THE ETHICS OF SECRECY: INTELLIGENCE AGENCIES AND DEMOCRATIC ACCOUNTABILITY

Sveva Gaglione, Università di Torino, sveva.gaglione@unito.it

José Fontes, Academia Militar, jose.fontes.pt@gmail.com

https://doi.org/10.60746/8_19_47964

ABSTRACT

This article explores the ethical and legal dilemmas regarding intelligence activities within liberal democracies, where the operational demands of secrecy often collide with the democratic imperatives of accountability and protection of fundamental rights. Through case studies from the European Union, it investigates how historical legacies, public trust, and legal frameworks shape intelligence practices and influence their legitimacy. Underscoring the inherent moral ambivalence of intelligence – being an indispensable tool for national security, yet prone to overstep in the absence of effective constraints – the study ultimately insists on the need for normative structures capable of reconciling national security with civil liberties. Without meaningful oversight and transparency, intelligence agencies risk becoming incompatible with democratic principles. Yet, a key question persists: where should the line be drawn between democratic legitimacy and operational secrecy?

Keywords: Intelligence Ethics; Democratic Accountability; Rule of Law; National Security.

RESUMO

Este artigo explora os dilemas éticos e jurídicos relacionados às atividades de inteligência nas democracias liberais, onde as exigências operacionais de sigilo muitas vezes entram em conflito com os imperativos democráticos de responsabilização e proteção dos direitos fundamentais. Através de estudos de caso provenientes da União Europeia, investiga-se como legados históricos, confiança

pública e quadros jurídicos moldam as práticas de inteligência e influenciam a sua legitimidade. Ao destacar a ambivalência moral inerente à inteligência – sendo uma ferramenta indispensável para a segurança nacional, mas propensa a excessos na ausência de restrições eficazes – o estudo enfatiza a necessidade de estruturas normativas capazes de conciliar segurança nacional e liberdades civis. Sem uma supervisão efetiva e uma transparência significativa, os serviços de inteligência correm o risco de se tornarem incompatíveis com os princípios democráticos. Contudo, permanece uma questão fundamental: onde deve ser traçada a linha entre legitimidade democrática e sigilo operacional?

Palavras-chave: Ética dos Serviços de Informações; Responsabilização Democrática; Estado de Direito; Segurança Nacional.

1. **INTRODUCTION**

Secret intelligence activity is often depicted as an "extra-ethical" domain, where conventional moral rules are apparently suspended in the name of national security. Yet both history and contemporary practice reveal that intelligence cannot escape the ethical and legal principles underpinning liberal democracies. Tasked with collecting, analysing, and disseminating information critical to the protection of the state, intelligence agencies must navigate a delicate balance between operational necessity and democratic accountability. This tension lies at the heart of this study, which explores how intelligence functions within a framework of legal, ethical, and institutional constraints.

Writing on intelligence services is an inherently complex undertaking, as the knowledge available represents only a fraction of their actual operations, essentially consisting of the information that these agencies themselves choose to make public. While it is possible to delineate their mission, objectives, and general principles, their operational methods largely remain shielded by institutional secrecy.

In Europe, intelligence services do not enjoy the same notoriety and visibility as agencies such as the Central Intelligence Agency (CIA) in the United States or MI6 in the United Kingdom. The CIA, the intelligence organ of the world's leading power in the post–Cold War period, has become globally renowned for its several interventions and influence it has exerted on international politics. This explains why a substantial body of studies, articles, and debates has developed around its activities, fostering a robust academic tradition on American intelligence, now regarded as a reference model in the scholarly literature on the subject.

2. EUROPEAN CHALLENGES IN DEFENCE

The American experience represents the cornerstone of contemporary political and academic reflection on intelligence, serving as a benchmark for the development of modern security and intelligence architectures. Europe observes this model with interest but still struggles to fully replicate it. Indeed, within the European context, there is no central agency comparable to the CIA, nor a federal

body like the FBI capable of coordinating investigative and intelligence activities at a continental extent. This gap is partly attributable to Europe's own history, traditionally marked by difficulties in coordinating common defence. It is a recurring theme in the continent's politics, proposed multiple times in various formulations, yet never resulting in a genuinely integrated structure. Even the most recent international events – from terrorist attacks on European soil to conflicts increasingly close to the Union's borders – have been insufficient to generate a common system of defence and intelligence.

