UNIVERSITY OF CYPRUS - DEPARTMENT OF LAW

Master of Laws Programme (LL.M.)

SUPERVISOR: Dr CONSTANTINOS KOMBOS

MASTER THESIS

LEGAL ASPECTS OF CLASSIFIED INFORMATION IN THE EUROPEAN UNION

GEORGIA ARESTI

December 2021

Word Count: 17999

ACKNOWLEDGMENTS

To my daughters, Evelina and Natalia

My sincere gratitude to my supervisor, Dr. Constantinos Kombos, for his support, guidance, motivation and immense knowledge.

Angelos, Andria, Chryssis and Andreas thank you so much for everything.

ABSTRACT

Undoubtedly, information is emerging as a powerful tool in the modern turbulent environment of security for states, organisations and individuals. This paper aims to contribute to the legal-theoretical discussion signalling that the EU values and human rights are threatened by the handling of classified information in the EU.

By analysing the legal nature of the EU Council Security Rules and its applicability to the MS, in conjunction with the supranational judicial review on human rights and fundamental freedoms, the impact of policies regarding classified information on EU values and human rights becomes more transparent. Having established that, this paper adds to the legal-theoretical understanding that EU needs to reconsider its rules regarding classified information, which must be restructured carefully in order to safeguard the rule of law, transparency, accountability and the rights of the individuals, especially the right of access to documents.

Keywords:

European Union, classified information, access to documents, national security, transparency, intelligent services, confidentiality, Court of Justice of the European Union, European Court of Human Rights, Cyprus, EU Regulation 1049/2001, Council Decision 2013/488/EU.

TABLE OF CONTENTS

ABBREVIATIONS

CI	Classified Information
CIS	Communication and Information System
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Council Decision 2013/488/EU	Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information OJ L 274/1, 15.10.2013.
ECHR	European Convention on Human Rights/ Convention for the Protection of Human Rights and Fundamental Freedoms
CSR	Council Security Rules
ECtHR	European Court of Human Rights
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCI	European Union Classified Information
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Police Office
FRONTEX	European Border and Coast Guard Agency
MS	European Union Member States
NGO	Non-governmental organization

OECD	Organization for Economic Co-operation and Development
Regulation 1049/2001	Regulation (EC) No. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 on public access to European Parliament, Council and Commission documents OJ EE L145/43, 31.5.2001.
TEU	Treaty on European Union OJ C 326/1
TFEU	Treaty on the Functioning of the European Union OJ C 326/47, 26.10.2012.
UN	United Nations

LEGAL ASPECTS OF CLASSIFIED INFORMATION IN THE EUROPEAN UNION

1

INTRODUCTION

In such a threatening and volatile environment, security has been a continuous concern for modern societies. Colossal asymmetric threats, such as terrorism, climate change, weapons of mass destruction, pandemics, cybercrime and natural hazards may come from governmental or non-governmental actors, such as terrorists, insurgents, or criminals. They can be of domestic or external nature to such threats, their *raison d'être* may be found in the instability in various parts of the world and can be connected to extremist ideology. States, international, regional, and local organizations, as well as private entities and individuals, have been constantly[1] seeking effective solutions to protect themselves.

Concurrently, energy, economic and social interests are, nowadays, the most decisive factors in achieving the goals of stability and development. The interlink between these and the rapid development of the worldwide web and technology, identifies information as one of the most critical indicators of power.[2]

EU is an important player in the international arena, especially in terms of economic and foreign policy. Externally, it is often involved in international trade negotiations, where unintended or malicious disclosure of negotiating positions can damage the Union's interests. Internally, hybrid threats and organised crime are of

[1] Citation on spies can be found in the Bible (Egyptians), in ancient Greece (Trojan horse in Homer's Iliad) and in ancient China [Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18(1) Chicago Journal of International Law 10].

[2] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (Crown 2010) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf> accessed 5 October 2021.

significant concern. Following the terrorist attacks in Paris and Brussels, in 2015 and 2016, respectively, and the on-going refugee crisis, the counterterrorism and control of EU's external borders became much more critical than before.

EU and its MS acknowledge that collaboration is essential to deal with threats and challenges created by economic volatility, climate change, energy insecurity and illegal migration.[3] Indicatively, the *ENISA Threat Landscape Report 2021* points out that cybersecurity attacks have continued to increase through the last couple of years, not only in terms of numbers but also in consequences. Finely targeted and persistent attacks on high-value data, like state secrets and intellectual property, are being methodically planned out and executed. The report also notes that it is reasonable to expect that there will be a new social and economic norm after the Covid-19 pandemic, one that will be even more dependent on a secure and reliable cyberspace.[4]

For all these reasons, more information sharing and intelligence cooperation is encouraged between MS and EU agencies in order to prevent acts that are detrimental to the Union's interests. Undoubtedly, the EU needs to shield the autonomy of its decision-making processes and information sharing between EU institutions and agencies. These are vital elements for the Union in order to be able

[3] European External Action Service, *Shared Vision, Common Action: A Stronger Europe a Global Strategy for the European Union's Foreign and Security Policy* (2016) <https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf> accessed 7 October 2021; European Parliament, *Understanding EU Counter-Terrorism Policy* (2021) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/659446/EPRS_BRI(2021)659446_EN.pdf> accessed 30 September 2021.

[4] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2021* (2021) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> accessed 29 September 2021.

to conduct its foreign and security policy, to pursue its economic interests and to ensure internal security.

In the aftermath of global counterterrorism, secrecy has become one of the most interesting global legal issues. However, while the necessity for non-disclosure and safeguarding valuable information increases, EU and its anti-terrorism and security legislation have been subject to severe criticism for the impact they have on EU values and ideals. For instance, there is evidence that core principles of the EU treaties, like openness, transparency and accountability, human rights and fundamental freedoms as enshrined in CFREU and ECHR, are negatively affected when dealing with security strategies and EUCI legal rules and policies.[5]

Paradoxically, while the balancing of security, secrecy and fundamental rights emerges as an increasing challenge for both the executive and the judicial authorities, disproportionate attention has been given to the issue by the academic community. Several scientific publications exist on EU counter-terrorism policies, but the study of EU information classification policies and its impact on MS and EU citizens remains insufficient.[6] The difficulty in accessing such policies, because quite

[5] Transparency International, 'Classified Information: A review of current legislation across 15 countries & the EU' (2014) <https://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf> accessed 30 September 2021; Vigjilenca Abazi and Maarten Hillebrandt, "The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In 't Veld" [2015] 52 Common Market Law Review 825; European Parliament, *Openness, Transparency and the Right of Access to Documents in the EU: In-Depth Analysis* (2016) <https://op.europa.eu/en/publication-detail/-/publication/32d52e3d-3cf3-11e6-a825-01aa75ed71a1> accessed 1 October 2021; Marieke de Goede and Mara Wesseling, 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39(3) Journal of European Integration 253; Pieter Van Cleynenbreugel, 'Confidentiality behind Transparent Doors: The European Central Bank and the EU Law Principle of Openness' (2018) 25(1) Maastricht Journal of European and Comparative Law 52.

[6] Vigjilenca Abazi and Maarten Hillebrandt, "The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In 't Veld" [2015] 52 Common

a lot of them are classified, partly explains this insufficiency. Mostly, it is due to the perception that this is an inter-organisational issue of lesser importance; not affecting the citizens, at least not visibly; and technical in nature.

The purpose of this paper is to contribute to the public debate on democratic oversight and scrutiny in EU, reviewing the existing EUCI legal framework in terms of legislative provisions and legal jurisprudence. Firstly, it sets the essential legal-theoretical framework: it clarifies the terminology of the research and it, briefly, describes the relevant international context. Then, it attempts a critical analysis of the current legal regime governing the protection of CI in the EU. The focus is placed on the most critical set of EU security rules, namely the CSR, established by the Council Decision 2013/488/EU. Having described CSR's legal nature, the paper then explores the applicability of the CSR to MS, both theoretically and practically. To illustrate the impact of EUCI supranational legal provisions on national level, the example of Cyprus is used. Cyprus is a unique case on the subject examined, due to its strong tradition of safeguarding human rights in harmonisation with the ECHR but especially due to the Cyprus problem. Moreover, a critical analysis of the EUCI classification system is endeavoured and an understanding on the way EUCI handling impacts EU when CI comes from third countries is attempted. The fourth chapter of the paper studies the impact on the public's right to information through the judicial review of the CJEU and the ECtHR in order to extract conclusions on the way human rights, in the sphere of public law, are affected when issues concerning

Market Law Review 825; Marieke de Goede and Mara Wesseling 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39(3) Journal of European Integration 253; Vigjilena Abazi, *Official Secrets and Oversight in the EU: Law and Practices of Classified Information* (OUP 2019).

security and protection of EUCI are raised. Finally, a number of recommendations are listed in order to add to the discussion regarding ways to overcome the deficiencies highlighted in the previous sections.

Despite the efforts made, the study inevitably faced a few challenges. Inherently, access to only publicly available and free information, along with the scarcity of relevant case law impacted on the scope of the research. Judicial decisions are generally limited on CI issues because states tend to avoid allowing proceedings concerning CI evolve before the courts. This is due to, inter alia, the negative publicity surrounding their national security and sovereignty and the difficulties arising from requirements demanding publicity of court proceedings, the rights of the accused and the disclosure of documents.[7] Especially in Cyprus, where CI and intelligent services, until recently, were not operating under a legislative framework, these issues were not examined under judicial review.[8]

In conclusion, EU institutions have not yet adequately detected the significant impact of EUCI handling on EU citizens' lives. The existing situation in the EU prioritizes secrecy while the current legislative regime suffers from fragmentation, complexity, and vagueness. Furthermore, the status quo fails to provide adequate protection for the citizens' fundamental rights. Moreover, even though the existing legal framework on EUCI is mandatory for the MS, the EU does not provide the

[7] Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Michigan Journal of International Law 687.

[8] Instead, they were exempted as 'acts of government', which are acts of the Administration that are surrounded by judicial immunity because they relate to the management of political power [Costas Paraskeva, *Κυπριακό Συνταγματικό Δίκαιο: Θεμελιώδη Δικαιώματα και Ελευθερίες* (Νομική Βιβλιοθήκη 2015); Nikos Charalambous, *Εγχειρίδιο Κυπριακού Διοικητικού Δικαίου* (3rd edn Typografia Livadioti 2016].

necessary guidance to adequately harmonise MS' national regimes. This is partly due to fact that EU introduces legislative measures based on an implied power and partly because CI issues are considered procedural rules of secondary importance. Finally, the paper aims to be used as a base for highlighting the shortcomings of the current EUCI legal framework and as an indicator of the challenges it needs to confront. By emphasising these shortcomings, governments, practitioners and analysts can identify the deficiencies and discuss ideas on the appropriate methods that need to be deployed in order to balance the interests protected by CI and human rights.

2

LEGAL-THEORETICAL FUNDAMENTALS OF THE STUDY

2.1. Terms and Definitions

Protection of CI becomes significant due to the broader 'information security' necessity. The term 'information security' aims to protect the information itself, along with the resources of an information system, from potential damage that can diminish their value. 'Information security' is also used to describe the process of protecting information; this process is usually distinguished in the stages of prevention, detection, and reaction. As Fruhlinger interestingly notes, 'information security' is based on three fundamental factors: (a) confidentiality - ensuring that information is accessible only by authorized persons, (b) integrity - protecting the information from any undesirable alteration or destruction, and (c) availability - the ability to provide the information when requested, without hindrance or delay.[9] Ensuring the above parameters should be pursued, to the greatest possible degree, at the stages of information transfer (data in transit), during processing (data in processing) and during storing (data in storage).[10]

Another author comments that information security is achieved when

[9] Josh Fruhlinger, 'What is information security? Definition, principles, and jobs' <https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html.> accessed 25 September 2021.

[10] Ioannis Mavridis, *Ασφάλεια Πληροφοριών στο Διαδίκτυο* (ΣΕΑΒ 2015); Josh Fruhlinger, 'What is information security? Definition, principles, and jobs' (CSO 2020) <https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html.> accessed 5 October 2021.

confidentiality, validity, authenticity, integrity and availability are guaranteed. To reach these, a systematic framework of concepts, perceptions, principles, policies, procedures, techniques and measures is required in order to protect those essential elements of an information system. However, this cannot be guaranteed only by legal requirements. Therefore, the purpose of security focuses on early diagnosis of potential threats and the development of pre-emptive measures and procedures for the detection and prevention of their occurrence.[11]

Paradoxically, the most critical EU legal measure regulating CI issues, Council Decision 2013/488/EU[12] (which will be discussed in section 3.3), does not include a definition of the term 'security' or 'information security'. Instead, Article 10(1) includes the term 'Information Assurance in the field of communication and information systems', which in part resembles the above concept. This term is defined as "[…] *the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users*." It then states that effective Information Assurance shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation, and authenticity and shall be based on a risk management process. This special term used by the Council Decision 2013/488/EU is more restrictive and diminishes the status of information security sending the message of a marginal, internal procedure of trivial importance. It is an example, that EU Council treats EUCI as a procedural and technical matter;

[11] Lilian Mitrou, 'Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες: Η νομική διάσταση' in Stephanos Gritzalis, Konstantinos Lamprinoudakis, Socrates Katsikas, Lilian Mitrou (eds), *Προστασία της Ιδιωτικότηταw και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Νομικά και Τεχνικά Θέματα* (Παπασωτηρίου 2010).

[12] Council Decision 2013/488/EU, of 23 September 2013, on the security rules for protecting EU classified information [2013] OJ L 274/1.

attributing to it meaning only in terms of information systems and procedures, instead of a matter affecting a plethora of aspects of EU citizens' lives.

Focusing on the confidentiality aspect, the issue of classification emerges. CI can be defined as *information accompanied by relevant notices that serve various purposes: as a warning of their existence, as a notification of the level of classification, guidance on the disclosure of information, degradation, or declassification, provision of information on the source and reasons for classification and notification of specific access, control, or security requirements*.[13] CI may include intelligence, state or trade secrets and product development data, customer data, as well as personal and family information that is sensitive or its disclosure is not desirable. In the EU context, classifying information as EUCI guarantees the continuity of its protection when exchanged.

Classification of information is a matter that concerns other sectors as well, such as professional secrecy. For example, healthcare professionals are legally and ethically responsible for maintaining the confidentiality of information that they are made aware of or handle for the purpose of providing appropriate care. Another example is researchers ensuring the protection of the privacy of individuals involved in clinical trials and other research projects.

Interestingly there are circumstances where the need to protect information must be balanced with other important needs, such as ensuring a satisfactory level of ethics. For instance, health care professionals, in addition to their legal obligations and the duty to protect their clients' human rights, are required to balance the moral

[13] United States of America Defense Security Service, *Marking Classified Information: Job Aid* (2017).

dilemma of discretely handling sensitive information regarding the health and well-being of the patient with the protection of their own and others.

In the case of private law firms, CI may include trade secrets and product development data, customer data, as well as personal and family information that is sensitive or whose disclosure is not desirable. In general, disclosure of companies' and private legal entities' CI, may result in loss of income and/or civil or other liability. A shortfall on handling CI can lead to serious damage of the company's reputation, as well as to the deterioration of its relationships with its partners. Moreover, disclosure of personal data may result in sanctions imposed by different data protection authorities.[14]

It is critical though not to confuse CI with intelligence, which is only a part of CI. Intelligence is about secret information collected by intelligence agencies which is then supplied to policymakers and executive authorities in order to provide the necessary support when making decisions concerning national security.[15]

This notion of national security becomes relevant in the broader field of CI as well and it is quite regularly part of political and legal debates in the EU and internationally. However, there is incoherence and legal uncertainties inherent to the term 'national security'. An accurate definition of what national security means is absent from EU and worldwide. The few definitional features that appear in MS' legal

[14] European IPR Helpdesk, *Fact Sheet: How to Manage Confidential Business Information* (2015) <https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-How-to-Manage-Confidential-Business-Information.pdf> accessed 30 September 2021.

[15] Tuomas Ojanen, "Administrative counter – terrorism measures – a strategy to circumvent human rights in the fight against terrorism?" in D. Cole, F. Fabbrini and A. Vedaschi (eds), *Secrecy, National Security and the Vindication of Constitutional Law* (Edward Elgar Publishing 2013).

regimes[16] and doctrinal practices fail to meet legal certainty and rule of law principles, such as the "in accordance with the law" test.[17] This frequently leads to a disproportionate degree of appreciation for the executive and over-protection from independent judicial oversight. The disparities and heterogeneous national legal protection regimes indicate that citizens who are suspects in judicial procedures are protected differently or to divergent degrees across the EU and elsewhere. There are variable 'areas of justice' when it comes to the rights of defence of suspects in cases dealing with national security and state secrets. This diversity is at odds with the ambition of achieving non-discrimination between EU nationals when it comes to the delivery of fundamental rights.[18] Nevertheless, before focusing on the EU, a brief review of the international legal status quo on CI and secrecy handling is useful in order to frame the broader picture.

2.2 The International Legal Order

There are no international regulatory acts that address issues related to CI. Culpable actions that may be related to CI and which are punishable, are scattered in

[16] For more information, see European Court of Human Rights Research Division, *National Security and European Case-Law* (European Court of Human Rights 2013).

[17] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights* safeguards *and remedies in the EU Mapping Member States' legal frameworks* (Publications Office of the European Union, 2015); Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer, *National Security and Secret Evidence in legislation and before the Courts: Exploring the Challenges* (European Parliament 2014) <https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf> accessed 30 September 2021.

[18] Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer, *National Security and Secret Evidence in legislation and before the Courts: Exploring the Challenges* (European Parliament 2014)<https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf> accessed 30 September 2021.

various provisions of international law, such as the *Rome Statute of the International Criminal Court*,[19] the *International Covenant on Civil and Political Rights*[20] and the *ECHR*.

The umbrella of espionage/intelligence activities, which is a relative field,[21] is also characterised by scarcity, confusion and ambiguity of regulation despite the occasional concerns that have been recorded. International treaties are generally silent about intelligence, except minor exceptions, such as the *Hague Convention*, which, inter alia, provides that, in time of war, information obtained from the enemy is generally permissible.[22] The UN Charter provides little guidance on these issues. On one hand, the purposes of the UN,[23] with particular emphasis on paragraphs 1 and 3

[19] Rome Statute of the International Criminal Court (adopted on 17 July 1998, entered into force on 1 July 2002) 2187 U.N.T.S. 90.

[20] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

[21] For more information about espionage and intelligence activities in international law see Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Michigan Journal of International Law 687; Michael Defeo, 'What international law controls exist or should exist on intelligence operations and their intersections with criminal justice systems?' (2007) 78(1) Revue Internationale De Droit Pénal 57.

[22] Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Michigan Journal of International Law 687; Michael Defeo, 'What international law controls exist or should exist on intelligence operations and their intersections with criminal justice systems?' (2007) 78(1) Revue Internationale De Droit Pénal 57; Afsheen J. Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 Mich. J. Int'l L. 595; Maria Daniella Marouda, 'Διεθνές ανθρωπιστικό δίκαιο των ενόπλων συρράξεων' in Constantinos Antonopoulos and Constantinos Magliveras (eds), *Το Δίκαιο της Διεθνούς Κοινωνίας* (Νομική Βιβλιοθήκη 2017).

