EXPLORING EXISTING AND POTENTIAL NORMATIVE SOLUTIONS FOR AN EU-WIDE LEGAL FRAMEWORK FOR SECURITY OF INFORMATION IN THE CONTEXT OF DEFENCE AND SECURITY PROCUREMENT

Simion-Adrian PURZA[*]

Abstract

In the current international environment, an effective implementation of national security objectives is to a great extent dependant on the ability of national governments to ensure the highest possible degree of confidentiality to information used in strategical, as well as tactical decisions. Ensuring security of information has been a conundrum for all international organisations seeking to reach varying degrees of coordination, cooperation or integration. As the most ambitious of all, thus far, the EU has raised the bar even higher, especially in terms of desired cooperation in defence and security, where the drive for integrated defence procurement takes centre stage. Consequently, the issue of sharing (classified) information between the Member States and their relevant authorities is of fundamental importance. Against this backdrop, this paper seeks to identify potential regulatory solutions for the management of classified information that would effectively contribute to the final objective of integrating defence and security procurement, as envisaged by the Defence Procurement Directive 2009/81/EC. An essential prerequisite in this respect is to determine what legal solutions could better serve this purpose, starting from normative instruments already implemented at various levels in the EU institutional mechanism. To this end, the paper is based on a two-phased theoretical approach: (1) the material segment – the characteristics of an effective integrated system for security of information (within the scope of defence procurement integration) and (2) the procedural segment – how to apply a potential solution at EU level (by what means). Ancillary research questions are aimed, first, at understanding the current state of play of the EU regulatory framework pertaining to handling classified information, in terms of granting security clearances to both individuals and legal persons (private, as well as public).

Keywords: *security of information, classified information, defence procurement, EU integration.*

1. Introduction

Information, understood in its widest possible definition, is a critical part of any decision-making process and even more so for strategic planning and action in the realm of national security. The delicate balancing act of ensuring security of information has been a conundrum for all international organisations seeking to reach varying degrees of coordination, cooperation or integration, such as the UN or NATO. As the most ambitious of all, thus far, the EU has raised the bar even higher, especially in terms of desired cooperation in defence and security. Consequently, the issue of sharing (classified) information between the

[*] Ph.D. Candidate with a joint supervision from Babeș–Bolyai University of Cluj-Napoca (Romania) and Hasselt University (Belgium). Associate researcher at the Centre for Good Governance Studies, Babes–Bolyai University. Researcher at the Centre for Government and Law of Hasselt University. The views and opinions expressed in this article are those of the author alone (if not indicated otherwise) and do not necessarily reflect any official policy or position. (e-mail: simion-adrian.purza@uhasselt.be).

Member States and their relevant authorities took centre stage.[1]

The main hypotheses of this paper are based on the idea that a highly coordinated (if not unitary) regime for classified information among EU Member States[2] – for the purpose of defence procurement integration – could be achieved following the same rationale used for the gradual integration of defence and security matters into the EU institutional mechanism (still an ongoing process).[3] The key starting point is the contention that, albeit some positive feedback, the fit-for-purpose provisions of Directive 2009/81/EC[4] on security of information have proved to be of little effect in terms of enabling and encouraging cross-border tendering. It should also be reiterated that, in general terms, despite an initial positive feedback from the member states and the various stakeholders after the publication of the Defence Procurement Directive, the most recent report on its effectiveness[5] underlines its limited overall impact, in terms of both legal harmonization and concrete results for the EU defence industrial base.

Although debatable, it can be said that the EU has established a proprietary and functional framework for dealing with classified information, covering both its institutional actors, as well as its dynamics with the member states and among themselves, when dealing with EU classified information. What is, then, the missing link for establishing an integrated and functional framework for the protection of classified information that would also benefit the integration of defence procurement – i.e. what needs to change?

An evaluative study conducted by the Commission in 2016 has shown that 61% of contracting authorities strongly agreed or agreed that the Defence Directive"s provisions on security of information are sufficient to ensure the protection of classified information.[6] The same study revealed that, among business respondents, a "relative majority" of 33% expressed a favourable view, while "only" 9% disagreed.[7] Based on these statistical iterations and additional interview-based feedback, the Commission seems content with the effectiveness of the security of information provisions in the Defence Procurement Directive.

On this point, if the benchmark is the contribution that the Directive effectively brings to opening defence procurement for the EU market, then the appropriateness of the security of information provisions must be weighed considering their concrete contribution towards achieving this goal. Therefore, as long as the provisions are only

[1] For an EU perspective on the relevance of information-sharing, *see* MK Davis Cross, 'Security Integration in Europe. How Knowledge-Based Networks are Transforming the European Union' (The University of Michigan Press, 2014) 49-72.

[2] For a discussion on the need for an EU-wide integrated regime for security of information, see M Trybus 'Buying Defence and Security in Europe. The EU Defence and Security Procurement Directive in Context' (Cambridge University Press, 2014), pp. 393-394.

[3] See SA Purza, 'Setting the Scene for Defence Procurement Integration in the EU. The Intergovernmental Mechanisms' (2018) 4 European Procurement & Public Private Partnership Law Review 257, 260.

[4] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, Official Journal of the European Union, L 216, 20.8.2009 (hereinafter "Defence Procurement Directive").

[5] Commission Staff Working Document: Evaluation of Directive 2009/81/EC on public procurement in the fields of defence and security, SWD (2016) 407 final, p. 94.

[6] SWD (2016) 407 final, *op.cit.*, p. 77.

[7] Ibid.

considered sufficient from the point of view of the contracting authorities (and even the industry, although to a lesser extent), but they do not actually facilitate increased market access and equal opportunity, then it must be ascertained that their appropriateness is at least questionable. In this respect, the market access barrier created by the lack of a harmonised regime for access to and protection of classified information is a strong argument as to the insufficient effectiveness of the Defence Directive"s provisions on security of information.

Although outside the field of regulatory competence of the EU, the protection of classified information has been dealt with at an *ad-hoc* basis, while gradually undergoing a process of harmonisation between the main institutional actors of the EU. This evolutionary experience could provide (normative) solutions for a wider and more substantive integration of the protection of classified information at EU level, for the benefit of harmonised procurement aimed at integrating the markets for defence and security products and services.

Thus, the overarching interrogation of this paper seeks to identify potential avenues for future regulatory solutions for the management of classified information (beginning with security clearances) that would effectively serve the final objective of integrating defence and security procurement, as envisaged by the Defence Procurement Directive. An essential prerequisite in this respect is to determine whether there is legal basis to enact new EU legislation that would alleviate (or even solve) the issues pertaining to security of information. The objective is therefore that of a principled discussion with no pretention to elaborate concrete normative solutions – which could form the object of a subsequent study.

Determining if and what (regulatory) solution can be implemented is based on a two-phased theoretical approach to the issue: (1) the material segment – the characteristics of an effective integrated system for security of information (within the scope of defence procurement integration) and (2) the procedural segment – how to apply the envisaged solution at EU level (by what means). Ancillary research questions are aimed, first, at understanding the current state of play of the EU regulatory framework pertaining to handling classified information, in terms of granting security clearances to both individuals and legal persons (private, as well as public).

Aside from literature and legislative analysis, the research is complemented by an examination of the relevant case-law of the European Court of Justice dealing with security of information at large. The examination seeks firstly to find indications as to the underlying principles that the Court has defined in this field, especially in the logic of striking a balance between (national) security interests and democratic access to information. Secondly, the analysis might reveal a confirmation or critique of potential regulatory solutions that have been implemented or should be implemented in the field of security of information at EU level.

2. Defining the main concepts

The protection of classified information is an essential prerequisite for contracting authorities, but it also bears significance for the industry – national security interests and commercial confidentiality requirements dovetail, especially in fields such as defence and security. To put the issue in context, it is important to underline that, in the field of defence procurement, potential tenderers often require access to classified information

while the contracting authorities seek a solid guarantee of the reliability of said tenderers regarding their ability and will to safeguard the necessary level of confidentiality. Therefore, on the one hand, there is a specific need emanating from the industry, and on the other, a (potentially) contending need of the member states, stemming from national security.