Nevertheless, the European Union avails of Europol, the EU Agency for Law Enforcement Cooperation, which assists, analyses, and coordinates the policing activities of member states; yet it lacks direct investigative or arrest powers. As such, it cannot be equated to a true intelligence agency: its powers are limited, and its function remains essentially supportive. Despite being a fundamental instrument in the fight against organized crime and terrorism – and having been strengthened following the 2015 Paris attacks – Europol does not possess the operational capacities or the mandate typical of a federal agency such as the FBI.

Similarly, Interpol, the international police cooperation organization with 196 member countries, addresses transnational crime on a global scale but does not wield direct policing powers, limiting itself to facilitating information exchange and operational coordination among national forces.

Overall, the European defence system is still in the process of formation, posing as an institutionally fragile structure that still lacks a full common operational capacity. Although the Union has established a strategic framework – articulated through the Common Security and Defence Policy (CSDP) and the Strategic Compass adopted in 2022 – its implementation remains partial and fragmented. Within this context of incomplete integration, European defence systems remain heterogeneous, and responses to major international threats continue to rely heavily on individual member states, despite the existence of a shared regulatory framework.

One element, however, seems to unite various European powers: the public perception of intelligence services, which is markedly different from that observed in the United States. In the absence of a consolidated tradition, European public opinion often maintains a certain distance, if not outright suspicion, toward these agencies.

2.1. THE PORTUGAL'S CASE

The case of Portugal is particularly emblematic, as the country possesses a legal framework governing surveillance that significantly limits the operational prerogatives of intelligence services within its territory. This approach finds its roots in recent history, which profoundly influenced the role, public perception, and institutional evolution of these agencies.

During António de Oliveira Salazar's and Marcello Caetano dictatorship (1933–1974), political repression was largely exercised through the PIDE (Polícia Internacional e de Defesa do Estado, 1945–1969), the principal instrument of the repressive apparatus of the Estado Novo, the official name of the authoritarian regime. The PIDE held broad powers of investigation, detention, and arrest against anyone suspected of subversive activity against the state. It operated as secret political police, conducting espionage operations and repressing so-called "political and social crimes" through arbitrary imprisonment, special tribunals, and torture. It constituted one of the pillars of a system of fear, denunciation, and persecution within a regime of clearly police-oriented nature.

After the Carnation Revolution of 1974, a commission was established to dissolve the political police. The collective memory of PIDE's abuses left a profound mark on Portuguese society, such that for about a decade the new democratic Republic avoided re-establishing a national secret service. Moreover, the totalitarian and repressive nature of the intelligence service during that period generated a deep-seated aversion toward intelligence, still perceptible among both the elite and the general population. This aversion decisively shapes the distrust with which these services are perceived today: the long history of the PVDE and subsequent PIDE as oppressors of individual freedoms has resulted in contemporary services being viewed not as essential instruments of the state but rather as adversaries of citizens.

This historical legacy continues to influence the perception of the two main contemporary intelligence agencies: the Serviço de Informações de Segurança (SIS), established in 1986, and the Serviço de Informações Estratégicas de Defesa (SIED), created in 1997. Their competencies remain limited to the collection and analysis of information, report drafting, and transmission of data to other authorized investigative bodies, in order to facilitate subsequent investigations. They do not possess the authority to conduct direct criminal investigations or to intercept communications, tools that in many other Western countries constitute a central element of intelligence operations.

This restrictive framework strongly affects the efficacy of the services, whose powers are legally limited in the name of protecting citizens' liberties and fundamental rights. The result is a system in which intelligence services are almost "expelled" from the national security sphere, a role increasingly occupied by police forces. This overlap of competencies, fuelled by underlying political ambiguity, generates institutional friction, internal competition, and a lack of cooperation, which negatively impacts the quality of intelligence outputs and the stability of the overall security system.

