WISTHLEBLOWING

FREEDOM OF SPEECH, RIGHT TO KNOW AND REPORTING UNLAWFULNESS

THE LIFEBLOOD OF PREVENTING ABUSE OF POWER AND CORRUPTION IN THE DEFENCE SECTOR

This report was authored by Francisco Cardona, International Expert

CIDS- CENTRE FOR THE INTEGRITY IN THE DEFENCE SECTOR, ROYAL MINISTRY OF DEFENCE OF NORWAY | OCTOBER 2020

Contents

1. Introduction

The "right to know" is increasingly featuring among the array of rights citizens of democratic societies are endeavouring to conquer. Such an endeavour is not general, is not yet solid and its success is not to be taken for granted. Many vested interests stand in their way.

This paper is meant to portray the situation concerning the efforts to achieve a more consistent right to know and how the vibes conducive to strengthening the right to know, that is, the freedom of speech and the protection of whistleblowing are progressing (or not) in democratic societies. The whistleblowing of wrongdoings, ethical misbehaviours and illegalities is inseparable of the individual right and obligation not only to stand up and refuse to comply with improper or murky instructions in organisations, either public or private, but also to report illegality and unethical actions.

The right to know, whistleblowing protection, refusing compliance with illegal instructions, along with preventing conflict of interest, rotating doors and putting lobbying in order are the lifeblood of any policy oriented to prevent corruption and abuse of power.

All in all, freedom of speech, whistleblowing and refusal to comply with unlawful directions of those in the higher ladders of hierarchies are the several sides of the same endeavour: to construct democratic and rule of law-based societies and institutions. This gives us an understanding of the polyhedric nature of building a democratic governance accountable to the electorate and to the citizens at large.

The multisided enterprise of democracy building needs to be parcelled into its various components for it to be actionable. Reform actions must be properly identified and sequenced to be effective and produce change in human societies, as not everything can be dome at the same time. However, if the issue is to advance and consolidate the right to access to information of public interest, this must be worked out in parallel with enhancing the effective protection of whistle-blowers, the protection of those who decide to stand up against unlawfulness in organisations and the protection of those who decide to use their freedom of speech.

This paper will essentially focus on the interrelations between resisting illegality, whistleblowing and the right to know in general and especially in the defence sector.

If we bring the military and security services into the picture, it means that we are to cope with the protection of official confidentiality and state secrets and, consequently, confront two main European traditions, namely the northern European strong culture of transparency and the southern one (and also that of the former Communist countries) of strong protection of state secrets and confidentiality. Oversimplifying we could say that northern countries have been seen transparency as a fundamental right of the citizen-elector and a better service to the public interest, whereas the southern countries and many of those in the former Soviet tradition see transparency as a rather capricious fashion to sate the curiosity of the populace. In these latter countries many people see confidentiality and secrecy as better serving the public interest.

In this context, the European Directive of 2019 represents a major cultural change for the whole of the European Union. The Directive comes to compel private corporations and public administrations of the European administrative space to promote a culture of "speaking up" as a fundamental principle of management and especially of organisational risk-management.[1] This Directive, if implemented, will

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which is to be transposed by EU Member States into national legislation by the 17 of December of 2021 (article 26). At: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937

indeed represent a major gamechanger concerning the interplay between transparency and confidentiality. However, we need to bear in mind that both transparency and confidentiality are political instruments which have separate and distinctive goals to accomplish. Both are necessary and legitimate.

This makes it problematic the protection of those refusing to comply with illegality and that of the whistle-blowers, as well as the freedom of speech. Solving this conundrum requires striking a wise balance between confidentiality and transparency and a compromise between the general rule (transparency) and the exceptions (secrecy). This paper holds the ambition to contribute to forge that sound balance and provide feasible (actionable) policy proposals.