In moral or sociological terms, confidence building is key in any endeavour pertaining to the protection of classified information. Various legal instruments have been developed by national or international legislators to ensure that this notion gets empirical validation and a concrete system of accountability is in place. Nonetheless, the fundamental issue is whether the originating source of the information feels enabled and safe enough to entrust said information onto one or more third parties, and more so to accept the possibility of it being subsequently distributed. Confidence building is not just an abstract moral issue, as it is also manifested in the relation between EU bodies and institutions, the most relevant case being that of the negotiations between the European Parliament and the Council on access to classified information handled by the latter.[8]

Amongst various other considerations, the foremost legal and operational principles in the field of security of information are authorization or clearance (subject to meeting a set of requirements) and need-to-know. They represent two sides of the same coin, as interdependent and cumulative conditions to be met in order that a person (private or legal) is granted access to documents and materials containing classified information. Of course, the classification policy employed by the national authorities of each state also bears important significance, but it goes further into the inner workings of security of information mechanisms and beyond the scope of this analysis.[9]

"Authorization" or "clearance" is a type of formal validation granted to a person, natural or legal, in confirmation of their capacity to handle classified information, based on the requirement to meet strict criteria and subject to evaluation thereof.[10] This can be regarded as the first line of defence in security of information and a universal tool used to control access and contain the risks of unwarranted disclosure of information.

"Need-to-know" is to a great extent a self-explanatory notion. In context, it can be defined as a principle according to which a person can have access to classified information only if knowledge of said information is needed in carrying out their duties.[11] Establishing the existence of the need-to-know in a particular situation is generally the attribute of the originator of the information or, in some cases, the holder. This concept is widely used at national and international level,[12] either intrinsically, as a

[8] D Galloway, 'Classifying secrets in the EU' (2014) 52 3 Journal of Common Market Studies 668, 681.

[9] For details on what classification policy entails (tailored for NATO) *see* A Roberts, 'Entangling Alliances: NATO's Security of Information Policy and the Entrenchment of State Secrecy' (2003) 36 Cornell International Law Journal 329, 332-340.

[10] A Roberts (2003), *op.cit.*, pp. 338-339.

[11] A Roberts (2003), *op.cit.*, p. 337; s*ee* also R Dover, MS Goodman, C Hilldebrand (eds), 'Routledge Companion to Intelligence Studies' (Routledge, 2014) 258; B Driessen, 'Transparency in EU Institutional Law: A Practitioner's Handbook' (2nd ed, Kluwer Law International, 2012) 32.

[12] For an EU-level example, *see, inter alia*, Interinstitutional Agreement of 12 March 2014 between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, OJ 2014 C 95/1, article 4.4.(a).

transversal notion, or expressly stated in legal or administrative acts as a mandatory prerequisite for access to information.

For clarity of argument, basic concepts such as "classified information", "security of information" or "sensitive information" should be defined herein. These notions have been defined on numerous occasions and in various contexts but have retained their underlying meanings throughout. For that reason, an in-depth comparative analysis of the various definitions, although an interesting debate, would not provide any meaningful contribution to the present analysis. Therefore, for the purposes of this paper, it is most appropriate to recourse to legal definitions that have been provided within EU legislative acts (where available) and relevant policy documents.

"Classified information" has been defined[13] as "any information or material, in any form, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union, or of one or more of the Member States, and which bears" one of the EU or corresponding classification markings.[14] The Defence Procurement Directive provides a similar definition, albeit more complex and from a national security perspective: "any information or material, regardless of the form, nature or mode of transmission thereof, to which a certain level of security classification or protection has been attributed, and which, in the interests of national security and in accordance with the laws, regulations or administrative provisions in force in the Member State concerned, requires protection against any misappropriation, destruction, removal, disclosure, loss or access by any unauthorised individual, or any other type of compromise" (article 1.8). [15]

On the other hand, "sensitive information" is a more elusive concept. It can be understood as a quality or characteristic of documents or information whose unauthorised disclosure is liable to bring prejudice to private or public interests, in the general sense. Therefore, it is not inherently different from classified information, the distinctive element residing solely in terminology, as classification can be regarded as the formal or administrative confirmation of the sensitive nature of a document or a piece of information. Still, doctrine has at times referred to sensitive information as a distinct category (other than classified) that warrants some level of confidentiality (such as commercial information or personal data) but does not bear a formal security classification[16] or as unclassified information with controlled dissemination.[17] Nonetheless, the notion has received a formal, legal definition in Regulation 1049/2001 on public access to

[13] Article 2 of the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, Official Journal of the European Union C202, 8.7.2011, hereinafter 'Member States' Agreement on classified information'.

[14] Other EU legal acts have provided similar definitions, such as, *inter alia*: Council Decision of 23 September 2013 on the security rules for protecting EU classified information, Official Journal of the European Union L 274, 15.10.2013, article 2.1.; Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, Official Journal of the European Union L 72, 17.3.2015, article 3.1.

[15] For a doctrinal perspective, *see, inter alia*, D Curtin, 'Official Secrets and the Negotiation of International Agreements: Is the EU Executive Unbound?' (2013) 50 Common Market Law Review 423, 425-426; Galloway (2014), *op.cit.*, p. 672.

[16] Galloway (2014), *op.cit.*, p. 672.

[17] D Curtin, 'Overseeing Secrets in the EU: A Democratic Perspective' (2014) 52 Journal of Common Market Studies 684, 686 and 691.

EU documents,[18] which effectively equates it with classified information (the wording of the Regulation refers to "sensitive documents" and "classified documents"). Building on this approach and considering that the differentiation proposed by doctrine is of no consequence for the analysis made in this paper, any further reference to "sensitive information" should be considered equivalent to "classified information" if not expressly stated otherwise.

Against this background and seen in the context of the Defence Procurement Directive, "security of information" can be described as both a characteristic and a set of requirements. Thus, it can be regarded as "the ability and the reliability of economic operators to protect classified information"[19] or as a set of "measures and requirements necessary to ensure the security of such information",[20] the two perspectives bearing equal relevance.

Focusing on the field of procurement for defence and security, the most pressing issues from the perspective of the contracting authorities, when dealing with industry representatives, are national security clearances (or authorisations, needed to access classified information pertaining to this field) and the criteria used for granting them, as well as ensuring appropriate means of protection and control of the security of information throughout its lifecycle. Considering the aim to push for integration in this field, the cross-border dimension of the two bears considerable significance. As the Commission concluded, the "lack of a harmonisation of national security clearance systems can create problems and market access barriers."[21]

The Defence Procurement Directive is the keystone of defence procurement integration in the EU. Its central position is tributary to both its daringly ambitious goal as well as to its absolute novelty to date. As such, the red thread of its philosophical approach and key concept is *integration*, on the backdrop of which each individual normative instrument is sized and adjusted. In this respect, by resorting to an analogy with the harmonising drive of internal market law in general, Trybus underlines the similar impetus of the Defence Directive, which seeks to "bridge the gap" between the internal market objectives of the EU and what he describes as the "legitimate concerns of the Member States", including those pertaining to public security.[22]

This read thread is applied – albeit unevenly – to security of information as well. To this end, the recitals of the Directive outline the symbiotic link between procurement in the fields of defence and security and security of information requirements – paragraphs (9), (20) and (47) – while hinting the urgency (or usefulness, in a blander interpretation) of "an Union-wide regime on security of information". Although the Directive does not reach that level of ambition, it nonetheless transposes the overall approach towards the importance of security of information concerns in provisions that allow contracting authorities to include requirements pertaining to security of information in various key elements of the procurement procedure,

[18] 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, Official Journal of the European Union L145, 31.5.2001, article 9.1.

[19] M Trybus (2014), op.cit., 43-44.

[20] Directive 2009/81/EC, article 22.

[21] SWD (2016) 407 final, *op.cit.*, p. 77.

[22] M Trybus (2014), op.cit., p. 280.

such as conditions of performance, selection criteria or exclusions.

As with complex issues in general, where opposing interests are confronted, compromise was often used to agree on various solutions pertaining to the publicity and transparency of the procedure, while safeguarding security concerns. The Commission Staff Working Document presenting the impact assessment of the future Defence Directive showcased numerous such compromises in terms of security of information, starting with the possibility to disclose sensitive information pertaining to the procurement procedure only to the successful bidder, at a later stage – which the document considered to be "best-suited, since it allows safeguarding security of information while still ensuring equality of treatment and a fair level of transparency".[23]

3. The EU regulatory perspective

Owing to their exclusively economic scope, significantly narrower than today"s comprehensive agenda, the initial European Communities had neither the incentive nor the legal justification to set up rules on protecting classified information.[24] Somewhat unsurprisingly, the exception to this rule was provided by domains such as defence and security, particularly related to aspects of nuclear safety under the Euratom Treaty.[25]

Further on, advances in cooperation on military and civilian management operations,[26] as well as in tackling criminal matters (with a focus on transnational terrorism), have prompted exponential evolutions in the management of classified information within the EU. Therefore, it can be said that the EU"s step by step involvement in defence and security matters, albeit by way of an intergovernmental approach,[27] has also served as the driving force behind initiatives focused on the protection of classified information.