In conclusion, persistent public distrust has constrained the operational capacity and effectiveness of Portuguese intelligence, which remains strictly bound by the principles of the 1976 Constitution and respect for fundamental rights,

particularly privacy and civil liberties. While this constraint ensures adherence to democratic values, it often conflicts with the functional requirements of intelligence work, based on the collection and analysis of confidential information.

In particular, contemporary debate, both in Portugal and in many other democracies, revolves around the delicate balance between liberty and security. Determining which of these two values should prevail, and to what extent, represents one of the most complex and pressing issues in democratic governance.

3. ETHICAL PARTICULARITY OF INTELLIGENCE AGENCIES

Over the past century, intelligence has become one of the most crucial instruments within the political community, as it provides the information necessary for the protection and security of its members. The sector underwent profound transformation following the September 11, 2001 attacks, when the United States radically altered its foreign policy doctrine, abandoning the principle of deterrence in favour of pre-emptive action, aimed at preventing the emergence of external threats before they materialized. This shift also entailed institutional reforms, including the creation of the office of the National Director of Intelligence, tasked with coordinating the various services and ensuring the effective exchange of information among them.

A comparable level of organization and theoretical reflection is not observed in Europe, where a common ethical and normative framework defining the legitimacy and limits of intelligence activity is still lacking. This regulatory gap is particularly evident in the differing national responses to recent security crises, within a context in which threats have evolved on a global scale. Consequently, there is a clear absence of a shared normative theory governing the actions of national security intelligence agencies, or at the very least the recognition of its necessity.

Intelligence has been interpreted as an activity apparently devoid of ethical limits, or even as an intrinsically immoral domain, especially when viewed through a Machiavellian lens in which power, success, and survival prevail over moral considerations. This interpretation, however, risks reducing intelligence to a mere instrument of national security, severing any connection with ethics. Paradoxically, it is precisely the reference to national security that constitutes its primary ethical foundation: all actions and institutions intended to safeguard it derive their principal moral justification from this objective. The moral dilemma of intelligence becomes even clearer when compared with the ethics of war.

3.1. INTELLIGENCE AND WAR TRADITION

For a long time, the study of intelligence operations has been associated with the tradition of just war, whose ethics are considered largely analogous. Both practices, in fact, can be seen as forms of moral exceptionalism, in which certain

actions are exempted from ordinary ethical evaluation. In both epistemic and military competition, distinct codes and rules are applied to legitimate otherwise impermissible behaviours, since common moral norms do not fully apply in these contexts.

Nevertheless, this perspective is only partially adequate, as it overlooks the profound differences between the two phenomena. War, after all, occurs within a specific temporal and spatial framework, a condition that provides its justification; intelligence, by contrast, is a continuous activity, lacking any clear temporal boundary between peace and conflict. Such dissimilarity stems from the nature of the threat being addressed: whereas war responds to a manifest danger, intelligence aims to act before any threat materializes. In this sense, intelligence focuses primarily on internal surveillance rather than battlefield engagement, constituting a systematic process of data collection and analysis in order to identify and monitor potential dangers while they are still latent.

Accordingly, intelligence activity can be conceived as a form of continuous and preventive defence, operating incessantly and often before a full ethical assessment of legitimacy is even possible. It thus emerges as a primary resource to be mobilized before any other form of action, given its essential role in the decision-making process.

Hence, intelligence occupies an intermediate space between the political and security domains. Its ethical burden differs fundamentally from that of warfare because, rather than entailing the direct taking of human life, intelligence aims to prevent such outcomes by pursuing less destructive alternatives. Precisely because of these differences, several scholars caution that extending the just war framework to intelligence may legitimise an overly permissive understanding of its practices.

Finally, the principles of jus ad bellum offer a useful starting point for understanding the moral implications of intelligence activity, but cannot alone constitute a normative framework for developing principles of jus ad intelligentiam. For this very reason, intelligence services require their own ethical framework. They engage in practices that, if judged by the moral rules of everyday life – particularly from a Kantian or traditional just war perspective – would often be unacceptable.

