. This handbook should be available in 2021, and give insights on the compliance between fundamental rights and cybercrime fight. This reclamation was promoted by the increasing concern about cybercrime, which is seen as an important challenge to EU security, and a profound fear of being victim of cybercrime[26].

The issue of cybercrime must be fought through cooperation between States. In fact, according to Susan W. Brenner, professor of Law at the University of Dayton (USA) and

---

[22] Article 6(1), Consolidated version of the Treaty on European Union "*The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union […], which shall have the same legal values as the Treaties*".

[23] CJEU (Grand Chamber). 13 May 2014. Decision *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and mario Costeja González* Case C-131/12

[24] European Commission, *Why do we need the Charter?*, What it covers. Available at: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en#relatedlinks

[25] European Union Agency for Fundamental Rights. *Handbook on European law relating to cybercrime and fundamental rights*. Available at: https://fra.europa.eu/en/project/2018/handbook-european-law-relating-cybercrime-and-fundamental-rights

[26] 20 March 2019. Eurobarometer report on Internet security and crime: *79% of the interviewed declare themselves believing that the risk of becoming a victim of cybercrime is greater than in the past.*

expert in cyber-criminal law, "*Because technology has made national borders permeable, cybercrime is not a phenomenon that can be dealt with only at the national level*"[27]. In that regard, through Secondary Law, the European Union exercises an action to build a harmonized and cooperative legal framework.

2. The action through Secondary Law

Secondary law refers to "unilateral acts and agreements"[28] which are listed at the Article 288 TFEU: regulations, directives, decisions, recommendations and opinions[29]. The Amsterdam Treaty introduced Framework Decisions (a), which are legally binding acts that are no longer used since the Treaty of Lisbon came into force in December 2009. However, these acts are still important to analyse since their adoption reveals the strategy of the European Union to fight against cybercrime and inspired its further actions. Since 2009, the European Union uses Directives (b) in order to implement the European Union's law at the level of the States.

a. The Framework decisions around the notion of cybercrime

The Article 34 of the Treaty on European Union, amended by the Treaty of Nice and before the Treaty of Lisbon, proclaimed that the Council could create framework decisions, that would require Member States to achieve a certain objective, leaving to these States a freedom to incorporate it. This instrument differs from the actual directives since Framework decisions were not directly applicable. Thus, Framework Decisions are an instrument trying to build a harmonized legal framework. Regarding cybercrime, several Framework decisions were enacted by the Council, and led the Member States in building a common legal framework against these computer-related offences.

On 24th February 2005, the Council of the European Union adopted the Framework Decision 2005/222/JHA on attacks against information systems[30]. With this text, the Council intended to improve the cooperation between Member States in the field of criminal law and cyber offences. This Framework Decision, by essence leaves to the

[27]W BRENNER, S. *The Role of Penal and Procedural law*, Cybercrime Investigation and Prosecution, university of Dayton School of Law. Cybercrime: An Overview of the Problem, p.11
[28] European e-justice forum, *EU law.* Available at: https://e-justice.europa.eu/content_eu_law-3-en.do
[29]Article 288, Consolidated version of the Treaty on the Functioning of European Union
[30] Idem: DE HERT, P.; GONZÁLEZ FUSTER, G.; and KOOPS, B. *Fighting cybercrime in the two Europes*, Revue Internationale de droit pénal 2006/3-4 -Vol.77, p.506

Member States a freedom to the Member States when implementing it. However, the text is directly inspired by the Cybercrime Convention of 2001. The advantage of the Framework Decision is to bring the cybercrime texts into the scope of European law, more then international law, and thus, strengthening the will of harmonizing and reinforcing cooperation between Member States by pushing them to modify their own national system.

Another important Framework Decision is the Council Framework Decision of 2001 against fraud with non-cash means[31]. This instrument created a definition of fraudulent behaviours that European Union's States need to consider as punishable criminal offences[32]. Thus, it brought a consistent definition and helped developing harmonized law between Member States regarding the notion of cyber-related fraud.

Although Framework Decision are not adopted since the entry into force of the Treaty of Lisbon, their value is still relevant to analyse. Besides, the Council Framework of 2001 on non-cash fraud, was very recently replaced by the Directive 2019/713[33]. In fact, directives are now the instrument used by the European Institutions to build a harmonized legal system between Member States.

b. The Directives around the notion of cybercrime

The Article 288 TFEU explains that the European Union's institutions exercise their competences by adopting "*regulations, directives, decisions, recommendations and opinions*". The same article defines Directives as a binding instrument that needs to be transposed by Member States by leaving the latter a freedom on how to implement it into their own legal system. Directives are thus important since they lead the Member States to modify their own legal system by implementing the directive which are elaborated at the European level. Member States have deadlines to implement the directives, and the European Institutions can sanction them in case of a wrong or non-implementation. Finally, Directives can sometimes have a direct effect and be directly relied on by individuals in national courts. Thus, it appears as an efficient mean of fighting against cybercrime since they push Member States to cooperate and build a common legal background.

---

[31] 28 May 2001. Council of the European Union. Framework Decision 2001/413JHA on combating fraud and counterfeiting of non-cash means of payment

[32] European Commission, *Cybercrime*, Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

[33] 17 April 2019. European Parliament and the Council Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, and replacing Council Framework Decision 2001/413/JHA

In 2011, a Directive concerning sexual abuse and exploitation of children[34] has been enacted. This directive relies on one of the objectives of the fight against cybercrime posed by the European Strategy on cybercrime. This Directive forces Member States to create criminal penalties in their national legislation, framed by the European law. Compared to the previous Framework Decision[35], the Directive better addresses new developments in the online environment, such as grooming.

Another important Directive regarding the fight against cybercrime is the Directive from 2013 on attacks against information systems[36] that replaces the previous Framework Decision from 2005 mentioned above. In fact, the Directive implements into Member States' legal systems common definitions of cybercrime destined to improve cooperation between them, and to set standards regarding the fight against cybercrime. A report from the Commission [37] explains that the Directive led to significant improvement in criminalizing cyberattacks and facilitating cross-border cooperation. The efforts regarding common definitions (Article 2 of the Directive) led to a better cross-border cooperation upheld by the Directive, which improves the reaction of the Member States regarding cybercrime. However, according to the Commission, the implementation of the Directive still needs to be improved, since Member States find some difficulties building common definitions of actions in relation to offences (Article 3 to 7) and including common standards for penalties (Article 9). This Directive shows with precision the situation of a European Union enabling a fight against cybercrime with serious means but struggling to implement them.

In April 2019, a directive aiming on combating fraud and counterfeiting of non-cash means of payment[38] replaced the Council Framework Decision 2001/413/ JHA. This recent Directive considers non-cash payments as a threat to security since it represents a source of income for organised crime, and therefore enables other criminal activities such as

[34] 13 December 2011. European Parliament and the Council Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

[35] 22 December 2003. Council Framework Decision 2004/68/JHA on combating sexual exploitation of children and child pornography

[36] 12 August 2013. European Parliament and the Council Directive 2013/40/EU on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA

[37] Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA COM/2017/0474 final. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52017DC0474

[38] 17 April 2019. European Parliament and the Council Directive (EU) 2019/713

terrorism or drug trafficking. Besides, the Directive brings up the fact that many differences in Member States' laws are refraining the detection and sanctions of such crimes.

It can be osberved that the European Institutions are trying to harmonize on a wide variety of criminal behaviours. The issue is that the legal process is long, and fastidious since the implementation of Directives is complex. However, according to the annual Internet Organised Crime Threat Assessment (IOCTA) 2019 of Europol[39], new threats in cybercrime arise from known vulnerabilities in existing technologies. Thus, there is a need for European Institutions to react quickly. The issue of the delays in the legal process in the fight against cybercrime also comes from the nature of criminal law in European Union, which needs to be analysed.

C. The matter of criminal law and cooperation

Criminal law in the scope of European Union's law differs from other judicial systems since the Member States are mainly in control of their criminal legislation. Because cybercrime constitutes serious offences that lead to criminal sanctions, it is relevant to understand how the European Union behaves regarding this matter. In fact, criminal law is a matter that is hardly delegated to the European Union's by the Member States. Therefore, the matter of criminal law inside European law has followed a progressive evolution (1) that must be analysed in order to understand the challenges related to cybercrime. Besides, a significant evolution occurred since the entry into force of the Treaty of Lisbon in 2009[40]. In fact, criminal law, to which cybercrime is directly linked, changed in the sense of a stronger implication of the European Union to the Member States (2). Thus, it must be noticed how a criminal cooperation is installed inside the European Union between Member States on the one hand, and the European Institutions on the other hand.

1. The evolution of criminal law inside the European Union

Cooperation of Member States in the area of penal law inside the European Union was first regulated by the Maastricht Treaty making up the European Community in December 1991. Since its adoption, three pillars were the core of European Union's legal system.

[39] EUROPOL, iOCTA, 2019: https://www.europol.europa.eu/iocta-report
[40] Treaty of Lisbon amending the Treaty of European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, 2007/C 306/01

The first pillar concerns the European Communities which addresses the responsibilities of the European Communities in terms of social policy, regional policy and environmental policy. This pillar encompasses economic and social matters such as Single market, European Citizenship, competition law, healthcare… The second pillar is referred as Common Foreign and Security Policy (CFSP). Foreign policy refers to matters such as Human Rights and Democracy, whereas Security Policy concerns Peacekeeping, Common Security and Defence Policy… The third pillar named Police and Judicial Co-operation in Criminal Matters, referred to matters such as drug trafficking and weapons smuggling, terrorism, trafficking in human beings… It is in this third pillar that cybercrime is labelled. There was a different legislative procedure to each pillar, which allowed a better reaction of the institutions toward each issue.