In this respect, it is relevant to note that the EU has previously shown the political will power and the necessary means to respond to legitimate concerns voiced by its partners in terms of security of information. A case in point is the largely debated initiative promoted in 2000 by High Representative Javier Solana, seeking to provide reassurances to NATO on the protection of classified information it exchanged in its cooperation with the EU, which was on a strong path of consolidation at that time.[28]

The road to harmonization still faces many challenges, brought on especially by the Member States" different perspectives on how classified information should be managed, a fact that had been taken into consideration by the Defence Procurement

[23] Commission of the European Communities, 'Commission Staff Working Document – Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on the coordination of procedures for the award of certain public works contracts, public supply contracts and public service contracts in the fields of defence and security – Impact Assesment', Brussels, 5.12.2007 SEC(2007) 1598, pp. 47-48, available at: https://secure.ipex.eu/IPEXL-WEB/dossier/document/SEC20071598FIN.do [last accessed 8 January 2021]; see also M Trybus (2014), op.cit., p. 364.

[24] D Galloway, 'Classifying secrets in the EU' (2014) 52 3 Journal of Common Market Studies 668 and 675.

[25] ibid.

[26] ibid 674.

[27] SA Purza, 'Setting the Scene for Defence Procurement Integration in the EU. The Intergovernmental Mechanisms' (2018) 4 European Procurement & Public Private Partnership Law Review 257, 260.

[28] Rosén, G. (2015), 'EU Confidential: The European Parliament's Involvement in EU Security and Defence Policy', Journal of Common Market Studies 53:2, pp. 388-389.

Directive but to no conclusive solution. For example, one such element of distinction was the position of Sweden and the United Kingdom, which practically invalidated the principle of originator control[29] in situations where there is a request for the content of a classified document to be made public or to be sent to judicial authorities.[30] In such a scenario, public authorities are required and empowered to assess whether disclosure is in the public interest, thus disregarding the obligation to obtain the agreement of the originator.

David Galloway has astutely observed that the EU was required to have an original approach to regulating the management of classified information, since the Treaties lacked the proper legal basis for binding rules in this field.[31] Moreover, article 352 TFEU paragraph 4 expressly prohibits the Union from relying on the mechanism established by this article to attain objectives pertaining to the Common Foreign and Security Policy (CFSP) while also reiterating the limitations to adopt acts, enshrined in article 40 TEU. Thus, there was no possibility of having a unified legislative instrument addressing the protection of classified information. For that reason, the EU institutions, guided by the driving force of the Council, have adopted a sectoral approach, seeking to implement measures that would ensure an adequate level of protection for information deemed classified, focused on their own specific administrative procedures and processes.[32]

The EU"s relationship with classified information has been split between two imperatives which carry varying weights both within the Union itself (different perspectives of the executive and parliamentary branches) and those of the public (NGOs and lobby groups especially). Thus, the EU is tasked with conciliating democratic governance (which entails extended access to sensitive information for the public) with efficient political action (which for its part might require a heightened level of discretion). A renewed legislative response could be a way to respond to both imperatives, that is to ensure the exercise of the fundamental right of access to information while also to provide a clear and effective framework to legitimately protect classified information.

In her paper on how the EU deals with classified information,[33] Deirdre Curtin asserts that adopting general rules on how the EU Council shares classified information with the European Parliament is "a matter of broader democratic concern". Extrapolating from this conclusion, it could be argued that the need for an EU-wide regime for clearance and access to classified information for industry representatives – seen as *sine qua non* for taking part in defence and security procurements – also touches on issues pertaining to democratic governance, in the context of common market rules and observing the need to ensure an effective benefit of the possibilities afforded by the Defence Procurement Directive. On this issue, research has underscored the contrast between the EU"s approach towards intra-community transfers, which benefit from an EU Directive, and the recognition of security clearances, which has yet to be regulated at a similar level.[34]

[29] For more details on the principle of originator control *see Curtin* (n 15) 691.
[30] Galloway (2014), *op.cit.*, p. 674.
[31] *See* Galloway (2014), *op.cit.*, pp. 675-676.
[32] Ibid.
[33] *Curtin* (n 15) 696.
[34] M Trybus (2014), op.cit., p. 362.

One issue identified by doctrine, also building on the perspective of legitimate access, is that a lack of substantive classification criteria leads to intentional or unintentional abuse of power by the EU institutions – the Council in particular – when exercising their discretion in granting low-level classified status to information (such as "restricted").[35] This practice can effectively limit or ban otherwise relevant information from legitimate public knowledge, in the disadvantage of both individual citizens as well as NGOs or the industry. Similar issues concern the way national governments make use of their prerogative to declare information of a certain type or pertaining to a specific sector as classified on the lowest possible level, but which still makes it undisclosable to third parties, thus providing a valid reason to apply the Article 346 TFEU exemption or at least inhibit the participation of (some) tenderers.

The analysis on relevant EU legislation provided further on seeks to identify and explain specific instruments of governance regulated at EU level for the management of classified information, with a focus on the degree to which the competent authorities of the Member States are involved in the process and how the distribution of tasks and authority is made. The documentary results should in turn provide a basis for evaluating if the mechanisms in place satisfy the Member States" desire to exercise an adequate level of control. To this end, the scope of the legal framework analysis includes a selection of legal/procedural instruments specially tailored for the needs of the EU institutional framework pertaining to handling classified information. The analysis is predicated *inter alia* on the notion that the Commission has had an early leading role in terms of security of information, but its position has been taken by the Council, especially considering its competences and those of the Member States in areas such as the CFSP and the Common Security and Defence Policy (CSDP).[36]

3.1. The EU regulatory perspective

The first iteration in terms of regulating the management of classified information within the EU came as an early onset, by means of Regulation (Euratom) No 3 implementing Article 24 of the Treaty Establishing the European Atomic Energy Community, a regulation which is still in force.[37] Viewed in the context of modern-day regulatory initiatives, it can be regarded as a landmark achievement in a field of profound reluctance on the part of the Member States, and, even more so, as the blueprint for future rules.[38]

Still, in the interest of objectivity, it should be underscored that the adoption of the Euratom Regulation had benefited from several favourable circumstances, such as the limited number of Member States that had to come to an agreement at the time, inspired, moreover, by the obvious and stringent need for close cooperation, following the aftermath of the Second World War. The fact that the regulation had a limited sectoral scope also came as an advantage, thus streamlining each Member States" calculations on the potential strategic and security impact of the new rules.

[35] *Curtin* (n 15), 690.
[36] Curtin, D. (2013), op.cit., p. 424.
[37] Published in the Official Journal of the European Communities no. 406/58, hereinafter 'Euratom Regulation'.
[38] Curtin, D. (2013), op.cit., p. 427.

The main issues under consideration of the still germinating Community legislator at the time of the Euratom Regulation were the defence interests of the Member States, as explained by the only argumentative paragraph of the very concise preamble. It is interesting to note, on this point, that the preamble, as well as the normative text of the regulation[39] make no reference to the interests of the Community, as opposed to subsequent legislation that has incorporated the notion of Community/Union interests.

The underlying goal of the regulation was to empower the Commission to manage security measures applied to sensitive information, acting as a supervisory body in matters pertaining to both the content of the information as well as its dissemination. That is why the scope of the Euratom Regulation includes the two main dimensions of security of information, i.e. security grading and protective measures, which cover both information acquired by the Community, in its capacity as a standalone collective body, and that which is communicated by the Member States.[40]

Article 24.1. of the Treaty establishing the European Atomic Community[41] mandates the Council to regulate issues pertaining to security of information, following a proposal from the Commission, including a system of security gradings and complementary security measures. It is noteworthy that the Commission is entrusted with a significant margin of discretion traditionally afforded exclusively to national governments – the ability to decide on the appropriate classification (grading) level for sensitive information.[42] This courageous transfer of an inherently national prerogative to the supranational level gives additional weight to the novelty and long ranging impact that the Euratom rules have had in the field of security of information within the EU.

A general assessment of the Euratom Regulation reveals that its normative structure is based on a tailored assimilation of the fundamental principles, processes and authority instruments that define protection of classified information (indicated *supra*). The main considerations underpinning the Regulation are evident from its brief preamble, which focuses on the pre-eminence of the defence interests of the Member States, the central role of the Commission and the reach of its security measures, intended to cover both the subject matter of the information and its distribution regimen.