2. The Right to Know

The classical *arcana imperii* remained through the institutionalization of the state secrets in all countries born out of the Vienna Congress (1815).[2] It mutated into the state secrets privilege (SSP) in England where the law allowed the king or queen the "Crown Privilege" granting the monarch the absolute right to refuse to share information with Parliament or the courts. The U.S. Supreme Court borrowed the State Secret Privilege (SSP) or "executive privilege" almost entirely during a Cold War case, *Reynolds v. United States (*1953*)*. When the SSP is invoked, the US government submits an affidavit saying that any court proceedings would risk disclosure of secrets that would threaten national security and then asks the court to dismiss the suit based solely on those grounds. This institution was extensively, and many think also improperly, used by U.S. Governments since 2001, in the wake of the terrorist attacks on the Twin Towers.[3]

The sequels of September 11, 2001 in Europe led the European Court of Human Rights to put limits to the state secrets privilege in a landmark judgement of 23 February 2016.[4] The case concerned an instance of extrajudicial transfer (or "extraordinary rendition"), namely the abduction by CIA agents, with the cooperation of Italian officials, of the Egyptian imam Abu Omar, who had been granted political asylum in Italy, and his subsequent transfer to Egypt, where he was held in secret for several months. The Court established that the Italian authorities were aware that the applicant had been a victim of an extraordinary rendition operation which had begun with his abduction in Italy and had continued with his transfer abroad. The Court had already held in previous cases that the treatment of "high-value detainees" for the purposes of the CIA's "extraordinary rendition" programme was to be considered as torture within the meaning of Article 3 of the Convention. In the present case, the Court held that the legitimate principle of "State secrecy" had clearly been misused by the Italian government in order to ensure that those responsible did not have to answer for their actions. In fact, the investigation and trial had not led to the punishment of those responsible, who had therefore ultimately been granted impunity.

One can say that today the mainstream democratic political culture proclaims openness and transparency as values while suspecting of secrecy and opaqueness as disvalues. In this context, the state prerogatives to classify information as secrets are largely questioned perhaps because they have been extensively abused. For many the protection of the general interest, and therefore the national interest, is better ensured through transparency than through confidentiality. This latter is considered to serve the personal interest or personal agendas of those wielding political or bureaucratic power rather than the general interest of the nation.

[2] See CIDS Good Governance Guides # 4 (2016) : *Access to information and limits to public transparency* https://cids.no/wp-content/uploads/pdf/7933-DSS-Access-to-information-GGG-4-skjerm.pdf
[3] See Dean, John, 21 September 2014: https://verdict.justia.com/2014/09/19/resurrecting-dubious-state-secrets-privilege
[4] ECtHR judgement 23 February 2016, case Nº 44883/09 Nasr and Ghali v Italy, also known as the Abu Omar case

One major problem with the state secrets is that they are meant to protect the national security or the security of the defense. These are extremely vague, undefined notions. National legislation often refers interchangeably to national security, state security, public security, public safety, national defense, national interest, state secrets, security of the kingdom, of the republic and so forth. Governments either in Laws of Access to Information or in Laws on Official State Secrets oppose that blurred notion, which is undefined by national legislation, to the quest for information by their citizens and to judicial review by courts. In this way it is an obstacle to the right of free access to information which does not meet any recognized standards of legal certainty required in any restrictions of rights. The use of such nebulous notion easily gives way to a high risk that the executive or secret services may act arbitrarily in concealing information from the public eye.[5]

An important international step in proposing sound balances between the right to information and the preservation of the confidentiality of state secrets on national security and defense is represented by the Tshwane Principles (Global Principles on National Security and the Right to Information), adopted in Tshwane, Pretoria, South Africa, on 12 June 2013. This document was born fundamentally from civil society organizations and academic centres in consultation with international experts and special rapporteurs on freedom of expression, human rights and counter-terrorism of various international intergovernmental organizations such as the United Nations (UN), the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE) and the African Commission on Human and Peoples' Rights (ACHPR).[6] The approach of this document is minimalistic in that the restrictions of the right to access information should not go below the standards provided in it, but encourages states to provide greater openness than the baseline approach of the document suggests.

Protection of good faith whistleblowers is the other side of the coin of access to information. As shown above, both sides are dimensions of the same fundamental right of freedom of expression and the right to know. Like the right to access to information, the protection of whistleblowers is not yet to be taken for granted in many democratic countries.