With the Maastricht Treaty, under the third pillar, three different instruments could be adopted: common positions, common activities and conventions. These instruments appeared weak[41]. Therefore, the Amsterdam Treaty brought framework decisions under the third pillar. However, as we have seen before, these framework decisions aren't strict enough since it doesn't have a direct effect. Thus, the harmonization of Member States' legal systems wasn't consistent enough.

In fact, criminal law as such wasn't part of the Community's competences. As a matter of fact, the ECJ[42] stated that the competence regarding criminal matters is owned by the Member States and that European Community doesn't have a competence to regulate criminal law and criminal procedure. Thus, the competence of the European Union seems restricted since the Member States are reluctant to delegate their competence in the matter of criminal law.

Before the Treaty of Lisbon, the competence of the European Communities regarding criminal law was restricted. Thus, the adoption of rules regulating cybercrime were difficult to establish, meaning that a harmonized judicial system on that matter was hard to promote. Since 2009, the situation has evolved.

[41] ROZMUS, M.; TOPA, I.;, WALCZAK, M. The *Current Status and the Impact of the Treaty of Lisbon,* Harmonisation of Criminal Law in the EU Legislation. Available at : <http://www.ejtn.eu/Documents/Themis/THEMIS%20written%20paper%20-%20Poland%201.pdf>

[42] ECJ (Grand Chamber). 13 September 2005. Decision *Commission of the European Communities v Council of the European Union* C-176/03

2. Criminal law in the Lisbon Treaty era

According to the article 83 of the TFEU, the European parliament and the Council may establish minimum rules regarding definition of criminal offences and sanctions in the areas of "*serious crime with a cross-border dimension*" with a significant need to combat them. It can be observed that this definition leads directly to the matter of cybercrime since it is a serious threat with a cross-border dimension. Thus, the European Institutions have now a power to rule out on criminal matters. The modification of the Treaties means that Member States are not anymore the only actors able to regulate criminal matters. This was one of the aspects of the Treaty that created a serious debate before its adoption, since the Member States are conceding a part of their sovereignty to the European Union. However, it can be considered to enhance the possibility to create harmonized legal systems. In fact, with the entry into force of the Treaty of Lisbon, Member States are not able to reject a proposal for a Directive. This new procedure poses many questions, but regarding cybercrime, it as a better way to react against new threats and to create more harmonized law, and hence promote cooperation between States.

Moreover, the new article 83 TFEU enlarged the areas of crimes covered and included "*computer crime*" as a new form of crime that can be regulated by the European Union. Thus, it gives legitimacy to the Institutions of the European Union to regulate on cybercrime through Directives. This led to various Directives regarding cybercrime, and especially the one from 2013 on attacks against information systems.

However, according to the Article 83 TFEU, if a Member State is opposed to a Directive as it would affect fundamental aspects of its criminal judicial system, it can request the draft of the Directive to be addressed to the European Council, which within 4 months will debate[43]. This emergency brake must be motivated by the referring Member State who can suspend the procedure. Thus, there is a possibility for a Member State to block the procedure, which would lead to slowing down the possibility to react.

Through its evolution, the criminal matter in the European Union went from a State held aptitude to a broader competence of the European Union. In practice, it is believed that the power of the European Institutions, led by the Commission and a stronger European Parliament, are more able to produce texts. However, since 2009, only a few Directives with specific scope regarding cybercrime were produced. Thus, the broader legislative

[43] *Idem :* ROZMUS, M.; TOPA, I.;, WALCZAK, M. The *Current Status and the Impact of the Treaty of Lisbon,* Harmonisation of Criminal Law in the EU Legislation

power granted to the European Institutions, reducing the sovereignty of the Member States, doesn't lead to much more control from the European Union. This can be seen through the difficulties regarding delays to implement the Directives from the Member States.

Cybercrime is a complex notion that encompasses many different crimes. The European Union understood the importance to fight it. Thus, a large legal framework is progressively taking place in order to rule out the cyber space. The need to ensure security and protection of the fundamental rights of the citizens of the European Union is central. Through its Directives, the European Union is building a common harmonized legal system that encourages Member States to cooperate in order to fight cybercrime. Thus, the legal mean of fighting against cybercrime is central and strong. The European Union intends, not without difficulties, to reach the objectives set in the European Strategy to fight against cybercrime. In fact, the European Institution's polls show the large number of crimes that are still committed. Therefore, there are still a many challenge that need to be overcome in order to ensure cyber security, must now be considered. In fact, the role of the courts in the fight against cybercrime must be analysed.

II – The Judicial aspect of the fight against cybercrime

As cybercrime relates to criminal behaviours, there is a necessity to sanction them. The illegality of these crimes is characterised by the contrariety to the legal texts developed by the European Institutions. In that regard, the Court of justice of the European Union plays a central role since it ensures the right application of the law (A). In fact, the European Court have a competence to sanction Member States in case of a wrong application of the European law. In that regard, the Courts are safeguarding the rights proclaimed by the legal texts, and thus appear to be an important mean of fighting against cybercrime. Moreover, the judicial aspect of European law plays an important role in the fight against cybercrime by enhancing the judicial cooperation between Member States through several instruments (B). In that regard, the importance of the principle of mutual recognition on the one hand, and the European arrest warrant on the other hand must be studied. Furthermore, the creation of specific evidences, named the *E-evidences* (C), helped sanctioning computer-related which are by essence immaterial, making evidences harder to use and collect.

A. The role of the Court of Justice of the European Union

The Court of Justice of the European Union is the judicial organ of the European Union. It consists of two courts, namely the Court of Justice and the General Court. Its role is to ensure the correct interpretation of European Law (1). In that regard, its role is central since it ensures the correct interpretation and application of both primary and secondary Union law in the EU. However, since the European Union's competences regarding criminal law doesn't exist as such, its main role consists in providing interpretation of Union law when requested by national judge. This process is referred to as preliminary ruling (2).

1. The cooperation through the action of the CJEU

The Court of Justice of the European Union can be considered as a guardian of the right application of the European law. Its action forces Member States to cooperate, through its decisions (a) that poses common criteria of appreciation of European law. Furthermore, its ability to sanction Member States that would comply with European law (b), supports this dynamic by ensuring that the States are following the guidelines set by European law.

a. A cooperation supported by the Court's decisions

The Court of Justice of the European Union's (CJEU) competence is set in the article 19 TEU according to which, the Court's role is to ensure that the interpretation and application for the Treaties are followed. It must be observed that the Court's mission goes towards a logic of harmonizing the interpretation of the texts, since the judgements of the Court cannot be denied by the Member States, and especially the national judges.

The European Judge gives precisions on the application of the European law and its relationship with national law. The dominance of European law over national national law was very soon imposed by the European judge. In its judgment of the 15th July 1964 Cost v Enel[44] and Van Gend & Loos[45] the Court defined European Community law as prevailing over national law. Furthermore, in the case of the 11th of November 1981 Guerrino Castati[46], the Court considered that a national criminal legislation should be dismissed if it is in contradiction with the law of the Community. Therefore, even criminal law, being a sensitive area to harmonize is subject to the control of European law. The CJEU through its decisions harmonizes the interpretation of Union law. Moreover, although criminal law

[44] ECJ. 15 July 1964. Decision *Flaminio Costa v E.N.E.L* C-6-64
[45] ECJ. 5 February 1963. Decision *Van Gend & Loss v Netherlands* C-26-62
[46] ECJ. 11 November 1981. Decision *Guerrino Castati* C-203/80

is mainly a state held competence in terms of procedure, it finds its limits in the European law since it can't be in contradiction to the latter. Thus, there is a need for the States to adapt their criminal law system under the standards set by the European Union.

A strength of the system in that regard, is the competence of the Court to sanction non-complying Member States. This possibility to sanction brings a higher level of control by forcing States to comply with the harmonized legal system.

b. A cooperation reinforced by the sanction to non-complying Member States

According to the article 260 TFEU, when the Court finds out that a Member State has failed to fulfil an obligation under the Treaties, the latter is obliged to take measures in order to comply with the judgment of the Court. If the Member State still doesn't take the necessary measures, the Commission may bring the State to the Court and lead to a financial sanction. This action was specified by the Court in the case Commission v Republic of France regarding fishing measures judged against European law in 1991[47]. France still didn't take sufficient measures and was sanctioned. In this procedure, it is whether the Commission after a preliminary procedure under Article 158 TFEU, or another Member State (Article 259 TFEU), that can bring the non-complying Member State to the Court[48]. The Court needs then to confirm that the State has failed to fulfil its obligations and require him to stop its infringement. If the Member State still didn't stop its infringement, the Court may impose a fixed lump and or a periodic penalty payment. The amount is determined by the Court after a proposal of the Commission

Therefore, the Court of justice of the European Union acts as a guardian of the cooperation of the Member States through the control of the application of European law. The Treaty of Amsterdam, and later the Lisbon Treaty, by building the third pillar, gave the European Union some competences in criminal law. However, the Court doesn't substitute itself to national Courts. Thus, the European judges are not granted competences to judge national cases on behalf of the national judges. In order to indirectly promote the action of the European judge in terms of cybercrime, preliminary rulings are used to implement his judgment into national cases.