The provisions of Articles 1 through 5 of the Euratom Regulation, regarding its scope, have a threefold approach, providing criteria to discern according to subject matter and personal capacity, while also touching on the interaction with the dedicated regulations of the Member States. In terms of subject matter, the Euratom Regulation covers both the various security levels or gradings and their respective protective measures, which apply to information communicated by Member States within the framework of the Treaty and to that acquired *ad novum* by the Community. All information that is subject to protective measures is considered under the common denomination "Euratom Classified Information".

Article 5 provides guidelines regarding the interaction between the

[39] *See, inter alia,* article 10 of the Euratom Regulation.
[40] Article 1.1. of the Euratom Regulation.
[41] *See* Consolidated Version of the Treaty Establishing the European Atomic Energy Community, OJ 2016 C 203/1, hereinafter 'Euratom Treaty'.
[42] Article 24.2. of the Euratom Treaty.

Euratom Regulation and other sector specific normative instruments enacted either at Community level or by the national authorities of the Member States. The main principle in this respect is that the rules within the Regulation are to be construed as minimum requirements in terms of the protection of classified information. As such, the Community and the Member States are provided with a limited prerogative to supplement the framework with new rules tailored for the needs of their jurisdictions. The limited aspect is indeed puzzling, as it is formulated somewhat counterintuitively, in that while it opens the possibility to adopt "appropriate provisions of their own" it also excludes complementary provisions that would "adversely affect the uniform treatment of Euratom classified information", without providing adequate criteria to discern between acceptable and unacceptable provisions. Thus, it seems difficult to envision any type of complementary rule, adopted at national level, that would not, to some extent, affect the prescribed uniform regime.

In terms of one of the fundamental building blocks of security of information – the clearance process – the Regulation establishes the primacy of the two essential (pre)conditions for access to classified information – prior authorisation and need-to-know.[43] While the need-to-know ("need to be informed") is only briefly explained by reference to the official duties of the person seeking access, the authorisation procedure is described in detail, touching upon granting authority, recognition and the distribution of competences between Community bodies and the Member States. The authority to grant clearances is shared by the Security Bureau and the relevant authorities of the Member States. Nevertheless, the Member States retain fundamental control in granting clearances, as the Security Bureau is afforded only a slim margin of appreciation in this respect.

Once granted, the authorisation is provided with universal recognition, i.e. it is opposable to all other bodies of the Community, as well as the Member States. This is as an important step forward in terms of the Member States investing confidence and abandoning their innate reluctancy towards sharing their prerogatives and instruments of control in matters pertaining to classified information. Although it would be far-fetched to consider this a milestone, it is nonetheless an indication as to the national authorities" willingness to stretch their own limitations in the interest of cooperation, when there is a strong political will and pragmatic incentives to do so.

3.2. The EU Council Model Rules

In a pragmatic acknowledgment of the need to exchange classified information, EU Member States resorted once again to the intergovernmental framework as a panacea for solving predicaments that held back effective cooperation. Therefore, an overarching covenant was negotiated and implemented under the title "Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union".[44]

While at first glance this Agreement on classified information would appear as nothing more than a fit-for-purpose international cooperation document, its underlying value should not be

[43] Article 14.1. of the Euratom Regulation.

[44] Published in the Official Journal of the European Union, C 202, 8 July 2011, hereinafter 'Agreement on classified information'.

underestimated. It establishes a basic legal framework of general rules applicable to the protection of European Union Classified Information (EUCI) during its exchange between the Member States, on one hand, and the EU institutional body (as a whole), on the other. This represents a cornerstone firstly because it enshrines the Member States" formal recognition of the EU institutional model for the protection of classified information, thus overcoming their initial reluctancy[45] by applying similar protection measures as those provided by national laws and regulations. Secondly, it marks the determination of the Member States (and, conversely, that of their national authorities) to apply a complementary and supranational model for the classification and protection of information. Thus, this Agreement represents a form of consensus between all Member States, under the guidance of the EU, on sensitive issues pertaining to classified information. Moreover, it can be perceived as a much-needed first iteration in terms of a formalised, systemic approach towards regulating classified information in the EU, to which more in-depth rules quickly followed suit.

It is worth noting that, at the time the Agreement came into force, the EU had already developed a mechanism for the protection of EUCI, starting with internal protection regimes developed by the Commission as early as 1986[46] and decisions of the Secretary-General of the council, starting with 1995,[47] followed by Council Decisions to date.[48] In this respect, doctrine has pointed out that the Council explicitly sought to promote and institute its self-devised rules as a uniform solution for the EU as a whole (institutions and Member States alike).[49] The said reluctance of the Member States to formally adhere to the EU mechanism for handling classified information, despite the latter"s sensible record of accomplishment until 2011, is in itself indicative as to complex underpinnings of such a decision.

According to Article 1 of the Agreement on classified information, its scope is twofold, in the sense that it covers two main categories of classified information according to its originator, namely: originating in the EU institutional mechanism (institutions, agencies, bodies or offices) and originating in the Member States. From an operational point of view, the Agreement covers information related to the interests of the EU, i.e. information that is classified according to EU standards, communicated either between the Member States themselves or between EU institutions and the member states.

On the backdrop of the general framework provided by the Agreement on classified information, the analysis will further touch upon one of the main pillars of

[45] Galloway (2014), *op.cit.*, p. 674.

[46] Ibid.

[47] Decision 24/95 of the Secretary-General of the Council of 30 January 1995 on measures for the protection of classified information applicable to the General Secretariat of the Council (not published); Decision of the Secretary-General of the Council/High Representative for the Common Foreign and Security Policy of 27 July 2000 on measures for the protection of classified information applicable to the General Secretariat of the Council (Official Journal of the European Communities, C 239, 23 August 2000).

[48] Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations (Official Journal of the European Communities, L 101, 11 April 2001); Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information (Official Journal of the European Union, L 141, 27 May 2011); Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (Official Journal of the European Union, L 274, 15 October 2013).

[49] Curtin, D. (2013), op.cit., pp. 437-438.

EU legislation in terms of the protection of classified information, represented by the latest iteration of the Council Decision on protecting classified information (i.e. Council Decision 2013/488/EU on the security rules for protecting EU classified information[50]).

Of all the regulatory documents pertaining to security of information in the EU, Council Decision 2013/488 is the most comprehensive and, as such, could be regarded as somewhat of a standard for all other rules enacted by various institutions – in this respect, recital (7) provides that EU bodies and agencies should apply the basic principles and minimum standards laid down in the Decision.[51] This notwithstanding, the analysis reveals that the system of rules it enforces has inherent vulnerabilities stemming from the safeguards afforded to national authorities, coupled with the high level of expectations they thus create for the Member States.

From the outset, it should be noted that the scope of the Decision, however complex, is intrinsically curtailed by the limited regulatory reach afforded by its legal basis – Article 240(3) TFEU, the provisions of which enables the Council to act only in procedural matters or for the adoption its own rules of procedure. This does not necessarily mean that the normative power of the Decision is limited to the activities of the Council or its various bodies, nor does it preclude the applicability of its provisions to actions of the Member State or its national institutions, whether within the Council itself or on national territory.

The Council Decision"s status as a standard for other norms of EU institutions pertaining to the protection of classified information is confirmed by the breadth of its scope, as defined by Article 3.1., which also includes Member States, as mentioned *supra*. This is especially evident when seen in comparison to the similar normative act of the Commission (i.e. Commission Decision 2015/444) which is expressly limited *ratione personae* and *ratione loci* to Commission staff and premises, respectively.

The normative structure of Council Decision 2013/488 is built on the foundation of the well-established universal legal and operational principles of originator consent (for altering the classification level – Article 3.2.), need-to-know and security clearance (Article 7.1.).

According to Article 4.3., classified information originating from Member States and with a national classification level already ascribed is protected by means of the equivalency principle, which determines the necessary protection measures according to the requirements applicable to EUCI. This provision applies not only to classified information introduced by the Member States in the EU Council or its General Secretariat, but also to that which is introduced "into the structures or networks of the Union". This last phrase seems to indicate that the equivalency principle is deemed to have a transversal application throughout the institutional architecture of the EU, even though the scope of the Decision is, as mentioned above, limited to the activities of the EU Council and its General Secretariat. This potential normative conflict should be clarified by cross-referencing the relevant provisions of the various regulatory instruments enacted by EU institutions in this field. The prerogatives afforded to the originator of the information, in application of the aforementioned principle, are wide-reaching

[50] Council Decision of 23 September 2013 on the security rules for protecting EU classified information, Official Journal of the European Union, L 274, 15.10.2013 (hereinafter "Council Decision 2013/488").