[23] Article 1: "The Purposes of the United Nations are:

(1) To maintain international peace and security, and to that end: to take effective collective measures for the prevention aAnd removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;

(2) To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;

of Article 1 and in conjunction with Articles 2(3)[24] and 2(4)[25] of the Charter, shall not permit action against the territorial integrity or political independence of a State. On the other hand Articles 33 and 51, although they do not authorize the act of collecting information, it is an inherent right in the context of self-protection.[26] The deadlock in establishing an international framework for espionage is acutely described by Radsan:

> *«[...] Around and around we go with the second oldest profession. What we do to them is "gathering intelligence"-something positive, worthy of praise. What they do to us is "performing espionage" -something negative, worthy of punishment. But without the negative sign that depends on the circumstances, X equals X. Gathering intelligence is just the flip side of performing espionage, and performing espionage is just one part of a country's broader effort for survival. Beyond any international consensus, countries will continue to perform espionage to serve their national interests. Negative or positive, it all depends on who does what to whom. International law does not change the reality of espionage. [...] Espionage dates from the beginning of history, while*

(3) To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and

(4) To be a centre for harmonizing the actions of nations in the attainment of these common ends."

[24] Article 2(3): "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."

[25] Article 2(4): "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

[26] Michael Defeo, 'What international law controls exist or should exist on intelligence operations and their intersections with criminal justice systems?' (2007) 78(1) Revue Internationale De Droit Pénal 57.

> *international law, as embodied in customs, conventions, or treaties, is a more recent phenomenon. They are also based on contradictory principles. The core of espionage is treachery and deceit. The core of international law is decency and common humanity. This alone suggests espionage and international law cannot be reconciled in a complete synthesis. Perhaps we should leave it at that[...]».*[27]

Some other relevant issues to CI, like cybersecurity and cybercrime, have been regulated to some extent. An example is the Council of Europe *Convention on Cybercrime*, known as the *Budapest Convention*.[28] This Treaty serves as a guideline for any country developing comprehensive national cybercrime legislation and as a framework for international cooperation between the parties to the Treaty.[29] Also relevant is the *African Union Convention on Cyber Security and the Protection of Personal Data*[30] and the *Protocol Additional to the Geneva Conventions*[31] of August 1949.[32]

There are also some other transnational relevant documents issued by international organizations, such as the OECD's *"Guidelines for the Security of*

[27] Afsheen J. Radsan, The Unresolved Equation of Espionage and International Law, (2007) 28 Mich. J. Int'l L. 595.
[28] Council of Europe, Convention on Cybercrime (ETS No. 185) (adopted on 23 November 2001, entered into force on 01 July 2004).
[29] https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[30] African Union, African Union Convention on Cyber Security and the Protection of Personal Data (adopted 27 June 2014) <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf> accessed 30 September 2021.
[31] United Nations, Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 <https://www.ohchr.org/EN/ProfessionalInterest/Pages/ProtocolI.aspx> accessed 1 October 2021.
[32] Raphael Bitton, 'The Legitimacy of Spying Among Nations' (2014) 29(5) American University International Law Review 1009.

Information Systems and Networks: Towards a Culture of Security" [33] and NATO's "*Tallinn Manual of Cooperative Cyber Defence Centre of Excellence",* but of course these are not universally binding.[34]

The international standard ISO/IEC 27014 developed by the International Organization for Standardization, is a newly developed tool, which is based on its ancestor ISO/IEC 27001. The standard provides guidance on concepts, objectives and processes for the governance of information security. Its use allows organizations of any kind to manage security of their assets such as financial information, intellectual property, employee data or information outsourced.[35] In addition to the above, useful information can be gleaned from an OECD publication[36] which presents the results of a comparative analysis of the critical information infrastructure protection policies between Australia, Canada, Korea, Japan and the Netherlands, United Kingdom, and the USA. This report shows that the above-mentioned countries had their own clear policies and objectives for the protection of these infrastructures, adapted to their own culture. One of the most important findings highlighted by the OECD is the commitment and support of respective governments, through the structures and organization of government roles and responsibilities. It was further revealed that the seven countries had similar security

[33] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2015) <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf> accessed 5 October 2021.
[34] Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18(1) Chicago Journal of International Law 10.
[35] ISO, <https://www.iso.org/isoiec-27001-information-security.html> accessed 30 September 2021.
[36] OECD, "Development of Policies for Protection of Critical Information Infrastructures", 130 OECD Digital Economy Papers (OECD Publishing, Paris) <https://www.oecd-ilibrary.org/docserver/231008575813.pdf?expires=1638947808&id=id&accname=guest&checksum=01F1858307AAD75DF5E596FD64A3CDAF> accessed 1 October 2021.

management systems, with a national authority that (a) is responsible for developing safety standards and guidelines, (b) ensures government compliance, (c) assesses and analyses impacts and weaknesses of the security management system's threats, and (d) had activated an effective national risk management strategy with policies and objectives, complemented by a national risk management framework with detailed organization, tools and monitoring mechanisms at all levels. Clearly, all seven countries were pursuing similar strategies to mitigate their weaknesses and threats.

Relevant impact assessments were conducted using a variety of approaches and methodologies and threat analysis was performed based on national priorities. However, no common method was found for conducting the evaluations. Nevertheless, according to the report, mapping similar roles and responsibilities for cross-border cooperation between countries has been complex due to cultural differences. However, it could be facilitated by a better understanding of the distribution of principles, responsibilities and powers of government sectors, as well as setting rules regarding events and circumstances that a nation would not be able to deal with on its own.

All seven countries[37] recognized the need for international cooperation. Furthermore, they acknowledged that the legal framework as well as culture are the biggest cross-border challenges in protecting critical information infrastructures, security against the rapid development of technology and their consequent social changes. Finally, it is noted that the exchange of information on an international and

[37] Australia, Canada, Korea, Japan and the Netherlands, United Kingdom, and the USA.

national scale, both at operational and strategic level, could be improved through the development of relationships of trust and cooperation between the CERT/CSIRT teams of governments.[38]

This last point is embodied in the plethora of bilateral agreements, regarding the exchange of information between states and organizations.[39] Noticeably, while on a bilateral and multinational organisational level, agreements have been extensively used by states for cooperation concerning CI, a universal agreement on use, protection and handling of CI had never been explored. One possible explanation may be that an accurate, widely accepted, definition of national security is non-existent, as noted in section 2.1. Another explanation may be the differences in culture as explained in the above mentioned OECD comparative analysis.

However, one might expect that the CI handling issue could have concerned the EU more than other supranational institutions. As a *suis generis* entity, strongly oriented towards homogeneity, equality and uniformity regarding several fundamental fields but especially human rights, EU could have been the pioneer in establishing an efficient regulatory framework that both protects EUCI and its citizens' freedoms.

[38] OECD, "Development of Policies for Protection of Critical Information Infrastructures" (2007) 130 *OECD Digital Economy Papers* <https://doi.org/10.1787/231008575813> accessed 1 October 2021.
[39] For example, Cyprus has concluded Security Agreements on the Exchange and Mutual Protection of CI with Bulgaria, France, Estonia, Israel (Exchange of Classified Information on Military and Defense Matters), Lebanon (ratification of the agreement expected), Montenegro, Ukraine, the Russian Federation, Slovakia, Slovenia, the Czech Republic, Austria, Romania, Latvia, Belgium (ratification of the agreement expected), Luxembourg, Poland, Hungary, Spain, Federation of Germany, the Republic of Germany, Armenia, Italy, Greece (ratification of the agreement expected), Serbia and Georgia. [Cyprus National Security Authority, <http://www.nsa.gov.cy/mod/nsa/cynsa.nsf/page13_gr/page13_gr?OpenDocument> accessed 15 October 2021].

3

THE EUROPEAN UNION LEGAL REGIME

The essence of the EU Treaties is that only unity based on fundamental values such as freedom and equality, which are protected and translated into reality by law, can be expected to last.[40] In light of this, Article 2 TEU explains the values of the Union:

> "*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to all MS in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail*."

Moreover, in accordance with Articles 4(1)[41] and 5(1)[42] TEU, the competences

---

[40] Andrej Zwitter, 'The Rule of Law in Times of Crisis: A Legal Theory on the State of Emergency in the Liberal Democracy' (2012) 98(1) Archives for Philosophy of Law and Social Philosophy 95; François Foret and Oriane Calligaro, 'Challenges and opportunities for EU governance' in François Foret, Oriane Calligaro (eds), *European values* (Routledge 2018); Konstantinos Margaritis, 'Strengthening the founding values of the EU: The potential role of the Fundamental Rights Agency' (2019) 18(1) European View 97; Kim Lane Scheppele, Dimitry Vladimirovich Kochenov and Barbara Grabowska-Moroz, 'EU Values Are Law, after All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union' (2020) 39 Yearbook of European Law 3.

[41] Article 4 TEU:

"1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the MS.

2.(…) In particular, national security remains the sole responsibility of each Member State.

3. Pursuant to the principle of sincere cooperation, the Union and the MS shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The MS shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of

not conferred upon the Union in the Treaties remain with the MS[43] and the limits of Union competences are governed by the principle of conferral.[44] Accordingly, MS have limited their legislative sovereignty. Consequently, they have created a self-sufficient European body of law that is binding on them, their citizens, and their courts.[45] In this respect, EU may adopt regulatory acts with effects equivalent to

---

the Treaties or resulting from the acts of the institutions of the Union. The MS shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives."

[42] Article 5 TEU:

"1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality.

2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.

3. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.

The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol.

4. Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.

The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality.

[43] Case 22-70 *Commission of the European Communities v Council of the European Communities* EU:C:1971:32; Case 9-72 *Georg Brunner KG v Hauptzollamt Hof* EU:C:1972:81; C-280/93 *Federal Republic of Germany v Council of the European Union* EU:C:1994:367; C-466/93 *Atlanta Fruchthandelsgesellschaft mbH and others v Bundesamt für Ernährung und Forstwirtschaft* EU:C:1995:370.

[44] For more information on the principle of conferral, see Marise Cremona, 'External competences and the principle of conferral', in Robert Schutze and Takis Tridimas (eds), *Oxford principles of European Union law* (OUP 2018) 1110.

[45] Case 26-62 *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* EU:C:1963:1; Case 6-64 *Flaminio Costa v E.N.E.L.* EU:C:1964:66; Case 11-70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* EU:C:1970:114; Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal* SpA EU:C:1978:49; Joined cases C-10/97 to C-22/97 *Ministero delle Finanze v IN.CO.GE.'90* EU:C:1998:498.

those adopted under national sovereignty.

Pursuant to Article 4(2) TEU, national security remains the sole responsibility of each MS. However, EU institutions, in order to execute their multiple competences and powers effectively, need to handle information. Further, in most cases such information must be treated with care in order to protect the Union's interests. In addition, the EU is known to have established several bodies with roles and capabilities in the collection, analysis, and operation of information, such as EUROPOL, FRONTEX, the European Union Intelligence and Situation Center and others. In order for these institutions to implement their roles, the need for EUCI legislative rules had emerged.

3.1 The Anterior Legal Situation

Even though pursuant Article 240 TFEU,[46] national security remains under the sovereign domain of competence of each MS, the EU gathers and analyses information autonomously in order to be able to make decisions on matters of its competences. The first EU classification system was launched in 1958 when the

[46] Article 240 — (ex Article 207 TEC):
"1. A committee consisting of the Permanent Representatives of the Governments of the MS shall be responsible for preparing the work of the Council and for carrying out the tasks assigned to it by the latter. The Committee may adopt procedural decisions in cases provided for in the Council's Rules of Procedure.
2. The Council shall be assisted by a General Secretariat, under the responsibility of a Secretary-General appointed by the Council.
The Council shall decide on the organisation of the General Secretariat by a simple majority.
3. The Council shall act by a simple majority regarding procedural matters and for the adoption of its Rules of Procedure."

Euratom Classified Information[47] had been established together with a security vetting infrastructure. On 19 March 2001, pursuant to Article 207(3) of the TEU and Article 24 of the then Decision 2000/396/EC,[48] the Council adopted Decision 2001/264/EC,[49] forming its own internal rules on classification of documents.[50] It is noteworthy that this decision entered into force[51] just two months before the adoption of the new legislative rules on public access to documents, a subject analysed in this study's *Chapter 4 - The Impact on EU Citizens' Fundamental Rights – The Right of Access to Information*. In December of the same year, the Commission followed the Council's lead by adopting its own internal security rules.[52]

In the course of time these decisions had been replaced by the Council Decision 2011/292/EU[53] of 31st March 2011 on the security rules for protecting EUCI. According to the preamble of this Decision, this legal act was taken because it was considered appropriate for the Council to establish a comprehensive security system for protecting CI covering the Council, its General Secretariat and the MS, in order to develop its activities in all areas which require handling EUCI. The word 'appropriate'

[47] Regulation No.3 implementing Article 24 of the Treaty establishing the European Atomic Energy Community [1958] OJ L17/406.
[48] 2000/396/EC, ECSC, Euratom: Council Decision of 5 June 2000 adopting the Council's Rules of Procedure [2000] OJ L 149/21.
[49] As stated in the preamble to the Decision in question, its purpose was to establish an integrated security system covering the Council, its General Secretariat, and the MS to develop the Council's activities in areas where confidentiality is required, but also to concentrate in a single text all the previous decisions and provisions that had been adopted in the specific field.
[50] 2001/264/EC: Council Decision of 19 March 2001 adopting the Council's security regulations [2001] OJ L 101/1.
[51] On 1st December 2001.
[52] Commission Decision 2001/844/EC,ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure [2001] OJ L 317/1.
[53] Based on Article 240(3) TFEU and on Decision 2009/937/EU, Rules of procedure of the Council of the European Union [OJ L 325/35].

in this context has a different meaning than usual, and thus it can be inferred that this EU legislation initiative could have been avoided or the whole issue otherwise handled. For example, the Council could have elaborated on Decision 2009/937/EU,[54] which was also based on Article 240(3) TFEU.

Furthermore, the framework set only basic principles and minimum standards to the Council and the General Secretariat and should be respected by the MS in accordance with their respective national laws and regulations so that each may be assured that an equivalent level of protection is afforded to EUCI. Under these new rules, classification of documents could be justified by simply invoking in general terms “the interests of the European Union and its MS”. The spectrum of these rules turned out to be much farther reaching in terms of scope and width of application than its 2001 precursor and constituted an illustration of the expanded scope of supranational executive activity in the EU context. The same philosophy characterises the existing framework as well.

3.2 The Current Framework

In this section a broad overview of the legal framework of the EU will be presented, focusing on Council Decision 2013/488/EU, i.e. the CSR in force. The general legal framework for EUCI applicable to the Council, European Council, General Secretariat of the Council and MS consists of the following decisions, rules, policies, and guidelines:

[54] Council Decision of 1 December 2009 adopting the Council's Rules of Procedure (2009/937/EU) [2009] OJ L 325/35.

No.	Title
1	The Council Decision on the Security Rules for Protecting EU Classified Information 2013/488/EU[55]
2	Decision 33/2028 of the Secretary-General of the Council implementing in the GSC the Security Rules for Protecting EUCI (Council Decision 2013/488/EU)[56]
3	Business ownership and security risk acceptance for IT platforms or systems and platforms processing documents and files for Council decision-making[57]
4	Information Assurance Security Policy on Security throughout the Communication and Information System Life Cycle[58]
5	Information Assurance Security Guidelines on CIS Security Accreditation[59]
6	Information Assurance Security Guidelines on System-specific Security Requirement Statement (SSRS)[60]
7	Information Assurance Security Guidelines on Security Operating Procedures (SecOPs)[61]
8	Policy on creating EU Classified Information[62]
9	Policy on registration for security purposes[63]
10	Guidelines on marking EU classified information[64]

[55] [2013] OJ L 274/1.
[56] DE 33/18 of 28 August 2018.
[57] ST 6888/16 LIMITE of 9 March 2016 and ST 7386/16 of 2 May 2018 (approved by Coreper).
[58] ST 16268/12 of 16 November 2012.
[59] ST 10346/14 LIMITE of 28 May 2014.
[60] ST 16085/13 of 14 November 2013.
[61] ST 16086/13 of 14 November 2013.
[62] ST 10872/11 LIMITE of 30 May 2011.
[63] ST 16751/11 of 11 November 2011.
[64] ST 10873/11 of 23 August 2011.

11	Guidelines on downgrading and declassifying Council documents[65]
12	Policy on security awareness and training[66]
13	Guidelines on procedures in case of EUCI compromise[67]
14	Guidelines on industrial security[68]
15	IA Security Policy on Cryptography IASP 2[69]
16	IA Security Policy on Public Key Infrastructure[70]
17	IA Security Guidelines on the Application of the Policy on Cryptography IASG 2-01[71]
18	IA Security Guidelines on Second Party Evaluation IASG 2- 02[72]
19	IA Security Guidelines on Approval of Cryptographic Products IASG 2-04[73]
20	IA Security Policy on Interconnection IASP 3[74]
21	IA Security Guidelines on Boundary Protection Services IASG 3-02[75]
22	IA Security Policy on Network Defence IASP 4[76]
23	IA Security Guidelines on Network Defence IASG 4-01[77]

[65] ST 14845/11 of 28 September 2011.
[66] 5998/15.
[67] 12207/17.
[68] 15643/16 5156/1/21 REV 1 JST 15 SMART LIMITE EN.
[69] ST 10745/11.
[70] ST 11660/13.
[71] ST 12022/13.
[72] ST 13910/12.
[73] ST 10199/19.
[74] ST 6488/15.
[75] ST 139909/12.
[76] ST 8408/12.
[77] ST 9650/15.

24	IA Security Guidelines on Intrusion Detection and Prevention in CIS IASG 4-02[78]
25	IA Security Guidelines on CIS Security Incident Handling IASG 4-03[79]
26	IA Security Policy on CIS Security Engineering IASP 5[80]
27	IA Security Guidelines on Access Control IASG 5-04[81]
28	IA Security Guidelines on Web Applications IASG 5-06[82]
29	IA Security Guidelines on Data Separation IASG 5-07[83]
30	IA Security Policy on TEMPEST IASP 7[84]
31	IA Security Guidelines on Selection and Installation of TEMPEST Equipment IASG 7-01[85]
32	IA Security Guidelines on TEMPEST Zoning Procedures IASG 7-02[86]
33	IA Security Guidelines on User generated Passwords and Password Management IASG BP-08[87]

The European Commission issued the Commission Decision (EC, Euratom) 2015/444 on security rules for the protection of EU classified information on 13

[78] ST 7867/15.
[79] ST 7049/16.
[80] ST 10416/15.
[81] ST 17547/13.
[82] ST 7124/13.
[83] ST 12131/14.
[84] ST 16311/12.
[85] ST 14006/13.
[86] ST 9507/16.
[87] ST 17745/11.

March 2015, which replaced its initial decision[88] of 2001. Furthermore, special internal rules apply to the Commission laid down by Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission.[89] Moreover, on 17 October 2019, the Commission issued Commission Decision 2019/1961.[90] Several other Commission Decisions and guidelines are in force forming the framework of handling EUCI.