[47] ECJ (Grand Chamber).12 July 2005. Decision *Commission of the European Communities v French Republic* C-304/02

[48] European Parliament, *Competences of the Court of Justice of the European Union.*Available at : <https://www.europarl.europa.eu/factsheets/en/sheet/12/competences-of-the-court-of-justice-of-the-european-union>

2. The preliminary rulings

Preliminary rulings are a strong tool that create a bridge between the two spheres of national and European judicial systems. In fact, they overlap and could be permeable without an efficient control of national judges' decisions. Through preliminary ruling, the European judge can ensure the legality of Union law (a). Furthermore, preliminary rulings are a way for the European judge to legislate (b) by granting essential precisions.

a. The control of the legality of the European law through preliminary rulings

The Article 267 of the TFEU grants a competence to the Court of Justice of the European Union to give preliminary rulings regarding the interpretation of the Treaties or the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union. Any jurisdiction of a State can ask the Court for a preliminary ruling when it has to give a decision on a case. This procedure allows national Courts to anticipate a question brining a misunderstanding of the application of European law instead of miss judging and being contested afterwards. The mechanism of preliminary ruling supports the idea of a European Court controlling the national Courts judgments.

The Court of Justice of the European Union is often confronted to preliminary rulings from national Courts, especially in the matter of cybercrime and data protection. The Google Spain Case C-131/12[49] concerned a preliminary ruling on the interpretation of the Directive 95/46/EC on protection of individuals with regard to the processing of such data. The Court had to analyse the impact of such directive by crossing it with other rights from the treaties and also fundamental rights such as respect for private life and protection of personal data (Article 7 and 8 of the Charter of Fundamental Rights of the European Union).

The European judge seems to be a guarantor of the freedoms between the European Institutions and the Member States. Thus, the cooperation appears on vertical sense between the Member States and the European Institutions, and not only between Member States together which helps building a consistent legal framework that doesn't ignore citizens' rights, since they have a possibility of remedy in case of a harm of their rights by European law.

[49] *Idem*: CJEU (Grand Chamber). 13 May 2014. Decision *Google Spain SL and Google Inc v. Agencia Española de Proteccion de Datos (AEPD) and Mario Coste and Costeja Gonzalez*, C-131/12

One of the main characteristics of preliminary ruling is that the judge is pronouncing its point of view on the application of European law. However, the judge often goes further and uses the preliminary ruling to produce principles or classifications.

b. The preliminary rulings as a way for the European judge to legislate

In the matter of competences, the Court of Justice of the European union is mainly solicited by national judges. Through clarifying competence aspects, the European judge sometimes goes further and proposes legal qualifications and clarifying the interpretation of directives. In fact, through several cases such as the Football Dataco case of the 1st march 2012[50] and the Wintersteiger case of the 19th April 2012[51], asking directly preliminary rulings to the Court of Justice of the European Union, the latter gave interpretations of the application of the directives.

For instance, in the Football Dataco Case, the Court is facing a preliminary ruling from the Court of Appeal of Englands and Wales regarding the Article 7 of the Directive 96/9/EC on the legal protection of databases. The Court, through its argumentation, gives a definition of the concept of "re-utilisation" of the Directive, as well as a precision on the localisation of the act of re-utilisation.

Furthermore, the famous Google Spain case of 2014 is one of the preliminary rulings following this logic. In fact, the Court was confronted to the application of the Articles 2,4,12 and 14 of the Directive 95/46/EC on the Protection of individuals with regard to the processing of such data. In fact, the Court invokes fundamental Rights from the Charter of Fundamental Rights of the European Union in order to consider that under certain conditions, a search engine may be ordered to remove the links from search results. Although the Court didn't expressly declare it, a right to be forgotten was proclaimed. Thus, through a preliminary ruling, the Court of Justice creates principles and rights regarding telecommunication technologies.

Therefore, we see that these Court decisions following preliminary rulings are creating a jurisprudence of the Court that seem to consolidate the right around telecommunications. In fact, cyber law is still new and needs to be structured. In that sense, the Court is playing a significant role in consolidating the newly created law. Thus, since cybercrime mainly

[50] ECJ (Third Chamber). 18 October 2012. Decision *Football Dataco Ltd and Others v Sportradar GmbH Sportardar AG* C-173/11

[51] ECJ (First Chamber). 19 April 2012. Decision *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH* C-523/10

takes advantage of legal vacuums, building a more consistent cyber law will help fighting against it.

B. The judicial cooperation in criminal matters

The development of a borderless market inside European's territory facilitates the free movement of persons and goods, but also made it easier for criminals to cooperate transitionally. Thus, cross-border crimes involve cooperating on a judicial aspect among Member States in order to response efficiently to these crimes. Regarding cybercrime, the cross-border nature is inherent to the computer-related crimes, which make it a dangerous threat to the internal market and the citizens. In fact, according to G. Christou *"Cybercrime in the global market has become a serious issue given the growth of the Internet and its importance to our economic and social lives"* [52]. The most efficient remedy to such a threat stands in cooperation in criminal matters. The aim is to build a judicial cooperation space of security, justice and freedoms (1). Furthermore, the importance of the European Arrest warrant (2), which is a practical result of such a cooperation, must be brought up.

1. Judicial cooperation in the space of security, justice and freedoms

According to the Article 3(2) TEU, the Union shall offer its citizens an area of freedom, security and justice without internal frontiers. Judicial cooperation in the European Union wasn't new and was developed through various conventions and legal texts. The Convention on Mutual Assistance in Criminal Matters (a) already developed a common approach of cooperation. Moreover, the Title V of the TFEU regarding the area of Freedom, Security and Justice contains provisions on Judicial cooperation in criminal matters. The Article 82 TFEU stresses the principle of mutual recognition (b).

a. The extension of judicial cooperation through the convention on Mutual Assistance in Criminal Matters

One of the first instruments developed in order to establish judicial cooperation, is the Convention on Mutual Assistance in Criminal Matters [53] from 1959 which enabled a judicial cooperation between the parties to the Convention. They agreed to afford each other

[52] CHRISTOU, G. *Cybersecurity in the European Union* 2016, p.87
[53] 1959. Council of Europe, European Convention on Mutual Assistance in Criminal Matters,

the "*widest measure of mutual assistance with a view to gathering evidence, hearing witnesses, experts and prosecuted persons*"[54]. This Convention from 1959 is an old instrument but was reinforced by various protocols.

In fact, the additional protocol of 17th of March 1978 completes the Convention. It withdraws the possibility offered by the Convention on its Article 2.a, to refuse assistance to another party in case of fiscal offences[55]. The protocol also extends international co-operation to the service of documents concerning the enforcement of a sentence and similar measures.

The second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters from the 8th of November 2001, aims to enhance States' ability to react to cross-border crime "*in the light of political and social developments in Europe and technological developments through the world*"[56]. In fact, the Protocol tends to broaden the range of situations in which mutual assistance may be requested in order to make it easier, quicker and more flexible.

Finally, the Convention was completed by the Regulation (EC) No 1882/2003[57] which brings a procedure to frame the action of the competences of execution of the organs, namely the Commission and the Parliament, that use this Convention.

According to the fact that this convention is old but was several times improved and modernised, it must be observed that it plays a powerful role in enhancing the judicial cooperation between States parties. Thus, this cooperation, also extended to technological matters, reinforces the fight against cybercrime. Beyond the textual aspect of the judicial cooperation, one of the most important principles that enables it, is the principle of mutual recognition.

---

[54] Council of Europe, Details of Treaty No.030. Available at : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030>

[55] Article 1, Additional Protocol to the European convention on Mutual Assistance in Criminal Matters, 17 March 1978, European Treaty Series – No. 99

[56] Council of Europe, Details of Treaty No 182. Available at : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182>

[57] 29 September 2003. European Parliament and the Council Regulation (EC) No 1882/2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure reffered to in Article 251 of the EC Treaty

b. The cooperation through the principle of mutual recognition

According to the Article 82 TFEU, the principle of mutual recognition of judgments and judicial decisions is the core of the judicial cooperation in the European union. This principle is a direct response to the progressive elimination of border controls with the EU as it is induced in the Article 67 TFEU.

Since judicial cooperation is linked to criminal law, its application still shows reticence from the States. In fact, most measures for judicial cooperation are adopted following the ordinary legislative procedure and can be reviewed by the Court of Justice of the European Union[58]. However, the Commission shares its power of initiative with the Member States if they represent a quarter of the members of the Council[59]. Besides, Parliament has a reduced impact on this kind of measures since the Council needs to adopt them unanimously. If there is no unanimity, Member States can work together on the basis of enhanced cooperation.

In that regard, many legislative acts were adopted, such as Directive 2013/40/EU on attacks on information systems, or the Directive 2019/713 from 2019 on combating fraud and counterfeiting of non-cash means of payment.

We can see that the principle of mutual recognition in criminal matters bring Member States to apply a consistent application of criminal law. This helps actions against cybercrime through cooperation between the States. One of the most important outcomes of this principle is the creation of a European Arrest Warrant.

2. The importance of the European Arrest Warrant

The European Arrest Warrant is a powerful tool that has been created by the European Union at the beginning on the century. Its creation was motivated by observation of the territorial limits of formal extradition procedure[60]. Therefore, the creation of the European Arrest Warrant (a) must be studied, in addition to its impact (b).