On the contrary, most countries can prosecute public personnel if they disclose classified national security related information in making an internal complaint (Belgium, Czech Republic, France, Hungary Moldova, Norway, Poland, Romania, Russia, Slovenia, Spain and Sweden).[7] Paradoxically enough, many countries encourage public personnel to make internal complaints concerning wrongdoings they may have witnessed, but few countries have established safeguards to provide protection against retaliation, with the outstanding exceptions of the UK, where the Public Interest Disclosure Act of 1998 (PIDA) provides for compensatory remedies in the event of retaliation along with disciplinary measures against those who retaliate, Ireland (Protection Disclosure Act of 2014 or PDA) and the United States. The Ireland system has been praised as the best in Europe and the more effective in providing legal protection against retaliation. In Spain, a 2016 Law of the regional parliament of the Valencia Region established a Whistleblower Statute conferring legal protection from any kind of retaliation and imposing heavy fines to those who retaliate. The protection is secured by the Regional Antifraud Office.[8] In France, the Law Sapin II of 2016 is a comprehensive regulation of whistleblowing protection under the authority of the Defender of Rights (ombudsman), but its disadvantage is that it requires to demonstrate good faith in the reporting person. Romania has a good

[5] See Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe
See also: Didier Bigo et al (2014): *National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*. European Parliament. Study for the LIBE Committee: At: http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf

[6] See it at: http://www.right2info.org/exceptions-to-access/national-security/global-principles

[7] Jacobsen, Ibidem

[8] Law 11 of 2016, of 28 de November, creating the Regional Antifraud Agency of the Valencian Autonomous Community. Article 14 of this Law contains the Whistle-blower Statute, the first adopted in Spain, a country lacking a nationwide whistleblowing protection system.

law, but it has seemingly been applied only once by the courts in a positive way for whistleblowers in a much-mediatized case.[9]

When it comes to the exculpation of whistleblowers, in Denmark the public interest test requires that the accused was disclosing information in order to achieve an obvious public interest and that this interest does exceed the interest in keeping the information secret. Most countries require that the actual or likely harm to the national security resulting from the disclosure is proved for a criminal penalty to be imposed (e.g. Germany, Italy, the Netherlands, Norway, Spain and Sweden). Other countries do not require any evidence of harm to the national security: the revelation of secret information is a crime (e.g. Belgium, France, Hungary, Poland, Russia, Slovenia, Turkey and the UK), even if some of them admit that the lack of harm to the national security can be raised as a mitigating circumstance in a criminal trial against a whistleblower.

Some countries (six out of the twenty of those surveyed by Jacobsen (see footnote 5) have enacted whistleblowers protection laws, namely Hungary, Romania, Serbia Slovenia, Sweden and the UK. Most countries do not have a specific, separate law, but provide protection to whistleblowers under other laws (e.g. Norway). Other countries do not provide any protection at all. Those countries which provide protection include personnel in the security sector within the scope of the legal protection. However, in general, the protection of whistleblowers leaves much to be desired in many European countries and offer no reliable protection (they offer 'cardboard shields' protection, in the words of Tom Devine).[10]

3. International Standards to Whistleblowing Protection

Apart from the European Directive of 2019, which we will analyze below, there have been several initiatives to promote legal protection to whistle-blowers. The need for effective whistle-blower protection is recognised in numerous multilateral anti-corruption treaties. The current international legal framework against corruption, binding upon signatory parties, requires countries to take appropriate measures to provide protection for persons who report any facts concerning acts of corruption in good faith and on reasonable grounds to the competent authorities (UNCAC, article 33).

Several international soft law instruments also provide for the protection of whistle-blowers:[11]

- The 2014 Council of Europe Recommendation of the Committee of Ministers to member states on the protection of whistle-blowers envisages protection of both public and private sector whistle-blowers who report or disclose information either within an organisation or enterprise, to relevant external regulatory or supervisory bodies or law enforcement agencies, or to the public on a threat or harm to the public interest in the context of their work-based relationship (Council of Europe Parliamentary Assembly, 2009).
- The 1998 OECD Recommendation on Improving Ethical Conduct in the Public Service includes the Principles for Managing Ethics in the Public Service and the 2003 OECD Recommendation on Guidelines for Managing Conflict of Interest in the Public Service. These were among the first soft law instruments to highlight the importance of public sector whistle-blower protection.
- The OECD 2009 Anti-bribery Recommendation called for the protection of whistle-blowers in the public and private sectors.