3.2. ETHICAL AMBIGUITY OF THE INTELLIGENCE

The moral dilemma of intelligence lies in its fundamental ambivalence: on one hand, it encompasses actions that infringe established ethical norms; on the other, it plays a crucial role in preventing serious threats to the security of a State and its citizens. Intelligence thus emerges as a morally ambiguous practice, oscillating between crime and necessity, between the pursuit of a lesser evil and the protection of a higher good.

Defining an adequate ethical and normative framework for intelligence proves complex, primarily due to the ambiguous definition of the concept of security, which lies at the core of any justification for intelligence operations. Security is inherently variable, changing according to political, social, and cultural contexts, as well as the nature of threats – whether military, criminal, or economic – that a State seeks to confront. One may ask, for instance, whether security should be regarded as a duty of the State, a component of foreign policy, or a minimal condition for survival. Each country formulates its own definition based on the vital interests it aims to safeguard; in general terms, however, security can be understood as the set of processes and measures designed to preserve those interests. In this perspective, intelligence is inextricably linked to the very notion of national security, representing one of the core elements of its institutional architecture.

In short, the value of security is implicit in the capacity of a State to safeguard the vital interests of its citizens. It should not be conceived as an abstract entity detached from the population, but rather as a common good intrinsically connected to their well-being. Indeed, the fundamental challenge for any State is to counterbalance the protection of individual rights with the pursuit of collective safety. It's important not to reduce this tension to a simple trade-off between privacy and security – as if an increase in one implied a decrease in the other – since both exist on a continuum of values that varies according to context and risk perception.

However, in the aftermath of the September 11 attacks, the United States came to believe that strengthening national security powers would be justified even at the expense of fundamental rights and civil guarantees. Following the U.S. model, many world powers adopted similar policies, enhancing counterterrorism capacities at the cost of individual civil liberties, under the assumption that only such measures could ensure a genuine strategic decision advantage. Yet Benjamin Franklin's famous advice remains profoundly relevant today: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety".

3.3. SECRECY AND ACCOUNTABILITY

Intelligence operations are often conceived as a third option between diplomacy and war, activated when the first proves ineffective and the second excessive. Contrary to cinematic portrayals, intelligence activity is predominantly epistemic: it aims to enhance understanding of the world and provide policymakers with the information necessary to act with maximum awareness. Strictly speaking, intelligence is not merely an epistemic action but a shared epistemic activity conducted within a context of competition. In this sense, it performs interpretive functions regarding the environment, supports decision-making processes, and strategically intervenes against threats through the collection, analysis, and dissemination of information.

Such functions require cooperation among multiple actors operating across different domains, especially in contemporary contexts where threats are increasingly complex, interconnected, and not solely military. But most importantly, the epistemic competition compels secrecy in order to preserve informational advantage concerning both conventional and unconventional threats to national security, whereas extreme disclosure would be self-defeating. In this sense, secrecy is not merely a tactical choice but a fundamental condition for the effectiveness of intelligence, constituting a defining feature of its institutional character.

Secrecy, however, inherently conflicts with the principle of transparency that characterizes liberal democracies, meaning that intelligence agencies rely on an element that, by definition, limits accountability and challenges democratic representativeness. This constitutes a structural dilemma, unsolvable yet unavoidable, as relinquishing secrecy would compromise national security itself.

The culture of secrecy is particularly relevant in two areas: scholarship and justice, both intimately linked to institutional responsibility. Firstly, a true understanding of how intelligence services influence events is possible only through the study of their history, which in turn depends on the publication of archives. Analysis and resulting scholarship are therefore limited to what the State chooses to make accessible.

Secondly, while operations are often shielded from public scrutiny, officers must, at least in principle, remain morally accountable for their activity, which in turn needs to be actionable by political authorities. Parliament and the executive are therefore required to exercise rigorous oversight to ensure that intelligence activities conform to democratic principles.

The difficulty lies in the recurrent tendency of intelligence officers to withhold information from the government, on the grounds that its members are insufficiently trained to maintain secrecy and might jeopardize the security of ongoing operations. The lack of reliable information regarding the actions undertaken – and the motives behind them – generates a confused public opinion, unable to understand or justify secrecy.