The European Parliament issued[91] the European Parliament decision of 13 September 2012 on the conclusion of an interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of CI held by the Council on matters other than those in the common foreign and security policy.[92]

Finally, the European External Action Service of the High Representative of the Union for Foreign Affairs and Security Policy issued its own multi-page document on security rules.[93] EU agencies and bodies established under Title V Chapter 2 of the TEU, such as EUROPOL and EUROJUST apply their own rules of EUCI, which are the basic principles and minimum standards laid down in the Council's Decision for protecting EUCI, as provided for in their respective founding acts. At the same time,

[88] Initially issued Decision 2001/844/EC, ECSC, Euratom: Commission Decision, of 29 November 2001, amending its internal Rules of Procedure [2001] OJ L 317/1.
[89] [2015] OJ L 72/41.
[90] Commission Decision (EU, Euratom) 2019/1961 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information *[2019]* OJ L 311/1.
[91] Based, among others, on Articles 1(2), 2, 6, 10 and 11 of the TEU and Articles 15 and 295 of the TFEU.
[92] [2013] OJ C 353E/156.
[93] Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service [2018] OJ C 126/1].

other EU Resolutions of bilateral level, as well as internal documents of bodies such as EUROPOL, the European Central Bank and ENISA, are also in force. As stated in the texts of the European executive bodies, the Commission, the Council and the European External Action Service are committed to applying equivalent safety standards for the protection of EUCI. The plethora of bodies involved in handling EUCI on European and national level is another factor that adds confusion to the already foggy ground. This demonstrates an unclear strategy and a rather debatable level of expertise and specialisation.

The above puzzle of legislation and stakeholders gets even more complicated, considering the regulations that are also in force in the wider field of information protection. Examples of these are Regulation (EU) 2019/881, widely referred to as the Cybersecurity Act,[94] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,[95] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents[96], and the General Data Protection Regulation.[97]

This patchwork of rules and standards is the result of the fact that, unlike most

[94] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15.
[95] [2016] OJ L 194/1.
[96] [2001] OJ L 145/43.
[97] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

democratic regimes, the legal framework governing CI in the EU developed gradually and incrementally rather than as a specific legislative measure dedicated to the subject.[98] This is possibly due to the implied power of the EU in the field of securing CI along with the perception that handling EUCI is purely a procedural matter. The pluralism of provisions, although it can serve the specific purposes and institutional responsibilities of each body, undoubtedly creates complexity and inhomogeneity. The current regime fails the test of clarity, while gaps and incompatible arrangements between MS and the EU institutions themselves make it difficult to enforce effectively.

There is also an important accountability gap, since oversight bodies (European Parliament, European Commission, Court of Auditors) did not adequately address the issue. The unsurmountable issue of complexity and vagueness of the relevant legal regime was only part of the discussions and suggestions of the European Court of Auditors, according to which the development of any action concerning the protection of EUCI must be in line with the general objectives of the EU security strategy. Furthermore, the body of auditors criticised the lack of measurable targets and infrequent data collection that weaken accountability, evaluation, and clear orientation towards a performance culture with built-in evaluation practices difficult.[99]

In democratic societies, any developed legal system must have a mechanism for testing the legality of such measures. Courts provide an avenue for individuals to complain about interference with their rights and to seek a remedy. In this case, EU

[98] Vigjilena Abazi, *Official Secrets and Oversight in the EU: Law and Practices of Classified Information* (OUP 2019).
[99] European Court of Auditors, *Challenges to effective EU cybersecurity policy: Briefing Paper* (2019).

Courts do have jurisdiction under Articles 263 and 267 TFEU.[100] EU courts play a key role in securing and promoting an effective implementation of the rule of law principles on which the EU has been established without interfering with the MS national sovereignty in national security matters. However, several obstacles stand in place for an individual complaining about intelligence and secrecy measures: the courts' lack of specialisation;[101] general procedural obstacles (such as costs, delays or complexity); a lack of concrete evidence; a high burden of proof for establishing the veracity of evidence, or a possible invocation of secrecy privilege (including 'neither confirm nor deny' stances). In the case of EU, the complexity increases significantly because of the Court's problematic interpretation of access to courts provided by the Treaties under Article 263[102] and the conditions a reference for a preliminary ruling must meet in order to be considered by the Court under Article 267[103] TFEU. The existing significant gaps in the fundamental right to judicial

[100] For example, see Case 294/83, *Parti écologiste "Les Verts" v European Parliament* EU:C:1986:166; Case 222/84 *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* EU:C:1986:206; C-354/04 P *Gestoras Pro Amnistía, Juan Mari Olano Olano and Julen Zelarain Errasti v Council of the European Union* EU:C:2007:115; Case C-626/11P *Polyelectrolyte Producers Group GEIE (PPG) and SNF SAS v European Chemicals Agency (ECHA)* EU:C:2013:595.

[101] For example, see ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006, para.118; ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 78; CJEU, C-300/11 *ZZ v. Secretary of the State of Home Department* EU:C:2013:363.

[102] Case 25-62, *Plaumann & Co. v Commission of the European Economic Community* EU:C:1963:17; Joined cases 41 to 44-70 *NV International Fruit Company and others v Commission of the European Communities* EU:C:1971:53; Joined cases 789 and 790/79 *Calpak SpA and Società Emiliana Lavorazione Frutta SpA v Commission of the European Communities* EU:C:1980:159; Case C-50/00 P, *Unión de Pequeños Agricultores v Council of the European Union* EU:C:2002:462.

[103] For example, see Joined cases C-320/90, C-321/90 and C-322/90 *Telemarsicabruzzo SpA and Others v Circostel, Ministero delle Poste e Telecomunicazioni and Ministero della Difesa* EU:C:1993:26; C-343/90 *Manuel José Lourenço Dias v Director da Alfândega do Porto* EU:C:1992:327; Case C-83/91 *Wienand Meilicke v ADV/ORGA F. A. Meyer AG* EU:C:1992:332; Case C-18/93 *Corsica Ferries Italia Srl v Corpo dei Piloti del Porto di Genova* EU:C:1994:195; Case C-428/93 *Monin Automobiles-Maison du Deux Roues* EU:C:1994:192; Case C-318/00 *Bacardi-Martini*

protection of individuals in the EU has for long been the subject of strong criticism from legal, scientific, academic and other parts of the society.[104] No case was found to be brought to an EU Court about anything related to the legal framework in question. This indicates the difficulty for EU citizens to complain and seek remedy in the field discussed.

The foggy scenery described above, does not become clearer when one focuses on the specific provisions concerning EUCI. To illustrate this, the CSR are analyzed below.

3.3. The Council's Security Rules (Council Decision 2013/488/EU)

On the 14th of September 2013, the Council issued Council Decision 2013/488/EU, which is currently in force. This Decision's preamble mentions that for the Council to be able to work in all areas which require the use of EUCI, a comprehensive security system is needed to protect this information. Council Decision 2013/488/EU forms the basic principles and minimum standards of security for protecting EUCI. It covers several axes, including personnel security, physical security, management of the information, information assurance, industrial security, the way EUCI is exchanged within the EU institutions or with third states and

SAS and Cellier des Dauphins v Newcastle United Football Company Ltd EU:C:2003:41; Case C-458/06 *Skatteverket v Gourmet Classic Ltd* EU:C:2008:338.

[104] For further information on access to EU Courts, see Paul Craig and Grainne de Burca, *EU Law Text, Cases and Materials* (7th edn, OUP 2020); Catherine Barnard and Steve Peers, *European Union Law* (OUP 2017); Norbert Reich, 'Judicial Protection in the EU' (2005) 1 DIREITO GV L Rev 111; Takis Tridimas, 'Knocking on Heaven's Door: Fragmentation, Efficiency and Defiance in the Preliminary Reference Procedure' (2003) CML Rev 40.

international organisations.[105] These principles and standards apply to the Council and its General Secretariat, and according to the Decision's provisions, they also need to be respected by MS when handling EUCI. In order to provide a better insight into the CSR, an analysis of their legal background, nature, applicability to MS and the system of classification used is endeavoured in the following subsections.

3.3.1 Legal background

Council Decision 2013/488/EU is legally based on Article 4 of the TEU[106] and Articles 240(3),[107] 288(4)[108] and 291(1)[109] of the TFEU. This signifies that it is not intended to execute any of the establishing purposes of the EU, to regulate a fundamental area, or to implement a collective strategy in a critical area. The articles of the treaties on which they are based, as well as the form of the legislative act, denote that the issue regulated is considered internal and procedural and is not intended to embody a comprehensive and oriented strategy or to grant any rights or

[105] European Council <https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/> accessed 25 September 2021.

[106] Article 4 TEU:
"1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the MS. 2.(…) In particular, national security remains the sole responsibility of each Member State. 3. Pursuant to the principle of sincere cooperation, the Union and the MS shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The MS shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The MS shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives."

[107] Article 240(3) TFEU:
"3. The Council shall act by a simple majority regarding procedural matters and for the adoption of its Rules of Procedure."

[108] Article 288(4) TFEU:
"4. A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them."

[109] Article 291(1) TFEU:
"1. MS shall adopt all measures of national law necessary to implement legally binding Union acts."

obligations to European citizens or the MS. Thus, it can be connoted that the CSR, which will be discussed in this Section (Section 3.3), cannot and do not harmonise national rules on national security, as that remains the sole responsibility of each MS.[110]

However, as it will be explained in the same section, factually the case is different. A simple comparison of the Council Decision 2013/488/EU to the Cybersecurity Act reveals the different approach. According to Article 1 of Cybersecurity Act, its purpose is to ensure the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience, and trust within the Union. Therefore, the Regulation on Cybersecurity Act establishes the objectives, tasks and organizational issues related to ENISA. Additionally, it lays out the framework for the establishment of European cybersecurity certification systems to ensure an adequate level of cybersecurity for information technology, services and processes, and communications in the EU, as well as to avoid internal market fragmentation of EU cybersecurity certification schemes.

It can be observed that while the same aims and objectives exist in the field of EUCI, in the field of the internal market, which, in contrast to national security and public safety, falls within the powers transferred to EU, a completely different approach is followed.

Regarding security, Article 1 of the Council Decision 2013/488/EU provides that "[…]1. *This Decision lays down the basic principles and minimum standards of security for protecting EUCI. 2. These basic principles and minimum standards shall*

[110] Klaus-Dieter Borchardt, *The ABC of EU Law* (European Union 2017).

apply to the Council and the General Secretariat of the Council and be respected by the MS in accordance with their respective national laws and regulations, in order that each may be assured that an equivalent level of protection is afforded to EUCI.[…]" and Article 24, stipulates that "[…] *The rules on security shall be adopted by the Council acting by a qualified majority […]*". Moreover the Decision explains that it applies *"where the Council, its preparatory bodies and the General Secretariat of the Council handle EU classified information (EUCI)"* and that *"In accordance with national laws and regulations and to the extent required for the functioning of the Council, the MS should respect this Decision where their competent authorities, personnel or contractors handle EUCI,*[111] *in order that each may be assured that an equivalent level of protection is afforded to EUCI.*"

3.3.2 Legal nature

The legal nature of the CSR is obvious from the title[112] of the legal act itself. Decisions are EU legal acts, the legal effects of which are set in Article 288(4) TFEU. According to this paragraph, decisions are legally binding in their entirety. The legally binding nature of decisions has been underlined by the CJEU on several occasions.[113]

Notably, Council Decision 2013/488/EU does not limit its addressees. Article 1(2) lays down how the basic principles and minimum standards of security for

[111] Emphasis added.
[112] Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information.
[113] Case 9-70 *Franz Grad v Finanzamt Traunstein* EU:C:1970:78, para. 5; C-156/91, *Hansa Fleisch v Landrat des Kreises Schleswig-Flensburg*, EU:C:1992:423, paras. 12–19; C-18/08, *Foselev Sud-Ouest*, EU:C:2008:647, paras. 15–19.

protecting EUCI create obligations for the Council, the General Secretariat and the MS. This specific provision, though, does not define or in any way limit the addressees of the security provisions. Even if a limitation of addressees was considered, it could not limit the obligations of MS under Article 4(3) TEU which sets out the principle of sincere cooperation to ensure fulfilment of the obligations arising from the Treaties and the acts of Union institutions as well as Article 291(1) TFEU to adopt all measures of national law necessary to implement legally binding Union acts. Therefore, CSR, as adopted by Council Decision 2013/488/EU, which is a decision within the meaning of Article 288(4) TFEU, are legally binding in their entirety.

3.3.3 Applicability to Member States

Bearing the above in mind, any answer to the subsequent question of whether and to what extent the CSR also apply to MS must consider the Council's competence to adopt its security rules, the MS' obligation to implement legally binding Union acts and the principle of sincere cooperation along with the principal of conferral. But, as stated above, the CSR cannot and do not harmonise national rules on national security, as that remains the sole responsibility of each MS.

The legal basis for the CSR, as is clear from the preamble to Council Decision 2013/488/EU, is Article 240(3) TFEU as further framed by Article 24 of the Council's Rules of Procedure,[114] pursuant to which the Council lays down the rules on security

[114] [2009] OJ L 325/35.

acting by a qualified majority.[115] Thus, the CSR are based on the "power of internal organisation" of the institution,[116] which authorises the Council to take appropriate measures in order to ensure its internal operation in conformity with the interests of good administration.[117] As CJEU expressed it, "*the need to ensure that the decision-making body is able to function corresponds to a principle inherent in all institutional systems*."[118]

Although relating to the internal organisation of the Council, nothing prevents the measures adopted based on Article 240(3) TFEU from having legal effect vis-à-vis third parties.[119] In fact, CJEU has repeatedly found that measures of internal organisation can have legal effects vis-à-vis third parties, especially where these measures pursue the interest of good administration.[120] Furthermore, one must certainly bear in mind that the CFREU[121] applies[122] to the discussed regime as well as the general principles of EU law.[123] The human rights dimension will be elaborated in Chapter 4.

[115] Since the CSR are not adopted acting on a proposal by the Commission or the High Representative, the so-called reinforced qualified majority under Article 238(3)(b) TFEU applies.
[116] Case 66/75 *Macevicius v Parliament* EU:C:1976:66, para. 7; Case 230/81 *Luxembourg v Parliament* EU:C:1983:32 para. 38; Joined Cases 358/85 and 51/86 *France v Parliament* EU:C:1988:431 para. 32; C-58/94 *Netherlands v Council* EU:C:1996:171 para. 37; C-345/95 *France v Parliament* EU:C:1997:450 para. 31. In Joined Cases C-7/56 and C-3/57 to C-7/57 *Algera and Others v Common Assembly* EU:C:1957:7 and Case 208/80 *Lord Bruce of Donington* EU:C:1981:194 para. 17 CJEU speaks of functional autonomy of the institution.
[117] C-58/94 *Netherlands v Council* EU:C:1996:171 para. 37.
[118] Case 5/85 *AKZO Chemie v Commission* EU:C:1986:328 para. 37.
[119] Opinion of Advocate General Léger in Case C-353/99 *Council v Hautala* EU:C:2001:392 para. 103.
[120] C-137/92 P *Commission v BASF and Others* EU:C:1994:247 paras. 75 and 76; C-58/94 *Netherlands v Council* EU:C:1996:171 paras. 37 and 38.
[121] Article 6 TEU.
[122] Case C-617/10 *Åklagaren v Hans Åkerberg Fransson* EU:C:2013:105.
[123] Case 29-69 *Erich Stauder v City of Ulm – Sozialamt* EU:C:1969:57; Case 11-70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* EU:C:1970:114; Case 4-73 J. *Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities* EU:C:1974:51.

Moreover, Article 291(1) TFEU lays down the principle that the MS must adopt all measures of national law necessary to implement legally binding Union acts.[124] First articulated by the Court,[125] this principle is now enshrined in Article 291(1) TFEU and extends to all legally binding Union acts – including decisions within the meaning of Article 288(4) TFEU, such as the CSR. In situations where the implementation is not entirely determined by Union law, MS should apply their national law provided that the primacy, unity, and effectiveness of Union law are not compromised.[126]

In addition, the principle of sincere cooperation enshrined in Article 4(3) TEU requires the Union and the MS to assist each other in carrying out tasks which flow from the Treaties.[127] This entails MS having to take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising from the Treaties or resulting from the acts of the institutions of the Union. MS are required to facilitate the achievement of the Union's tasks and refrain from any measures which could jeopardise the attainment of the Union's objectives. According to CJEU, the principle of sincere cooperation entails a duty for MS "*to cooperate in good faith, which means in particular that MS are to take all appropriate measures, whether general or*

[124] C-521/15 *Spain v Council* EU:C:2017:982 para. 47; C-183/16 P *Tilly-Sabco v Commission* EU:C:2017:704 para. 89.
[125] Joined Cases 205-215/82 *Deutsche Milchkontor GmbH* EU:C:1983:233 para. 17.
[126] See to this effect C-399/11 *Melloni* EU:C:2013:107 para. 60; C-617/10 *Åkerberg Fransson* EU:C:2013:105 para. 29 in the context of the protection of fundamental rights and the implementation of Union law by MS in Article 51(1) of the Charter.
[127] C-266/03 *Commission of the European Communities v Grand Duchy of Luxemburg* EU:C:2005:341; C-433/03 *Commission of the European Communities v Federal Republic of Germany* EU:C:2005:462; C-45/07 *Commission of the European Communities v Hellenic Republic* EU:C:2009:81.

particular, to ensure fulfilment of their obligations under European Union law."[128]

This principle of sincere cooperation must be considered when interpreting and applying provisions of the CSR. This also includes Article 1(2) Council Decision 2013/488/EU, which distinguishes between the Council and the General Secretariat on the one hand and the MS on the other hand. Whereas the basic principles and minimum standards for protecting EUCI "shall apply" to the former, they "shall be respected" by the latter in accordance with their respective national laws and regulations. Council Decision 2013/488/EU explains that in accordance with national laws and regulations and to the extent required for the functioning of the Council, MS should respect the CSR where their competent authorities, personnel or contractors handle EUCI, in order that each may be assured that an equivalent level of protection is afforded to EUCI.

Therefore, under Article 1(2) of the Council Decision 2013/488/EU, the CSR establish legal obligations for MS. It requires them to respect the basic principles and minimum standards of security for protecting EUCI in accordance with their respective national laws and regulations.

CJEU has underlined that MS are under a duty to refrain from applying any national provisions that are likely to hinder the effective application of a decision.[129] Similarly, in situations where the implementation is not entirely determined by Union law, MS should apply their national law provided that the primacy, unity and

[128] See C-355/04 P *Segi and Others v Council* EU:C:2007:116 para. 52 with reference to Case C-105/03 *Pupino* EU:C:2005:386 para. 42.
[129] Case 249/85 *Albako v BALM* EU:C:1987:245 para. 17 with reference to Case 6/64 *Costa v ENEL* EU:C:1964:66 and Case 106/77 *Simmenthal* EU:C:1978:49.

effectiveness of Union law are not thereby compromised.[130]

MS, in their implementation of national laws and regulations, are instrumental in giving effective application to the CSR, the purpose of which is to establish a level playing field of security where all apply similar standards so that a weak element does not undermine the security of all. This can be illustrated by three examples.

