Cent. Eur. J. Public Policy 2025; 19(2): 77-86
DOI: 10.2478/cejpp-2025-0007

Małgorzata Grześków[1]

When Security Overrides Transparency: The National Security Clause in Whistleblower Protection (Polish and EU Perspective)

ABSTRACT: *This article examines how the undefined concept of "national security" in both the EU Whistleblower Protection Directive and the Polish Whistleblower Protection Act complicates the application of whistleblower safeguards. It highlights the practical challenges authorities face in determining when the national security exclusion applies, and calls for clear criteria and procedures to balance transparency and whistleblower protection with legitimate national interests. The article argues that the vague nature of this exception in both EU and Polish laws generates legal uncertainty and may enable Member States to circumvent whistleblower protections without adequate justification. The Polish Whistleblower Protection Act excludes disclosures related to national security, particularly those that would violate legal confidentiality. Court of Justice of the European Union jurisprudence, however, requires that such exclusions be grounded in a concrete threat to fundamental state interests. This creates a significant interpretive burden for administrative and judicial authorities, undermining legal certainty and consistent application of the law.*

KEYWORDS: Whistleblower protection, national security, EU law, Poland, legal doctrine, public interest.

JEL: K23, K33, K10

RECEIVED 28 June 2025; **ACCEPTED** 30 June 2025.

INTRODUCTION

Whistleblower protection is one of the key mechanisms for promoting transparency and combating misconduct in both the public and private sectors. Directive 2019/1937 on the protection of persons who report breaches of Union law introduces comprehensive safeguards, including legal mechanisms designed to protect individuals from retaliation after disclosing wrongdoing. While the Directive and national implementing acts represent significant progress, they must also consider the potential implications for national security. As a result, a careful balance must be maintained between transparency and the protection of essential state interests, allowing for disclosures while safeguarding key security functions.

In EU law, national security is treated with sensitivity, often resulting in explicit derogations. Directive 2019/1937 includes a provision commonly known as the "national security exclusion" – a clause allowing Member States to limit whistleblower protections when the national security may be at stake. This may significantly reduce the scope of protection in sensitive areas such as intelligence or defense.

The case of Hungary illustrates how the national security exclusion can affect the practical application of whistleblower protections. The Hungarian law implementing Directive 2019/1937 has been criticized for allowing broad exemptions in cases involving classified information or evidence from criminal investigations, even though such matters could be regulated more proportionately under national legislation. In addition, due to the expansive application of this clause, certain public officials, including members of law enforcement, may be excluded from protection if they breach internal rules. These limitations, particularly within Hungary's national security framework, risk deterring potential whistleblowers, even in serious corruption cases. A notable example is the Schadl–Völner affair, in which senior justice officials were charged with bribery. Despite the gravity of the case, employees of the Ministry reportedly refrained from speaking out due to a lack of trust and fear of retaliation (Transparency International Hungary, 2023).

1 Faculty of Law, Administration and Economics, University of Wrocław, Poland; Email: malgorzata.grzeskow@uwr.edu.pl; ORCID: https://orcid.org/0000-0002-8449-898X

In Poland, even before the formal implementation of the Directive, similar concerns emerged following public disclosures about the use of Pegasus spyware by security services. Here, national security was invoked to justify secrecy and restrict accountability (Amnesty International, 2022).

Such cases show that the national security clause is not a theoretical legal device but a potentially far-reaching tool. Its interpretation may allow governments to sidestep core protections offered by EU law.

This article examines the scope and impact of the national security clause in the Polish Whistleblower Protection Act, assessed against EU law and key legal principles such as legal certainty, proportionality, and effective protection. The structure is as follows: the next section reviews relevant literature on national security in legal contexts, following which an outline of the methodology is given. The analysis then covers the legislative background of EU and Polish whistleblower frameworks, the legal meaning of "national security," and how the exclusion clause was implemented in Poland. It concludes with interpretive challenges, relevant Court of Justice of the European Union (CJEU) case law, and recommendations for improving legal clarity and consistency.

LITERATURE REVIEW

The concept of whistleblower protection has garnered increasing academic and regulatory attention over the past two decades, particularly considering its role in enhancing transparency and accountability across both public and private sectors. Simultaneously, national security has remained a highly sensitive and legally vague domain – one that often serves as a ground for limiting the right to report misconduct. This section reviews existing literature, highlights comparable studies and methodologies, and identifies research gaps relevant to the interpretation and legal consequences of the national security exclusion under Directive 2019/1937.