[58] European Parliament, *Judicial cooperation in criminal matters,* Fact Sheets on the European Union. Available at : <http://www.europarl.europa.eu/factsheets/en/sheet/155/la-cooperation-judiciaire-en-matiere-penale>

[59] Article 76 TFEU

[60] 13 June 2002. Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States

a. The creation of a European Arrest Warrant

The Council Framework Decision 2002/584 in its Article 1(1) defines it as "*a judicial decision issued by a Member State with a view to the arrest and surrender by another Member State of a requested person, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order*". It is executed on the basis of the principle of mutual recognition. The absence of freedom of circulation of judicial decision inside the European Union is at the origin of the creation of such a warrant.

The territorial competence of the States is linked to their sovereignty and constitutes an obstacle to the execution of a judicial decisions in cross-border situations. In fact, in the case of a cyber-attack located in the territory a State directed towards State, the victim State cannot act, and no rule seem to oblige the host State to take any measures. Yet, cybercrime mostly consists in cross-border situations. Therefore, the use of a European Arrest Warrant seems necessary to sanction these crimes. In fact, the Article 2 of the Framework Decision depicting the grounds of the warrant refers to "*computer-related crimes*". The European Arrest Warrant is although different from a national warrant as it was confirmed by the Court [61]. The European Arrest Warrant seems to be an evolution of the European Convention on Extradition from 1957[62], by replacing these lengthy procedures. It was operational since 1 January 2004.

It is important to mention that the European Arrest Warrant is not a political involvement, since it is a decision made by a judicial authority without political considerations. It was confirmed by the European Court of Justice in a Lithuanian case[63], where the Court had to decide if a Ministry of Justice could correspond to the term "judicial authority" required by the texts. This criterion is a safeguard since it can't be used for political purposes and is only an instrument to perform a judicial decision

The European Arrest Warrant was thus created in response to the difficulty to cooperate on criminal matters in the European Union. Thus, it is an important instrument in the fight against cybercrime and its cross-border nature by promoting cooperation between States and enabling more efficient sanctions.

[61] CJEU. 1 June 2016. Decision *Bob-Dogi* C-241/15
[62] 13 december 1957. European Convention on Extradition, Paris, ETS No.024
[63] CJUE. 10 November 2016. Decision *Kovalkosas* C-477/16

b. The impact of the European Arrest Warrant

The European Arrest Warrant is a request by a judicial authority in one EU country to arrest a person in another and surrender them for prosecution. The country where the person is arrested has 60 days ti arrest the person, and 10 days if the person consents to surrender. Furthermore, EU countries can no longer refuse to surrender their ow nationals. This is a significant evolution since the penalty will prevail over the residence in a protective space. Thus, the sanctioning of criminals is much more frequent, and States are forced to cooperate, which constitutes a significant perk for fighting against cybercrime.

However, there are some grounds for refusal. According to the ne bis in idem principle, a person cannot be judged twice for the same offence. Furthermore, minor's person might constitute a ground of refusal. Finally, the amnesty can lead to a refusal as well. This can be a limit to the effectivity of the arrest warrant, but these criteria are restricted, and are more constituting safeguards rather than an obstacle to the good application of the warrant.

Concerning the impact of the Warrant, the European Commission published a Handbook on how to Issue and Execute a European arrest warrant[64]. This helps the concerned judicial authorities in requesting it. Furthermore, the European Commission issued statistics on the use of the warrant[65]. It shows that in 2017, almost 17500 warrants were issued, and 6317 were executed. This statistic leads to understand that the cooperation between Member States is significantly improving and that the reaction towards cross-border criminal issues, such as cybercrime, can be solved quicker.

The cooperation on judicial matters is significantly increasing. In fact, Member States with the help of the European Union, seem to be willing to cooperate more with the other States on criminal matters. This is a significant improvement since criminal law has always been challenging to harmonize. Besides, the results might lead to an improvement of the sanctioning of cybercrimes. Furthermore, a significant step forward in the production of European judgements on cybercrime, are the elaboration of E-evidence.

---

[64] Commission Notice, *Handbook on How to issue and execute a european arrest warrant,* 28 September 2017. Available at : <https://e-justice.europa.eu/content_european_arrest_warrant-90-en.do>

[65] 28 August 2019. Commission Staff Working Document, *Replies to questionnaire on quantitative information on the practical operation European arrest warrant* year 2017

C. The use of E-Evidence as a mean to fight cybercrime

One of the main challenges regarding cybercrime is its immaterial nature since this activity is performed through computers, clouds and data bases which are breaking with the former kind of evidences such as fingerprints. More and more, criminals use digital services such as emails to commit crimes, which can be used to trace the illegal activity and thus, be used as evidence. These evidences are sometimes difficult to obtain. Thus, the E-evidence issue is developing significantly

1. The development of E-evidence

Nowadays, the use of new telecommunication technologies is everywhere and touches everyone. Therefore, the use of social media, webmail, messaging services and applications to communicate are linking hundreds of millions of users to one another. If these technologies are beneficial to our society, many missuses can be revealed. Therefore, these services are often the only place where investigators can find leads to determine who committed a crime and obtain evidence that can be used in Court[66]. Thus, there is a necessity to develop a cooperation regarding E-evidence. This development promoted by the European Institutions led to recent changes, with a major proposal from the Commission was issued which leads to consider the future of e-evidence cooperation.

Electronic evidence is a central notion on cybercrime, since most of the evidence used in the judicial process are contained in many different locations, under different forms. Thus, it is necessary to cooperate and share the relevant evidence in order to improve the efficiency of judicial systems regarding cybercrime. This need to cooperate has been understood by the European Union who works to enable it. The cooperation, although effectively concerns the States together (a), also affects the Internet Services Providers (b).

a. A cooperation between States regarding evidence

It is stated that millions of attacks against computers and data are recorded each day worldwide. Only a few are actually prosecuted as cybercrimes. In many situations, the evidence is stored in clouds. Clouds storage consists in a model of computer storage in which digital data is stored. There is a physical storage that can be separated in multiple

[66] 17 April 2018. European Commission, Regulation 2018/0108(COD) of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters

locations. Thus, judicial institutions wishing to obtain this data, need to cooperate with the hosting State, and the result might depend on the latter's good will. This process can be long and will make the prosecution inefficient since the criminal will sometimes be able to vanish before he gets judged. Besides, the possibility to hide data will make the trackability of the crimes extremely difficult.

In 2003 the European Union pointed out the need for immediate mutual recognition in the transfer of evidence to impede its destruction or transformation. On that ground, the Framework Decision from 2003[67] was enacted. However, this instrument is limited to the freezing phase, which requires to be accompanied by a separate request for the transfer of the evidence. Therefore, the process is divided into two steps which goes against an efficient transfer of the evidence. This Framework Decision was followed in 2008 by another one regarding the European Evidence Warrant[68], destined to improve judicial cooperation by applying the principle of mutual recognition for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters. The intention regarding this instrument was positive, but it only applied to evidence which already existed and thus wasn't useful to the investigators, as it was mentioned in the Directive 2014/41/EU regarding the European Investigation Order in criminal matters.

The article 1(1) of the Directive from 2014[69] defines European Investigation Orders (EIO) as *"judicial decisions which has been issued or validated by a judicial authority of a Member State (Article 1(1) of the Directive) to have one or several specific investigative measures carried out in another Member State to obtain evidence in accordance with this Directive"*. The Directive also brings an obligation to impose the EIO on the ground of the principle of mutual recognition. This Directive is a significant step forward[70] since it reduces the wide discretion of the Member States to comply with the request of another Member States, by basing the request on the principle of mutual recognition. But in practice, there is still a time-related challenge regarding transfer of data since the Directive requires a 90 days timeframe to respond to the request. It is indeed a long period that slows down the prosecution process.

---

[67] July 2003. Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property of Evidence

[68] 18 December 2008. Council Framework Decision 2008/978/JHA on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters

[69] 3 April 2014. European Parliament and the Council Directive 2014/41/EU regarding the European Investigation Order in criminal matters

[70] OSULA, A. *Mutual Legal Assistance & Other Mechanisms For Accessing Extraterritorially Located Data.* DOI 10.5817/MUJLT2015, Estonia, 2018. p.49

b. An evidence cooperation regarding Internet Service Providers

In 2016, the EVIDENCE project was created in order to "*provide the European Commission with a roadmap for harmonisation of the exchange of this type of evidence in the Member States*", said Maria Angela Biasiotti of Italy's Consiglio Nazionale delle Ricerche[71]. The European Union points out the difficulty for judicial institutions to get relevant electronic evidence due to their multiple forms such as CCTV, social media platforms content. If it is remembered that the rules applied on the acquisition of evidence may differ from one State to another, it can also differ from the consideration of an Internet Service Provider (ISPs) and a law enforcement agency. In fact, ISP own a huge data base that would help in the judicial process, but the disclosure of such personal data isn't systematic from the ISPs who try to protect their users and sometimes consider the data they own with monetary value.

According to Maria Angela Biasiotti, the project EVIDENCE created a dialogue between these entities and fostered the emergence of a European electronic evidence community where all sides are represented. Thus, the cooperation between them seems to be on a progressive way. She infers that an agreement between the ISP and the law enforcement agencies would help their cooperation, with the intention to convince ISPs to disclose this information without delays. Furthermore, she brings up the necessity to share information on the dangers related to cybercrime to those involved in exchanges of the material and wouldn't get a clear understanding of the potential stakes.

Thus, the States are not the only actors in the cooperation on evidence, since most of its content is detained by private entities who play a massive role, but are not bound by the same obligations and objectives as States can be. It seems important to bring all the entities under a same goal, enabling cooperation between them. More recently, the European Union developed new instruments on the cooperation regarding electronic evidence.