As previously mentioned, much depends on the ambiguity surrounding the notion of national security, whose overly expansive interpretation has been at the root of many intelligence-related scandals. When invoked too broadly, the notion risks legitimising excessive classification and fostering an unnecessary culture of secrecy; conversely, a more limited use of secrecy would benefit the intelligence community itself, enhancing its credibility while saving time and resources otherwise devoted to classifying even the most innocuous information. Greater transparency would, in fact, minimize the fear of abuse, ineptitude, corruption and

illegality within intelligence services, as officers would become accountable for their actions without the shield of secrecy to protect them from potential sanctions.

Moreover, within a liberal democracy, secrecy should represent the exception rather than the rule. The emphasis should rest on openness with limited exceptions, rather than on secrecy with limited openness. Any alternative interpretation of this principle of exceptionalism would verge on authoritarianism. National security must never serve as a pretext for abandoning the rule of law, which remains the cornerstone of any democratic system. If intelligence agencies do not derive their powers from the legal order, they cannot claim legitimacy and would be indistinguishable from any other clandestine or even terrorist organization.

The European oversight architecture provides a multi-layered mechanism, where primary control is entrusted to national parliaments while supranational oversight is largely exercised through human rights and data protection law. Strictly speaking, intelligence activities remain an area of national competence not formally transferred to the EU, where each State has its own system of parliamentary, judicial and executive oversight, shaped by the constitutional framework and historical context. At the same time, intergovernmental cooperation and European-level principles contribute indirectly to the supranational dimension, complementing and reinforcing national levels.

The core supranational forms of control are exercised by the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU), both of which have addressed intelligence practices in their jurisprudence. Additionally, the Fundamental Rights Agency (FRA) publishes non-binding reports and recommendations that exert political and normative pressure to ensure the protection of fundamental rights.

A particularly illustrative case is Big Brother Watch and Others v. United Kingdom, in which the ECHR assessed the lawfulness of the United Kingdom's "secret surveillance regime including bulk interception of communications and intelligence sharing". The case concerned many surveillance activities carried out by the Government Communications Headquarters (GCHQ), the country's principal intelligence, security and cyber agency. In its 2021 judgement, the Court ruled that the system violated Articles 8 and 10 of the European Convention on Human Rights, respectively protecting 'Respect for private life' and 'Freedom of expression'. Indeed, the framework lacked adequate safeguards, especially for journalistic sources. As a result, the United Kingdom was prompted to revise its surveillance legislation and introduce clearer procedures for the authorization, oversight, and use of intercepted data.

Beyond its national implications, the case established a jurisprudential milestone in Europe, reaffirming that, even in the realm of national security, intelligence activities must remain subject to the rule of law.

4. EUROPEAN LEGAL FRAMEWORK

4.1. THE SNOWDEN CASE

The Big Brother Watch and Others applications were filed in the wake of Edward Snowden's revelations, which shook public confidence in the balance between national security and individual privacy. In 2013, Snowden, a contractor for the U.S. National Security Agency (NSA), disclosed a substantial collection of classified documents. These leaks exposed extensive surveillance programs carried out by the NSA and its international partners – including GCHQ's operation Tempora – revealing how large-scale data analysis had been systematically employed in the preceding years.

The NSA's operations formally took place within a framework of legality under two main conditions: first, they were legitimised by the 2008 Amendment to the U.S. Foreign Intelligence Surveillance Act (FISA); and second, they targeted individuals who had consented to the sharing of their data, naively self-waiving their privacy rights – often through the uncritical acceptance of online terms of service on platforms such as Facebook or Gmail.

Nevertheless, Snowden's disclosures sparked deep socio-political concerns and marked a turning point in the global debate on intelligence ethics. This watershed moment prompted governments worldwide to reconsider the regulation of their intelligence agencies in order to ensure a stronger protection of citizens' rights. At the European level, the most significant legal and institutional reforms include the 2016/279 and the 2016/680 European Directives. The current legislative framework is comprehensively outlined in "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", a two-volumes study issued by the European Union Agency for Fundamental Rights (FRA) in 2017 and updated in 2023.