The ambiguity of national security

EU law does not offer a legal definition of "national security" and, in addition, frequently resorts to closely related or overlapping notions such as "public security," "state security," and "national defense." The definition of national security was likewise not introduced by the Polish legislator in the Polish Whistleblower Protection Act. In this area, one can therefore rely only on case law and legal scholarship. As a result, responsibility for interpreting and applying the relevant provisions falls on those who implement them. In practice, the risk linked to the accurate interpretation of these terms ultimately rests with those applying the law (Tokarczyk, 2024).

The inherent ambiguity of the concept of national security has long been recognized in academic literature. Arnold Wolfers (1952) was among the first to highlight this issue, noting: "It would be an exaggeration to claim that the symbol of national security is nothing but a stimulus to semantic confusion, though closer analysis will show that if used without specifications it leaves room for more confusion than sound political counsel or scientific usage can afford." Building on this observation, David A. Baldwin (1997) cautions that: "The purpose is to define security as a policy objective distinguishable from others. Since security competes with other goals for scarce resources, it must be distinguishable from, yet comparable with, such goals. This requires that the relative importance of security be left open rather than built into the concept in terms of 'vital interests' or 'core values'."

Interdisciplinary and functional approaches to national security

Contemporary legal scholarship broadly associates national security with the preservation of a state's existence, institutional stability, and core societal functions, although the term itself remains conceptually fluid and highly context dependent (Sibiga, 2021; Brzeziński, 2009; Stańczyk, 1996). This conceptual vagueness has led to different interpretations across disciplines. Some authors approach "national security" from an economic perspective, defining it as "the set of public policies that protect the safety or welfare of a nation's citizens from substantial threats" (Murphy & Topel, 2013). In this view, national security extends beyond traditional defense concerns to include broader aspects of social and economic resilience. In addition, the concept is closely linked to actions taken by states to safeguard their national identity, cultural continuity, and territorial integrity (Kurek, 2017).

The balance between transparency and national security

A particularly significant contribution to the debate on balancing transparency and national security is Kagiaros's (2015) analysis of freedom of expression under the European Convention on Human Rights. His study offers a nuanced comparative perspective by evaluating three distinct legal models for managing disclosures related to national security, employing a doctrinal and case law-based methodology. These models are: (1) an absolute ban on external disclosures by intelligence officials; (2) a broad exemption from sanctions when the public interest in the disclosure outweighs national security concerns; and (3) protection limited to a narrowly defined list of specific types of wrongdoing, exhaustively enumerated in the law. Kagiaros examines the compatibility of each model with Council of Europe standards and concludes that, despite its limitations, the third model offers the most balanced way to uphold freedom of expression while safeguarding legitimate national security interests. This analysis provides a useful reference for assessing national-level exemptions.

Other useful contributions include Abazi (2020), who evaluates the transformative potential of Directive 2019/1937 through doctrinal and policy analysis. The study not only highlights the Directive's broad scope and emphasis on strengthening internal and external reporting channels, but also concludes that the exclusion of information protected under national security regimes – due to Member States' exclusive competence – represents a significant limitation. Abazi notes, however, that this gap could be addressed by national legislators choosing to include such disclosures in domestic transpositions of Directive 2019/1937. Another relevant source is Transparency International's 2023 comparative report on national implementations of Directive 2019/1937, which identifies best practices and remaining legal loopholes (Transparency International, 2023).

Together, these studies inform the present analysis and clarify the broader legal and institutional context.

METHODOLOGY

This article applies a legal-dogmatic method. The analysis focuses on interpreting binding legal acts, including Directive 2019/1937 and the Polish Whistleblower Protection Act. The study also considers relevant case law of CJEU, legislative materials, and selected doctrinal commentaries to examine the scope, application, and limits of the national security exception in whistleblower protection law.

The legal-dogmatic method is appropriate for this research, as it allows for a systematic and structured analysis of normative texts, institutional interpretations, and their mutual coherence. This method is particularly suited for assessing the internal consistency of legal instruments and their compliance with general principles of EU law, such as legal certainty and proportionality.

To guide the analysis, the article addresses the following research questions:

1) How is the concept of "national security" framed in EU law?
2) To what extent does the Polish Whistleblower Protection Act reflect the scope and intent of the national security exception under Directive 2019/1937?
3) Who is the addressee of the exclusion clause in the Polish Whistleblower Protection Act?
4) What are the legal consequences of excluding certain disclosures from whistleblower protection?
5) Does the Polish approach to the national security exception align with the standards developed in the case law of CJEU?

FINDINGS

This section presents a structured analysis of the national security exception in both EU and Polish whistleblower protection laws. It outlines the relevant legal provisions, legislative developments, and implementation mechanisms, aiming to identify how the concept of national security is framed and operationalized. The findings are thematically aligned with the five research questions guiding this study.

How is the concept of "national security" framed in EU law?

In response to the first research question, this subsection examines how the concept of "national security" is constructed in EU primary and secondary law and how it limits Member States' discretion.