[9] For an exhaustive account about the whistleblower protection in Europe, see: Mark Worth, Suelette Dreyfus, Cannelle Lavite, Garreth Hanley (2018): *Safe or Sorry: Whistleblower Protection Laws in Europe Deliver Mixed Results*, a report by Blueprint for Free Speech. At: https://www.blueprintforfreespeech.net/

[10] http://www.whistleblower.org/sites/default/files/pictures/Best_Practices_Document_for_website_March_13_2013.pdf

[11] See OECD (2016), *Committing to Effective Whistleblower Protection*, OECD Publishing, Paris. *http://dx.doi.org/10.1787/9789264252639-en*

- The 2010 OECD Good Practice Guidance on Internal Controls, Ethics and Compliance (annexed to the 2009 Anti-Bribery Recommendation) is the first guidance to companies by governments at an international level and highlights the fundamental elements of an effective anti-bribery programme. In particular, it recommends effective measures for "internal and where possible confidential reporting by, and protection of, directors, officers, employees, and, where appropriate, business partners, not willing to violate professional standards or ethics under instructions or pressure from hierarchical superiors, as well as for directors, officers, employees, and, where appropriate, business partners, willing to report breaches of the law or professional standards or ethics occurring within the company, in good faith and on reasonable grounds".

Providing protected reporting and preventing retaliation against those who report may also invoke fundamental human rights. For example, the International Convention on Civil and Political Rights, Article 19(2) provides for the "freedom to seek and impart information and ideas of all kinds". International human rights law jurisprudence reinforces the protection of whistle-blowers explicitly in circumstances where they are the only person aware of the reported situation and in the best position to alert the employer or the public at large.

According to the OECD (2016) there are a variety of complex measures in place across OECD countries to protect whistle-blowers. These range from broad and general stipulations to more specific and explicit arrangements. Three situations can be observed, depending on the inclusion of public sector whistle-blower protection in countries' legal frameworks:

1. No legal provisions specifically providing public sector whistle-blower protection: The country does not have any form of legislative provision related specifically to protected reporting or prevention of retaliation against whistle-blowers.
2. Varying degrees of public sector whistle-blower protection: The country has provisions, in one or more laws, related specifically to protected reporting or prevention of retaliation against whistle-blowers, but it does not have a dedicated, standalone whistle-blower protection law. These provisions do not necessarily provide protection to all categories of employees or misconduct to be reported. As a rule, employees in security services, national defence and intelligence services are excluded from the legislation on whistle blowing protection.
3. Dedicated public sector whistle-blower protection law: The country has a dedicated law to protect whistle-blowers in the public sector, although this may not provide protection to all categories of public sector employees (for example, employees of state-owned or controlled enterprises) and may not cover the reporting for all categories of misconduct, such as corruption offences.

4. The 2019 European Directive on Whistleblowing

Europe, as a set of countries, has been in delay to understand that the protection of whistle-blowers is a matter of public interest and to act on that problem accordingly. In the words of the Council of Europe (CoE), the "public interest is understood as the "welfare" or "well-being" of the general public or society. Protecting the welfare and wellbeing of the public from harm, damage or breach of their rights is at the heart of this recommendation".[12] In fact, the European Union followed closely this 2014 CoE

[12] Principle 2 of the Council of Europe Recommendation CM/Rec (2014)7 and explanatory memorandum. At: https://rm.coe.int/16807096c7

Recommendation in the preparation of the Directive.[13] However, it went beyond the CoE Recommendation by heightening the standards of whistle-blowers' protection.

In the preparation of the Directive, an ICF study commissioned by the European Commission stated that: "Whistle-blower legislation at national level has often followed major disasters, large financial scandals or failures to exercise of duty of care in the delivery of health and care services. This study has considered an alternative approach that makes use of the evidence on good practice in whistle-blower support and protection that is now available. This involves adoption of minimum EU standards for whistleblowing support and protection that mandate provision of reporting channels and protection of whistle-blowers against retaliation as a means of helping to address the problems of under-reporting of wrongdoing and the harms currently experienced by whistle-blowers. Such standards will not eliminate fraud, corruption or other wrongdoings in the workplace, but they should help ensure that more of the people who break the law are brought to justice. Also, by increasing the probability that workers will make reports and those reports will be followed up, such standards should help to change the calculated balance of risk and reward for those who commit such acts and discourage them".[14] This is indeed the essence of the fundamental public interest nature of whistleblowing.

Hence, the exclusion of whistleblowing on defence and security sectors from the legal protection must be assessed as negative in the light of this core public interest nature of whistleblowing in the mentioned sectors of public activity.