2. The future of E-evidence cooperation

Facing the difficulty surrounding the collection of evidences on cross-border situations and especially regarding electronic evidences, the European Institutions acted to make law enforcement and judicial authorities to obtain electronic evidences more easily and faster.

[71] European Commission, *Electronic evidence, expertly explored*. Available at : <https://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/headlines/news/article_17_03_16_en.html?infocentre&item=Infocentre&artid=43496>

In fact, on the 17th of April 2018, the Commission proposed new rules regarding cooperation in the matter of evidence, through a Regulation[72], and a Directive[73].

The Regulation on European Production and Preservation Orders for electronic evidence in criminal matters aims to enable the possibility for competent authorities of a Member State to request directly from a service provider established or represented in another Member State, access to or preservation of E-evidence such as emails, text or messages in apps, as well as information to identify a perpetrator. This data is needed for investigation and prosecution of crimes that fall in the scope of the Regulation. It must be mentioned that the location headquarters of the service provider doesn't impact this capacity.

This proposal also takes into account fundamental rights by providing safeguard and effective remedies. Besides, it also offers the possibility for the service provider to request a review of the received order on defined grounds such as technical issues in case of orders which are "*manifestly abusive or violating the Charter of Fundamental Rights*"[74].

One of the most important aspect of the proposal stands in the intention to bring clarity and to significantly speed up the process of obtaining e-evidence since it imposes an obligation for the service providers to respond within 10 days and up to 6 hours in case of emergency. This requirement breaks with the former timeframe of 10 months in average for the Mutual Legal Assistance procedure.

Besides, the rules impose the service providers to designate a legal representative in the Union in order to ensure that they are subject to the same obligations even if their headquarters are outside of the Union. Finally, it provides legal certainty for businesses and service providers in order to apply the same rules for access to all service providers to improve legal certainty and clarity, whereas today's law depends on the good will of the service provider.

---

[72] Proposal COM/2018/225 for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters

[73] Proposal COM/2018/226 for a Directive of the European Parliament and of the council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings

[74] Legislative Train Schedule, *European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, Area of Justice and Fundamental Rights, , 2017. Available at : <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders>

These instruments are the product of a two-year process including a thorough impact assessment[75], which means that the European Union understood all the stakes regarding the importance of e-evidence, and thus, its impact on the fight against cybercrime.

However, these instruments are still at the stage of proposals, and need to be modified. The European Economic and Social Committee (EESC) gave its opinion in 2018[76] and welcomed the proposal, encouraging the development of Europe-wide uniform standards regarding access to data, but stressing the need to protect fundamental rights. Besides, the European Data Protection Board (EDPB)[77] pointed out that the proposals should be more consistent with European Data protection law and safeguard more the rights of individuals. The Justice and Home Affairs Council published recommendations aiming to modify the proposals, especially on information requirements for Orders such as unique identifiers like ID names or account names for the person sought as well as more details on evidence requested. Finally, the European Data Protection Supervisor (EDPS), on the 6th of November 2019, underlined the necessity to ensure involvement of the judicial authorities in the enforcing Member State and taking into account the Court of Justice of the European Union's case-law.

The judicial aspect of cybercrime is complex. It relates to international criminal law, which is a sensitive area since the States can be reluctant to delegate their sovereignty in this area. However, the European Union managed to create a solid base of judicial cooperation in that matter. Thus, the Court of Justice of the European Union plays a central role. Besides, the judicial cooperation is encouraged by the measures of the European Union and the principle of mutual recognition. Finally, the matter of evidence in this field is essential since it is the core of a judgment. The fight against cybercrime is also perpetrated by stakeholders whose action are crucial. Therefore, the organic aspect of the fight against cybercrime must be considered.

---

[75] Commission staff working document impact assessment accompanying the two documents, SWD/2018/118 final. Available at : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:118:FIN>

[76] 11 July 2018. European Economic and Social Committee, *Evidence in criminal proceedings*, , COM(2018) 225 final. Avaialble at : <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/evidence-criminal-proceedings>

[77] 17 October 2018. European Data Protection Board 2018/0107(COD). Available at : <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/evidence-criminal-proceedings>

III – The organic aspect of the fight against cybercrime

Organic aspect refers to every stakeholder that are acting on the fight against cybercrime. In fact, the institutional landscape contains many different entities which are coexisting and share a common goal in fighting against cybercrime but are devoted to different fields of action. The goal in this section is to show the large number of different entities working in the field of cyber security and trying to annihilate cybercrime. The methods employed by the different organs can differ, from competences in order to enact texts, to competences of law enforcement or knowledge broadcasting. Also, this title aims to show the plurality of organs. In fact, since cybercrime is a matter that carries many forms, it is a first indication of the reason of having many different entities governing this subject.

The European Union is a strong union that develops many tools and agencies in order to fight the new threats brought by the evolution of new technologies, which reveal many challenges. The first aspect of these institutions concerns cooperation and harmonization of the law (A). Furthermore, there is a significant aspect regarding law enforcement (B). Finally, it must be observed that the transfer of knowledge is a substantial part of the fight against cybercrime (C).

A. Organisations regarding cooperation

The European Commission (1) is the core institution of the European Union. It has many missions and plays a central role in the fight against cybercrime. One of its most important mission on that matter, is to develop legal instruments in order to obtain cooperation between Member States and thus, building a stronger defence against it. Besides, the main institution regarding cooperation between Member States, is EUROJUST (2) which has an essential position in the development of a strong interstate cooperation. Finally, a presentation of the European Defence Agency (3) seems relevant since it has an important role in terms of cooperation in the European Union.

1. The European Commission

Through this work, the importance of the Commission has been demonstrated. In fact, it is a central institution in the functioning of the European Union. Regarding cybercrime, it seems to lead the fight since it develops the Strategies against cybercrime. Moreover, regarding the new challenges, the Commission together with the High Representative,

proposed a wide-ranging package of cybersecurity proposals aiming to: Building EU resilience to cyber-attacks and stepping up the EU's cybersecurity capacity, creating an effective criminal law response and strengthening global stability through international cooperation[78]. These proposals are the core of the competence of the Commission which has an initiative competence. Also, the proposals of April 2018 regarding electronic evidence can be remembered.

In September 2018, the European Commission proposed the creation of a Network of cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence, aiming to help the Union retain and develop the capacities necessary to secure its Digital Single Market by coordinating the work of the Community inside cyberspace. These measures from the Commission seem full of ambition since they plan on creating new mechanisms and procedures which are breaking significantly with former status. Thus, the Commission seem to be willing to solve the emergency situation of cybercrime, in order to promote competitiveness of the European Union's cybersecurity industry and turning it into an advantage of other European Industries.

The Commission is already building a new strategy for 2021-2027. It will help the Member States to take a more proactive approach of cybersecurity, and not only stakeholders needing to create solutions to cybersecurity challenges. In short, the Commission is willing to delegate more responsibility to the Member States regarding cybercrime instead of carrying the burden alone of the promotion of cooperation between Member States.

Furthermore, the Commission is leading a fight against cybercrime by helping in the effective implementation of the first cybersecurity law: the Directive on Security of network and Information Systems (NIS Directive) entered into force in August 2016. In fact, Member States had to transpose the Directive into their national laws by 9 May 2018[79], but was more complicated in practice. This Directive requires Member States to be appropriately equipped via a Computer Security Incident Response team (CSIRT), in order to bring up the standards of defence. The Directive also ensures cooperation among Member States by setting up cooperation groups which are aiming to achieve high common

[78] *Idem*: REHRL, J. The Common Security and Defence Policy of the European Union. *European Handbook on Cybersecurity*, 2018. p.80

[79] European Commission, *The Directive on security of network and information systems.* Available at : <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

level of security network and sharing information regarding cybercrime. Finally, the Directive intends to ensure a culture of security across sectors vital society and that rely heavily on Communication technologies, such as energy, transport or water. Therefore, it is understood that the Commission through this Directive intends to bring up higher defence standards in European Union. The Commission also works to ensure the full implementation of Directive 2013/40/EU on attacks against information systems.

We can see that the Commission is playing a significant role in the fight against cybercrime inside the European Union. This Institution is central and coordinates all the actions of the other European Institutions, as well as Member States. The European Commission although doesn't gather the all keys of the functioning in its hands. Other Institutions are extremely important, such as EUROJUST.

2. EUROJUST

The mission of Eurojust is to support judicial coordination and cooperation between national authorities to combat terrorism and serious organised crime affecting more than one EU country where it coordinates investigations and prosecutions. Besides it helps to resolve conflicts of jurisdiction and facilitates the drafting and implementation of EU legal instruments, such as European Arrest Warrants and confiscation and freezing orders, for example.

Each year, Eurojust opens a growing number of cases and holds about 250 coordination meetings and runs 10 coordination centres. We can see that Eurojust is a very active institution that promotes the cooperation between States. Therefore, its action is primary since cooperation in judicial matters is essential in the fight against cybercrime.

A recent development from the 12th of December 2019, became officially an Agency for Criminal Justice Cooperation with the application of Eurojust Regulation[80]. This new regulation makes Eurojust more liable to fight increasing levels of cross-border crime. It now has an Executive Board dealing with administrative matters and it gives the college of prosecutors from all Member States a wider liberty to focus on the rising number of criminal cases. An exception concerns Denmark who isn't bound by Eurojust's regulation. Thus, a cooperation agreement between Denmark and Eurojust was enacted. It requires

[80] 14 November 2018. European Parliament and the Council Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council decision 2002/187/JHA

new representatives who will be allowed to assist the meetings without any voting competence.