First, as part of personnel security, National Security Authorities or other competent national authorities are responsible for ensuring that security investigations are carried out on their nationals who require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above. To this end, Council Decision 2013/488/EU[131] creates an obligation for the relevant national authorities to cooperate with the Council and the General Secretariat as well as to cooperate among themselves. In discharging their obligations MS act in accordance with national laws and regulations and the principle of sincere cooperation.

Second, as part of industrial security, national competent authorities shall ensure,[132] to the extent possible under national laws and regulations, that contractors and subcontractors registered in their territory take all appropriate measures to protect EUCI in pre-contract negotiations and when performing a classified contract. Moreover, these authorities must ensure,[133] in accordance with national laws and regulations, that contractors or subcontractors registered in their MS participating in classified contracts or sub-contracts which require access to EUCI classified

[130] See to this effect C-399/11 *Melloni* EU:C:2013:107 para. 60; C-617/10 *Åkerberg Fransson* EU:C:2013:105 para. 29 already referred above.
[131] Article 7 and Annex I.
[132] Article 11(4) Council Decision 2013/488/EU.
[133] Article 11(5) Council Decision 2013/488/EU.

CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, hold a Facility Security Clearance at the relevant classification level.

Third, where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, the national competent authority shall take all appropriate measures in accordance with the relevant laws and regulations to inform the originator of the EUCI and investigate the incident.[134]

These three examples show that MS are under an obligation to give effective application to the CSR. The concrete obligations for MS depend on the interpretation of the specific provisions in the CSR.

In conclusion, Council Decision 2013/488/EU constitutes a decision within the meaning of Article 288(4) TFEU, and this Council Decision is binding in its entirety. Moreover, pursuant to Article 1(2) Council Decision 2013/488/EU, and in accordance with Article 291(1) TFEU about MS adopting all measures of national law necessary to implement legally binding Union acts and with the principle of sincere cooperation enshrined in Article 4(3) TEU, CSR must be respected by MS in accordance with national laws and regulations. This entails an obligation for MS to give effective application to the CSR regarding the protection of EUCI and therefore to follow, among other procedures, exactly the same classification system.

3.3.4 The CSR classification system

Council Decision 2013/488/EU categorizes EUCI in the following four levels:

[134] Article 14(4) Council Decision 2013/488/EU.

TRÈS SECRET UE/ EU TOP SECRET	the unauthorised disclosure of this information could cause exceptionally grave prejudice to the essential interests of the EU or one or more of the MS.
SECRET UE/ EU SECRET	the unauthorised disclosure of this information could seriously harm the essential interests of the EU or one or more of the MS.
CONFIDENTIEL UE/ EU CONFIDENTIAL	the unauthorised disclosure of this information could harm the essential interests of the EU or one or more of the MS.
RESTREINT UE/ EU RESTRICTED	the unauthorised disclosure of this information could be disadvantageous to the interests of the EU or one or more of the MS.

However, there are numerous weaknesses in this system. The above categorisation is possessed by a strong ambiguity in the boundaries between the categories and great subjectivity in the description of them thus making the system prone to arbitrary classifications. Moreover, not listing the subjects which may require classification, and not developing an expiry of classification periods restricts arbitrarily the capacity of access.[135] Given that this categorization is used by 27 MS, with multiple relevant government actors, as well as several institutions, there is no doubt that the system implemented is an enigma to its implementers. It is also important that the MS are not at the same level of preparedness and expertise

[135] Transparency International 'Classified Information: A review of current legislation across 15 countries & the EU' (2014); C. Warren Axelrod, Jennifer L. Bayuk and Daniel Schutzer, *Enterprise Information Security and Privacy* (Artech House 2009).

regarding the protection of CI, as there is no horizontal support or control mechanism.

A similar classification policy is followed in Australia.[136] Contrary, in the United States, any initial classification decision must be accompanied by sufficient justification for the classification, which can only be applied to the information described in predefined categories,[137] specified in a specific executive decree.[138] As far as European countries are concerned, it is worth noting that the relevant Polish law allows for eternal classification of certain sensitive data. Similarly, in Lithuania the classification period of state secrets can be extended by 10 years as many times as needed. The Austrian system is an anomaly in Europe since secrecy is still the default position and access to information is treated as an exception.[139]

3.3.5. Concluding remarks on the Council Security Rules

In general, EU classification rules are perceived as purely technical and receive little attention from stakeholders, as they are adopted and amended in the form of an internal procedure that does not involve any interest. At the same time, oversight mechanisms in the EU, especially the European Parliament, cannot provide any compensatory pressure. Undoubtedly, more public debate is needed on when and for how long ratings can be maintained and how oversight mechanisms are built into

[136] Australian Government, *Information Security Management Guidelines: Australian Government Security Classification System* (2011).
[137] For example, military plans, cryptology, scientific actions, mass destruction weapons and national security, etc.
[138] United States of America, Executive Order 13526.
[139] Transparency International 'Classified Information: A review of current legislation across 15 countries & the EU' (2014).

this horizontal EU legislation.[140]

According to Transparency International, good practice in CI classification legislation includes rules on the following four dimensions: (a) any restriction on right to information has to meet international legal standards which have to be also present in the applicable national legislation; (b) the authority to withhold or classify information needs to be well defined and has to originate from a legitimate source of power and be performed in line with procedures prescribed by published legal rules; (c) information may be protected by classification and/or exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm; (d) if information is withheld there should be procedures, accessible to all, that allow for substantial review by independent bodies.[141]

In contrast, there are argumentators who believe that the EU has developed an integrated internal and external framework for the protection of EUCI, which sets out common principles and standards across all institutions, agencies, and MS. Furthermore, it is argued that the EU has rightly avoided a legislative approach concerning EUCI based on policy areas, thus achieving a broad degree of convergence between the institutions and the MS in a realistic approach based largely on internal rules. This has allowed the EU to appeal as a credible and capable security player to MS and international partners.[142]

The impact on MS and of international partners is examined in the following two

[140] Deirdre Curtin, 'Overseeing Secrets in the EU: A Democratic Perspective' (2014) 52(3) Journal of Common Market Studies 684.
[141] Transparency International 'Classified Information: A review of current legislation across 15 countries & the EU' (2014).
[142] David Galloway, 'Classifying Secrets in the EU' (2014) 52(3) Journal of Common Market Studies 668.

subsections, respectively. Firstly, to study how the MS actually harmonized their national legal frameworks in order to apply the CSR, the example of Cyprus was chosen.

3.4 Member States' Harmonization - The Case of Cyprus

Traditionally, the Cypriot legal system[143] has depicted a history of remarkable openness in the field of public law, even though a number of peculiarities and idiosyncrasies can be identified.[144] EU legislative framework's power is greater of any other national provision in Cyprus, because of the supremacy of the EU law[145] and of the provisions[146] of the Cypriot Constitution.[147] Finally, it is important to note that Cyprus has a strong tradition of following the rulings of ECtHR when human rights and freedoms are under scrutiny.[148]

[143] For more information on the legal history of Cyprus and the the Cypriot legal order see C.G. Tornaritis, *Cyprus and Its Constitutional and other Legal Problems* (Nicosia 1980); Andreas Neocleous and David Bevir in Dennis Campbell (ed), *Introduction To Cyprus Law* 6 (Yorkhill Law Publishing, 2000); Nikitas Hatzimihail, 'Cyprus as a Mixed Legal System' (2013) 6 Journal of Civil Law Studies 42; Nikitas Hatzimihail, 'Reconstructing Mixity: Sources of Law and Method in Cyprus' in V. Palmer et al, *Mixed Legal Systerms East and West* (Ashgate 2015); Constantinos Kombos, *The Impact of EU Law on Cypriot Public Law* (Sakkoulas 2015).

[144] Constantinos Kombos, *The Impact of EU Law on Cypriot Public Law* (Sakkoulas 2015); C. Lykourgos "Cyprus Public Law as Affected by Accession to the EU" in Constantinos Kombos (ed) *Studies in European Public Law* (Sakkoulas 2010) 101.

[145] Case 26-62 *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* EU:C:1963:1; Case 6/64 *Costa v ENEL* EU:C:1964:66; Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal* SpA EU:C:1978:49; Case C-213/89 *The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others* EU:C:1990:257; Joined cases C-10/97 to C-22/97 *Ministero delle Finanze v IN.CO.GE.'90 Srl, Idelgard Srl, Iris'90 Srl, Camed Srl, Pomezia Progetti Appalti Srl (PPA), Edilcam Srl, A. Cecchini & C. Srl, EMO Srl, Emoda Srl, Sappesi Srl, Ing. Luigi Martini Srl, Giacomo Srl and Mafar Srl*. EU:C:1998:498.

[146] Articles 1A and 146(3) of the Constitution.

[147] *Attorney General of the Republic v Costas Constantinou* [2005] 1 CLR 1356.

[148] For more information see N. Kyriakou "National Judges and Supranational Laws on the Effective Application of the EC Law and the ECHR: The Case of Cyprus" (June 10, 2010). Available at SSRN: https://ssrn.com/abstract=1623560 or http://dx.doi.org/10.2139/ssrn.1623560.

Regarding CI, even though no provisions are provided in the Constitution itself, the fundamental law of the Republic includes extensively terms such as 'security of the Republic', 'constitutional order', 'public security' and 'public order'.[149] Moreover, several relevant bilateral or multilateral international agreements[150] are in force.

Legal provisions, concerning national CI, have been in force since the establishment of the Republic of Cyprus.[151] From 1960, year of the establishment of the Republic of Cyprus, to 2004, year of the accession of Cyprus to the EU, scattered provisions concerning national CI, could be found in various legislations. There is no doubt that the majority of these provisions, which are still in force, do not correspond to nowadays demanding environment, especially in terms of the severity of penalties imposed, the advancements of technology and the emergence of cyberspace. For example, see Articles 50C,[152] 135,[153] 136[154] και 137,[155] of the Penal Code[156]; the fourth[157] and the eighth part[158] of the Military Penal Code named "Espionage" and "Offenses concerning Confidentiality", respectively; Article 67[159] of the Public Service Law. Articles 25[160] and 30[161] of the Cyprus Information Service were enacted in

[149] See for example, Articles 15,17,18,19,20,21,23,25,27,30,134,154,156 of the Constitution.
[150] Article 169(3) of the Constitution provides for international agreements greater power than the national legal provisions.
[151] Provisions enacted before the establishment of the Republic of Cyprus do not within the scope of this paper.
[152] Espionage.
[153] Violation of official secret and disclosure of state secret.
[154] Disobedience to provisions of laws that impose a duty.
[155] Disobedience to legal orders.
[156] The Cypriot Penal Code was enforced in 1973 and the relevant provisions are still in force without substantial changes.
[157] Articles 19-28 of the Military Penal Code.
[158] Articles 66-70 of the Military Penal Code.
[159] Official information, testimony and documents.
[160] Obligation of confidentiality of Cyprus Information Service personnel.
[161] Criminal offences.

2016 and are the only ones aligned to today's challenges. As mentioned before, judicial review was completely absent since these matters were exempted as 'acts of government', i.e. acts concerning the general policy of the state protected by judicial immunity.

Cyprus introduced, for the first time, a *lex specialis* on CI and EUCI on 27 December 2002, for the purposes of EU accession. On the eve of its accession to the EU, Cyprus enacted its first legislative act[162] on CI: the Law on the Security Regulations of Classified Information, Documents and Material and Related Matters of 2002.[163] As indicated in the preamble of the Law, its adoption was deemed necessary for the purposes of implementing the then in force Council Decision 2001/264/EC[164] and in the context of measures taken by the Republic as a participant in the Common Foreign and Security Policy and the Common Policy European Union Security and Defense Policy, to facilitate the implementation and maintenance of an integrated security system covering the Council of the EU, the General Secretariat of the Council and the Member States, as well as to develop Council activities in areas where confidentiality arises. It is worth noting that while Commission Decision 2001/844/EC had been already issued at the time of the adoption of the basic Law, the Republic limited itself to harmonization only with the original Council Decision 2001/264/EC, amending the Law in question in order to fully comply with its obligations to comply with the European acquis. This Decision in

[162] Immediately after the enactment of the 2002 Law, the Council of Ministers issued the Decree on the Security of Classified Information, Documents and Material of 2002. This Decree was replaced in 2004 with the Validity of the Security of Classified Information, Documents and Material of the European Union Decree of 2004, which was amended in 2004 and 2017.
[163] Cyprus Government Gazette no. 3666, Appendix I(I), 27.12.2002.
[164] Council Decision of 19 March 2001 adopting the Council's security regulations [2001] OJ L101/1.

2015 was repealed and replaced by Decision 2015/444,[165] but no action was taken in relation to it by the Republic, at least in terms of the legislative framework.

The above-mentioned legislation was recently replaced by the Law on the Security Regulations of Classified Information Documents and Material and Related Issues of 2021 which was enacted on May 5th, 2021.[166] The new legislation's purpose was the harmonization of the national legal framework with the European legal framework and specifically with the Council Decision 2013/488/EU. According to the Attorney General the new law provides for the upgrading of the legal framework providing for the handling and protection of CI of the Republic of Cyprus. Council Decision 2013/488/EU is now included as an Annex to the law, a few technical enhancements were introduced because of the multidisciplinary environment of the public services involved and the Minister of Defence was given the power of issuing Decrees for the application of the law and of repealing the Annex mentioned above whenever the Council issues new or modifies Council Decision 2013/488/EU.

Considering the above analysis, it can be observed that this method of harmonization does not meet the requirements expected of a diligent MS. Any modification of the CSR by the Council has immediate effect on national regimes, thus the authority of the competent Minister to repeal the national law's Annex including the relevant Decision is contrary to the obligations of a MS.

Furthermore, the provisions included in the main text of the law are not allowed

[165] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information OJ L72/53.
[166] Cyprus Government Gazette no. 4836, Appendix I(I), 05.05.2021.

to contradict the provisions of the Council Decision 2013/488/EU. Regarding this issue the term “information security”, also discussed in section 2.1 is taken as an example. The Cypriot law includes the term ‘security’[167] but has not precisely followed the EUCI definition of the Council Decision.[168] Instead it defines EUCI as "any information or material classified by the European Union whose unauthorized disclosure could possibly harm the interests of the EU or one or more MS in various ways".[169] At the same time, the terms “information” and “material” are not defined. Examining whether any of the theoretical concepts were incorporated in the definition of this term it can be observed that even though some of the dimensions were included, the main philosophy was centralised around espionage, leakage, unauthorized disclosure and acquisition through sabotage or other damage, electronically or physically, while the definition in question includes the protection of premises and facilities within the Republic or other spaces belonging to its authority where CI or EUCI is being stored. In addition, the term includes the interference, infringement or attempt to infringe on the protection systems of CI and EUCI, the

[167] the term "security" includes -
(a) the protection of classified information and EU classified information from unauthorized espionage, leakage, or disclosure;
(b) the protection of classified information and EU classified information circulating in communications and information systems and networks;
(c) the protection of premises and installations within the Republic or, in general, premises under the control of the authorities of the Republic, where classified information and / or EU classified information is stored, from the possibility of sabotage and malicious damage;
(d) in the event of an intervention, interference, infringement or attempted infringement of the protection systems of classified and EU classified information, the assessment of the damage, the reduction of its consequences and the taking of the necessary remedial measures. "

[168] The same definition was included in the 2001 legal act.

[169] Article 2 of the Law on the Security Regulations of Classified Information Documents and Material and Related Issues of 2002; Article 2 of the Law on the Security Regulations of Classified Information Documents and Material and Related Issues of 2021.

assessment of the damage, the reduction of its consequences and the taking of the necessary remedial measures. The above amalgam, however, does not achieve the purpose of defining, in the clearest possible way, the concept of security of EUCI, but instead creates an abundance of questions and a foggy scenery.

National CI was not regulated until 2013 when the Decree on the Security of Classified Information was issued, which is still in force. This opt provided the greatest possible flexibility to the government but circumvented transparency and accountability which would have been carried out by the parliament if the adoption of a regulatory administrative act was preferred. This Decree's intention was to introduce regulations on national CI similar to the ones regarding EUCI. However, this practice, in the way it was introduced, caused confusion and difficulties to the users of the legislative framework, especially with the parallel procedures that must be elaborated. For example, while the same classification categories as those of the EU (see Section 3.3.4) were correctly introduced no provision was made for the distinction of ratings, in a characteristic way, which facilitates the user to easily and quickly perceive whether the origin of information is public or private, national or European.

Summarising, Cyprus' obligation to adopt all measures of national law necessary to implement the legally binding Council Decision 2013/488/EU cannot be perceived as performed. In general, despite the obligation for MS to give effective application to the CSR, described in section 3.3.3, one of the weakest elements in the legal-political edifice of today's EU is the one which was almost entirely taken for granted by its founders: ensuring that the national governments are faithful to the

basic principles of democracy, protection of fundamental rights, and the rule of law. This goes to the very core of the European project which promised a peaceful, prosperous, and democratic Europe.[170] On the other hand, EU's effort to appeal as a credible and capable security player to international partners seems to prevail.

3.5 EUCI and third countries

Established security cooperation between EU and third countries or other organizations allows these third parties to have the right to submit CI into the EU, provided that they remain henceforth classified. Some authors say that one of the crucial elements of EUCI rules is the extent to which these rules are supervised but also influenced by the stakeholders themselves in terms of general principles, structures and boundaries.[171]

In January 2015, EU Ombudsperson Emily O'Reilly stated at a hearing before a Committee of the European Parliament that she had been '*unable to exercise [her] democratic powers*' by being denied access to the inspection report of the EUROPOL supervisory body into the Terrorism Finance Tracking Programme. After a fierce debate, O'Reilly concluded that '*the US has effectively been given a veto over the democratic oversight of EU institutions*.' O'Reilly's strong wording shows

[170] Kim Lane Scheppele, Dimitry Vladimirovich Kochenov and Barbara Grabowska-Moroz, 'EU Values Are Law, after All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union' (2020) 39 Yearbook of European Law, 3.

[171] Deirdre Curtin, 'Challenging executive dominance in European democracy' in C. Joerges and C. Glinski (eds.) *The European crisis and the transformation of transnational governance: authoritarian managerialism versus democrtic governance* (Oxford Hart 2014); Marieke de Goede and Mara Wesseling 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39(3) Journal of European Integration 253.

how the Terrorism Finance Tracking Programme dossier has become a focal point for discussions about secrecy and democracy in the EU, especially as they relate to post 9/11 security cooperation with the United States.[172]

In fact, this battle over secrecy and publicity was only one of many since the creation of the Terrorism Finance Tracking Programme. Initiated by the Bush government immediately after 9/11, this secret Central Intelligence Agency program was disclosed in June 2006by the New York Times. Within the programme, large quantities of data are subpoenaed from a financial telecommunications company, transferred to United States Treasury in encrypted form, and subjected to software-led analyses in the name of mapping terrorist networks and identifying suspect associates. Once disclosed, the European Parliament, other EU institutions, and the United States of America engaged in intense negotiations, from 2006 to 2010, on the inclusion of more data protection and privacy safeguards and on an increased insight into and oversight of the programme. Even after the conclusion of EU-US Treaty on the Terrorism Finance Tracking Programme in 2010, the programme continued to be subject of recurring 'secrecy controversies,' in which the visibility and oversight of transatlantic security cooperation were subject to public debate.