[51] *See* Curtin, D. (2013), op.cit., p. 13.

and have a significant impact throughout the life-cycle of EUCI.

The corner stone of any system for security of information – personnel security – is regulated in detail throughout the Council Decision, with implementing rules provided in Annex I. The three fundamental caveats that must be respected for an individual to be granted access to EUCI are: to have the need-to-know established by the competent authority; to have the appropriate security clearance; to have been duly briefed on the responsibilities incumbent upon the person in connection with handling classified information.

Although Article 7.3. of Council Decision 2013/488 grants the General Secretariat of the Council (hereinafter "GSC") the power to authorise its personnel to access EUCI, it is nonetheless dependant on the result of the vetting procedure carried out by the National Security Authorities (hereinafter "NSA") – or other competent authorities – of the Member States, according to Article 4, corroborated with Articles 7, 16 and 18 of Annex I to the Council Decision. Thus, NSAs are primarily tasked with providing *de facto* security checks, according to the applicable national laws and regulations. This is both a burden of responsibility, as well as an essential leverage tool afforded to the Member States in the decision process as to whom is granted access to EUCI.

The leverage is indeed substantial. The "investigative and administrative procedures" – as coined by Article 1 of Annex I to the Council Decision – are built around the results of the security investigations conducted by the NSAs, which are decisive for approving or rejecting authorisation requests. The standards used by NSAs are essentially those established by national laws and regulations, although indicative criteria are provided in Article 7 of Annex I. The investigation results either in the issuance of a Personnel Security Clearance (PSC) – by the national authorities of the Member State for their own nationals –, either in the provision of "assurance" to the GSC that the individual concerned can be subsequently granted authorisation to access classified information. Thus, according to Article 18(a) of Annex 1, the GSC Appointing Authority is vested with the option (not obligation) to grant authorisation when the security check is positive, while it is expressly prohibited from granting authorisation when the result of the check is negative. Conversely, if the NSA withdraws the assurance given with regard to a person, the GSC has the obligation to withdraw said person"s authorisation for access to EUCI.

The prerogatives of the Member States in connection with the decision making process and the involvement of their NSAs in this respect are further consolidated through the establishment of a Security Committee. This collegiate body, defined in Article 17 of the Council Decision, is tasked with examining and assessing "any security matter within the scope of [the] Decision" and making recommendations to the Council. It is composed of representatives of the NSAs and its meetings are also attended by a representative of the Commission and the EEAS. From a hierarchical point of view, the Committee takes instructions primarily from the Council but it can also be convened at the request of the Secretary-General of the Council or of an NSA. Although the wording of Article 17 provides that the Security Committee"s central role is to "make recommendations on specific areas of security" – thus suggesting a consultative position – its standing in the overall mechanism established by the Decision is of a significant relevance, as it contributes with insights and recommendations in key moments of the decision-making process.

In terms of integration, Article 21 of Annex I to the Council Decision institutes a regimen of interinstitutional validity for authorisations for access to EUCI. Thus, the GSC is directed to accept authorisations granted by any other institution, body or agency of the EU – provided it is valid – with regard to any person working within the secretariat, irrespective of his or her assignment. This automatic recognition of authorisations is relevant, on the one hand, because it streamlines cooperation between institutions and fosters personnel mobility, contributing to enhanced operational capacity and, on the other hand, because it promotes a model of mutual institutional trust between bodies that have different – albeit complementary – roles in the Union.

Another interesting provision that could be construed as a discreet yet solid contribution to the supranational dimension of the system of prerogatives pertaining to security of information is the exceptional power of the Secretary General of the Council to grant access to EUCI to persons that have not been submitted to the prescribed security vetting procedure. According to Article 36 of Annex I, this possibility is limited to "very exceptional circumstances", which are not defined *per se* or linked to specific criteria, but only described through a non-exhaustive list of examples: "missions in hostile environments", "periods of mounting international tension", "the purpose of saving lives". Furthermore, access cannot be granted above the "EU SECRET" grading. Like the case of automatic validation of an existing authorisation, this is another situation in which the control and supervision attributes of the Member States are superseded by the supranational prerogatives of the EU. It should be noted that such an occurrence is of an exceptional nature and it cannot be construed as an unwarranted intrusion into the exclusive competences of the Member States in issues of national security. However, it could be argued that the rather vague description of what would constitute a "very exceptional circumstance" leaves room for potential dissenting perspectives between national authorities and the GSC.

The provisions of Council Decision 2013/488 dedicated to industrial security cover both the pre-contractual negotiations, as well as the entire lifecycle of classified contracts entered into by the GSC. From a personal point of view, the scope of said provisions includes contractors and subcontractors, so on a preliminary account it would seem that the regulations are generous in covering a wide range of possibilities.

Similar to standards developed in the field by the European Defence Agency[52], the Council Decision establishes a series of legal and contractual instruments aiming to ensure awareness and control of security related issues within a classified contract: the Security Classification Guide (SCG), the Security Aspects Letter (SAL) and the Programme/Project Security Instructions (PSI). The three are complementary and interconnected in providing standards for the contract awarding and execution phases.

Albeit consistent efforts throughout the Council Decision to ensure proper consideration and protection of the interests of Member States pertaining to national classified information and/or EUCI, the provisions on the transfer of the latter to contractors located in third states breaks this consistency. Thus, Article 30 of Annex V provides that EUCI shall be transferred to contractors and subcontractors located in

[52] For details on standards for the security of information developed by the European Defence Agency, *see* SA Purza, *op.cit.*pp. 261-265.

third states based on "security measures agreed between the GSC, as the contracting authority, and the NSA/DSA of the concerned third State". This solution, based on the individual action and assessment of the GSC, significantly departs from previous ones, which ensured some form of control or participation of the Member States, either through guidelines adopted by the EU Council or through the involvement of the Council Security Committee in key inflexion points of various procedures entailing classified information. The aforementioned solution could prove problematic for the security interests of the member states related to EUCI, considering that, According to Article 2.1. of the Council Decision, this type of classified information is by definition liable to cause prejudice to the interests of the Member States. Since there are no criteria provided to discern between the EUCI that can be shared, one could ask how the principle of originator consent is observed. This issue is particularly relevant in cases where contractors from third states are involved, with different approaches to security of information.

In terms of governance, the Council Decision seeks to achieve a much-needed balance between the prerogatives of the Member States and the margin for action afforded to the GSC for it to carry out its functions. In effect, the interweaving of exclusive and shared competences, as well as areas of direct cooperation, come together to create an original framework complete with the types of normative complexities one would expect in a *sui generis* construct such as the EU. Aside from providing the tools necessary to ensure that the goal of the Council Decision is reached, this mechanism also serves as a driving force for synchronicity at EU level in the field of security of information. The procedural and normative instruments devised to this end operate on two complementary yet distinct layers: technical/administrative and political, with varying degrees of effectiveness.

The Council Decision has a unitary approach to the operational and administrative tasks pertaining to the management of EUCI in terms of functions, as well as in terms of institutions, which are designed to be mirrored in the national systems of each Member State, as well as by the GSC. Thus, the competent authorities within the GSC and the Member States are tasked with establishing corresponding authorities for information assurance (for electronic means of communication, including operation tasks), cryptographic approval and distribution and security accreditation (Articles 10.8 and 10.9).

A key denominator in terms of distributing governance prerogatives is the algorithm applied with respect to the principle of originator consent. While it is abstract in nature and is not intended to give priority to the interests of either actors involved in the protection of EUCI, it is nonetheless a significant source of influence – whether direct or indirect – for the Member States because it affords them the possibility to control what happens to EUCI considered to have originated from them (e.g. Article 3 of Annex III to the Council Decision).

4. The Search for Middle Ground: CJEU Case-Law on Security of Information

The involvement of the Court of Justice of the European Union (CJEU) in matters pertaining to sensitive information has seen an early onset, with the EURATOM Treaty expressly mandating the Court to set the terms applicable to licenses or sub-licences granted by the Commission, in situations where the latter was unable to

come to an agreement with the licensee.[53] Building on the relevant jurisprudence developed since, this section provides a concise analysis of CJEU case law (covering both the Court *per se* and the General Court) that has ruled on issues pertaining to the protection of and access to classified information, both at EU and member state level.