The legal foundations for dividing competences between the European Union and Member States in the areas of national security and defense are found primarily in the EU treaties, especially the Treaty on the European Union (TEU, 2004) and the Treaty on the Functioning of the European Union (TFEU, 2004). According to Article 4(2) TEU, the EU must respect matters that remain within national competence, including foreign and defense policy. At the same time, Article 42 TEU establishes the Common Security and Defense Policy (CSDP), which supports but does not override national strategies. EU powers in this domain are limited and cannot undermine Member States' autonomy. In addition, Article 222 TFEU introduces the solidarity clause, enabling coordinated EU responses to terrorist attacks or other crises, provided these respect national prerogatives. Finally, Article 346 TFEU remains a key legal basis for derogations concerning essential state security interests, particularly in defense-related areas.

The above provisions confirm that national security is an exclusive responsibility, allowing states to take protective measures against external threats and to maintain internal order (Grzeszczak, 2023). However, this autonomy is not absolute. When exercising exclusive competences, especially in internal matters, Member States must still respect EU law obligations, particularly those under articles 2 and 19 TEU (Commission v Poland, Case C-619/18, EU:C:2019:531). In external affairs, state competences are safeguarded by CSDP procedures that require consensus or unanimity. The concept of national security does not extend to establishing general frameworks for counterterrorism or fighting organized crime, which are governed by the TFEU chapter on the Area of Freedom, Security, and Justice (Kurek, 2017).

While primary EU law does not define "national security," it gives Member States some discretion. From the perspective of national lawmakers, this calls for careful reflection on which areas should be excluded from general regulatory frameworks. The term "national security" appears in secondary EU law, mainly in the form of explicit exemptions aimed at safeguarding Member States' sovereignty. Such derogations can be found in directives concerning environmental protection (Directive 2004/35/EC), public procurement (Directive 2014/24/EU), and data protection (Directive 95/46/EC). For instance, Directive 95/46/EC explicitly permits derogations on the grounds of national security (Kurek, 2017).

CJEU has clarified the legal scope of national security in several cases. In *ZZ v. Secretary of State for the Home Department* (Case C-300/11), the Court found that national security includes both internal and external aspects (para. 38), and that restrictions on treaty freedoms must be justified by a genuine and verified threat and accompanied by procedural safeguards (paras 65–69). In *Tele2 Sverige* and *Secretary of State for the Home Department* (Joined Cases C-203/15 and C-698/15), the Court reiterated that such measures must respond to a real or foreseeable threat and comply with proportionality (paras 119–125). In *La Quadrature du Net* (Joined Cases C-511/18, C-512/18, and C-520/18), CJEU further stated that national security relates to threats that endanger essential state functions such as territorial integrity or constitutional order (paras 135–137). Even in these cases, mass or unlimited surveillance without safeguards is prohibited. In other rulings, CJEU confirmed that certain matters – such as asylum policy, national language protection, or noble titles – fall within Member States' exclusive competences (e.g., Case C-208/09, Case C-601/15). However, the Court has consistently ruled that the national security exception must not be misused to bypass EU law (e.g., Case C-615/10, *Insinööritoimisto InsTiimi Oy*). This stands in contrast to a rising trend among Member States to invoke broad and vaguely defined concepts as justifications for derogation (Barbou des Places, 2024). As Turmo (2021) observes, this reflects wider resistance to the core principles of EU integration, especially in the context of state surveillance.

To what extent does the Polish Whistleblower Protection Act reflect the scope and intent of the national security exception under Directive 2019/1937?

This section assesses the degree to which the Polish Whistleblower Protection Act reflects the scope and intent of the national security exception laid down in Directive 2019/1937, by first outlining the structure and purpose of this exclusion in EU law and then comparing it with the Polish implementation.

Directive 2019/1937 includes an explicit exclusion related to national security, reflecting the broader EU approach of treating this area with heightened sensitivity and preserving the sovereign competences of Member States. Recital 24 of the preamble to Directive 2019/1937 states that: "National security remains the sole responsibility of each Member State. This Directive should

not apply to reports of breaches related to procurement involving defence or security aspects where those are covered by Article 346 TFEU, in accordance with the case law of the Court. If Member States decide to extend the protection provided under this Directive to further areas or acts, which are not within its material scope, it should be possible for them to adopt specific provisions to protect essential interests of national security in that regard." A similar exclusion is contained in Article 3(2) of Directive 2019/1937, which provides that: "This Directive shall not affect the responsibility of Member States to ensure national security or their power to protect their essential security interests. In particular, it shall not apply to reports of breaches of the procurement rules involving defence or security aspects unless they are covered by the relevant acts of the Union." An important exclusion from the scope of the Directive is also reflected in Article 3(3)(a), which states that the Directive does not apply to the reporting of breaches involving information classified in the interest of national security, defense, or covered by professional secrecy (Directive 2019/1937, Art. 3(3)).