Nevertheless, the Czech model enables the Ombudsman and his/her deputy to have access to CI without clearance; in Slovenia, access is enabled to the Protector of Citizens and his/her deputy, as well as the Commissioner for access to information of public significance; while in Montenegro access to CI without clearance have the Protector of Human Rights and Freedoms as well as members of the Council of the

[172] Marieke de Goede and Mara Wesseling, 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39(3) Journal of European Integration 253.

independent supervisory body for the protection of personal data and access to information.[173]

The state of emergency in the United States, which has affected the EU and worldwide, continues to be felt to this day, creating a variety of controversial laws and regulations in the name of fighting terrorism and radical effects on the protection of privacy, as well as on the civil liberties of citizens. In this context, there is unilateral control of information and frequent decision-making without audit, is now a constant feature of most intergovernmental decision-making processes, including the Common Foreign and Security Policy.[174]

Having examined the legal status of the Council Decision 2013/488/EU and after highlighting the major deficiencies of the general EUCI legal framework, the conclusion that a lot of challenges need to be addressed by EU administration can effortlessly be derived. These challenges though impact not only procedurally and internally on EU institutions, but more importantly impact on EU citizens. When legal challenges arise about a regulatory framework the consequences on fundamental human rights are most of the times non-favorable.

[173] Center for Euroatlantic Studies, The Law on Classified Information (2015) <https://issat.dcaf.ch/download/92038/1612447/CEAS-Law%20on%20Classified%20Information-2015.pdf> accessed 1 October 2021.

[174] Deirdre Curtin, 'Challenging executive dominance in European democracy' in C. Joerges and C. Glinski (eds.) *The European crisis and the transformation of transnational governance: authoritarian managerialism versus democrtic governance* (Oxford Hart 2014).

4

THE IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS – THE RIGHT OF ACCESS TO INFORMATION

The status of human rights within the EU legal order has changed dramatically since the Union's foundation; human rights' nowadays central position is enshrined in the EU foundation treaties. According to Article 6 TEU, there are three formal sources for EU human rights law: the CFREU, ECHR, which is treated as 'a special source of inspiration' for EU human rights principles and the 'general principles of EU law', a body of legal principles which were articulated and developed by the European Union Courts over the years.[175]

While it may be argued that an effective public security policy may require a certain degree of secrecy, the use of CI as grounds for imposing severe legal consequences on individuals or entities, with the conservation of its inherent secrecy, has raised numerous constitutional concerns. EU is committed to promoting and protecting human rights, democracy, and the rule of law; these values are thought to prevail.[176] However, due to the multiplication and accumulation of a secrecy culture at all levels of governance, international, supranational, and national, the issue of safeguarding fundamental rights was bound to arise before the courts of the EU. In

[175] Paul Craig and Grainne De Burca, *EU Law: Text, Cases, and Materials* (7th edn, OUP 2020).
[176] Henri Labayle, Classified Information in light of the Lisbon Treaty (European Parliament, 2010) <https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/pe425616_/pe425616_en.pdf> accessed 1 October 2021.

the wake of the global threat posed by international terrorism, European courts are more and more often required to resolve the conflicts that inevitably arise between security considerations and the concomitant secrecy claims on the one hand and the protection of the fundamental rights enshrined in the CFREU on the other. But protecting the public from genuine threats to security and safeguarding fundamental rights involves a delicate balance and has become a particularly complex challenge in recent years.

Core principles of the EU treaties, like openness, transparency and accountability, the right of access to information, the right to freedom of expression, the rights to privacy and data protection, the adversarial principle, the rights of defence, the right to effective judicial protection and the right to a fair trial as laid down in CFREU and ECHR seem to be limited when dealing with security strategies and CI legal rules and policies.[177] This essay focuses on the impact on the right of access to information to illustrate the deficiencies that may derive when protecting EUCI becomes the priority for EU institutions without maintaining the needed attention on EU human rights and fundamental freedoms.

4.1. Legal basis

The right of access to public sector information is a key pillar that enables the free flow of information and advances the promotion and protection of human rights. This crucial right in the sphere of public law is vital for citizens to shape their political choices; companies to make good investment; journalism to explore crucial issues

[177] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks* (Publications Office of the European Union, 2015); Transparency International 'Classified Information: A review of current legislation across 15 countries & the EU' (2014).

and exercising opposition control over rulers; it also provides the legal basis of transparency, which in turn is a precondition to establishing a system of real accountability. It is enshrined in Article 10 of the Universal Declaration of Human Rights, Article 10 of the ECHR, Article 15(3) of the TFEU, as well as Article 42 of the CFREU.

EU, in the aftermath of the Maastricht Treaty signing procedures, following a period of pressure for more open and transparent procedures in the EU, enacted Regulation 1049/2001.[178] The purpose of the Regulation is to grant the widest possible right of public access to EU documents.[179] The revision of Regulation 1049/2001 regarding public access to documents coincides with the entry into force of the Lisbon Treaty. Article 15(3) TFEU was the basis for the adoption of the Regulation, marking a new era for the right.

However, the public's right of access to EU documents is not absolute. According to Regulation's article 4, the institutions shall refuse access to a document where disclosure would undermine, among other, the protection of the public interest as regards public security, defence and military matters, international relations, the financial, monetary or economic policy of the Community or a Member State, or privacy and the integrity of the individual, in particular in accordance with the Union's

[178] For more information, see Paul Craig, *EU Administrative Law* (3rd edn, OUP 2019) Ch13; Koen Lenaerts, "In the Union We Trust: Trust-Enhancing Principles of Community Law" (41) Common Market Law Review 317.

[179] Bogdana Neamtu and Dacian Dragos in Dacian C. Dragos, Polonca Kovač, Albert T. Marseille, *The Laws of Transparency in Action: A European Perspective* (Palgrave Macmillan 2019) 17; Paul Craig, *EU Administrative Law* (3rd edn OUP 2019) 389-391; Herwig Hofmann and Päivi Leino-Sandberg, 'An agenda for transparency in the EU' (2019) European Law Blog; Marios Costa, *The Accountability Gap in EU law: Mind the Gap* (Routledge 2017) 25; Hoffmann, Rowe and Türk, *Administrative Law of the European Union* (OUP 2012) 470.

legislation regarding the protection of personal data.[180] It is important to note that the term 'shall' indicates the mandatory nature of the legislative provision.

Article 4 provides for a system of exceptions under which the institutions, in the event that the disclosure of the requested document infringes any of the interests it protects, have the right to refuse access to that document.[181] Specifically, the institutions shall refuse access to a document where disclosure would undermine the protection of (a) the public interest as regards public security, defence and military matters, international relations, the financial, monetary or economic policy of the Community or a Member State and (b) the privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data. Furthermore, the institutions shall refuse access to a document where disclosure would undermine the protection of commercial interests of a natural or legal person, including intellectual property, court proceedings and legal advice, the purpose of inspections, investigations, and audits, unless there is an overriding public interest in disclosure.

4.2. Judicial Review on Classified Information

To map the extent of the right of access to information for the European citizens when CI issues arise, one must examine the relevant court judgements enforced.

4.2.1. Court of Justice of the European Union case law

[180] Bart Driessen, *Transparency in EU Institutional Law: A Practitioner's Handbook* (Cameron May 2008) 51; Damian Chalmers, Gareth Davies and Giorgio Monti, *European Union Law: Cases and Materials* (Cambridge University Press 2010) 390.

[181] C-514/07 P, C-528/07 P and C-532/07 P *Kingdom of Sweden v Association de la presse internationale ASBL (API) and European Commission* EU:C:2010:541 para. 71; C-280/11 P *Council of the European Union v Access Info Europe* EU:C:2013:671 para. 29.

In *Interporc Imund*[182] judgement, CJEU stressed the importance of the right of access to information and its linkage with the democratic nature of the institutions. It held that the above-mentioned Regulation was enacted '*in order to enable citizens to participate more closely in the decision-making process, to guarantee that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system and to contribute to strengthening the principles of democracy and respect for fundamental rights'*. The Court stated that this Regulation is part of the EU's efforts to ensure that the decisions of the European institutions are taken as openly and as close as possible to the people, thus expressing their democratic character[183] and aims to grant the widest possible right of public access to EU documents,[184] while in its provisions it also includes certain restrictions of the right, which are based on reasons of public or private interest.[185]

Simultaneously, according to the established CJEU case law, since the above-mentioned exceptions deviate from the principle of the widest possible public access to documents, they must be interpreted restrictively and strictly applied[186] so the mere fact that the requested document concerns an interest protected by one of the above exceptions is not sufficient to adequately justify the invocation of the

[182] T-92/98 *Interporc Imund Export GmbH v Commission of the European Communities* EU:T:1999:308 paras. 38-39.
[183] Paras. 1-2.
[184] Para. 4; Article 1; C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 para. 61; C-514/07 P, C-528/07 P και C-532/07 P, *Sweden v API and Commission* EU:C:2010:541 para. 69; C-280/11 P *Council of the European Union v Access Info Europe* EU:C:2013:671 para. 28.
[185] C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 para. 62.
[186] C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 para. 63; C-39/05 P and C-52/05 P *Kingdom of Sweden and Maurizio Turco v Council of the European Union* EU:C:2008:374 para. 36; C-280/11 P *Council of the European Union v Access Info Europe* EU:C:2013:671 para. 30.

exception.[187]

Initially, in the *Sison*[188] judgment, the CJEU drew almost impenetrable lines regarding access to documents relating to public security and international relations. In this case, the documents concerned the fight against terrorism and CJEU ruled that the lawfulness of a measure taken based on the exception in question was affected only if that measure was manifestly inappropriate in relation to the purpose pursued by the institution. Furthermore, it determined the scope of the judicial review of the legality of a decision of an institution refusing public access to a document based on one of the exceptions relating to the public interest provided for in Article 4(1)(a) of Regulation No 1049/2001. For this purpose, it ruled that the Council must be recognised as enjoying a wide discretion for the purpose of determining whether the disclosure of documents relating to the fields covered by those exceptions could undermine the public interest. The Court's review of the legality of such a decision, it added, must therefore be limited to verifying whether the procedural rules and the duty to state reasons have been complied with, whether the facts have been accurately stated, and whether there has been a manifest error of assessment or a misuse of powers.[189]

In such a strict interpretation of the relevant provisions, the Court has ruled that the institution's refusal is obligatory when disclosing a document to the public is likely to prejudice the interests protected by that provision, without even requiring a

[187] C-365/12 P *European Commission v EnBW Energie Baden-Württemberg AG* EU:C:2014:112 para. 64; T-2/03 *Verein für Konsumenteninformation v Commission of the European Communities* EU:T:2005:125 para. 69; T-471/08 *Ciarán Toland v European Parliament* EU:T:2011:252 para. 29.
[188] C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75.
[189] C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 paras. 32-34.

weighting of the requirements imposed by the protection of those interests with the requirements imposed by other interests.[190] As Timmermans characteristically reported «*the assessment is limited to a so-called harm-test excluding any balancing-test*».[191]

This ruling was strongly criticized, as contrary to the spirit of the Treaties and Regulation 1049/2001, that it gave enormous discretion to the institutions, and in addition drastically limited the role of the Court itself and the opportunity of any applicant to succeed in a later appeal. Undoubtedly, the grounds of public interest in the areas provided for in the provisions of Article 4(1)(a) must be protected, but there is no lawful justification for the limitation of judicial review, which must, in any case, weigh the interests and act as a guardian against any arbitrariness of the administration.[192]

It is worth noting that in this case Advocate General Geelhoed's Opinion had been even more formalistic regarding the exceptions to Article 4(1)(a) of Regulation 1049/2001, particularly public safety, and international relations, because he argued that:

> *"[…] the Community institutions involved must have complete discretion in respect of determining whether one of the interests listed in Article 4(1)(a)*

[190] C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 EU:C:2007:75 para. 43, paras. 46-48.
[191] Tinne Heremans, 'Public Access To Documents: Jurisprudence Between Principle And Practice' (2011) Egmont Paper 50.
[192] Vigjilenca Abazi, *Official Secrets and Oversight in the EU: Law and Practices of Classified Information* (OUP 2019) 115; Paul Craig, *EU Administrative Law* (3rd edn OUP 2019) 396-397; Vigjilenca Abazi and Maarten Hillebrandt, 'The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In't Veld' *(*2015) 52 Common Market Law Review 825.

could be undermined by disclosure of documents. If it considers that granting access to a document would undermine the interests of the European Union in these respects, it is under an obligation to refuse access, irrespective of the interests which the applicant may have in gaining access. […]"[193]

Over time, the CJEU appears to have somewhat softened its stance. *Sophie in't Veld*[194] can be considered a step towards democracy, transparency and the rule of law. In this case, the applicant requested access to the opinion of the Council Legal Service concerning the negotiations between the EU and the US on the conclusion of an international agreement on financial transactions relating to terrorism. The General Court ruled in favour of the applicant, stressing that the importance of transparency cannot be ruled out in international affairs, especially when a decision concerns the negotiation of an international agreement that may have an impact on EU law.[195] Similarly, the CJEU rejected the Council's appeal against the decision, stressing that it was necessary for the institutions to justify the sabotage in a concrete and real way, that the disclosure could undermine the protected interest, he was logically predictable and not just hypothetical.[196]

This decision created a strong crack in *Sison's* case law, as it established that issues of legality of administration and citizen participation are crucial when the Council acts as legislator and therefore matters of international relations cannot,

[193] C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 para. 30.
[194] T-529/09 *Sophie in 't Veld v Council of the European Union* EU:T:2012:215.
[195] European Parliament, *Openness, Transparency, and the Right of Access to Documents in the EU: In-Depth Analysis* (European Union 2016).
[196] C-350/12 P *Council v Sophie in't Veld* EU:C:2014:2039 para. 64.

automatically, be excluded.[197] As Abazi and Hillebrandt point out, the *Sophie in 't Veld* and *Access Info Europe* decisions - which was based on another exception to Regulation 1049/2001 - are the starting point for change in transparency in the EU.[198]

In *Evropaïki Dynamiki*,[199] the General Court held that if an institution decides to refuse access to a document requested to be disclosed, it must explain how disclosure of that document could undermine the protected interests concretely and realistically, along with proof that the danger is reasonably predictable and not purely hypothetical. Similarly, in *Besselink*[200] it ruled that the institution that refused access to a document must provide a reason on which it could be understood and ascertained whether the document in question really fell within the scope of the exception on which the denial was based and whether the need for protection associated with this exception is genuine and factual.

In *Jurašinović*[201] CJEU decreased the margin of arbitrariness for the institutions, after ruling that, if the applicant challenges the application of the exception relied on by the institution, the Court is obliged to request the relevant document for examination in order to assess *in concreto* whether the institution

[197] Marieke de Goede and Mara Wesseling, 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39(3) Journal of European Integration 253; European Parliament, *Openness, Transparency and the Right of Access to Documents in the EU: In-Depth Analysis* (European Union 2016); Vigjilenca Abazi and Maarten Hillebrandt, 'The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In 't Veld' (2015) 52 Common Market Law Review 825.

[198] Vigjilenca Abazi and Maarten Hillebrandt, 'The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In 't Veld' (2015) 52 Common Market Law Review 825.

[199] T-167/10 *Evropaïki Dynamiki – Proigmena Systimata Tilepikoinonion Pliroforikis kai Tilematikis AE v European Commission* EU:T:2012:651.

[200] T-331/11 *Leonard Besselink v Council of the European Union* EU:T:2013:419.

[201] C-576/12 P *Ivan Jurašinović v Council of the European Union* EU:C:2013:777 para. 27; C-135/11 P *IFAW Internationaler Tierschutz-Fonds v Commission* EU:C:2012:376 para. 75.

concerned legally and validly refused the disclosure and, consequently, verify the legality of its decision. This signifies the executive role of judicial control, which must weigh, in any case, the conflicting interests of access to public documents that comprise CI but also to act as a custodian against any arbitrariness of the administrative bodies becomes critical.[202]

However, the Court ruled that the exceptions to Regulation 1049/2001 deviate from the principle of the widest possible public access to documents, which must be interpreted restrictively and strictly enforced.[203] This means that an interest protected by any of the above exceptions, including security, is not sufficient to justify invoking the exception. Furthermore, the permissible actions of the institutions are limited, as when the institution concerned decides to refuse access to a document whose publication has been requested, it must first explain how access to that document could specifically and substantially affect the interest protected by the exception invoked.[204]

Despite the above progress towards the maximum possible access of the public

[202] Vigjilenca Abazi, *Official Secrets and Oversight in the EU: Law and Practices of Classified Information* (OUP 2019) 115; Paul Craig, *EU Administrative Law* (3rd edn OUP 2019) 396-397; Vigjilenca Abazi and Maarten Hillebrandt, 'The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In 't Veld' *(*2015) 52 Common Market Law Review 825.

[203] C-39/05 P and C-52/05 P *Kingdom of Sweden and Maurizio Turco v Council of the European Union* EU:C:2008:374 para. 36; C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75 para. 63; C-280/11 P *Council of the European Union v Access Info Europe* EU:C:2013:671 para. 30; **I.** Spahiu**, '**Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union**'** 2015, 31(80) Utrecht Journal of International and European Law 5.

[204] T-2/03 *Verein für Konsumenteninformation v Commission of the European Communities* EU:T:2005:125 para. 69; ; T-471/08 *Ciarán Toland v European Parliament* EU:T:2011:252 para. 29; C-365/12 P *European Commission v EnBW Energie Baden-Württemberg AG* EU:C:2014:112 para. 64; T-851/16 *Access Info Europe v European Commission* EU:T:2018:69 para. 36.

to CI documents, in its very recent decision, *Izuzquiza*,[205] the CJEU stated that its case law has established a special regime for the exceptions provided for in Article 4 of the Regulation 1049/2001, due to the highly sensitive and substantive nature of the public interest protected, in conjunction with the institution's obligation under those provisions to refuse access to a document that may affect those interests. The decision to be taken by the institution, as the Court explained, is complex and requires careful processing and special consideration, and in order for the institution to take a decision, the latter should have a margin of discretion. In this case, there is a setback in the reasoning of the CJEU as, it seems to slow down the momentum towards protecting the right to access to public documents, transparency and accountability that emerged to be formed in the period that followed the initial very strict interpretation.

Undoubtedly, the balance between the two interests, namely the preservation of the CI and the preservation of the right to access documents was a difficult case for the CJEU.[206] The problem seems to arise from the combination of the fact that the provisions of Article 4(1)(a) are mandatory exceptions to the Regulation and the strict grammatical interpretation that the CJEU selectively attributes to the relevant provision. The European Parliament considers that the change in the attitude of the

[205] T-31/18 *Luisa Izuzquiza and Arne Semsrott v European Border and Coast Guard Agency* EU:T:2019:815 paras. 63 και 64.

[206] I. Spahiu, 'Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union' (2015) 31(80) Utrecht Journal of International and European Law 5; Elinor Pecsteen, 'Public access to documents: effective rear guard to a transparent EU?' (2015) European Law Blog; Carol Harlow, Päivi Leino and Giacinto della Cananea, *Research Handbook on EU Administrative Law* (Edward Elgar 2017) 407; Anna-Sara Lind and Magnus Strand, 'A New Proportionality Test for Fundamental Rights?' (2011) 7 European Policy Analysis 1; Paul Craig, *EU Administrative Law* (3rd edn, OUP 2019) 396-399; Herwig Hofmann and Päivi Leino-Sandberg, 'An agenda for transparency in the EU' (2019) European Law Blog.