The case-law is analysed in chronological order, with emphasis on the evolution of relevant principles, where applicable, and takes into consideration both situations pertaining to access to information, in general, and those pertaining to defence and security related information, in particular. This dual approach is based on the consideration that mechanisms granting public access to information managed by EU institutions represent a primary hazard for the confidentiality of said information and arguments in favour or against increased confidentiality and the way they have been received or developed by the Court provide relevant insight as to how security of information works from an institutional perspective.

In a 1999 case relating to parliamentary access to EU documents, [54] the Court examined some of the key concepts related to access to information, including the meaning of the notion "public interest with regard to international relations". The examination was made in the context of the request made by a Member of the European Parliament to access a report drafted by the Working Group on Conventional Arms Export of the Council – the CJEU confirmed the initial ruling of the Court of First Instance,[55] which granted access to the document in question. Thus, the Court of First Instance implicitly included in the general concept of "public interest with regard to international relations" information related to the "exchanges of views between the Member States" on issues relative to third countries, which, on account that they contain "formulations and expressions which might cause tension with certain non-member countries" can be exempted from public access.[56] The Court of First Instance and, subsequently, the CJEU, therefore confirmed the Council"s assessment on the extent to which protection should be granted to information exchanged with the Member States on issues falling within the general scope of international relations.[57] Another relevant guiding interpretation that resulted from this case is the distinction made between access to documents and access to information. Thus, the principle of access is not limited to documents *per se*, as individual, identifiable material objects, but is naturally extended to include the more abstract notion of "information", which is contained by documents.[58]

In its judgment in the widely cited case of Sison v. Council,[59] the CJEU made important advances in clearing out the dense web of concepts and thus further streamlined the approach to be taken regarding the margin of appreciation afforded to the institutions in the protection of confidential documents and information. In this case, the Court was called to review an appeal

[53] Article 12 of the Euratom Treaty.

[54] Judgment of 6 December 2001, *Council v. Hautala,* C-353/99 P, ECLI:EU:C:2001:661 (hereinafter "C-353/99 P".

[55] Judgment of 19 July 1999, *Hautala v. Council*, T-14/98, ECLI:EU:T:1999:157 (hereinafter "T-14/98").

[56] T-14/98, para. 73-74.

[57] See, also, Rosén, G. (2015), op.cit., p. 389.

[58] T-14/98, para. 87-88; C-353/19, para. 23.

[59] Judgment of 1 February 2007, *Sison v. Council*, C-266/05 P, ECLI:EU:C:2007:75 (hereinafter "C-266/05 P".

brought against the judgment delivered by the Court of First Instance of the European Communities on 26 April 2005 in joined cases T-110/03, T-150/03 and T-405/03,[60] which found in favour of the Council"s decision to refuse access to documents and information requested by the applicant in connection with the adoption of a series of Decisions of the Council on specific restrictive measures directed against certain persons and entities with a view to combating terrorism. The applicant had requested *inter alia* disclosure of the identity of the States which had provided certain documents in that connection.[61]

In the initial ruling, the Court of First Instance upheld the need for classified information to be adequately protected against inappropriate dissemination when it is received from national authorities of Member States or those of third States, by reference to the need to protect the position of the EU in "international cooperation concerning the fight against terrorism".[62] The Court also explicitly gave weight to the third States" desire for their identity not to be disclosed and to the inherent secret or confidential nature of a particular type of information - concerning persons suspected of terrorism.[63] Furthermore, both the Court of First Instance[64] and the CJEU[65] explicitly confirmed the Council"s approach on the statement of reasons for non-disclosure, thus validating the latter"s option to provide only a brief statement of reasons, without additional information that might have been liable to breach the confidentiality they were aiming for. From a right of access perspective, the Court"s approach in this judgment has been considered as conservative, owing to the arguably limited margin of examination the CJEU had afforded itself.[66]

Furthermore, the CJEU confirmed the full applicability and effectiveness of the originator consent principle, as a tool to ensure that sensitive information is not made publicly available when the member or third state which sent it to the EU institutions opposes disclosure. Moreover, it confirmed the applicability of this principle to both the disclosure of a document"s content and to information regarding its very existence or its origin.[67] Thus, in interpreting the security exception of Regulation 1049/2001, the CJEU established a wide margin of appreciation for the EU institutions as well as the Member States, when exercising the principle of originator control. The classified nature of the document and the information it contains can also be extended to the identity of the originating Member State (or third state) and even to the very existence of such document. The

[60] Judgment of 26 April 2005, *Sison v. Council*, T-110/03, T-150/03 and T-405/03, ECLI:EU:T:2005:143 (hereinafter "T-110/03").

[61] See T-110/03, para. 2-4.

[62] See, also, Labayle, H. (2010), 'Principles and procedures for dealing with European Union Classified Information in light of the Lisbon Treaty', European Parliament – Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, pp. 7-8, available at: https://www.statewatch.org/media/documents/news/2010/may/ep-classified-information-study.pdf [last accessed: 15.03.2021].

[63] T-110/03, para. 80-81.

[64] T-110/03, para. 62-63.

[65] C-266/05 P, para. 82.

[66] Neamtu, B, Dragos, D. (2019), 'Freedom of Information in the European Union: Legal Challenges and Practices of EU Institutions', in Dragos, D., Kovač, P., Marseille, A. (eds.) (2019), 'The Laws of Transparency in Action. A European Perspective', Palgrave MacMillan, p. 41.

[67] C-266/05 P, para. 86, 101-102.

proportional character of such measures to protect the security of information has also been confirmed against the backdrop of additional difficulty incumbent on the applicant if a high degree of discretion were to be applied.[68]

In 2005, the European Commission brought an action against Germany for its failure to fulfil obligations because of its exemption from duty of imports of military materials, spanning a 4-year period.[69] In its defence, Germany argued that Article 346 TFEU (Article 296 EC at the time of the proceedings) allowed derogation from the application of the Common Customs Code, "where the imports are of equipment exclusively intended for military purposes, and where the objective is the protection of the essential interests of its security".[70] Furthermore, Germany made a without prejudice payment, failing to detail which imports and what periods it covered, arguing that the relevant information was confidential and that the system for processing information in customs declarations is liable to cause "serious damage to the essential security interests of Member States".[71]

In this case, the Court recognised the existence and overall effectiveness of the "obligation of confidentiality" imposed on both Member States" nationals and EU institutions" staff, as an instrument "capable of protecting the essential security interests of the Member States." Thus, it could be argued that, in this instance, the CJEU considered that the various approaches towards the protection of the security of information employed by the Member States and the institutions are capable of ensuring the requisite level of protection, notwithstanding the (most probable) elements of distinction, both form a procedural and principled point of view.[72] Nonetheless, the Court made its own assessment of the potential that third-party access to information of a certain type might damage the interests of Member States in respect of either security or confidentiality. This examination and subsequent conclusion of the Court arguably go against the very essence of what Article 346 TFEU intended - which is to afford the Member States a sufficiently wide enough margin of appreciation in such issues, to properly safeguard their national security interests as they see fit. The risk of this type of overriding action by the Court should be managed in any future regulation on an EU-wide regime for security of information.[73]

It is also interesting to note, in the fashion of the analysis made by Martin Trybus on this case,[74] the argument put forth by some Member States – among which, chiefly, Germany – that they were under no obligation to supply the information that the Commission needed to examine and prove an infringement of the provisions of the Treaties. Thus, based on the provisions of Article 346 TFEU, Germany claimed the Commission"s action was inadmissible due to the former"s prerogative to abstain from disclosing information, which would substantiate the case of the latter – a genuine situation of *probatio diabolica*. Of course,

[68] C-266/05 P, para. 103.

[69] Judgment of 15 December 2009, *Commision v. Germany*, C-372/05, ECLI:EU:C:2009:780 (hereinafter "C-372/05").

[70] C-372/05, para. 19.

[71] C-372/05, para. 25, 58-59.

[72] C-372/05, para. 74.

[73] C-372/05, para. 75.

[74] Trybus, M., *Buying Defence…*, p. 132.

the Court was not persuaded by this line of argumentation.