Both Recital 24 of the preamble and Article 3 of the Directive clearly confirm that national security remains the exclusive domain of each Member State. These provisions should be interpreted as a guarantee of regulatory autonomy in areas considered vital to state sovereignty, such as the protection of classified information or the functioning of security and intelligence services. The Directive 2019/1937 also grants Member States discretion to extend whistleblower protection to areas beyond the scope of EU law, while allowing for the adoption of specific rules to safeguard national security interests. Accordingly, states retain not only the right to invoke exclusions, but also the possibility of differentiating protection standards depending on the nature of the information being disclosed.

In Poland, concerns related to the relationship between national security and whistleblower protection emerged already during the legislative process, leading to the adoption of the act implementing Directive 2019/1937. One of the key issues that arose at that stage was whether to include soldiers and members of militarized services among the categories of potential whistleblowers. These individuals play crucial roles in safeguarding the territorial integrity of the state, maintaining public order, and responding to both internal and external threats. Moreover, members of militarized services and soldiers are subject to duties of official secrecy and protection of classified information. The very nature of their service is, therefore, inextricably linked with activities in the realm of national security.

The personal scope of the Polish Whistleblower Protection Act underwent multiple changes during the drafting phase. In the initial draft dated October 14, 2021, officers and soldiers were not explicitly included in the list of potential whistleblowers, which raised growing concerns about the possibility of affording them adequate protection. In the subsequent draft of April 6, 2022, members of militarized services and soldiers were added to this list (Government Legislation Centre, 2025). However, this solution was also met with criticism. The Polish Ministry of the Interior and Administration questioned the need to extend whistleblower protection to police officers, arguing in its opinion on the draft of December 13, 2022 that existing internal police procedures already provided sufficient safeguards. This opinion sparked a broader debate on the very possibility and potential effectiveness of whistleblower protection for officers and soldiers. The opinion emphasized that police officers already have appropriate channels for reporting violations such as corruption or irregularities in public procurement. According to the authors of the opinion, when disclosing such misconduct, officers should act in accordance with existing regulations and internal procedures specific to the police service (Government Legislation Centre, 2025). In the subsequent draft dated March 27, 2023, officers and soldiers were removed from the list of entities potentially eligible for protection under the new provisions. However, the next draft of July 12, 2023 once again included them in the list of potential whistleblowers, and the following drafts of January 8, 2024 and March 27, 2024 did not alter this approach. Although the list of potential whistleblowers remained open in each version of the draft, the difficulties encountered by the drafters suggest that there may be significant challenges in granting whistleblower status to members of uniformed services (Government Legislation Centre, 2025).

In the final version of the Act, the Polish legislator did not decide to extend the application of Directive 2019/1937 to areas not covered by EU law (Directive 2019/1937, Recital 24)[2]. However, bearing in mind the need to protect national security, the adopted legislation includes a catalog of exclusions. Article 5 of the Polish Whistleblower Protection Act introduces three categories of such exclusions. The provisions of the Act do not apply (in whole or in part) to (1) the information enumerated in Article 5(1), (2) breaches of law concerning procurement in the fields of defense and security as defined in Article 5(2), and (3) breaches of law directly related

2 According to Recital 24 of the Directive 2019/1937, *in fine*: "If Member States decide to extend the protection provided for in this Directive to additional areas or acts which do not fall within its material scope, they should be able to adopt specific provisions to protect the essential interests of national security in that context."

to the execution by special services of their statutory tasks aimed at ensuring national security (Article 5(3)). The first two categories of exclusions are comprehensive (the entire Polish Whistleblower Protection Act Whistleblower Protection Act does not apply), while the third category is partial (only Chapter 5 of the Polish Whistleblower Protection Act does not apply to the breaches listed therein).

The first category of exclusions includes information covered by (1) provisions on the protection of classified information and other information that, under generally applicable law, must not be disclosed for reasons of public security; (2) professional secrecy of medical and legal professions; (3) the secrecy of judicial deliberations; and (4) criminal proceedings insofar as it concerns the secrecy of preparatory proceedings and court hearings conducted in camera.

Article 5(1)(1) of the Polish Whistleblower Protection Act refers to "information" without linking it directly to a breach of law, making its scope broader than that of Article 5(2) (Sobczyk et al., 2025). This includes classified information, as defined by the Act of August 5, 2010, and "other information" that must not be disclosed under generally applicable law for reasons of public security. Unlike the clearly defined category of classified information, "other information" is open ended and context dependent. To fall under this category, the information must be (1) subject to a disclosure ban, (2) under general law, and (3) justified by public security concerns (Sobczyk et al., 2025). Examples include data protected under the Act on the Crown Witness (1997) and the Act on the Implementation of the Chemical Weapons Convention (2001).