CJEU to the exceptions provided for in Article 4(1), where no weighting of public interest is required, is not particularly significant, but acknowledges that this is not in line with international standards as expressed in ECHR. As it argues, in the field of international agreements, which can replace legislation in many ways, and have often had legal implications for citizens, the existing provisions under Article 4(1) need to be reconsidered.[207]

Regulation 1049/2001 includes more exemptions. In the field of public law, Article 4(3) states that access to a document, drawn up by an institution for internal use or received by an institution, which relates to a matter where the decision has not been taken by the institution, shall be refused if disclosure of the document would seriously undermine the institution's decision-making process, unless there is an overriding public interest in disclosure.[208]

In *Muñiz*,[209] the then Court of First Instance ruled that the infringement of the decision-making process within the meaning of Article 4(3) can be considered "serious", inter alia, when the disclosure of the documents concerned had a significant impact on the decision-making process. The assessment of the seriousness depends on all the circumstances of the case, including the negative effects on the decision-making process put forward by the institution concerned. This ratio decidendi was followed, inter alia, in the *Toland*[210] and *MasterCard*[211]

[207] European Parliament, *Openness, Transparency, and the Right of Access to Documents in the EU: In-Depth Analysis* (European Union 2016).
[208] Damian Chalmers, Gareth Davies and Giorgio Monti, *European Union Law: Cases and Materials* (Cambridge University Press 2010) 390.
[209] T-144/05 *Pablo Muñiz v Commission of the European Communities* EU:T:2008:596 75.
[210] T-471/08 *Ciarán Toland v European Parliament* EU:T:2011:252 71.
[211] T-516/11 *MasterCard, Inc. and Others v European Commission* EU:T:2014:759 62.

judgments, as well as in the more recent *De Capitani* judgment which is analysed below.

In *Access Info Europe*,[212] the Court dealt with a practice introduced by the Council in the legislative process, a few years after the entry into force of the Regulation. On this basis, it granted partial access to most legislative documents but without disclosing the identity of the MS proposing amendments or counterproposals. In this case, a strong ruling was placed that enhances citizens' wide access to documents in the EU: The Court has banned the above practice, rejecting the Council's allegations of the preliminary nature of the debates and the sensitive and subtle nature of the proposals of the MS delegations. At the same time, CJEU clarified that public access to documents during the formal legislative process is not considered sensitive and thus should not be marked as CI.[213]

However, the Council strongly opposed to public access to documents. It argued that disclosure of the information in question would lead the institutions to prefer oral to written proposals, a practice that would affect the transparency of the decision-making process.[214] Hillebrandt and Novak report that despite the Court's sharp ruling, the Council applied the identification of MS practice only where it considered it appropriate.[215]

The overall picture does not differentiate when the European Parliament is the

[212] T-233/09 *Access Info Europe v Council* EU:T:2011:105.
[213] <https://globalfreedomofexpression.columbia.edu/cases/ecj-access-info-europe-v-council-european-union/> accessed 30 September 2021.
[214] David A. O. in Edward and Robert Lane, *Edward and Lane on European Union Law* (Edward Elgar Publishing 2013) 91.
[215] Maarten Hillebrandt and Stéphanie Novak (2016) 'Integration without transparency? Reliance on the space to think in the European Council and Council' 38(5) Journal of European Integration 527.

relevant institution. However, in the seminal *De Capitani*[216] ruling, the General Court, strongly strengthened the right of public to access the documents when it annulled the decision of the European Parliament to deny full access to documents drawn up in the context of in progress tripartite[217] discussions, on an ordinary legislative procedures decision-making process. Until then, the tripartite meetings were a limited process within the circle of competent experts. Brandsma reports that this decision is fundamental, as most of the institutional reports and academic literature presented a rather bleak picture in terms of the transparency of the tripartite contacts, while this decision even went beyond the recommendations of the European Ombudsman. Furthermore, transparency at this point is crucial to the legality of EU law; at this point where decisions are made, it is vital to provide all information, explanations, and justifications to the public in a timely manner in order to the ability to submit views and concerns, but also to strengthen accountability on the part of decision-making bodies as negotiations continue.[218]

The context of this case reflects Costa's point regarding general presumptions: the Council and the Commission have intervened in the proceedings, seeking, inter alia, a general presumption of non-disclosure of such information. The institutions' defensive approach, instead of focusing on enhancing transparency and legitimacy. The Court rejected the request for a relevant presumption, indicating that they are secured in specific proceedings, contrary to the wide scope of the legislative activity in this case. The significance of this decision and its practical impact are reflected,

[216] T-540/15 *Emilio De Capitani v European Parliament* EU:T:2018:167.
[217] Between the European Parliament, the Council, and the Commission.
[218] Gijs Jan Brandsma, 'Transparency of EU informal trilogues through public feedback in the European Parliament: promise unfulfilled' (2019) 26(10) Journal of European Public Policy 1464.

inter alia, in the European Parliament 's annual report; the range of information made public by the European Parliament following this decision is greater.[219]

The field concerning the general presumptions that the CJEU itself recognized in its case law, dominated in another revolutionary decision, issued on 4 September 2018. In the appeal brought by the environmental organization *ClientEarth*,[220] the CJEU annulled the judgment of the General Court acquitting the Commission when it refused to grant access to impact assessment documents on access to justice and environmental inspections under Article 4(3) of the Regulation. In particular, the Commission claimed that the documents were impact assessments under way for legislative initiatives and that they were intended to assist its decisions in preparing legislative proposals and strategic choices. Further, it alleged that disclosure of the disputed documents at that stage of the procedure would seriously affect the ongoing decision-making processes and it argued that this would limit its space for maneuver, its ability to find compromises and run the risk of creating external pressures that could hamper the proceedings, which should be carried out in a climate of trust.[221] Arguments like these, not only are irrational but also fail to hide the fact that the Commission did not act independently; instead it was guided by the opinions of the MS.[222] Moreover, a severe issue emerges on how the Commission itself perceives the overall matter of transparency and the constitutional mantle of the right of access

[219] European Parliament's Annual Report 2018, *Public Access to Documents* (2019) 13.
[220] C-57/16 P *ClientEarth v European Commission* EU:C:2018:660.
[221] C-57/16 P *ClientEarth v European Commission* EU:C:2018:660 para. 13.
[222] Laurens Ankersmit*, '*Case C-57/16P ClientEarth v Commission: Citizen's participation in EU decision-making and the Commission's right of initiative' (2018) European Law Blog.

to documents.[223]

However, the Court has made it clear that although the submission of a legislative proposal by the Commission is, at the impact assessment stage, uncertain, the disclosure of these documents can improve the transparency and openness of the legislative process as a whole, and in particular the preparatory stages of this process, and thus strengthen the democratic character of the EU by giving citizens the opportunity to have a meaningful opinion before their enforcement.[224] Wyatt notes that the *ClientEarth* ruling is a success, as on time transparency, especially on matters of legislation, is an essential aspect of democracy and the rule of law. If the Court allowed, as it explains, the Commission to remain behind a veil in its preparatory legislative activities, this would clearly be a step away from such ideals.

Although the CJEU ultimately did not accept in this case the extension of the doctrine of the presumption of confidentiality, the ease with which the General Court accepted the Commission's argument is distressing. It should be noted that the presumptions have no legal basis in the Regulation and, moreover, their application in any case is clearly contrary to the philosophy of the widest possible access and transparency. Finally, it should be noted that presumptions are a problematic point in the case law of the Court, as they seem to be based in part on a questionable interpretation of the Regulation which argues that there is a legal difference between legislative and non-legislative documents. CJEU, while understanding the emphasis

[223] Daniel Wyatt, 'Is the Commission a "lawmaker"? On the right of initiative, institutional transparency and public participation in decision-making: ClientEarth' (2019) 56 Common Market Law Review 825.
[224] C-57/16 P *ClientEarth v European Commission* EU:C:2018:660 para. 92.

on wider access to legislative documents, it interprets it as a reason for a narrower understanding of the right of access to non-legislative documents, thus effectively justifying the application of presumptions of confidentiality.[225]

Paradoxically, although Regulation 1049/2001 has been in force for several years, the CJEU did not address extensively the exception provided by Article 4(1)(a). Finally, although CJEU is considered an important factor in the EU, it tends to be abandoned in access rights discussions and therefore there is no academic literature that sheds light on its contribution to the development of the EU access to documents right regime.[226]

However, in cases where the CJEU was engaged, as seen above, its impact was increasingly favourable to citizens concerning the general protection of human rights in EU and the inclining demand for transparency and accountability by the EU institutions. The same trend was followed by the other European supranational court even though the progress is more remarkable.

4.2.2 European Court of Human Rights case law on access to information

Prior to the enactment of the CFREU, the main international instrument for the protection of human rights in EU was the ECHR and the rulings of ECtHR, which

[225] Daniel Wyatt, Is the Commission a "lawmaker"? On the right of initiative, institutional transparency and public participation in decision-making: ClientEarth' (2019) 56 Common Market Law Review 825.
[226] I. Spahiu, 'Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union' 2015, 31(80) Utrecht Journal of International and European Law 5.

served as 'a key source of inspiration' for the general principles of EU law.[227] Since the enactment of the CFREU, Article 52(3)[228] specifies the relevance of the ECHR in the EU and thus the ECtHR's rulings. Consequently, ECtHR's judgements are of great importance when discussing human rights in EU.

The freedom to hold opinions, and to receive and impart information and ideas is enshrined in Article 10[229] of the Convention. According to Diamandouros,[230] the Strasbourg court went through a long period of restraint and reluctance to recognize the public's right of access to documents. The ECtHR was called upon to rule on the issue for the first time in the 1980s, at a time when the requirements of transparency and open government did not concern most European countries.

[227] C-260/89 *Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others* EU:C:1991:254; *Opinion 2/94 on Accession by the Community to the ECHR* EU:C:1996:140; C-299/95 *Friedrich Kremzow v Republik Österreich* EU:C:1997:254.

[228] Article 52(3) of the CFREU:
'3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

[229] Article 10 – Freedom of expression:
"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[230] Nikiforos Diamantouros, Δικαίωμα πρόσβασης σε έγγραφα και πληροφορίες κατά το ευρωπαϊκό δίκαιο ΣΥΓΧΡΟΝΟΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΕΠΙΠΕΔΟ, Εθνική Σχολή Δικαστικών Λειτουργών, Θεσσαλονίκη 23 και 24 Φεβρουαρίου 2012, Α΄ Συνεδρίαση https://www.ombudsman.europa.eu/en/speech/el/11308.

In the *Leander*[231] judgment, the Court, approaching the matter formally, held that the secret scrutiny of persons who had applied for key national security posts was not contrary to the prerequisite of necessity for a democracy. The Court considered that states have a wide margin of appreciation and ruled that freedom of expression prohibited states from preventing the individual from obtaining information that third parties wished to provide to him. However, without granting the individual access to records containing information about her/his person. At the same time, the Court did not impose an obligation on the authorities to provide it. The right of the individual, it added, to be informed of such information could be claimed by invoking Article 8, provided that the requested information could affect the applicant's private or family life.

In the *Guerra* case[232], the ECtHR missed the opportunity to establish the obligation for the authorities to provide access to information for reasons of public interest. The reasoning was that the requested information did not belong to the narrow sphere of privacy but concerned the authorities' failure to inform the public about the risks to the environment and the health of citizens living in the area of a factory emitting harmful substances. This decision could be described as a bleak page in the history of the Strasbourg Court because its strict grammatical interpretation prioritised public health in a second place. The ratio decidendi of this decision was reversed in the *Roche*[233] judgment. ECtHR ruled that the United Kingdom's refuse to grant access to documents relating to the applicant's exposure

[231] ECtHR, *Leander v. Sweden*, Application no. 9248/81, 26/3/1987.
[232] ECtHR, *Guerra and Others v. Italy*, Application no. 116/1996/735/932**,** 19/2/1998.
[233] ECtHR, *Roche v United Kingdom*, Application no. 32555/96, ECHR 2005-X, (2006) 42 EHRR 30, IHRL 3210 (ECHR 2005), 19/10/2005.

to harmful chemicals was contrary to the Convention.

In the ground-breaking decision *Observer and Guardian*,[234] the ECtHR ruled that time passing, whatever CI published by the well-known newspaper had lost its confidentiality and there was no longer any need for a state to take measures. Another notable shift in ECtHR case law took place in 2007 in *Matky*[235] decision. This case concerned a non-governmental organisation appealing against the refusal of the Czech authorities to grant access to documents for a nuclear power plant. The Court has implicitly acknowledged that the applicant 's right of access to such documents falls within the scope of Article 10 of the ECHR and that the authorities' refusal to grant access to it constituted an infringement. Although the recognition of the right of access to public documents was done indirectly, the progress made was remarkable, and this decision undoubtedly laid the foundations for the opening of the road that would lead to its foundation. Subsequently, in the *Stoll* case,[236] the Court held that the ECHR's provision "obstruction of the disclosure of confidential information" includes disclosure of CI received by a non-disclosure entity, or by a third party, including a journalist, who receives such information in the absence of such an obligation.[237]

An important launch of the recognition of the right under Article 10 ECHR took place a little later in two decisions against Hungary. In the *Kenedy* judgment,[238] the ECtHR requested access to documents from the Hungarian Ministry of the Interior,

[234] ECtHR, *Observer and Guardian v the United Kingdom*, Application no. 13585/88, 26/11/1991.
[235] ECtHR, *Sdružení Jihočeské Matky v. Czech Republic*, Application no. 19101/03, 10/7/2007.
[236] ECtHR, *Stoll v Switzerland*, Application no. 69698, 10/12/2007.
[237] Costas Paraskeva, *Κυπριακό Συνταγματικό Δίκαιο: Θεμελιώδη Δικαιώματα και Ελευθερίες* (Νομική Βιβλιοθήκη 2015).
[238] ECtHR, *Kenedy v Hungary*, Application no. 31475/05**,** 26/5/2009.

which was submitted by a researcher-historian to conduct a study on the Hungarian secret services in the 1960s. In that case the Hungarian courts had acquitted the applicant, but the administrative authorities systematically refused to enforce the judgments and grant access to the documents in question. In examining the case, the ECtHR acknowledged that access to archives in the context of legal historical inquiry is an integral part of the right to freedom of expression. What is striking in this case is the fact that the ECtHR did not hesitate to extend its case law in the field of intelligence services.

A month earlier, in the *Szabadságjogokért* judgment,[239] the ECtHR examined the refusal of the Hungarian authorities and courts to allow an NGO to become aware of the constitutional complaint lodged by a member of the parliament concerning amendments to criminal provisions. Despite the remarkable progress, the ECtHR, insisting on its reluctance, did not recognise a general right of public access to public documents, but examined the case from the point of view of the public's right to receive information and the role of the press in informing the public. It aligned the role of NGOs in promoting public debate with that of journalists, naming them as "guardians of society". Consequently, the judgement ruled that the refusal of the Hungarian authorities was an interference to the role of the NGO but not a denial of a general right of access to information. Despite the reluctance for universal and direct recognition of the right of access to public documents, the *Szabadságjogokért* decision is an important legal precedent especially for NGOs, since by designating them as "guardians of society", they have been given the role of

[239] ECtHR, *Társaság a Szabadságjogokért v Hungary*, Application no. 37374/05, 14/4/2009.

enhancing transparency and democracy.

The significance of the above case law in the field of CI and public access to public documents is evident in the case of the NGO *Youth Initiative*,[240] which requested access to information on the number of persons subject to electronic surveillance by the Serbian intelligence service during 2005. In this decision, the ECtHR recognized more clearly than ever the right of citizens to access documents held by public authorities, based on Article 10 of the Convention but also the importance of NGOs to act in the public interest. Furthermore, in this judgment the Court clarified that in Europe security and intelligence services must necessarily respect both national law and the ECHR.

Extremely enlightening is the very recent decision of the *Center for Democracy and the Rule of Law*[241] where the Ukrainian government denied NGOs access to information on education and work history contained in the CVs of political leaders running in the parliamentary elections. The government's reasoning was that the requested information is confidential and can only be fully disclosed with the consent of the parties concerned. In this case, the ECtHR issued a decision based on four axes: the purpose of the request for information, the nature of the information requested, i.e., whether the information requested met the public interest test, the specific role of the information requester in "receiving and transmission to the public, i.e., whether the applicant had an important "guardian" function and, finally, whether the requested information is ready and available. The ECtHR, however, did not

[240] ECtHR, *Youth Initiative for Human Rights v Serbia*, Application no. 48135/06, 25/6/2013.

[241] ECtHR, *Centre for Democracy and the Rule of Law v. Ukraine*, Application no. 10090/16, 26/3/2020.

support press freedom unconditionally. It ruled that certain limitations must apply on its operation so that the public interest would not be harmed. In that regard, as far as the press is concerned, the Court has made it clear that the content of a journalistic text containing CI, in order to benefit from the protection of Article 10 of the ECtHR, must be capable of contributing to the public debate.[242] In addition, in the event of damage to a public authority or an individual as a result of disclosure in the public interest, the provisions of Article 10 protect the journalist unless the damage outweighs the public interest in obtaining the information. According to the reasoning of the Court, the sanctions that may be imposed on journalists who reveal CI should not prevent them from contributing to the discussion of issues that affect public life, nor discourage the press from expressing criticism, nor, of course, prevent it in the performance of its duties as an information provider.[243] In this way, the Court put all the parameters in a balance, creating a framework for all stakeholders that promotes, among other things, legal certainty.

Relevant is the decision *Telegraaf Media*[244] where the Court examined the case where the publisher and two journalists of the daily Dutch newspaper De Telegraaf were ordered to hand over documents related to the activities of the Dutch intelligent services. Based on these documents, the newspaper published articles related to

[242] See ECtHR, *Stoll v Swizerland*, Application no. 69698/01, 10/12/2007; *Bédat v Switzerland*, Application no. 56925/08, 29/3/2016; *Vereniging Weekblad Bluf! v the Netherlands*, Application no. 16616/90, 9/2/1995; *Pinto Coelho v Portugal* (n° 2), Application no. 48718/11, 22/03/2016; *Dupuis and Others v France*, Application no. 1914/02, 7/6/2007; *Dammann v Switzerland*, Application no. 77551/01, 25/4/2006.

[243] Council of Europe, 'Freedom to Impart Confidential Information and Its Limits', *Thematic factsheet*, 9 May 2016.

[244] ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands* – Application no. 39315/06, 22/11/2012.

investigations of the country's intelligence services, concerning CI that had been placed in the criminal circuit of Amsterdam. The Dutch court did not find that the rights protected by ECHR Article 10 were violated, as applicants were not required to cooperate in identifying their sources, also ruling that the protection of state CI justified interference with the right to source protection. The ECtHR, however, did not agree and ruled that there had been a violation of various articles of the ECHR in this case.