4.2. THE 2016/679 AND 2016/680 DIRECTIVES

The EU Directive 2016/679, commonly known as the General Data Protection Regulation (GDPR), represents the core legal framework governing data protection within the European Union. In force since May 2018, it regulates the processing of personal data by private entities and strengthens the protection of individuals' privacy rights across all Member States. The Regulation reinforces existing safeguards and enhances individuals' control over their personal information. The principles enshrined in the document are upheld by the European Data Protection Board (EDPB), the supervisory and coordination body established under Articles 68–76 to ensure uniform application throughout the Union. To this end, the EDPB

issues guidelines and recommendations, such as the Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces, which delve into the principle of transparency and provide practical guidance for preventing deceptive design practices that may compromise users' ability to provide free and informed consent. In this context, particular attention has also been devoted to the transparent design of website interfaces, especially regarding cookie banners.

However, as stated in its Article 2(2)(d), the GDPR does not apply to data processing carried out by competent authorities for purposes related to national security or law enforcement. This regulatory gap made it necessary to adopt a complementary instrument specifically addressing security operations: Directive (EU) 2016/680 "on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties". Still, by its very nature, the Law Enforcement Directive (LED), as it is commonly known, offers a more limited and flexible framework than a regulation, allowing Member States discretion in determining the means to achieve compliance. Moreover, transparency does not play the same central role as under the GDPR, where it constitutes a guiding principle. This is because the Directive concerns activities such as criminal investigations, video surveillance, and other forms of covert data analysis carried out by competent authorities in connection with

criminal offences, where a lower degree of transparency is justified by operational requirements.

"[…] The LED does not explicitly require controllers to process personal data "in a transparent manner in relation to the data subject" (cf. Art. 5(1)(a) GDPR). The principle of "lawfulness, fairness and transparency" (Art. 5(1)(a) GDPR) has been narrowed down to a principle of lawfulness and fairness (Art. 4(1)(a) LED). The information to the data subject has to be provided not in a "concise, transparent, intelligible and easily accessible form" (Art. 12(1) GDPR) but in a "concise, intelligible and easily accessible form" (Art. 12(1) LED)."

Hence, while there exists an almost absolute legal prohibition against the deliberate killing of innocent individuals, no comparable restriction applies to intrusions into their privacy. Nevertheless, intelligence activities must be guided by normative principles capable of ethically justifying actions that inherently involve the violation of people's privacy rights. Indeed, the practice of bulk data access, particularly when supported by machine learning, inevitably entails the collection of information concerning innocent citizens, who constitute the vast majority of entries in intelligence databases despite being of no operational relevance.

Only a reasonable prospect of achieving legitimate security objectives could justify such practices, where the ethical risks and the harm caused are outweighed by the perceived gains. Any intrusion must therefore be proportionate, necessary and justified in relation to its intended purpose. In this regard, the principle of proportionality follows a purely rational logic: no actor would perform an action if

the moral good of an end is outweighed by the cost of its mean. However, in the field of national security, the line between proportionate and disproportionate intelligence measures may be blurred, particularly when bulk data collection is involved. This ethical tension is partly mitigated by anonymisation techniques, forms of information sanitization designed to ensure that only the privacy rights of genuine suspects are substantively affected. By limiting the identifiability of most data subjects, these methods reduce the ethical and legal impact of mass surveillance while still enabling the operational use of sensitive information.

In conclusion, the Directive represents a crucial tool within the European legal framework: up to date, it is the major targeted effort to enact laws on data analysis in security activities, establishing a minimum set of safeguards in a domain otherwise characterised by structural secrecy.

4.3. THE PEGASUS PROJECT

It is noteworthy that the reforms introduced in the aftermath of Snowden's scandal failed to ensure reliable guarantees for the protection of privacy rights. In 2021, an investigation by Amnesty International, Forbidden Stories and eighteen partner organisations exposed the extensive use by governments worldwide of surveillance spyware against individuals who posed no legitimate security threat. Indeed, the targets included activists, opposition figures, journalists, politicians, law enforcement officials, diplomats, and lawyers. Shielded by broad invocations of

national security, also European countries – meaning their intelligence services – were incriminated in the Pegasus allegations, having deployed malware tools far beyond legitimate criminal investigations but rather for political purposes, in a clear systematic abuse of such technology.