The Polish Whistleblower Protection Act does not apply to breaches of law around defense and security procurement, as defined in Article 7(36) of the Public Procurement Law of September 11, 2019, if such contracts are excluded from its scope. This also includes offset agreements regulated by the Act of June 26, 2014 and other measures adopted pursuant to Article 346 of TFEU. Unlike the general exemption under Article 5(1) of the Polish Whistleblower Protection Act, which refers to specific categories of information, this exclusion concerns breaches of law as defined in Article 3 of the Whistleblower Protection Act. Under EU law, these exclusions are reinforced by Directive 2009/81/EC and further detailed in national legislation (e.g., Article 2(1)(3) and Article 13 of the Public Procurement Law). Consequently, breaches related to contracts falling under Article 7(36) of the Public Procurement Law are not subject to whistleblower protections (Public Procurement Law, 2019).

Another exclusion concerns violations of law related to other measures taken to protect the fundamental or essential interests of national security under Article 346 of TFEU. According to Article 346 TFEU: "1. The provisions of the Treaties shall not preclude the application of the following rules: (a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security; (b) any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material; such measures shall not adversely affect the conditions of competition in the internal market regarding products which are not intended for specifically military purposes. 2. The Council, acting unanimously on a proposal from the Commission, may make changes to the list of products drawn up by it on 15 April 1958 to which the provisions of paragraph 1(b) apply."

The final subject matter exclusion (of limited scope) concerns violations of law directly related to the execution by the intelligence services referred to in Article 11 of the Act of May 24, 2002 on the Internal Security Agency and the Foreign Intelligence Agency[3] of their statutory tasks aimed at ensuring national security. In this area, only Chapter 5 of the Polish Whistleblower Protection Act (i.e., the provisions concerning public disclosure) shall not apply. For this category of exclusions, it is essential to identify a direct link between the legal violation and the performance of statutory tasks. This quality will not extend to various types of technical activities that only indirectly support the fulfillment of statutory duties or the actions performed incidentally in the course of carrying out such duties. An additional condition for the application of the exclusion (with regard to Chapter 5 of the Polish Whistleblower Protection Act) is that the given task must be aimed at safeguarding national security (Łaguna & Wieczorek, 2025).

Who is the addressee of the exclusion clause in the Polish Whistleblower Protection Act?

The Polish legislator opted to introduce a catalog of exclusions in Article 5 of the Whistleblower Protection Act. By introducing these exclusions, the legislator uses the phrases "this Act shall not apply" or "the provisions of Chapter 5 shall not apply." The application of the law falls within the competence of administrative or managing authorities. From the structure and wording of these

3 Pursuant to Article 11 of the Act on the Internal Security Agency and the Intelligence Agency, the following bodies are classified as special services: the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, and the Central Anti-Corruption Bureau.

provisions, it follows that the addressees of the exclusion clause are not only the individuals making disclosures, but also primarily the administrative and managerial authorities responsible for applying the Act. The exclusions are thus framed as prohibitions directed at those authorities, effectively precluding them from applying the whistleblower protection mechanisms in specific cases. These entities should not apply the mechanisms of the Polish Whistleblower Protection Act to information for which the application of the Act has been excluded. Consequently, legal authorities are required to possess extensive knowledge across various fields.

Despite the central role of these authorities, the Act also places a burden of self-assessment on whistleblowers. As a result, individuals making disclosures must anticipate whether their report falls within an excluded category – an obligation that may discourage reporting in sensitive sectors. At the time of writing, there appear to be no publicly available cases in which the exclusion clause has been formally applied in practice. In fact, no such cases have yet reached courts or administrative bodies in Poland in a manner that would make them publicly known. This may be since the law was only adopted in July 2024, following a legislative delay of nearly 3 years in implementing Directive 2019/1937. Nonetheless, the formulation of the clause and its open-ended structure may generate interpretive uncertainty in the future. For instance, a potential scenario might involve a whistleblower reporting suspected corruption in a military procurement process; depending on whether the relevant contract is exempt under public procurement law, the authorities may be barred from applying protective provisions. Such ambiguities underscore the importance of clear administrative guidance and judicial oversight.

What are the legal consequences of excluding certain disclosures from whistleblower protection?

Although public authorities are responsible for applying the law, this does not relieve whistleblowers of personal responsibility. Individuals must independently assess whether the information they intend to disclose falls within the scope of the Whistleblower Protection Act. If the report concerns information excluded from protection under the Whistleblower Protection Act, the reporting person may still face disciplinary, administrative, civil, or even criminal liability (Tokarczyk, 2024).