As the Court points out, the tendency is to require national bodies to verify that any threat has a reasonable basis.[245] Recognizing that the public right to information, including CI, may conflict with equally important public and private interests, such as the protection of national security, the protection of privacy, the effectiveness of criminal investigations and presumption of innocence, the Court stresses the necessity of striking a fair balance between the various interests at stake.[246]

On the other hand, ECtHR's position differentiates when military information is under scrutiny. In the *Hadjianastassiou* judgment,[247] the ECtHR set out two important guidelines: that not all military information is deleted from the public debate and that it is for national courts to determine in each case, based on the principle of proportionality,[248] whether such information poses a real and serious threat to national security. Accordingly, in *Pasko*[249] ruling, the Court agreed with the Russian

[245] European Court of Human Rights, *National security and European case-la*w (2013).
[246] Council of Europe, 'Freedom to Impart Confidential Information and Its Limits', *Thematic factsheet*, 9 May 2016.
[247] ECtHR, *Hadjianastassiou v Greece*, Application no. 12945/87, 16/12/1992.
[248] For more information on the principle of proportionality see Takis Tridimas, *General Principles of EU Law* (OUP 2007).
[249] ECtHR, *Pasko v Russia,* Application no. 69519/01, 22/10/2009.

authorities. In this case, a Russian naval officer, working as a military journalist, who on a free-lance basis had also been in contact with Japanese media, was searched before flying to Japan. A number of his papers were confiscated with the explanation that they contained CI. On his return from Japan he was arrested for having collected CI containing actual names of highly critical and secure military formations and units, with the intention of transferring this information to a foreign national. The ECtHR ruled that the Russian courts had struck the right balance of proportionality between the aim of protecting national security and the means used to achieve that purpose, namely the sentencing of the applicant, when after careful scrutinization of the applicant's arguments, convicted him of treason though espionage as a serving military officer and not as a journalist.

Another ruling of special jurisprudential significance is *Wille v Liechtenstein*,[250] where ECtHR ruled that any national legislation imposing absolute restrictions on the confidence or confidentiality of certain categories of public officials, such as those serving in the intelligence services, the army or members of the judiciary, violates ECHR Article 10. Such restrictions may be adopted by the Council of Europe Member States only when they are not general in nature but are limited to specific categories of information, of civil servants or only to certain persons belonging to such categories and on a temporary basis. When Member States invoke duties of fidelity or confidentiality in the interests of national security, as the ECtHR points out, they must define the concept strictly and closely in the real field of national security. Similarly, states must demonstrate that there is a real risk to the protected interest,

[250] ECtHR, *Wille v Liechtenstein*, No. 28396/95, 28 October 1999.

as well as take into account the public interest in accessing certain information.[251]

Concluding, ECtHR judgments and decisions undoubtedly elucidated, safeguarded and developed the right enshrined in Article 10 of the Convention, thereby contributing to the observance by the states of the engagements undertaken by them as Contracting Parties.

4.2.3. Comparison of judicial approaches

Assessing the routes of the two supranational European Courts, one can observe that both started from a point rather unfavourable for the right of citizens to access information, but progressively enhanced the picture in favour of the individual.

The CJEU's approach revolves around the fact that the institutions have a wide discretion when proving the existence of a public interest reason for denying access to documents, because it is considered part of their "political responsibilities" deriving from the Treaties. The Luxembourg Court therefore conducts a relatively limited or marginal review of such decisions in order to verify compliance with the rules of procedure, the fulfillment of the obligation to state reasons, the accuracy of the facts and the assessment of the institution without manifest error or misuse of powers. In addition to the above, the Court requires that evidence is provided for each document to which access is denied and that there is a reasonably foreseeable rather than hypothetical risk that the disclosure would undermine the protected public interest.

[251] Dominika Bychawska-Siniarska, 'Protecting The Right To Freedom Of Expression Under The European Convention On Human Rights: A handbook for legal practitioners' (Council of Europe, 2017).

ECtHR, as a court with pure human rights jurisdiction, which is not required to take into account political or other dimensions, despite its initial reluctance, has established and maintains a significantly more favorable approach to citizens and the protection of their right of access to information even when these are classified. The Strasbourg Court's decisions are mainly based on the purpose of the application for access, the actual safeguarding of the public interest and the role of the information seeker in relation to the benefit of society as a whole. It can be concluded that its approach is based substantial guidelines on balancing the conflicting interests and the pursued goals, rather than the procedural requirements enforced by the CJEU.

It can be observed that the Strasbourg Court maintains a significantly different approach to the protection of human rights concerning CI than the Luxembourg Court. The former seems to have a more favorable attitude towards citizens, while the latter has been criticized for insufficient protection of human rights, unreasonably deciding in favor of the EU institutions. The whole issue exacerbates the tug-of-war, which is generally recorded in academia, regarding the relationship between the two European courts in the field of human rights protection. [252]

Finally, the EU, which declares that security and respect for fundamental rights are not conflicting objectives but consistent and complementary policy objectives, should re-evaluate its overall and comprehensive approach to the issue. Its attitude, if it is to be based on democratic values, including the rule of law, should be grounded on respect of fundamental rights as these are set out in the CFREU and in

[252] Lize R. Glas and Jasper Krommendijk, 'From *Opinion 2/13* to *Avotiņš*: Recent Developments in the Relationship between the Luxembourg and Strasbourg Courts' (2017) 17(3) Human Rights Law Review 567; Giacomo Biagioni, 'Avotinš v. Latvia: The Uneasy Balance Between Mutual Recognition of Judgments and Protection of Fundamental Rights' (2016) 1(2) European Papers 579.

particular that the commitment to all security measures and legality, with appropriate safeguards to ensure accountability and litigation, is embodied effectively and realistically.[253]

Nevertheless, the MS are all bound by minimum international human rights law standards developed by the UN, which are of universal application. Likewise, the Council of Europe provides a minimum standard. Moreover, the EU is bound by its Treaties to promote human rights, democratization and development. However, safeguarding human rights and fundamental freedoms is not all about declarations. It is a critical challenge.

[253] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: The European Agenda on Security* COM(2015) 185.

5

EPILOGUE

EU must pursue multiple and often competing goals at home and abroad. Information is a critical asset that enables the European institutions to exercise their Treaty mandates and achieve their objectives. The need for safeguarding valuable information often leads executive bodies to adopt exceptional measures. However, at all events, there must be statutory guarantees preventing any misuse. No state or organisation has the right to disregard the principle of the rule of law. Democratic legitimacy must take precedence over confidentiality.

5.1 Recommendations

As seen in the analysis preceding, the EUCI legal regime is complicated, procedural, bureaucratic, strictly internal, technical in nature and interferes greatly with individuals' rights. EU and its MS are all bound by international, regional and national human rights law standards. Aside from existing international human rights law and given that a limited number of applicable international regulations apply, the role of self-regulatory measures and soft law should be further assessed. Traditionally, inaccessible national security and defence sectors need to accommodate new values of transparency and accountability.

While acknowledging the difficulty of balancing the executive's concern to protect certain information with the requirements of openness and transparency, there should be at least a public debate on the matter rather than of leaving it to be decided by committees, beyond the public eye, as is the current system in most

cases. The delicate balance between confidentiality and accountability can be managed through elements such as clear and accessible legislation, strong oversight mechanisms, proper control mechanisms, and effective remedies. These shall create the level of accountability which encourages the trust society should have vis-à-vis its CI policies.

In addressing these issues, EU must take into account the full range of interests and values that it is pursuing, including the protection of the Union against threats, the promotion of security and foreign policy interests, fundamental rights, democracy, transparency, accountability and the rule of law. Civil society requires more insight and better guarantees concerning security measures that are relevant to them. There is no reason why a functional defence and security sector cannot coexist with legal codes which allow for access to information, transparency, and accountability.

In order to improve the current situation in EUCI area, EU needs to reform the existing legal framework with a view to enhancing democratic legitimacy of the EU's practices as well as protection of fundamental rights such as access to information, fair trial and the rights of the defense; clarify the exact powers deriving from the Treaties on handling EUCI; eliminate shortcomings identified in practice; clearly define the manner of prequalification of EUCI; establish balance between EUCI and information of public significance within the principles of a democratic society; intensify the oversight of national authorities handling EUCI; and implement adequate training of relevant representatives of public authorities on the matter of EUCI, human rights and other relevant legal matter.

Additionally, any system handling CI in support of decision-making and/or information sharing must be reliable and trustworthy and its security objectives in a broad sense shall be to safeguard EUCI against threats to confidentiality.

5. Epilogue

Democratic supervision makes use of a series of specific tools intended to ensure the political accountability and transparency of the security sector. These instruments include institutional and logistical provisions, constitutional principles and legal rules, as well as more general activities aimed at fostering good relations between the various parts of the security sector on the one hand, and the political powers (the executive, legislative and judiciary) and representatives of civil society (NGOs, the media, political parties, etc.) on the other. Clear legal frameworks, robust safeguards and effective oversight are needed to enhance security and respect fundamental rights. Transparency International[254] has collected a lot of guidelines and good practice regarding access to information by oversight bodies, freedom of information laws, automatic declassification procedures (or time limits for period of classification), procedures to follow when declassifying information, external review of classification procedure, prohibited classifications and protective markings. Legislation in this area must be updated regularly and take into account developments in modern technologies and cybercrime.

In terms of soft law, EU is called upon to adopt a European code of ethics: a professional code for the transnational management and accountability of data in the EU. The European Parliament could call for the inter-institutional adoption of an EU code for the transnational management and accountability of information addressed to the MS. The goal should be to ensure that the practices of intelligence services and other national authorities are in accordance with fundamental rights and rule of law principles. Most importantly, it would present a common EU understanding of the basis on which national security should not be invoked by MS authorities. An EU

[254] Transparency International 'Classified Information: A review of current legislation across 15 countries & the EU' (2014).

observatory body should be established to map and follow up EUMS' uses and evolving interpretations of national security and state secrets.

Executive measures must be both lawful and legitimate. Consequently, some form of democratic supervision is required. Oversight bodies contribute to a better understanding of how CI policies work. Despite the great diversity and the predominantly national competences of oversight bodies, exchanges on practices between actors help clarify and enhance relevant control standards. Such exchanges and cooperation should, however, not be limited to oversight bodies. Exchanges on the manner in which intelligence services and national security agencies uphold fundamental rights in their work could be beneficial. There is also the need to ensure full cooperation and complementarity between various oversight bodies so there is continuous coverage of all surveillance steps – from authorization to implementation.

The essence of such a supervision must be carried out by the European Parliament, as an accountability forum, since it is the only democratically elected EU institution at the supranational level capable of performing functions of democratic oversight over a secretive EU executive. The European Parliament should call for a consolidated partnership with supranational human rights actors such as the Council of Europe and the UN. An EU framework for the protection of whistle-blowers in cases related to national security should be adopted.

The judiciary, in turn, plays a crucial role because it can punish any misuse of exceptional measures in which there may be a risk of human rights violations. Strengthening the ways in which the courts and judicial actors fulfil their duty to uphold the rule of law with increased vigilance is a necessity. The EU can play a role in consolidating, promoting and ensuring more effective implementation of

supranational fundamental and human rights principles developed by European Courts and the rule of law. In light of this, the new EU framework to strengthen the rule of law should encourage MS to modify their current legislation on the use of national security, state secrets and intelligence information in judicial proceedings. The growing reliance of certain MS on the use of secret evidence in courts constitutes a direct challenge to judicial scrutiny, as well as to the rights of the defence and freedom of the press laid down in the EU Charter of Fundamental Rights. Freedom of the press and the audio-visual media must be preserved in law and in practice. Restrictions imposed in cases of absolute necessity must not entail any infringement of the international principles of fundamental rights.

The central role of the European Parliament does not mean that there is no role for national parliaments; there clearly is, but the relevant national regimes are still fragmented and scattered, as was shown in the case of Cyprus. National parliaments should have an appropriately functioning specialised committee. It could be a system of collective consultation between national parliaments on security and defence issues. This could behave as an interparliamentary body to which the relevant European executive body would report and with which it would hold regular institutional discussions on all aspects of European security and defence.

Regarding national level, EU institutions must prepare and adopt guidelines for governments setting out the political rules, standards and practical approaches required to apply the principle of democratic supervision of the security sector in MS. The functioning of intelligence services or any other office handling EUCI must be based on clear and appropriate legislation supervised by the courts. Cyprus and any other MS need to harmonize other relevant national regulations, such as the Criminal Code; evaluate more appropriate practical deadlines for supplementing the legal

framework and harmonization with it in case of amendments to the existing Law or adoption of a new one. In doing so, they could pre-emptively prevent the possible existence of idle walk in the enforcement of the Law caused by the inability to adopt all the necessary associated regulations within the set deadline; and review the competences of the Commissioner of Data Protection in accordance with her/his powers within the meaning of supervision over the implementation of the Law on Classified Information, as the only independent specialized-expert body for the area of information.

5.2. Summary of Conclusions

The purpose of this paper was to contribute to public debate on democratic oversight and scrutiny as well as intrigue the interest of legal and political science scholars on the relevant EUCI legal framework. The concluding point is that (a) the existing situation in EU prioritizes security and secrecy, (b) the legislation regime suffers from fragmentation, complexity, and vagueness and (c) the status quo fails to provide adequate protection of citizens' fundamental rights. Moreover, even though the existing legal framework on EUCI is mandatory for the MS, EU does not provide the necessary guidance to adequately harmonise MS' national regimes. This is partly due to fact that EU introduces legislative measures based on an implied power and partly because CI issues are considered procedural rules of secondary importance.

The EU institutions must fulfil their role deriving from the Treaties and address the inefficiencies. However, further research must be initiated regarding matters such as the extent of the impact on other human rights in public or private law, whether the competences of EU should be regulated differently in light of its increasing role as a

security actor and finally, whether CJEU and ECtHR could play a more decisive role on protecting human rights.

Finally, this paper can be used as a base of knowledge of the shortcomings of the current EUCI legal framework and the challenges it needs to confront. By highlighting these shortcomings, governments, practitioners, and analysts can identify the deficiencies and discuss ideas on the appropriate methods to balance the interests protected by CI and human rights.

LIST OF REFERENCES

Abazi V, *Official Secrets and Oversight in the EU: Law and Practices of Classified Information* (OUP 2019) 114.

Abazi V and Hillebrandt M, "The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In 't Veld" [2015] 52 Common Market Law Review 825.

African Union, African Union Convention on Cyber Security and the Protection of Personal Data (adopted 27 June 2014) <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf > accessed 30 September 2021.

Ankersmit L*, '*Case C-57/16P ClientEarth v Commission: Citizen's participation in EU decision-making and the Commission's right of initiative' (2018) European Law Blog.

Australian Government, *Information Security Management Guidelines: Australian Government Security Classification System* (2011).

Axelrod C W, Bayuk J L and Schutzer D, *Enterprise Information Security and Privacy* (Artech House 2009).

Barnard C and Peers S, *European Union Law* (OUP 2017).

Biagioni G, ‘Avotinš v. Latvia: The Uneasy Balance Between Mutual Recognition of Judgments and Protection of Fundamental Rights’ (2016) 1(2) European Papers 579.

Bigo C, Carrera S, Hernanz N and Scherrer A, *National Security and Secret Evidence in legislation and before the Courts: Exploring the Challenges* (European Parliament 2014) <https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf> accessed 30 September 2021.

Bitton R, ‘The Legitimacy of Spying Among Nations’ (2014) 29(5) American University International Law Review 1009.

Borchardt K, *The ABC of EU Law* (European Union 2017).

Brandsma G, ‘Transparency of EU informal trilogues through public feedback in the European Parliament: promise unfulfilled’ (2019) 26(10) Journal of European Public Policy 1464.

Bychawska-Siniarska D, ‘Protecting The Right To Freedom Of Expression Under The European Convention On Human Rights: A handbook for legal practitioners’ (Council of Europe, 2017).

Center for Euroatlantic Studies, The Law on Classified Information (2015) <https://issat.dcaf.ch/download/92038/1612447/CEAS-Law%20on%20Classified%20Information-2015.pdf> accessed 1 October 2021.

Chalmers D, Davies G and Monti G, *European Union Law: Cases and Materials* (Cambridge University Press 2010) 390.

Charalambous N, *Εγχειρίδιο Κυπριακού Διοικητικού Δικαίου* (3rd edn Typografia Livadioti 2016].

Cleynenbreugel P, 'Confidentiality behind Transparent Doors: The European Central Bank and the EU Law Principle of Openness' (2018) 25(1) Maastricht Journal of European and Comparative Law 52.

Commission Decision 2001/844/EC,ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure [2001] OJ L 317/1.

Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information OJ L72/53.

Commission Decision (EU, Euratom) 2019/1961 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information [2019] OJ L 311/1.

Costa M, *The Accountability Gap in EU law: Mind the Gap* (Routledge 2017).

Council Decision 2000/396/EC, ECSC, Euratom: Council Decision of 5 June 2000 adopting the Council's Rules of Procedure [2000] OJ L 149/21.

Council Decision 2001/264/EC: Council Decision of 19 March 2001 adopting the Council's security regulations [2001] OJ L 101/1.

Council Decision 2001/844/EC, ECSC, Euratom: Commission Decision, of 29 November 2001, amending its internal Rules of Procedure [2001] OJ L 317/1.

Council Decision 2009/937/EU of 1 December 2009 adopting the Council's Rules of Procedure [2009] OJ L 325/35.

Council Decision 2013/488/EU, of 23 September 2013, on the security rules for protecting EU classified information [2013] OJ L 274/1.

Council of Europe, Convention on Cybercrime (ETS No. 185) (adopted on 23 November 2001, entered into force on 01 July 2004).

Council of Europe, 'Freedom To Impart Confidential Information And Its Limits' *Thematic factsheet*, 9 May 2016.

Craig P, *EU Administrative Law* (3rd edn OUP 2019).

Craig P and Burca G, *EU Law Text, Cases and Materials* (7th edn, OUP 2020).

Cremona M, ‘External competences and the principle of conferral’, in Robert Schutze and Takis Tridimas (eds), *Oxford principles of European Union law* (OUP 2018) 1110.

Curtin D, ‘Overseeing Secrets in the EU: A Democratic Perspective’ (2014) 52(3) *Journal of Common Market Studies* 684.

Curtin D, ‘Challenging executive dominance in European democracy’ In C. Joerges, & C. Glinski (Eds.) *The European crisis and the transformation of transnational governance: authoritarian managerialism versus democrtic governance* (Oxford Hart 2014).

Cyprus National Security Authority, <http://www.nsa.gov.cy/mod/nsa/cynsa.nsf/page13_gr/page13_gr?OpenDocument> accessed 15 October 2021.

David AO in Lane, *Edward and Lane on European Union Law* (Edward Elgar Publishing 2013) 91.

Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service [2018] OJ C 126/1.

Defeo M, ‘What internation law controls exist or should exist on intelligence operations and their intersections with criminal justice systems?’ (2007) 78(1) Revue Internationale De Droit Pénal 57.

Diamantouros N, Δικαίωμα πρόσβασης σε έγγραφα και πληροφορίες κατά το ευρωπαϊκό δίκαιο ΣΥΓΧΡΟΝΟΙ ΠΡΟΒΛΗΜΑΤΙΣΜΟΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΕΠΙΠΕΔΟ, Εθνική Σχολή Δικαστικών Λειτουργών, Θεσσαλονίκη 23 και 24 Φεβρουαρίου 2012, Α΄ Συνεδρίαση https://www.ombudsman.europa.eu/en/speech/el/11308.