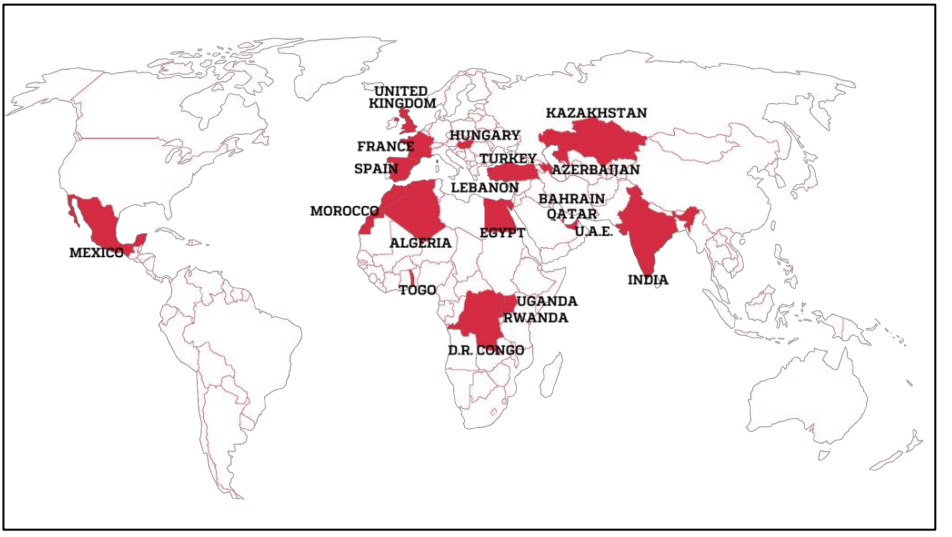

Illustration 1. Countries where journalists were selected as targets.
Source. P. Rueckert. July 2021. *Pegasus: The new global weapon for silencing journalists*. Forbidden stories. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

The disclosure primarily concerned Pegasus, an intrusion software developed by the Israeli firm NSO Group to hack into smartphones and provide full access to their data, including text messages, call interceptions, passwords, locations, microphone and camera recordings. Unlike mass surveillance, a spyware targets specific individuals in order to collect information without their knowledge; hence Pegasus has come to epitomize digital repression worldwide, particularly due to its

implementation by authoritarian regimes. Yet, even within Europe – where the malware was reportedly acquired by at least fourteen government intelligence agencies – the scandal highlighted persistent structural vulnerabilities: the opacity surrounding espionage activities and the absence of robust mechanisms of public accountability.

5. CONCLUSIONS

Even the most recent history underscores the enduring ambiguity inherent in intelligence activities, where the reliance on operational secrecy continues to generate fear of potential abuses of power and contributes to widespread public distrust – especially as a result of scandals such as the Snowden revelations or the Pegasus affair. While secrecy is an indispensable component of intelligence work, it is nonetheless essential to identify strategies capable of legitimising it at the societal level, starting from the introduction of stronger legal safeguards and clearer procedural guarantees. In fact, many agencies claim to adhere to fundamental principles and to acknowledge the importance of individual rights and civil liberties, deliberately refraining from more intrusive or aggressive methods in the pursuit of information.

Yet a lingering sense of doubt regarding possible unlawful practices concealed behind institutional secrecy is likely to persist. However, this represents a – perhaps

unavoidable – price that democratic societies must pay for the protection of national security. To this point, it is important to recall the unique role intelligence agencies play, both in shaping governmental decision-making and in ensuring the internal security of the State: they determine what action is best given the range of possibilities in a competitive environment related to threats. This function is indispensable and, in my view, cannot be relinquished – not even at the cost of certain individual freedoms. Nevertheless, there remains hope for enhanced accountability mechanisms, supported by a clearer and more robust legislative framework capable of defining, preventing, and sanctioning potential violations of professional and legal standards.