Furthermore, this change brings a new data protection regime, adapting it to the revised EU legal framework on data protection. It also strengthens the role of the European and national Parliaments in Eurojust's activities.

Eurojust was promoted to a higher rank of institution inside the European Union, showing its importance and the importance of judicial cooperation, confronted to the increasing number of criminal cases. The role played by the European Defence Agency (EDA) must now be considered.

3. The European Defence Agency (EDA)

The European Defence Agency (EDA) was developed in 2004 as an intergovernmental agency of the Council of the European Union under a Joint Action of the Council of Ministers[81]. It supports 27 States, all Member States except for Denmark, to improve their defence capabilities through European cooperation. In 2011, the Joint Action was replaced by a Council Decision[82] in order to implement the provisions of the Lisbon Treaty (Art 42 TEU).

The EDA has three main missions. The first one is to give a support to the development to defence capabilities and military cooperation among the European Union Member States. The second mission concerns the need to stimulate defence Research and Technology and strengthen the European defence industry. Finally, it acts as a military interface to EU policies.

Thus, the EDA has a role of monitor which ensures coherence among European Union's defence tools. In fact, through the EU Global Strategy from 2016[83], the EU raised the necessity to obtain a more coherent European defence landscape. To that end, Member States set up EU defence cooperation tools such as the Coordinated Annual Review on

[81] 12 July 2004. Council Joint Action 2004/551/CFSP of on the establishment of the European Defense Agency

[82] 12 October 2015. Council Decision (CFSP) 2015/1835 of defining the statute, seat and operational rules of the European Defence Agency

[83] European Union external action, *A Global Strategy for the European Union's Foreign and Security Policy*, 15 December 2015. Available at : <https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy_en>

Defence (CARD) or the Permanent Structured Cooperation (PESCO). The EDA ensures coherence between these tools.

Cooperation seems like a central notion that governs the efficiency of the fight against cybercrime. It is why the European Union develops many institutions that are promoting this cooperation between Member States. Moreover, an important element regarding cybercrime is law enforcement.

A. Organs for law enforcement

Law enforcement is also an essential matter on the fight against cybercrime, since it will ensure the right application of the law, and the sanctioning of criminal acts. Thus, it plays a role of guardian of the application of European law. In that regard, the main institution on law enforcement is EUROPOL (1). Besides, other specialised agencies are performing significant actions in the fight against cybercrime such as The European Agency for Law Enforcement Training (CEPOL) (2). Furthermore, the action of a specialised agency which protects the European Union, named the CERT-EU (3) must be mentioned.

1. EUROPOL

The borderless nature of the internet allows for criminal activities that are transnational, thus, actions need to be applied to counterfeit them. Europol is the Union Agency of Law Enforcement cooperation and plays a leading role in the fight of cybercrime by offering Member States a support in terms of coordination in cross-border investigations. Europol is a law enforcement agency since 2010 which means it accountable to Justice and Home Affairs (JHA). However, it is not a European police force and doesn't have executive powers. Its mission is to provide coordination and support to the law enforcement agencies of EU Member States. In the matter of cybercrime, Europol acts through two organisations. The EC3 fights against massive criminal activities on the Internet and Dark web (a). Besides, the IPC3 aims to counter intellectual property infringements on the internet (b).

a. The EC3

The main feature of Europol regarding Cybercrime is the European Cyber Crime Centre (EC3). It was established under Europol's authority on January 2013. It was mainly created to address the growing threat from cybercrime[84]. EC3 develops analytical products such as the Internet Organised Crime Threat Assessment (IOCTA) [85], which helps other Institutions, Member States, ISPs and even citizens to get a clearer point of view of cybercrime and brings to notoriety the alarming facts regarding cybercrime. Its action is divided into three main units: Operations, Strategy and Forensic Expertise.

The Operation Unit is composed with several teams. Some of them deal with the analysis projects on cybercrime, whereas the other are Cyber Intelligence Team and Dark Web Teams. These teams provide support to the Member States in their investigations. For instance, they helped in the arrest of the leader of a group who orchestrated Carbanak and Cobalt malware attacks[86].

The Strategy & Development Teams focus on strategic analysis of cybercrime threats, meaning how technological developments can introduce new opportunities for cybercrime and how law enforcement can respond. It thus tries to be proactive facing the potential threats. The team also works on enhancing the knowledge and skills of law enforcement officials through training courses.

Together with EC3, an action against major cybercrime cases is led by the Joint Cybercrime Action Taskforce (J-CAT), established in 2014. Its objective is to drive intelligence-led coordinated action against key cybercrime threats. In 2017, together with the FBI and the DEA, Europol managed to takedown AlphaBay and Hansa which are two of the largest criminal dark web markets[87].

---

[84] VENDIUS, T. T. *Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the growing Rôle of Law Enforement on the European Security Scene*, European Journal of Policing Studies, p.153

[85] EUROPOL, the Internet Organised crime Threat Assessment (IOCTA) of 2019. Available at : <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019>

[86] EUROPOL, *Mastermind behind Eur 1 Billion cyber bank robbery arrested in Spain*, 26 March 2018. Available at :<https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>

[87] EUROPOL, *Massive blow to criminal Dark web activities after globally coordinated operation, 20 July 2017*. Available at : https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

b. The IPC3

Goods coming from counterfeit merchandising are a problem that hits the EU, accounting for about 5% of imports[88]. According to Europol "*fighting intellectual property crime is key to sustaining jobs and growth in the European economy*"[89]. This threat relates to the objectives of the cybercrime strategy issued by the Commission which requires the fight against infringement of IP rights. Besides, Intellectual Property increasingly takes place online through illegal downloading, streaming of IP protected content.

In July 2016, Europol together with the European Union Intellectual Property Office (EUIPO) launched the Intellectual Property Crime Coordinated Coalition (IPC3). The missions of the IPC3 are multiple. First, it has an operational and technical support objective which must be provided to the competent authorities. Besides, it is required to facilitate and coordinate cross-border investigations. Furthermore, it must monitor and report online crime trends and emerging modi operandi. Finally, it must enhance the harmonization of legal instruments to counter intellectual property crime globally and raise awareness of the public and law enforcement and providing training.

Europol seems to incarnate a powerful institution with a significant impact on Cybercrime through its two organisations: EP3 and ICP3. In fact, the law enforcement agency goes further than the competences of the European Commission by acting on more concrete issues. Another law enforcement institution is the European Agency for law Enforcement Training (CEPOL).

2. The European Agency for Law Enforcement Training (CEPOL)

CEPOL is an agency dedicated to developing, implementing and coordinating training for law enforcement officials. It contributes to ensuring cyber security by facilitating cooperation and knowledge sharing among law enforcement officials on the European Union's member States and thus, to third countries on issues involving external threats.

The agency creates a network of training institutes for law enforcement officials in Member States and provides trainings on security priorities and works with European

[88] EUROPOL, *2017 Situation Report on Counterfeiting and Privacy in the European Union, 22 June 2017*. Available at : <https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union>

[89] EUROPOL, *Intellectual Property Crime Coordinated Coalition – IPC3* https://www.europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3

Union's Institutions and international organisations and third countries to ensure that the most serious security threats are considered consistently.

Within CEPOL's action, many aspects of cybersecurity are covered in its annual work programme. In fact, each year the agency provides education and training such as the Cyber security and cyber defence in November 2018[90]. This training brings closer cyber strategy formulation from military and law enforcement point of view, in order to enhance capacities of cyber warfare and intelligence in the Member States. This training is destined to the senior military and law enforcement officers and diplomats possessing leadership role in the domain of cyber security and defence. Furthermore, CEPOL cooperates with other agencies in order to promote the cooperation in the areas of information exchange training, such as the Memorandum of Understanding from 2009 with the European Network of Forensic Science Institutes (ENFSI), in order to outline issues concerning both institutions, such as advances in forensic sciences that could assist criminal investigations.

The training provided to law enforcement agents is extremely important. The European Union also works with specialised IT experts who protect the European Institutions themselves against cyberattacks, the CERT-EU.

3. The CERT-EU

CERT-EU is a permanent Computer Emergency Response Team for the EU institutions, agencies and bodies. It was created on 11 September 2012, after a pilot phase of one year. It was approved, thus, the EU institutions decided to set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies. It is composed with experts on IT security from the main EU institutions such as European commission or European Parliament.

This mechanism works closely with national peers and partners in Member States. Besides, it gets its resources from the European Institutions. In the long term, CERT-EU is destined to be part of a network of Computer Security Incident Response team under the NIS Directive aiming to ensure high common level of network and information security in the EU.

[90] 12 November to 14 November 2018. Cyber Security and Cyber Defence 104/2018. Available at : <https://www.cepol.europa.eu/education-training/what-we-teach/residential-activities/1042018-cyber-security-cyber-defence>

The CERT-EU seems like a new creation ensuring cyber security at a European level and providing support to the Member States. It is therefore an important practical mean of fighting against cybercrime, by protecting States against cyberattacks. But in the practice, its effectivity is limited according to the large amount of cyberattacks remaining.

It seems that law enforcement, the sanctioning of criminal computer-related acts, and the protection against cyberattacks are central in the fight against cybercrime. However, it is a matter that carries a lot of uncertainty due to its modernity and technicity. Thus, some organs are developed to train and transfer knowledge on cybercrime.