In a preliminary ruling concerning the interpretation of the provisions of EU law on freedom of movement, the Court made an assessment of the need to safeguard the classified nature of information pertaining to public and national security, in the context of the fundamental rights granted by the Charter in terms of effective judicial protection.[75] It argued that Member States need to do more in the way of ensuring an appropriate balance between non-disclosure and access to effective judicial review. Thus, while not challenging the prerogative of national authorities to withhold information pertaining to state security, it nonetheless set higher standards for what an appropriate conduct would be in relation to a person whose rights might be affected by administrative decisions based on classified information. By all accounts, this cannot be interpreted as undermining the possibility of national authorities to ensure effective protection of sensitive information by means of ascribing to it a classified (secret) nature, since, as already underlined, this point was not an issue in this case. Rather, it remains to be ascertained whether the additional requirement described by the Court in order to satisfy the right for effective judicial protection – i.e. the mandatory scrutiny by the judiciary of the proportionality of the authorities" non-disclosure decision – is liable to produce, in the medium to long terms, situations in which the security of sensitive information might be affected to a lesser or more serious degree.

Going further, the Court also confirmed a widely accepted reasoning of the national authorities contending that the evidence supporting a decision on grounds of national security could in itself be liable to "compromise State security in a direct and specific manner".[76] Thus, the obligation of national authorities to disclose, to the interested person, the grounds and evidence on which a decision is based (refusing a citizen of the European Union admission to a Member State on public security grounds) is limited to "that which is strictly necessary", with due account to the necessary confidentiality of the evidence in question.[77]

The reluctance of Member States to confide trust in each other"s national security authorities, in terms of handling classified information, has seen confirmation in a judgment against Austria in a case concerning its failure to fulfill its obligations related to public service contracts, which entailed the protection of essential security interests.[78] The CJEU once again proved that it is playing its part in ensuring that the need for security against transnational crime and terrorism, albeit tangible and urgent, does not become an umbrella for abuse of rights by the authorities of Member States, that would irrevocably turn the balance away from the founding principles of the common market and even the individual rights and freedoms, as guaranteed by the EU legal order.

In the cited case, the CJEU has approached the issue of classified information by using its well-established narrow or strict interpretation, based on the all-encompassing principle of proportionality. Thus, it argued that the non-disclosure provision of Article 346(1)(a)

[75] Judgment of 4 June 2013, *ZZ*, C-300/11, ECLI:EU:C:2013:363, para. 65 (hereinafter "C-300/11").
[76] C-300/11, para. 66.
[77] C-300/11, para. 69.
[78] Judgment of 20 March 2018, *Commission v. Austria (State printing office)*, C-187/16, ECLI:EU:C:2018:194, para. 68 (hereinafter "C-187/16").

TFEU does not apply indiscriminately to any type of information that a Member State might consider to be sensitive.[79] The Court even went so far as to assess the degree in which a facility under some form of control by a Member State is in fact better suited to ensure the confidentiality of sensitive information in a works contract than other companies operating in said Member State or others. In this respect, it argued that the necessary degree of confidentiality of information could be guaranteed by means of special arrangements imposed through private-law contractual mechanisms. It should be noted that the case under consideration did not entail high-level classified information. [80]

In a recent case[81] the General Court the General Court has recognised some limitations to its powers to examine and decide on the institutions" refusal to grant access to information. Thus, the General Court is mandated to assess only if the procedural rules and the duty to state reasons have been complied with and whether the facts have been accurately described. It follows, then, that in substantive terms only finding "a manifest error of assessment or a misuse of powers by the institution" would be grounds for censoring the institution"s decision to refuse access.[82] Case T-31/18 is exemplary in this respect, as the Court has established the pre-eminence of the need to protect operational information held by the institutions, *in casu* the European Border and Coast Guard Agency (FRONTEX).[83]

5. Conclusions

The research at the heart of this paper was based on the overarching idea that the provisions of the Defence Procurement Directive proved inapt to furnish a functional framework for managing the various security of information concerns and, thus, an alternative solution should be sought with a view to obtain a highly coordinated (if not unitary) regime for classified information among EU Member States.

Along these lines, the research has firstly sought to establish whether there are sufficient reasons to conclude that the EU has, thus far, managed to establish a proprietary and functional framework for dealing with classified information, covering both its institutional actors, as well as its dynamics with the member states and among themselves. On this point, the examination of the provisions of the EURATOM Regulation and those of Council Decision 2013/488 has shown that the inherent limitations of the EU"s approach to a sectoral/procedural dimension in defining rules and regulation for security of information has not impeded it from tackling more substantive aspects, such as granting clearances or their automatic recognition at EU institutional level.

This conclusion is based, on one hand, on the fact that the rules prescribed by the EURATOM Regulation for the protection of classified information have stood the test of time and have proven – even if for this reason alone – their ability to respond to the specific needs of the Member States and the Community as a whole. As shown, these

[79] C-187/16, para. 72.
[80] C-187/16, para. 84-85.
[81] Judgment of 27 November 2019, *Izuzquiza and Semsrott v. Frontex*, T-31/18, ECLI:EU:T:2019:815, para. 25 (hereinafter "T-31/18").
[82] T-31/18, para. 65.
[83] T-31/18, para. 91, 112.

rules touch on the fundamental issues underpinning security of information and have therefore proven that multinational consensus can be reached and effectively implemented. Secondly, the basic elements of the solutions enacted by the EURATOM Regulation have been subsequently confirmed in the relevant Council Regulations which, and the instruments provided therein have been tested and validated by the CJEU in various circumstances.

Thus, the analysis of the rules and procedures set up by the EU for the protection of classified information has outlined that the Union has taken this imperative security need very seriously since its very inception. Moreover, it has proven consistency and determination in monitoring, evaluating and improving the mechanisms in place, in close coordination with the relevant authorities of the Member States. Current regulations and procedures duly observe the fundamental legal and operational principles, instruments and requirements pertaining to the protection of classified information (on clearance, physical protection, administrative measures, management etc.) largely implemented by Member States – while reserving a margin of criticism, voiced *supra* in individual cases, where relevant. The question remains if this conclusion bears enough weight in the rationale of the Member States to encourage them to move forward towards an EU-wide legal and procedural mechanism for the management of classified information that would provide the tools needed for unimpeded access by potential tenderers to defence and security contracts in any member state at any time.

Furthermore, the aptitude of the EU institutional framework to provide the requisite level of security of information has been acknowledged by doctrine, albeit by specific reference to the experience of the Commission in handling professional secrecy in the context of competition cases.[84] In the same line of reasoning, another paper concluded that the internal rules-based system implemented by the EU has proved effective in providing a level of protection for classified information similar to that given in member states.[85]

This positive perspective has been – to some extent – confirmed by the case-law of the CJEU, as shown in the relevant section. Thus, some points of concern notwithstanding, the Court has shown that the basic concepts and principles related to security of information have been astutely adopted and implemented by the EU institutional framework and have stood the test of judicial scrutiny, including in the context of access to information, which is particularly demanding.

In the more challenging realm of identifying potential avenues for future regulatory solutions for the integrated management of classified information, which would ultimately serve *inter alia* the specific purpose of defence procurement integration, the main issue of contention is the legal basis for any such initiative. An analysis made by Deirdre Curtin has concluded, in general terms, "that there is no separate treaty based legal basis for adopting Union wide rules on the classification of documents".[86] From a strict, *ad litteram*, normative perspective, this conclusion holds true, as the TEU and the TFEU do not contain an explicit mandate for the Union to regulate in this field.

[84] M Trybus (2014), *op.cit.*, p. 130.
[85] Galloway (2014), *op.cit.*, p. 682.
[86] D. (2013), op.cit., pp. 433-436.

Nevertheless, the same analysis explores various indirect legal foundations that might be used to substantiate a regulatory initiative in this respect. It should be noted, at this point, that in Opinion 2/00 (EU:C:2001:664, paragraphs 5 and 6), the CJEU emphasised that to proceed on an incorrect legal basis is liable to invalidate the act concluding the agreement, and that that is liable to create complications both at EU level and in international law.

In the same spirit of intellectual debate and normative exploration, the research presented in this paper has hinted to some potential solutions for an EU-wide legal framework for the protection of classified information, whether in broader or more specific terms. These possibilities are presented herein, with the understanding that they require further and more in-depth research, which can form the topic of a future paper on the matter.

Before proceeding to the potential avenues of regulatory action, it is important to note that this research has revealed specific requirements pertaining to the protection of classified information, some of which have been adopted in security policies across the spectrum, ranging from civil to military organisations. Among these, the following concepts have stood out as legal and operational instruments used by national authorities to guarantee an effective level of control and protection and should thus be mandatorily included in any normative initiative in the field: security screening and authorisation; originator consent/control; physical security (premises and cyber); as a corollary to control mechanisms, the ability to invoke legal responsibility, from civil/administrative liability to prosecution under criminal law.