Each of the exclusion clauses introduced in Article 5 of the Polish Whistleblower Protection Act entails distinct legal consequences, depending on the nature of the information disclosed and the category of exemption invoked. These provisions determine not only whether the Act applies, but also the extent to which whistleblowers may benefit from protective measures. Firstly, Article 5(1) provides for a total exclusion from the scope of the Whistleblower Protection Act in cases involving the disclosure of specific categories of sensitive information. Any individual who discloses such information forfeits all rights under the Whistleblower Protection Act. This includes losing protection against retaliation, the right to remain anonymous, and access to any legal remedies. Moreover, the act of disclosing such information may expose the reporting person to disciplinary, administrative, civil, or even criminal liability. Secondly, Article 5(2) extends the full exclusion to reports concerning breaches of law related to public procurement in the fields of defense and security. In such cases, the Whistleblower Protection Act does not apply, regardless of the content or seriousness of the wrongdoing reported. As a result, whistleblowers in these contexts are left without any legal protection. Thirdly, Article 5(3) introduces a more limited exclusion. It renders Chapter 5 of the Whistleblower Protection Act which governs public disclosures inapplicable in situations where the reported breach of law is directly related to the execution of statutory duties by intelligence services aimed at safeguarding national security. In these instances, internal and external reporting channels remain open, but public disclosure is prohibited, and any whistleblower choosing this route forfeits the protections associated with it.

Importantly, Article 16 of the Whistleblower Protection Act introduces a general rule of immunity from liability for whistleblowers, stipulating that reporting or public disclosure shall not constitute grounds for disciplinary, civil, or other legal liability, provided that the whistleblower had reasonable grounds to believe that the disclosure was necessary to reveal a legal violation in accordance with the Act. However, this guarantee is explicitly subject to the exclusions set out in Article 5, which carve out entire categories of information from the Act's scope. As a result, the protection under Article 16 does not apply to disclosures involving, for example, state secrets, even if the whistleblower had reasonable grounds to believe that the disclosure was necessary to reveal a legal violation in accordance with the Act. In such cases, whistleblowers remain exposed to full legal liability. In particular, the unauthorized disclosure of classified information marked "secret" or "top secret" may lead to criminal sanctions.

Therefore, while Article 16 establishes a vital protective mechanism for whistleblowers acting within the bounds of the Whistleblower Protection Act, it also underscores that those who report information explicitly excluded under Article 5 do so at considerable legal risk – including the possibility of criminal prosecution – regardless of intent or perceived public interest.

Cent. Eur. J. Public Policy 2025; 19(2): 77-86
DOI: 10.2478/cejpp-2025-0007

Does the Polish approach to the national security exception align with the standards developed in the case law of CJEU?

CJEU has repeatedly emphasized that derogations from rules intended to ensure the effectiveness of the rights conferred by the Treaties – particularly in areas such as public procurement – must be interpreted strictly (CJEU, Case C-199/85, 1987). In the context of procurement involving defense and security, a key judgment is CJEU's ruling in *Commission v Italy* (Case C-337/05, EU:C:2008:203), which confirmed that Member States may rely on exemptions related to national security only when the conditions laid down in Union law, particularly Article 346 TFEU, are met. Such exemptions must be applied in good faith, must not be arbitrary, and must be limited to cases where the procurement genuinely aims to safeguard essential national security interests. This line of reasoning has been consistently reaffirmed in other judgments involving national security, including in the areas of data retention and surveillance (e.g., *Tele2 Sverige*, Joined Cases C-203/15 and C-698/15), where CJEU stressed that national security derogations must be based on a demonstrated, serious threat to the fundamental interests of the state and must be accompanied by procedural safeguards and proportionality review. Based on this jurisprudence, the following conclusions emerge: 1. The exclusion of the Directive's application to reports concerning public procurement in the field of defense and security is legally permissible only if the procurement in question serves fundamental national security interests, and this must be subject to strict scrutiny. 2. If the procurement falls within the scope of EU law, such as under Directive 2009/81/EC on defense and security procurement, the exclusion under Article 3(2) of Directive 2019/1937 does not apply. 3. Measures adopted in the name of national interest are not automatically exempt from EU law; their compatibility must be assessed considering principles such as proportionality, legal certainty, and effective judicial protection.