The ICF study also found out that "protection in law is a necessary but not sufficient component of change: socio-cultural influences operating at both the organisational level and in society are also very important. There is strong evidence of positive links between transparency, good governance and long term performance of enterprises, but also of the existence of many working environments in the EU where speaking up about wrongdoing that can harm the public interest is regarded as a breach of the employee's loyalty to the employer. More generally, whistle-blowers remain burdened with negative stereotypes and derogatory labels that prevent them from being recognised for taking personal risks to help the common good. This analysis emphasises the importance of awareness-raising and promotion of the positive value, in the individual workplace and in society as a whole, of speaking up about wrongdoing".[15]

The 2019 Directive goes beyond the whistleblowing arising from the strict workplace. As the Considering 37 of the Directive puts it: "Effective enforcement of Union law requires that protection should be granted to the broadest possible range of categories of persons, who, irrespective of whether they are Union citizens or third-country nationals, by virtue of their work-related activities, irrespective of the nature of those activities and of whether they are paid or not, have privileged access to information on breaches that it would be in the public interest to report and who may suffer retaliation if they report them. Member States should ensure that the need for protection is determined by reference to all the relevant circumstances and not merely by reference to the nature of the relationship, so as to cover the whole range of persons connected in a broad sense to the organisation where the breach has occurred". Article 4 specifies the persons included within the legal protection.

Let us review some of the features of the Directive:

[13] See Annex 12: Comparative Table on the Principles of the Council of Europe in the 17/04/2018 presentation of the draft Directive as a *"a package of measures to strengthen whistle-blower protection as a means to unveil unlawful activities and help enforce EU law"*. At: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=620400

[14] Page ii of the Study on the need for horizontal or further sectorial action at EU level to strengthen the protection of whistle-blowers - Final Report - Principal Report, by ICF Consulting Services Ltd, in association with Milieu, Blue Print for Free Speech, submitted on 27 November 2017 to the DG Justice of the European Commission. At: https://ec.europa.eu/info/sites/info/files/14_annex_-_icfs_study_whistleblower_report_-_vol_i_-_principal_report.pdf

[15] Ibid. page iii

Good faith and altruism: It is interesting to note that the text of the Directive (article 6-1(a) only requires from the whistle-blower to have reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this Directive. The reference to the "good faith whistleblowing" is not a requirement in the legal text, although somewhat the requirement of good faith is implicit in the Considering 32 of the Directive. Likewise, the Directive does not oblige the whistle-blower to act in an uninterested way, leaving up to the EU Member States the decision on establishing any compensation or remuneration for whistleblowing (articles 20-2 and 21-8).

Anonymity: The Directive does not impose the anonymity of the whistle-blower, but it leaves at the decision of the Member States, so considering the cultural differences across countries. However, the anonymity is an important instrument to prevent retaliation and so it is increasingly accepted by legislations in some Member States, but not all. At least these latter "shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced" (article 16-1).

Reporting channels: The choice between internal and external whistleblowing channels is left at the discretion of the whistle-blowers by the Directive (article 10). But the use of either internal or external reporting channels is compulsory before doing a public disclosure except if "the person has reasonable grounds to believe that: (i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or (ii) in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach" (article 15-1(b).

Forbidding retaliation: The Directive's essential goal is to prevent any kind of revenge against the whistle-blowers. Article 19 lists all kinds of possible forbidden retaliation: (a) suspension, lay-off, dismissal or equivalent measures; (b) demotion or withholding of promotion; (c) transfer of duties, change of location of place of work, reduction in wages, change in working hours; (d) withholding of training; (e) a negative performance assessment or employment reference; (f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; (g) coercion, intimidation, harassment or ostracism; (h) discrimination, disadvantageous or unfair treatment; (i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment; (j) failure to renew, or early termination of, a temporary employment contract; (k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income; (l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry; (m) early termination or cancellation of a contract for goods or services; (n) cancellation of a licence or permit; (o) psychiatric or medical referrals.