REFERENCES

Agenda digitale (04/06/2025). *GDPR, tutto ciò che c'è da sapere per essere in regola*. https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/

Born, H., & Leigh, I. (2005). *Making Intelligence Accountable: Legal Standards and Best Practice* (1st ed.). Geneva Centre for the Democratic Control of Armed Forces / Norwegian Parliamentary Intelligence Oversight Committee. https://www.dcaf.ch/sites/default/files/publications/documents/making-intelligence.pdf

Born, H., & Wills, A. (Eds.). (2012). *Overseeing Intelligence Services: A Toolkit* (1st ed.). Geneva Centre for the Democratic Control of Armed Forces (DCAF). https://www.dcaf.ch/overseeing-intelligence-services-toolkit-0#

ECHR – Grand Chamber (25/05/2021). *Applications nos. 58170/13, 62322/14 and 24960/15*. https://hudoc.echr.coe.int/fre?i=001-210077

EUR-Lex (04/05/2016). *Directive (EU) 2016/680 of the European Parliament and of the Council*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504

EUR-Lex (04/05/2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

EUR-Lex (07/01/2022). *Regolamento generale sulla protezione dei dati (GDPR)*. https://eur-lex.europa.eu/IT/legal-content/summary/general-data-protection-regulation-gdpr.htm

Feldstein, S., Youngs, R., (2023) *Pegasus and the EU's external relations*. Policy Department for Citizens' Rights and Constitutional Affairs (European Parliament). https://www.europarl.europa.eu/committees/en/pegasus-and-the-eu-s-external-relations/product-details/20230213CAN68766

Forbidden stories (18/07/2021). *About the Pegasus Project*. https://forbiddenstories.org/about-the-pegasus-project/

Forbidden stories (18/07/2021). *Pegasus: The new global weapon for silencing journalists*. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

FRA (24/05/2023). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update*. https://fra.europa.eu/en/publication/2023/surveillance-update

Henschke, A., Miller, S., Alexandra, A., Walsh, P.F., & Bradbury, R. (2024). *The Ethics of National Security Intelligence Institutions: Theory and Applications* (1st ed.). Routledge. https://doi.org/10.4324/9781003106449

Liger, Q., Gutheil, M., (2023). *The use of Pegasus and equivalent surveillance spyware*. Policy Department for Citizens' Rights and Constitutional Affairs (European Parliament).

Members' Research Service – European Parliament (02/06/2024). *What action has Parliament taken against spyware abuse?* https://epthinktank.eu/2024/06/02/what-action-has-parliament-taken-against-spyware-abuse/

Miller, S., Regan, M., & Walsh, P.F. (Eds.). (2021). *National Security Intelligence and Ethics* (1st ed.). Routledge. https://doi.org/10.4324/9781003164197

Parliamentary Assembly of the Council of Europe – Doc. 15825 (20/09/2023). *Pegasus and similar spyware and secret state surveillance*. https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68

Rossi Stefano – L'Unità Europea (04/2016). *Per un FBI europeo*. https://www.unitaeuropea.it/sito/index.php/collezioni-online/362-anno-2016/295-l-unita-europea-n-2016-2-marzo-aprile/2717-per-un-fbi-europeo

Taddeo, M. (2025). *Codice di guerra: Etica dell'intelligenza artificiale nella difesa* (1st ed.). Raffaello Cortina Editore.

Theodore Christakis, Kenneth Propp – Lawfare (08/03/2021). *How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*. https://www.lawfaremedia.org/article/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states

Tristan, R. (2020). The Concept of Joint Control under the Data Protection Law Enforcement Directive 2016/680 in Contrast to the GDPR. *Journal of Intellectual Property Information Technology and E-Commerce Law, 11*, 3, p. 242-251. https://www.jipitec.eu/jipitec/article/view/285/279

Vegar, J. (2007). S*ervicos Secretos Portugueses: Historia e Poder da espionagem nacional* (3rd ed.). A Esfera dos Livros.

Warner Michael – CIA (2002). Wanted: A Definition of 'Intelligence'. *Studies in Intelligence, 46*, 3. https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-46-no-3/wanted-a-definition-of-intelligence/