Against this backdrop, the Polish implementation of the national security exception raises significant concerns. Article 5 of the Polish Whistleblower Protection Act introduces several exemptions, including disclosures relating to classified information and to procurement in the defense and security sectors, as well as breaches linked to the statutory activities of intelligence services. These exclusions are broadly formulated, lack precise definitions, and do not require that the derogation be justified by a concrete and verifiable threat to essential state interests. Moreover, the Polish Whistleblower Protection Act does not include any procedural safeguards or proportionality test to guide the application of these exclusions, leaving discretion largely to administrative authorities. The reliance on vague and legally undefined phrases – such as "statutory tasks aimed at safeguarding national security" – further increases the risk of arbitrary or overly expansive interpretation. This absence of objective criteria and procedural control mechanisms appears inconsistent with the requirements established in the case law of CJEU, which demands a restrictive and justified application of national security derogations. Consequently, the Polish approach to the national security exception may not align with the standards developed by CJEU, particularly as it allows for exclusions without ensuring that such measures are necessary, proportionate, and subject to meaningful legal oversight.

DISCUSSION

The findings presented above highlight increasing friction between national discretion and EU-level legal oversight. Recent scholarship underscores this trend, noting how Member States' reliance on national security considerations can clash with CJEU's role in upholding the primacy and coherence of EU law. This dynamic is particularly visible in areas like digital surveillance and data retention, where domestic courts – such as the French *Conseil d'État* (*Conseil d'État*, 2022) – may effectively "neutralize" CJEU rulings by appealing to constitutional authority in preference to EU obligations (Barbou des Places, 2024).

The national security exception, while recognized, requires concrete justification and must be interpreted narrowly. Its abstract formulation and lack of procedural safeguards raise concerns about potential misuse, particularly in politically sensitive cases. This could enable Member States to circumvent EU obligations and weaken the protection of whistleblowers. The Polish Whistleblower Protection Act exemplifies these challenges. It does not provide a definition of "national security," nor does it establish clear interpretative criteria. In the absence of such criteria, authorities lack guidance on how and when the exemption should be applied, increasing the risk of inconsistent application and legal uncertainty. The coexistence of closely related but undefined terms – such as "national security," "public security," "fundamental or essential interests of state security," and "statutory tasks aimed at ensuring

national security" – further complicates interpretation. These terminological ambiguities are particularly significant when assessing the legal consequences of the exclusions introduced by the Act. In practice, the burden of legal precision falls on the entities applying the law (Tokarczyk, 2024), which may lead to a fragmented or overly cautious implementation of whistleblower protections.

CONCLUSIONS

This article has demonstrated that the use of the national security exception in whistleblower protection – both at the EU and national levels – raises fundamental legal and institutional challenges. While the Directive 2019/1937 acknowledges the exclusive competence of Member States in this area, CJEU case law establishes clear limits on how broadly this competence may be interpreted. The Polish implementation, as shown, does not align with these standards: it lacks both clear definitions and procedural safeguards, increasing the risk of arbitrary application.

Considering these findings, several key recommendations emerge. First, at the EU level, there is a pressing need for supplementary interpretative guidance – possibly in the form of soft-law instrument – clarifying the permissible scope of national security derogations under Directive 2019/1937. Second, national legislation implementing the Directive should incorporate proportionality assessments and minimum procedural guarantees to ensure that the national security exception is not used as a blanket justification to exclude entire sectors or categories of information. Third, judicial and administrative authorities applying such exemptions should receive targeted training and guidance, given the high interpretative burden placed on them. More broadly, this analysis points to a structural tension between national discretion in security matters and supranational guarantees of transparency and accountability. If left unresolved, this tension may weaken the effectiveness of whistleblower protection mechanisms, especially in contexts involving serious wrongdoing within state institutions. Future research should examine how other Member States have operationalized the national security clause and whether consistent standards of review are emerging across jurisdictions. The effectiveness of EU whistleblower protection cannot depend solely on formal transposition. It requires normative coherence, legal certainty, and a shared commitment to protecting the public interest, even when it intersects with sensitive domains such as national security.

ACKNOWLEDGMENTS

The author declares no relevant acknowledgments or funding sources.

REFERENCES

Abazi, V. (2020). *The European Union Whistleblower Directive: A "Game Changer"? Industrial Law Journal, 49*(4), 604–623.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, 23(1), 5–26.

Barbou des Places, S. (2024). Public order and public security in EU law. *European Papers*, 9(3), 1318–1335.

Brzeziński, M. (2009). Kategoria bezpieczeństwa. In S. Sulowski & M. Brzeziński (Eds.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia* (22-32). ELIPSA Dom Wydawniczy i Handlowy Włodzimierz Ulicki.

Case 199/85, Commission v Italy, EU:C:1987:121.

Case C-284/05, Commission v Finland, EU:C:2007:409.

Case C-285/98, Kreil, EU:C:2000:2.

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

Case C-337/05, Commission v Italy, EU:C:2008:203.

Case C-615/10, Insinööritoimisto InsTiimi Oy, EU:C:2012:324.

Case C-619/18, Commission v Poland, EU:C:2019:531.

Directive 95/46/EC. (1995). Directive on the protection of individuals with regard to the processing of personal data. *Official Journal of the European Union*, L 281, 31.