Support measures: Member States shall also be obliged to provide a number of support measures to reporting persons such as (article 20): (a) comprehensive and independent information and advice, which is easily accessible to the public and free of charge, on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned; (b) effective assistance from competent authorities before any relevant authority involved in their protection against retaliation, including, where provided for under national law, certification of the fact that they qualify for protection under this Directive; and (c) legal aid in criminal and in cross-border civil proceedings and, in accordance with national law, legal aid in further proceedings and legal counselling or other legal

assistance. Member States may provide, in addition, financial assistance and support measures, including psychological support, for reporting persons in the framework of legal proceedings. The support measures referred to in this Article 20 may be provided, as appropriate, by an information centre or a single and clearly identified independent administrative authority.

Legal liabilities: In judicial terms, reporting persons shall not incur liability in respect of the acquisition of or access to the information, which is reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence. In the event of the acquisition or access constituting a self-standing criminal offence, criminal liability shall continue to be governed by applicable national law (article 21-3). Any other possible liability of reporting persons arising from acts or omissions which are unrelated to the reporting or public disclosure or which are not necessary for revealing a breach pursuant to this Directive shall continue to be governed by applicable Union or national law (article 21-3).

5. Whistleblowing on Abuse of State Secrets and National Security

Whistleblowing protection is politically risky. Whistleblowing may create significant serious political problems to a country or its government. Caution is needed in building a protective framework for whistle-blowers in the area of security and defence. Whistleblowers are no saints, but they may be patriots, not traitors, and keen to serve the public interest, as it happened with Daniel Ellsberg who, by disclosing the "Pentagon Papers" in 1971, helped to ending the Vietnam War or more recently with Bradley (now Chelsea) Manning who helped uncover the atrocities made in Iraq in the name of the War on Terror and Edward Snowden who, through an act of boldness, helped to uncover the intrusive madness of an arrogant power subject only to phony judicial checks. And many more anonymous, good faith whistleblowers around the world who have endured ostracism, retaliation and prosecution because of their revolt against unbearable inhumanity, corruption or illicitness.

The civilization advances when some are ready to take political risks defying political correctness. Obedience may cause more harm than good, as history has repeatedly shown. Submissiveness may be a crime. Rebellion may be a moral imperative. The reflection of German jurists after WWII in the wake of the Nuremberg trials is illustrative in this respect. One of the most insightful was Gustav Radbruch (1878-1949), who trough his famous formula, justified disobedience to extreme unjust law (which he likened to non-law), as morally legitimate. The Radbruch formula was aimed to destroy the defense of Nazi criminals who were shielding themselves behind the "duty to follow orders" a doctrine which was subsequently embraced by the German courts.

The problem is in the way in which a balance could be struck in a legal framework to protect those who dare rebel against the hypocrisy of looking elsewhere. Sociologically speaking only 30% of the European population is in favour of uncovering state secrets while in the United States the figure reaches an equally meagre 50%.[16] There is a cultural resistance of societies to stare at their own bare indignities (Hartmann). This exposure disturbs the self-image that societies have been building over their past and present. Whistle-blowers may contribute to changing the political societies where they live if they are supported by "professional whistle-blowers" such as journalists and NGOs, but they generally will have to pay a heavy price.

In fact, article 3-2 of the EU Directive leaves outside the scope of the legal protection whistleblowing on matters affecting the national security.[17] And article 3-3-(a) leaves those whistle-blowers who

[16] Figures provided by Florence Hartmann: "*Lanceurs d'alerte*", Don Quichotte, Paris, 2014.

[17] "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".

disclose classified information unprotected. Nevertheless, it is worth remembering that this Directive sets common minimal standards or protective thresholds (articles 1 and 2). EU Member States can, and should, expand the matters and persons credited to receive legal protection, as article 2-2 suggests.

The bottom-line is that the protection of state secrets is legitimate insofar as it is justified, while transparency does not need any justification. However, this axiom is far from being a fact in many countries. Moreover, the "right to know" and the protection of the confidentiality of state secrets pull in opposite directions. Many people continue to believe that the national security and the national defense should stay outside of the law and democratic scrutiny. However, more and more people are progressively adhering to the idea that the national security and defense are better protected if subjected to public scrutiny and judicial review. There probably is a long way ahead towards achieving a more democratic and legal control of the state agents dealing with security and defense issues, one of the state governance areas where the rule of law (as opposed to arbitrariness) in the public administration largely remains absent insofar as many decisions remain grounded on the discretion of public officials. Surprisingly, little academic research is available in Europe about the importance of secrecy in policymaking in European countries.[18]