One way to act is still tributary to classical intergovernmental means of cooperation, considering that CFSP, CSDP – fields in which security of information is particularly relevant, especially in terms of defence and security procurement – are still outside the community acquis and out of the scope of EU regulatory instruments. In this respect, a potential solution could have a one-fold or two-fold approach. Thus, the one-fold solution envisages the Council adopting a Decision that tasks the Commission with establishing an open-ended (starting from a minimal base ensuring fundamental functionalities) EU-wide system for coordinating security of information mechanisms through an individual body set up within the European Defence Agency, having a separate governing body, comprised of designated representatives of each MS, mandated to decide on the pathway for the evolution of the mechanism for security of information tailored for defence and security procurement. The two-fold solution[87] would presume the creation of an adequate legal basis in an intergovernmental conference, within the co-decision framework and then use the mandate thus conferred to enact a normative instrument pertaining to the regime of classified information.[88] Additional research is required as to the advantages/disadvantages of each option and, more importantly, their applicability and effectiveness.

It is important to note that the solution of creating a legal framework through an international agreement should be subjected to the CJEU"s autonomy test. Thus, if the proposed solution would be completely outside the EU legal order (a consideration that should also face scrutiny), then it should

[87] *See* Curtin (2014), *op.cit.*, p. 693.

[88] The idea of a Directive that would regulate an EU-wide regime for security clearances has been mentioned by doctrine, *see* M Trybus (2014), *op.cit.*, p. 393.

be determined whether it is liable to affect the EU"s jurisdictional legal order, as defined by the concept of autonomy aiming at preserving the unity of the EU legal order and the uniform application of its rules.[89] In this respect, an original solution could be to circumvent the lack of legal basis in the Treaties by using an intergovernmental legal vehicle to which the EU can adhere.[90]

In any case, any regulatory solution should avoid ambiguous formulations, whatever the difficulties in managing various interests and sensitivities. Otherwise, the normative thread could be pulled in a direction that would potentially go against the interests of the stakeholders, amongst which national authorities of the Member States feature prominently. Thus, the wording of the regulation should be clear and concise, to avert the possibility that its scope and application be subjected to the interpretation of the CJEU.[91]

Whatever the avenue, it is without question that the art of compromise has been effectively used in solving complex issues pertaining to security of information, as proven by the relevant provisions of the Defence Procurement Directive, the system of Interinstitutional Agreements and the case-law of the CJEU on denial of access to sensitive information. In this respect, it is useful to note that a possible way towards compromise would be to limit the scope of the prescribed normative instrument to a clearly defined segment or sector. Along these lines, the fact the EURATOM Regulation had a limited sectoral scope – as shown in section 3.1. of this paper – also came as an advantage, thus streamlining each Member States" calculations on the potential strategic and security impact of the new rules.

References

- M Trybus "Buying Defence and Security in Europe. The EU Defence and Security Procurement Directive in Context" (Cambridge University Press, 2014);
- Neamtu, B, Dragos, D. (2019), "Freedom of Information in the European Union: Legal Challenges and Practices of EU Institutions", in Dragos, D., Kovač, P., Marseille, A. (eds.) (2019), "The Laws of Transparency in Action. A European Perspective", Palgrave MacMillan;
- MK Davis Cross, "Security Integration in Europe. How Knowledge-Based Networks are Transforming the European Union" (The University of Michigan Press, 2014);
- R Dover, MS Goodman, C Hilldebrand (eds), "Routledge Companion to Intelligence Studies" (Routledge, 2014) 258; B Driessen, "Transparency in EU Institutional Law: A Practitioner"s Handbook" (2nd ed, Kluwer Law International, 2012);
- JW van Rossem, "The Autonomy of EU Law: More is Less?" (2013) in RA Wessel and S Blockmans (eds), Between Autonomy and Dependence (Asser Press, 2013);
- D Galloway, "Classifying secrets in the EU" (2014) 52 3 Journal of Common Market Studies 668;
- D Curtin, "Official Secrets and the Negotiation of International Agreements: Is the EU Executive Unbound?" (2013) 50 Common Market Law Review 423;

[89] JW van Rossem, 'The Autonomy of EU Law: More is Less?' (2013) in RA Wessel and S Blockmans (eds), *Between Autonomy and Dependence* (Asser Press, 2013) 15-17 and 19.

[90] van Rossem (2013), *op.cit.*, p. 20.

[91] *See, inter alia*, Judgment of the Court (Grand Chamber) of 18 December 2007, *Sweden v. Commission*, C-64/05 P, ECLI:EU:C:2007:802, para. 33.

- D Curtin, "Overseeing Secrets in the EU: A Democratic Perspective" (2014) 52 Journal of Common Market Studies 684;
- Rosén, G. (2015), "EU Confidential: The European Parliament"s Involvement in EU Security and Defence Policy", Journal of Common Market Studies 53:2;
- A Roberts, "Entangling Alliances: NATO"s Security of Information Policy and the Entrenchment of State Secrecy" (2003) 36 Cornell International Law Journal 329;
- SA Purza, "Setting the Scene for Defence Procurement Integration in the EU. The Intergovernmental Mechanisms" (2018) 4 European Procurement & Public Private Partnership Law Review 257;
- Labayle, H. (2010), "Principles and procedures for dealing with European Union Classified Information in light of the Lisbon Treaty", European Parliament – Directorate General for Internal Policies, Policy Department C: Citizens" Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, pp. 7-8, available at: https://www.statewatch.org/media/documents/news/2010/may/ep-classified-information-study.pdf;
- Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, Official Journal of the European Union, L 216, 20.8.2009;
- Council Decision of 23 September 2013 on the security rules for protecting EU classified information, Official Journal of the European Union L 274, 15.10.2013;
- Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, Official Journal of the European Union L 72, 17.3.2015;
- 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, Official Journal of the European Union L145, 31.5.2001;
- Interinstitutional Agreement of 12 March 2014 between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, OJ 2014 C 95/1;
- Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, Official Journal of the European Union C202, 8.7.2011;
- Regulation (Euratom) No 3 implementing Article 24 of the Treaty Establishing the European Atomic Energy Community, Official Journal of the European Communities no. 406/58;
- Consolidated Version of the Treaty Establishing the European Atomic Energy Community, OJ C 203/2016 ;
- Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, the Official Journal of the European Union, C 202, 8 July 2011;
- Decision 24/95 of the Secretary-General of the Council of 30 January 1995 on measures for the protection of classified information applicable to the General Secretariat of the Council (not published);
- Decision of the Secretary-General of the Council/High Representative for the Common Foreign and Security Policy of 27 July 2000 on measures for the protection of classified information applicable to the General Secretariat of the Council (Official Journal of the European Communities, C 239, 23 August 2000);
- Council Decision 2001/264/EC of 19 March 2001 adopting the Council"s security regulations (Official Journal of the European Communities, L 101, 11 April 2001);

- Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information (Official Journal of the European Union, L 141, 27 May 2011);
- Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (Official Journal of the European Union, L 274, 15 October 2013);
- Council Decision of 23 September 2013 on the security rules for protecting EU classified information, Official Journal of the European Union, L 274, 15.10.2013;
- Commission Staff Working Document: Evaluation of Directive 2009/81/EC on public procurement in the fields of defence and security, SWD (2016) 407 final;
- Commission of the European Communities, "Commission Staff Working Document – Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on the coordination of procedures for the award of certain public works contracts, public supply contracts and public service contracts in the fields of defence and security – Impact Assesment", Brussels, 5.12.2007 SEC(2007) 1598;
- Judgment of 6 December 2001, Council v. Hautala, C-353/99 P, ECLI:EU:C:2001:661 ;
- Judgment of 19 July 1999, Hautala v. Council, T-14/98, ECLI:EU:T:1999:157 ;
- Judgment of 1 February 2007, Sison v. Council, C-266/05 P, ECLI:EU:C:2007:75;
- Judgment of 26 April 2005, Sison v. Council, T-110/03, T-150/03 and T-405/03, ECLI:EU:T:2005:143;
- Judgment of 15 December 2009, Commision v. Germany, C-372/05, ECLI:EU:C:2009:780 ;
- Judgment of 4 June 2013, ZZ, C-300/11, ECLI:EU:C:2013:363;
- Judgment of 20 March 2018, Commission v. Austria (State printing office), C-187/16, ECLI:EU:C:2018:194;
- Judgment of 27 November 2019, Izuzquiza and Semsrott v. Frontex, T-31/18, ECLI:EU:T:2019:815;
- Judgment of the Court (Grand Chamber) of 18 December 2007, Sweden v. Commission, C-64/05 P, ECLI:EU:C:2007:802, para. 33.