Directive 2004/35/EC. (2004). Directive on environmental liability with regard to the prevention and remedying of environmental damage. *Official Journal of the European Union*, L 143, 56.

Directive 2014/24/EU. (2014). Directive on public procurement and repealing Directive 2004/18/EC. *Official Journal of the European Union*, L 94, 65.

Directive (EU) 2019/1937. (2019). Directive on the protection of persons who report breaches of Union law. *Official Journal of the European Union*, L 305, 17–56.

French Conseil d'État. (2022, July 27). *Judgment in Case No. 463850*.

Government Legislation Centre. (2025). *Draft legislation – Whistleblower Protection Act*. Retrieved January 25, 2025, from https://legislacja.gov.pl/projekt/12352401/katalog/12822845#12822845

Grzeszczak, R. (2023). In D. Kornobis-Romanowska (Ed.), *Traktat o Unii Europejskiej. Komentarz*. Wolters Kluwer.

Jaroszyński, T. (2020). Podejmowanie i wykonywanie działalności prowadzonej na własny rachunek w świetle prawa Unii Europejskiej. *Zeszyty Prawnicze*, 3(67), 22–35.

Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Secretary of State for the Home Department, EU:C:2016:970.

Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others, EU:C:2020:791.

Kagiaros, D. (2015). *Protecting "national security" whistleblowers in the Council of Europe: An evaluation of three approaches on how to balance national security with freedom of expression*. *International Journal of Human Rights, 19*(4), 408–428.

Kurek, J. (2017). Zakres stosowania ogólnego rozporządzenia o ochronie danych osobowych i dyrektywy 2016/680/UE – wyzwania związane z wyodrębnieniem działań państwa w obszarze bezpieczeństwa narodowego i bezpieczeństwa publicznego. *Europejski Przegląd Sądowy*, (5), 43–48.

Łaguna, Ł., & Wieczorek, M. (2025). In B. Baran-Wesołowska (Ed.), *Ochrona sygnalistów. Komentarz* (commentary on Article 5). Wolters Kluwer.

Murphy, K. M., & Topel, R. H. (2013). Some basic economics of national security. *American Economic Review*, 103(3), 508–511.

Poland: Use of Pegasus spyware to hack politicians highlights threat to civil society, Amnesty International 2022, Retrieved June 25, 2025, from https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/

Sobczyk, A., Cebera, A., Firlus, J. G., & Iwański, M. (Eds.). (2025). *Ustawa o ochronie sygnalistów. Komentarz*. CH. Beck.

Stańczyk, J. (1996). *Współczesne pojmowanie bezpieczeństwa*. Instytut Studiów Politycznych Polskiej Akademii Nauk.

Sibiga, G. (2021). Wyłączenie stosowania RODO do przetwarzania danych osobowych ze względu na bezpieczeństwo narodowe. Glosa do wyroku WSA z dnia 6 sierpnia 2020 r., II SA/Wa 2222/19. *Orzecznictwo Sądów Polskich*, 7–8, 67–70.

Tokarczyk, D. (2024). In E. Rutkowska (Ed.), *Ustawa o ochronie sygnalistów. Komentarz* LEX/el.

Transparency International. (2023). *Are EU countries ready to protect whistleblowers? Assessing the transposition of the EU Directive*. Retrieved June 24, 2025, from https://www.transparency.org/en/publications/assessing-whistleblower-protection-eu-directive-2023.

Transparency International Hungary. (2023, December 6). *Speak up or stay silent? The need for greater whistleblower protection in Hungary*. Retrieved June 24, 2025, from https://www.transparency.org/en/blog/need-for-greater-whistleblower-protection-in-hungary

Treaty on European Union. (2012). *Official Journal of the European Union*, C 326/13.

Turmo, A. (2021). National security as an exception to EU data protection standards: The judgment of the Conseil d'État in French Data Network and Others (CE Ass., 21 April 2021, Req. no. 393099). Common Market Law Review 59(1), 203-222.

Wolfers, A. (1952). 'National security' as an ambiguous symbol. *Political Science Quarterly*, 67(4), 481–502.

Whistleblower Protection Act of 14 June 2024. (2024). *Journal of Laws*, item 928.

Public Procurement Law of 11 September 2019. (2019). *Journal of Laws*, item 2019.

Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002. (2002). *Journal of Laws*, Nb 74 item 676.

Offset Contracts Security Act of 26 June 2014. (2014). *Journal of Laws*, item 1379, 2020.

Protection of Classified Information Act of 5 August 2010. (2010). *Journal of Laws*, Nb 182 item 1228.

Chemical Weapons Convention Implementation Act of 22 June 2001. (2001). *Journal of Laws*, Nb 76 item 812.