Driessen B, *Transparency in EU Institutional Law: A Practitioner's Handbook* (Cameron May 2008) 51.

European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: The European Agenda on Security* COM(2015) 185.

European Court of Auditors, Challenges to effective EU cybersecurity policy: Briefing Paper (2019).

European Court of Human Rights Research Division, *National Security and European Case-Law* (European Court of Human Rights 2013).

European External Action Service, Shared Vision, Common Action: A Stronger Europe a Global Strategy for the European Union’s Foreign and Security Policy

(2016) <https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf> accessed 7 October 2021.

European IPR Helpdesk, *Fact Sheet: How to Manage Confidential Business Information* (2015) <https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-How-to-Manage-Confidential-Business-Information.pdf> accessed 30 September 2021.

European Parliament, *Openness, Transparency and the Right of Access to Documents in the EU: In-Depth Analysis* (2016) <https://op.europa.eu/en/publication-detail/-/publication/32d52e3d-3cf3-11e6-a825-01aa75ed71a1> accessed 1 October 2021.

European Parliament, *Understanding EU Counter-Terrorism Policy* (2021) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/659446/EPRS_BRI(2021)659446_EN.pdf> accessed 30 September 2021.

European Parliament's Annual Report 2018, *Public Access to Documents* (2019) 13.

European Union Agency for Cybersecurity, *ENISA Threat Landscape 2021* (2021) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> accessed 29 September 2021.

European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights* safeguards *and remedies in the EU*

Mapping Member States' legal frameworks (Publications Office of the European Union, 2015).

Fleck D, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Michigan Journal of International Law 687.

Foret F and Calligaro O, 'Challenges and opportunities for EU governance' in François Foret, Oriane Calligaro (eds), European values (Routledge 2018).

Fruhlinger J, 'What is information security? Definition, principles, and jobs' <https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html.> 25 September 2021.

Galloway D, 'Classifying Secrets in the EU' (2014) 52(3) *Journal of Common Market Studies* 668.

Glas L R and Krommendijk J, 'From *Opinion 2/13* to *Avotiņš*: Recent Developments in the Relationship between the Luxembourg and Strasbourg Courts' (2017) 17(3) Human Rights Law Review 567.

Goede M and Wesseling M, 'Secrecy and security in transatlantic terrorism finance tracking' (2017) 39(3) Journal of European Integration 253.

Harlow C, Leino P and Cananea G, *Research Handbook on EU Administrative Law* (Edward Elgar 2017) 407.

Hatzimihail N, ‘Cyprus as a Mixed Legal System’ (2013) 6 Journal of Civil Law Studies 42.

Hatzimihail N, ‘Reconstructing Mixity: Sources of Law and Method in Cyprus’ in V. Palmer et al, *Mixed Legal Systerms East and West* (Ashgate 2015).

Heremans T, ‘Public Access To Documents: Jurisprudence Between Principle And Practice’ (2011) Egmont Paper 50.

Hillebrandt M and Novak S ‘Integration without transparency? Reliance on the space to think in the European Council and Council’ (2016) 38(5) Journal of European Integration 527.

HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (Crown 2010) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf> accessed 5 October 2021.

Hoffmann, Rowe and Türk, *Administrative Law of the European Union* (Oxford University Press 2012).

Hofmann H and Leino-Sandberg P, ‘An agenda for transparency in the EU’ (2019) European Law Blog.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

ISO, <https://www.iso.org/isoiec-27001-information-security.html> accessed 30 September 2021.

Kombos C, *The Impact of EU Law on Cypriot Public Law* (Sakkoulas 2015).

Kyriakou N, "National Judges and Supranational Laws on the Effective Application of the EC Law and the ECHR: The Case of Cyprus" (June 10, 2010). Available at SSRN: https://ssrn.com/abstract=1623560 or http://dx.doi.org/10.2139/ssrn.1623560.

Labayle H, Classified Information in light of the Lisbon Treaty (European Parliament, 2010) <https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/pe425616_/pe425616_en.pdf> accessed 1 October 2021.

Lenaerts K, "In the Union We Trust: Trust-Enhancing Principles of Community Law" (41) Common Market Law Review 317.

Lind AS and Strand M, 'A New Proportionality Test for Fundamental Rights?' (2011) 7 European Policy Analysis 1.

Lykourgos C, "Cyprus Public Law as Affected by Accession to the EU" in Constantinos Kombos (ed) *Studies in European Public Law* (Sakkoulas 2010) 101.

Margaritis K, 'Strengthening the founding values of the EU: The potential role of the Fundamental Rights Agency' (2019) 18(1) European View 97.

Marouda M. N., 'Διεθνές ανθρωπιστικό δίκαιο των ενόπλων συρράξεων' στο Κωνσταντίνος Αντωνόπουλος και Κωνσταντίνος Μαγκλιβέρας (eds), *Το Δίκαιο της Διεθνούς Κοινωνίας* (Νομική Βιβλιοθήκη 2017).

Mitrou L, 'Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες: Η νομική διάσταση' σε Στέφανος Γκρίτζαλης, Κ. Λαμπρινουδάκης, Σωκράτης Κάτσικας, Λίλιαν Μήτρου (eds)**,** *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών: Νομικά και τεχνικά θέματα* (Papasotiriou 2010).

NATO, *Tallinn Manual του Cooperative Cyber Defence Centre of Excellence*.

Neamtu B and Dragos D in Dacian C. Dragos, Polonca Kovač, Albert T. Marseille, *The Laws of Transparency in Action: A European Perspective* (Palgrave Macmillan 2019).

Neocleous A and Bevir D in Dennis Campbell (ed), *Introduction To Cyprus Law* 6 (Yorkhill Law Publishing, 2000).

OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2007).

OECD, “Development of Policies for Protection of Critical Information Infrastructures”, 130 OECD Digital Economy Papers (OECD Publishing, Paris) <https://www.oecd-ilibrary.org/docserver/231008575813.pdf?expires=1638947808&id=id&accname=guest&checksum=01F1858307AAD75DF5E596FD64A3CDAF> accessed 1 October 2021.

OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2015) <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf> accessed 5 October 2021.

Ojanen T, “Administrative counter – terrorism measures – a strategy to circumvent human rights in the fight against terrorism?” in D. Cole, F. Fabbrini and A. Vedaschi (eds), *Secrecy, National Security and the Vindication of Constitutional Law* (Edward Elgar Publishing 2013).

Paraskeva C, *Κυπριακό Συνταγματικό Δίκαιο: Θεμελιώδη Δικαιώματα και Ελευθερίες* (Nomiki Vivliothiki 2015).

Pecsteen E, ‘Public access to documents: effective rear guard to a transparent EU?’ (2015) European Law Blog.

Pun D, ‘Rethinking Espionage in the Modern Era’ (2017) 18(1) *Chicago Journal of International Law* 10.

Radsan AJ, The Unresolved Equation of Espionage and International Law, (2007) 28 Mich. J. Int'l L. 595.

Regulation No.3 implementing Article 24 of the Treaty establishing the European Atomic Energy Community [1958] OJ L17/406.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

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

Reich N, 'Judicial Protection in the EU' (2005) 1 DIREITO GV L Rev 111.

Republic of Cyprus, Criminal Code, Cap.154.

Republic of Cyprus, Military Penal Code (Law 40/1964), Cyprus Government Gazette no. 338, Appendix I(I), 31.07.1964.

Republic of Cyprus, Law on the Security Regulations of Classified Information Documents and Material and Related Issues of 2002 [Law 216(I)/2002] Cyprus Government Gazette no. 3666, Appendix I(I), 27.12.2002.

Republic of Cyprus, Law on the Security Regulations of Classified Information Documents and Material and Related Issues of 2021 [Law 84(I)/2021] Cyprus Government Gazette no. 4836, Appendix I(I), 05.05.2021.

Republic of Cyprus, Security of Classified Information, Documents and Material of the European Union Decree of 2004 (ΚΔΠ 673/2004 και 67/2005) Cyprus Government Gazette Appendix III(I), 6.8.2004.

Rome Statute of the International Criminal Court (adopted on 17 July 1998, entered into force on 1 July 2002) 2187 U.N.T.S. 90.

Scheppele KL, Kochenov DV and Grabowska-Moroz B, 'EU Values Are Law, after All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union' (2020) 39 Yearbook of European Law 3.

Spahiu I**, '**Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union**'** 2015, 31(80) Utrecht Journal of International and European Law 5.

Tornaritis CG, *Cyprus and Its Constitutional and other Legal Problems* (Nicosia 1980).

Transparency International, 'Classified Information: A review of current legislation across 15 countries & the EU' (2014) <https://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf> accessed 30 September 2021.

Tridimas T, 'Knocking on Heaven's Door: Fragmentation, Efficiency and Defiance in the Preliminary Reference Procedure' (2003) CML Rev 40.

Tridimas T, *General Principles of EU Law* (OUP 2007).

United Nations, Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 <https://www.ohchr.org/EN/ProfessionalInterest/Pages/ProtocolI.aspx> accessed 1 October 2021.

United States of America, Executive Order 13526.

United States of America Defense Security Service, *Marking Classified Information: Job Aid* (2017).

Wyatt D, ‘Is the Commission a “lawmaker”? On the right of initiative, institutional transparency and public participation in decision-making: ClientEarth’ (2019) 56 Common Market Law Review 825.

Zwitter A, ‘The Rule of Law in Times of Crisis: A Legal Theory on the State of Emergency in the Liberal Democracy’ (2012) 98(1) Archives for Philosophy of Law and Social Philosophy 95

<https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/> accessed 25 September 2021.

<https://www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 25 September 2021.

LIST OF CASES

A. EUROPEAN COURT OF HUMAN RIGHTS

Bédat v Switzerland, Application no. 56925/08, 29/3/2016.

Centre for Democracy and the Rule of Law v. Ukraine, Application no. 10090/16, 26/3/2020.

Dammann v Switzerland, Application no. 77551/01, 25/4/2006.

Dupuis and Others v France, Application no. 1914/02, 7/6/2007.

Guerra and Others v. Italy, Application no. 116/1996/735/932**,** 19/2/1998.

Hadjianastassiou v Greece, Application no. 12945/87, 16/12/1992.

Kenedy v Hungary, Application no. 31475/05**,** 26/5/2009.

Leander v. Sweden, Application no. 9248/81, 26/3/1987.

Observer and Guardian v the United Kingdom, Application no. 13585/88, 26/11/1991.

Pasko v Russia, Application no. 69519/01, 22/10/2009.

Pinto Coelho v Portugal (n° 2), Application no. 48718/11, 22/03/2016.

Roche v United Kingdom, Application no. 32555/96, ECHR 2005-X, (2006) 42 EHRR 30, IHRL 3210 (ECHR 2005), 19/10/2005.

Sdružení Jihočeské Matky v. Czech Republic, Application no. 19101/03, 10/7/2007.

Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006.

Stoll v Swizerland, Application no. 69698/01, 10/12/2007.

Társaság a Szabadságjogokért v Hungary, Application no. 37374/05, 14/4/2009.

Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands – Application no. 39315/06, 22/11/2012.

Vereniging Weekblad Bluf! v the Netherlands, Application no. 16616/90, 9/2/1995.

Weber and Saravia v. Germany, No. 54934/00, 29 June 2006.

Wille v Liechtenstein, No. 28396/95, 28 October 1999.

Youth Initiative for Human Rights v Serbia, Application no. 48135/06, 25/6/2013.

B. EUROPEAN UNION COURTS

Joined Cases C-7/56 and C-3/57 to C-7/57 *Algera and Others v Common Assembly* EU:C:1957:7.

Case 25-62, *Plaumann & Co. v Commission of the European Economic Community* EU:C:1963:17.

Case 26-62 *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* EU:C:1963:1.

Case 6-64 *Flaminio Costa v E.N.E.L.* EU:C:1964:66.

Case 29-69 *Erich Stauder v City of Ulm – Sozialamt* EU:C:1969:57

Case 9-70 *Franz Grad v Finanzamt Traunstein* EU:C:1970:78.

Case 11-70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* EU:C:1970:114.

Case 22-70 *Commission of the European Communities v Council of the European Communities* EU:C:1971:32.

Joined cases 41 to 44-70 *NV International Fruit Company and others v Commission of the European Communities* EU:C:1971:53.

Case 9-72 *Georg Brunner KG v Hauptzollamt Hof* EU:C:1972:81.

Case 4-73 J*. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities* EU:C:1974:51.

Case 66/75 *Macevicius v Parliament* EU:C:1976:66.

Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal* SpA EU:C:1978:49.

Joined cases 789 and 790/79 *Calpak SpA and Società Emiliana Lavorazione Frutta SpA v Commission of the European Communities* EU:C:1980:159.

Case 208/80 *Lord Bruce of Donington* EU:C:1981:194.

Case 230/81 *Luxembourg v Parliament* EU:C:1983:32.

Joined Cases 205-215/82 *Deutsche Milchkontor GmbH* EU:C:1983:233.

Case 294/83, *Parti écologiste "Les Verts" v European Parliament* EU:C:1986:166.

Case 222/84 *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary* EU:C:1986:206.

Case 5/85 *AKZO Chemie v Commission* EU:C:1986:328.

Case 249/85 *Albako v BALM* EU:C:1987:245.

Joined Cases 358/85 and 51/86 *France v Parliament* EU:C:1988:431.

C-213/89 *The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others* EU:C:1990:257.

C-260/89 *Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others* EU:C: 1991:254.

Joined cases C-320/90, C-321/90 and C-322/90 *Telemarsicabruzzo SpA and Others v Circostel, Ministero delle Poste e Telecomunicazioni and Ministero della Difesa* EU:C:1993:26.

C-343/90 *Manuel José Lourenço Dias v Director da Alfândega do Porto* EU:C:1992:327.

C-83/91 *Wienand Meilicke v ADV/ORGA F. A. Meyer AG* EU:C:1992:332.

C-156/91, *Hansa Fleisch v Landrat des Kreises Schleswig-Flensburg*, EU:C:1992:423.

C-137/92 P *Commission v BASF and Others* EU:C:1994:247 paras. 75 and 76; C-58/94 *Netherlands v Council* EU:C:1996:171.

C-18/93 *Corsica Ferries Italia Srl v Corpo dei Piloti del Porto di Genova* EU:C:1994:195.

C-280/93 *Federal Republic of Germany v Council of the European Union* EU:C:1994:367.

Case C-428/93 *Monin Automobiles-Maison du Deux Roues* EU:C:1994:192.

C-466/93 *Atlanta Fruchthandelsgesellschaft mbH and others v Bundesamt für Ernährung und Forstwirtschaft* EU:C:1995:370.

C-58/94 *Netherlands v Council* EU:C:1996:171.

C-299/95 *Friedrich Kremzow v Republik Österreich* EU:C:1997:254.

C-345/95 *France v Parliament* EU:C:1997:450.

Opinion 2/94 on Accession by the Community to the ECHR EU:C:1996:140.

Joined cases C-10/97 to C-22/97 *Ministero delle Finanze v IN.CO.GE.'90* EU:C:1998:498.

T-92/98 *Interporc Imund Export GmbH v Commission of the European Communities* EU:T:1999:308.

Opinion of Advocate General Léger in Case C-353/99 *Council v Hautala* EU:C:2001:392.

Case C-50/00 P, *Unión de Pequeños Agricultores v Council of the European Union* EU:C:2002:462.

Case C-318/00 *Bacardi-Martini SAS and Cellier des Dauphins v Newcastle United Football Company Ltd* EU:C:2003:41.

C-105/03 *Criminal proceedings against Maria Pupino* EU:C:2005:386.

C-266/03 *Commission of the European Communities v Grand Duchy of Luxemburg* EU:C:2005:341.

C-433/03 *Commission of the European Communities v Federal Republic of Germany* EU:C:2005:462.

T-2/03 *Verein für Konsumenteninformation v Commission of the European Communities* EU:T:2005:125.

C-354/04 P *Gestoras Pro Amnistía, Juan Mari Olano Olano and Julen Zelarain Errasti v Council of the European Union* EU:C:2007:115.

C-355/04 P *Segi and Others v Council* EU:C:2007:116.

C-39/05 P and C-52/05 P *Kingdom of Sweden and Maurizio Turco v Council of the European Union* EU:C:2008:374.

C-266/05 P *Jose Maria Sison v Council of the European Union* EU:C:2007:75.

T-144/05 *Pablo Muñiz v Commission of the European Communities* EU:T:2008:596.

C-458/06 *Skatteverket v Gourmet Classic Ltd* EU:C:2008:338.

C-45/07 *Commission of the European Communities v Hellenic Republic* EU:C:2009:81.

C-514/07 P, C-528/07 P and C-532/07 P *Kingdom of Sweden v Association de la presse internationale ASBL (API) and European Commission* EU:C:2010:541.

C-18/08, *Foselev Sud-Ouest*, EU:C:2008:647.

T-471/08 *Ciarán Toland v European Parliament* EU:T:2011:252 71.

T-233/09 *Access Info Europe v Council* EU:T:2011:105.

T-529/09 *Sophie in 't Veld v Council of the European Union* EU:T:2012:215.

T-167/10 *Evropaïki Dynamiki – Proigmena Systimata Tilepikoinonion Pliroforikis kai Tilematikis AE v European Commission* EU:T:2012:651.

C-617/10 *Åklagaren v Hans Åkerberg Fransson* EU:C:2013:105.

C-135/11 P *IFAW Internationaler Tierschutz-Fonds v Commission* EU:C:2012:376.

C-280/11 P *Council of the European Union v Access Info Europe* EU:C:2013:671.

C-300/11 *ZZ v. Secretary of the State of Home Department* EU:C:2013:363.

C-399/11 *Stefano Melloni v. Ministerio Fiscal* EU:C:2013:107.

C-626/11P *Polyelectrolyte Producers Group GEIE (PPG) and SNF SAS v European Chemicals Agency (ECHA)* EU:C:2013:595.

T-331/11 *Leonard Besselink v Council of the European Union* EU:T:2013:419.

T-516/11 *MasterCard, Inc. and Others v European Commission* EU:T:2014:759 62.

C-350/12 P *Council v Sophie in't Veld* EU:C:2014:2039.

C-365/12 P *European Commission v EnBW Energie Baden-Württemberg AG* EU:C:2014:112.

C-576/12 P *Ivan Jurašinović v Council of the European Union* EU:C:2013:777.

C-521/15 *Spain v Council* EU:C:2017:982.

T-540/15 *Emilio De Capitani v European Parliament* EU:T:2018:167.

C-57/16 P *ClientEarth v European Commission* EU:C:2018:660.

C-183/16 P *Tilly-Sabco v Commission* EU:C:2017:704.

T-851/16 *Access Info Europe v European Commission* EU:T:2018:69.

T-31/18 *Luisa Izuzquiza and Arne Semsrott v European Border and Coast Guard Agency* EU:T:2019:815.

C. CYPRUS COURTS

Attorney General of the Republic v Costas Constantinou [2005] 1 CLR 1356.