B. Organs destined to transfer knowledge

Regarding the notion of cybersecurity, the knowledge and the training from experts is essential. In fact, the cyberspace in general is a dark matter that isn't understood by the majority. Thus, it is important for those who fight against it, to understand every aspects of that matter. Thus, several organs were funded in order to provide this knowledge. One of the most important of them is the European Union Agency for Network and Information Security (ENISA) (1). Mention is also made of the European Cybercrime Training and Education Group (ECTEG) (2).

1. The ENISA

The ENISA is the EU cyber security agency and was set up in 2004. Its role is to support the EU Commission and the Member States by giving guidance on the technicalities of network and information security, thus contributing of the proper functioning of the internal market. The Agency works closely with Member States to deliver advice and solutions as well as improving their capabilities. The ENISA is thus required to give an expert opinion on cyber technologies.

Another mission of ENISA is to support the development and implementation of the European Union's policy and law on matters relating to network and information security such as the NIS Directive.

In 2019, with the Regulation 2019/881[91] called Cybersecurity Act, ENISA has been tasked to prepare the 'European cybersecurity schemes'. ENISA appears as a promoting agency on which the European Union seems to count, to perform its task of fighting against cybercrime and drastically reducing it.

Although ENISA has a central role in the matter of transferring knowledge, other organs exist in that matter, such as the European Cybercrime and Education Group (ECTEG).

2. European Cybercrime Training and Education Group (ECTEG)

The ECTEG became officially an international non-profit association with founder members from the law enforcement academic world. It is composed of European Union and European Economic Area Member States' law enforcement agencies, international bodies, academia private industry and experts. It was funded by the European Commission and works closely with EC3 and CEPOL.

The ECTEG is working in transmitting knowledge on cybercrime at the international level. Its function is important for the internal European Union's security since many attacks directed to Europe come from third countries. Its mission is to support international activities to harmonise cybercrime training across international borders and share knowledge and expertise. It also promotes the standardisation of methods and procedures for training programmes and cooperation with other international organisations and collaborates with academic partners to establish academic qualifications in the field of cybercrime. Besides, it collaborates with industry partners to harmonise the delivery of training and thus, optimise the available resources. Finally, it provides training and education material to international partners in order to support the law enforcement on cybercrime issues globally.

[91] 17 April 2019. European Parliament and the Council Regulation (EU) 2019/881 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013. Available at : <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

CONCLUSION

1) Cybercrime is a complex notion due to its modernity, immateriality and cross-border nature. One of its main features refers to the multiplicity of forms it can take. Cybercrime seems to concern any malicious activity perpetrated using telecommunication technology devices. Facing this situation, and willing to ensure security in the Union required by the treaties, the Europeans Institutions and especially the Commission, developed a Strategy against cybercrime. This strategy acted as a kick-starter to the fight against cybercrime by setting objectives and involving Member States and European Institutions into the fight against cybercrime. It mainly encourages cooperation between Member States to improve the reaction against cross-border situations. Although hopeful, this strategy is still at the premises of its full effectivity. The European Institutions, as well as the Member States are bound to the founding treaties of the European Union, which frames their action. Thus, the European Commission assisted by the Council and the European Parliament developed an evolutive secondary law to lead the action of the Member States. A solid legal framework is being developed in order to ensure safety and competitiveness of the European Union on high-tech matters, but its effectivity is still limited according to the significant number of remaining attacks. Finally, the fight against cybercrime relies on a delicate notion, the implementation of criminal law into European law. The recent evolution of European Union law, especially with the Lisbon Treaty which reinforced the third pillar involving competences on criminal law to the European institutions. However, Member States are still reluctant to delegate all their competences in criminal law to the Union. Thus, the process of dealing with criminal activities online can be difficult. In that regard, the cooperation between Member States is essential.

2) The judicial system inside the European Union is special as it isn't equivalent to a classic State judicial system since the European Union doesn't substitute its competence to judge to the Member States. Thus, the European Union acts with distance in order to influence the judicial actions of the Member States without judging in their place. The CJEU plays an essential role in this matter. In fact, the third pillar opened criminal law to European Union. However, the law-making process doesn't allow the European Union to enact laws as such, and develops directives instead, which forces Member States to modify their legal system, with a margin of freedom in the process of implementation. The European Court plays a central role of ensuring the right application of the law, mainly through the process of preliminary ruling. Since the European Union gathers many different legal systems, sometimes with contradictions that cannot always cooperate easily. Although cooperation

isn’t perfect yet, it seems that the situation is progressing and that the European Union is attaining a certain level of homogeneity between Member States legal systems. In fact, the principle of mutual recognition is a substantial element of this cooperation, and the discretion of the Member States constituting a refusal has been significantly lowered by the Member States. The example of the European Arrest Warrant is central since it shows the increasing cooperation between Member States. Finally, the matter of electronic evidence is substantial regarding the question of judicial cooperation. In fact, evidence becomes more and more immaterial, and stored in data bases and clouds. Thus, a large cooperation program was upheld, but this system is still showing many weaknesses. To counterfeit this lack, the European Commission recently proposed an ambitious proposal that could significantly enhance the efficiency of the process. But many safeguard and conditions are still to be implemented in the project.

3) The European Commission together with EUROJUST are actively acting to ensure a large cooperation between Member States. In that regard, the European Commission is acting in order to lead the action of the Member States through major directives on the cybercrime issue, aiming to bring all of them under a same action. Other organs are trying to build a network to ensure cooperation and giving support to the Member States. Thus, it seemed from the explanation that their work is impacting efficiently the cooperation of Member States although their work isn’t fully accomplished, and many issues are to be treated under their control to ensure a better cooperation. Besides, the law enforcement aspect, mainly directed by the action of EUROPOL together with EC3 and IPC3 shows that the cybercrime deterrence expected in the European Strategy isn’t fully achieved yet. In fact, the law enforcement agencies seem to be chasing down internet related frauds and criminals. Finally, this aspect of knowledge transmission is central in the matter of cybercrime according to the modernity of this threat that breaks with former forms of crimes. Thus, the multiplication of organs that are providing trainings and advices to institutions is understandable and seems to work efficiently by sharing high knowledge and standards inside European Union’s considerations. Moreover, an important point lays in uniformizing the courses provided in order to ensure a harmonized knowledge transmitted and thus optimize the resources possessed.

LIST OF REFERENCES

INTERNATIONAL LEGAL ACTS

1. Convention on Cybercrime. *Council of Europe Portal*, 23 November 2001. ETS No. 185

EUROPEAN LEGAL ACTS

Convention

1. 1959. Council of Europe, European Convention on Mutual Assistance in Criminal Matters,
2. Article 1, Additional Protocol to the European convention on Mutual Assistance in Criminal Matters, 17 March 1978, European Treaty Series – No. 99
3. 13 december 1957. European Convention on Extradition, Paris, ETS No.024

Regulation

1. 29 September 2003. European Parliament and the Council Regulation (EC) No 1882/2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure referred to in Article 251 of the EC Treaty
2. 17 April 2018. European Commission, Regulation 2018/0108(COD) of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters
3. Proposal COM/2018/225 for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters
4. 14 November 2018. European Parliament and the Council Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council decision 2002/187/JHA
5. 17 April 2019. European Parliament and the Council Regulation (EU) 2019/881 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013. Available at : <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

Resolution

1. 3 October 2017. European Parliament resolution (2017/2068(INI)) on the fight against cybercrime. *OJ C 346, 27.9.2018, p. 29-43*
2. *Idem:* 3 October 2017. European Parliament resolution (2017/2068(INI)) on the fight against cybercrime. *OJ C 346, 27.9.2018, p. 29-43*

Recommendation

1. 13 September 1989. Committee of ministers to Member States, Recommendation R (89) 9 on Computer-Related Crimes.
2. 11 September 1995. Committee of ministers to member States, Recommendation R (95) 13 concerning problems of criminal procedural law connected with information technology

Framework Decision

1. 28 May 2001. Council of the European Union. Framework Decision 2001/413JHA on combating fraud and counterfeiting of non-cash means of payment
2. 13 December 2011. European Parliament and the Council Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA
3. 22 December 2003. Council Framework Decision 2004/68/JHA on combating sexual exploitation of children and child pornography
4. 13 June 2002. Council Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States
5. July 2003. Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property of Evidence
6. 18 December 2008. Council Framework Decision 2008/978/JHA on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for Use in Proceedings in Criminal Matters

Directive

1. 17 April 2019. European Parliament and the Council Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, and replacing Council Framework Decision 2001/413/JHA
2. 12 August 2013. European Parliament and the Council Directive 2013/40/EU on attacks against information systems, and replacing Council Framework Decision 2005/222/JHA
3. 17 April 2019. European Parliament and the Council Directive (EU) 2019/713
4. 3 April 2014. European Parliament and the Council Directive 2014/41/EU regarding the European Investigation Order in criminal matters
5. Proposal COM/2018/226 for a Directive of the European Parliament and of the council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings

Communication

1. 11 July 2018. European Economic and Social Committee, *Evidence in criminal proceedings*, COM(2018) 225 final. Avaialble at : <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/evidence-criminal-proceedings>

Joint Communication

1. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace /* JOIN/2013/01 final /*

Joint Action

1. 12 July 2004. Council Joint Action 2004/551/CFSP of on the establishment of the European Defense Agency

Council Decision

1. 12 October 2015. Council Decision (CFSP) 2015/1835 of defining the statute, seat and operational rules of the European Defence Agency

Primary law

1. Consolidated version of the Treaty on European Union, Article 3(2) and Article 5
2. Charter of Fundamental Rights of the European Union 2012/C 326/02
3. Consolidated version of the Treaty on European Union, Article 6(1)
4. Article 6(3), Consolidated version of the Treaty on European Union: "*fundamental rights, as guaranteed by the European Convention for the protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law*".
5. Article 6(1), Consolidated version of the Treaty on European Union "*The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union […], which shall have the same legal values as the Treaties*".
6. Article 288, Consolidated version of the Treaty on the Functioning of European Union
7. Treaty of Lisbon amending the Treaty of European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, 2007/C 306/01
8. Article 76 TFEU

COURT DECISION

1. CJEU. 25 October 2011. Decision *eDate Advertising v. Martinez*, Joined Cases C-509/09 and C-161/10
2. CJEU (Grand Chamber). 13 May 2014. Decision *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and mario Costeja González* Case C-131/12
3. ECJ (Grand Chamber). 13 September 2005. Decision *Commission of the European Communities v Council of the European Union* C-176/03
4. ECJ. 15 July 1964. Decision *Flaminio Costa v E.N.E.L* C-6-64
5. ECJ. 5 February 1963. Decision *Van Gend & Loss v Netherlands* C-26-62

6. ECJ. 11 November 1981. Decision *Guerrino Castati* C-203/80
7. ECJ (Grand Chamber). 12 July 2005. Decision *Commission of the European Communities v French Republic* C-304/02
8. *Idem*: CJEU (Grand Chamber). 13 May 2014. Decision *Google Spain SL and Google Inc v. Agencia Española de Proteccion de Datos (AEPD) and Mario Coste and Costeja Gonzalez*, C-131/12
9. ECJ (Third Chamber). 18 October 2012. Decision *Football Dataco Ltd and Others v Sportradar GmbH Sportardar AG* C-173/11
10. ECJ (First Chamber). 19 April 2012. Decision *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH* C-523/10
11. CJEU. 1 June 2016. Decision *Bob-Dogi* C-241/15
12. CJUE. 10 November 2016. Decision *Kovalkosas* C-477/16

ELECTRONIC DOCUMENTS

1. [online] *Cybercrime*. What is Cybercrime?. Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en
2. 18 Ocotber 2018. European Council conclusions, point 9. Available at: https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/
3. Council of Europe, *Cyber-attacks : EU ready to respond with a range of measures, including sanctions*, 19 June 2017. Available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
4. European Commission, *Primary versus secondary law*, Types of EU law. Available at: https://ec.europa.eu/info/law/law-making-process/types-eu-law_en
5. European Union Agency for Fundamental Rights. *Handbook on European law relating to cybercrime and fundamental rights*. Available at: https://fra.europa.eu/en/project/2018/handbook-european-law-relating-cybercrime-and-fundamental-rights
6. 20 March 2019. Eurobarometer report on Internet security and crime: *79% of the interviewed declare themselves believing that the risk of becoming a victim of cybercrime is greater than in the past*.

7. European e-justice forum, *EU law.* Available at: https://e-justice.europa.eu/content_eu_law-3-en.do
8. European Commission, *Cybercrime*, Migration and Home Affairs. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en
9. Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA COM/2017/0474 final. Available at: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52017DC0474
10. EUROPOL, iOCTA, 2019: https://www.europol.europa.eu/iocta-report
11. ROZMUS, M.; TOPA, I.;, WALCZAK, M. The *Current Status and the Impact of the Treaty of Lisbon,* Harmonisation of Criminal Law in the EU Legislation. Available at : <http://www.ejtn.eu/Documents/Themis/THEMIS%20written%20paper%20-%20Poland%201.pdf>
12. *Idem :* ROZMUS, M.; TOPA, I.;, WALCZAK, M. The *Current Status and the Impact of the Treaty of Lisbon,* Harmonisation of Criminal Law in the EU Legislation
13. Council of Europe, Details of Treaty No.030. Available at : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030>
14. Council of Europe, Details of Treaty No 182. Available at : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182>
15. European Parliament, *Judicial cooperation in criminal matters,* Fact Sheets on the European Union. Available at : <http://www.europarl.europa.eu/factsheets/en/sheet/155/la-cooperation-judiciaire-en-matiere-penale>
16. Commission Notice, *Handbook on How to issue and execute a european arrest warrant,* 28 September 2017. Available at : <https://e-justice.europa.eu/content_european_arrest_warrant-90-en.do>
17. 28 August 2019. Commission Staff Working Document, *Replies to questionnaire on quantitative information on the practical operation European arrest warrant* year 2017

18. Commission staff working document impact assessment accompanying the two documents, SWD/2018/118 final. Available at : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:118:FIN>
19. EUROPOL, the Internet Organised crime Threat Assessment (IOCTA) of 2019. Available at : <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019>
20. EUROPOL, *Mastermind behind Eur 1 Billion cyber bank robbery arrested in Spain*, 26 March 2018. Available at :<https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>
21. EUROPOL, *Massive blow to criminal Dark web activities after globally coordinated operation, 20 July 2017*. Available at : https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
22. EUROPOL, *2017 Situation Report on Counterfeiting and Privacy in the European Union, 22 June 2017*. Available at : <https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union>
23. EUROPOL, *Intellectual Property Crime Coordinated Coalition – IPC3* https://www.europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3
24. 12 November to 14 November 2018. Cyber Security and Cyber Defence 104/2018. Available at : <https://www.cepol.europa.eu/education-training/what-we-teach/residential-activities/1042018-cyber-security-cyber-defence>

PRINTED MONOGRAMS

1. REHRL, J. The Common Security and Defence Policy of the European Union. *European Handbook on Cybersecurity*, 2018. KUNASEK, M. <Forewords>
2. DE HERT, P.; GONZÁLEZ FUSTER, G.; and KOOPS, B. *Fighting cybercrime in the two Europes*, Revue Internationale de droit pénal 2006/3-4 -Vol.77, p.503
3. CSONKA, P. *The council of europe's convention on cyber-crime and other European initiatives*. Revue Internationale de droit penal, 2006/"-4 (Vol.77), p.473

4. W BRENNER, S. *The Role of Penal and Procedural law*, Cybercrime Investigation and Prosecution, university of Dayton School of Law. Cybercrime: An Overview of the Problem, p.11
5. Idem: DE HERT, P.; GONZÁLEZ FUSTER, G.; and KOOPS, B. *Fighting cybercrime in the two Europes*, Revue Internationale de droit pénal 2006/3-4 - Vol.77, p.506
6. CHRISTOU, G. *Cybersecurity in the European Union* 2016, p.87
7. OSULA, A. *Mutual Legal Assistance & Other Mechanisms For Accessing Extraterritorially Located Data.* DOI 10.5817/MUJLT2015, Estonia, 2018. p.49
8. *Idem*: REHRL, J. The Common Security and Defence Policy of the European Union. *European Handbook on Cybersecurity*, 2018. p.80
9. VENDIUS, T. T. *Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the growing Rôle of Law Enforement on the European Security Scene*, European Journal of Policing Studies, p.153

ARTICLES

1. RAIN, O. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Talinn : Cooperative Cyber Defence Centre of Excellence, 2018. Available at : <https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>
2. OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 23 September 1980.
3. Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/
4. European Commission, *Why do we need the Charter?*, What it covers. Available at: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en#relatedlinks
5. European Parliament, *Competences of the Court of Justice of the European Union.* Available at :

<https://www.europarl.europa.eu/factsheets/en/sheet/12/competences-of-the-court-of-justice-of-the-european-union>

6. European Commission, *Electronic evidence, expertly explored*. Available at : <https://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/headlines/news/article_17_03_16_en.html?infocentre&item=Infocentre&artid=43496>
7. Legislative Train Schedule, *European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, Area of Justice and Fundamental Rights, , 2017. Available at : <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders>
8. 17 October 2018. European Data Protection Board 2018/0107(COD). Available at : <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/evidence-criminal-proceedings>
9. European Commission, *The Directive on security of network and information systems*. Available at : <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>
10. European Union external action, *A Global Strategy for the European Union's Foreign and Security Policy*, 15 December 2015. Available at : <https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy_en>

SUMMARY

The use of tele communication devices is more and more frequent and develops the economy of modern society. This development is accompanied with missuses which consist in cybercrime. This notion brings up many challenges due to its modernity, immateriality and its cross-border nature. The thesis aims to determine what are the means used to fight against cybercrime and assess their effectivity.

The argumentation focuses on three different aspects. The textual legal instruments developed to fight against cybercrime (1). The judicial aspect, the role of the Court, the judicial cooperation and the matter of evidence (2). The organic aspect and the stakeholders acting against cybercrime (3).

The thesis argues that the fight against cybercrime is at its beginning. The European Institutions are trying hard to be as protective as possible by updating the legal background on that notion, but cybercrime also evolves on its side. However, a core legal system is being built, according to which cooperation between Member States is highly encouraged. Furthermore, judicial cooperation is also a central notion to the fight against cybercrime. With the help of the CJEU the law is being commonly applied and interpreted. Besides, the judicial cooperation supported by the principle of mutual cooperation gave the opportunity to improve the issue on evidence, and to develop a European Arrest Warrant. Finally, the organic landscape of the European Union around the notion of cybercrime is large. Many stakeholders exist, and develop a better cooperation, ensure the right application of the law, and share the knowledge relevant to fight against cybercrime.

The fight against cybercrime is difficult and the related law needs improvement. Cooperation is also important to develop. The issue gathers many concerns. Thus, the Institutions and agencies are active on that regard, meaning that cybercrime-related law will significantly evolve in the future.