Recommendation 2024 (2013) of the Parliamentary Assembly of the Council of Europe[19] encourages its Member States to "take into account" the Global Principles on National Security and the Right to Information" (i.e. the Tshwane Principles mentioned above) adopted on 12 June 2013 by an assembly of experts from international organisations, civil society, academia and national security practitioners in modernizing their legislation and practice.[20] Those principles are strict concerning restrictions to free access to information by considering that a threat to national security corresponds to a threat to the country's existence and it is "necessary to protect the country's political independence or territorial integrity from the use, or threatened use, of force. The Committee of Ministers replied to this recommendation 2024 (2013) negatively on 23 April 2014 by stating that: "The Committee of Ministers sees no need presently to review the policies it has thus laid down for the Council of Europe regarding access to information and classification of documents. However, it will inform the Parliamentary Assembly about any future developments in this respect".[21] At the level of international standards the situation has not moved since on the protection of whistle-blowers in the security and defence sectors. They remain unprotected, except under the terms of the reiterated case law of the European Court to Human Rights (ECtHR) on the freedom of expression of article 10 of the ECHR, as we will see below.

The Global Principles provided a comprehensive list of categories of information which whistle-blowers should be able to disclose, affecting any part of the public sector, without suffering retaliation, including information on:

- criminal offences;
- human rights violations;
- international humanitarian law violations;
- corruption;
- dangers to public health and safety;
- dangers to the environment;
- abuse of public office;
- miscarriages of justice;

[18] See Berthold Rittberger & Klaus H. Goetz (2018) *Secrecy in Europe*, West European Politics, 41:4, 825-845, DOI: 10.1080/01402382.2017.1423456, At: https://doi.org/10.1080/01402382.2017.1423456

[19] https://pace.coe.int/pdf/d657235b63e1582c3c0b0d8e97b374645ecb30243326667a8259ffe25682ae848428feba12/recommendation%202024.pdf

[20] The Tshwane Principles (2013): https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

[21] https://pace.coe.int/pdf/180c81c87b82e0257730880bf5bb7184d31c8e273326667a8259ffe25682ae848428feba12/doc.%2013503.pdf

- mismanagement or waste of resources;
- retaliation for disclosure of any of the above-listed categories of wrongdoing;
- deliberate concealment of any matter falling into one of the above categories.

The Principles conclude that, even if the disclosed information does not fall within one of these categories, whistle-blowers should be able to rely on the "public interest override" or the "public interest defence". Criminal prosecution of whistle-blowers should only take place in the most exceptional of circumstances, be prescribed by law and be proportionate to the harm caused to interests of national security.

The ECtHR in *Bucur and Toma v Romania* judged in 2013 the following facts:

> The applicant worked in the telephone communications surveillance and recording department of a military unit of the Romanian Intelligence Service (RIS). In the course of his work he came across several irregularities. In addition, the telephones of many journalists, politicians and businessmen were tapped, especially after some high-profile news stories received wide media coverage. The applicant affirmed that he reported the irregularities to his colleagues and the head of department, who allegedly reprimanded him. When the people he spoke to showed no further interest in the matter, the applicant contacted an MP who was a member of the RIS parliamentary supervisory commission. The MP told him that the best way to let people know about the irregularities he had discovered was to hold a press conference. In his opinion telling the parliamentary commission about the irregularities would serve no purpose in view of the ties between the chairman of the commission and the director of the RIS. On 13 May 1996, the applicant held a press conference which made headline news nationally and internationally. He justified his conduct by the desire to see the laws of his country – and in particular the Constitution – respected. In July 1996 criminal proceedings were brought against him. Amongst other things, he was accused of gathering and imparting secret information in the course of his duty. In 1998 he was given a two-year suspended prison sentence. The European Court held, on the contrary, that according to article 10 of the ECHR, the applicant's criminal conviction had interfered with his right to freedom of expression, with the legitimate aim of preventing and punishing offences that threatened national security. Concerns about the foreseeability of the legal basis for the conviction did not need to be examined in so far as the measure was, in any event, not necessary in a democratic society and that the general interest in the disclosure of information revealing illegal activities within the RIS was so important in a democratic society that it prevailed over the interest in maintaining public confidence in that institution.[22]

In its judgment of the case *Guja v Moldova* of 12 February 2008, the ECtHR again relied on article 10 of the ECHR (freedom of expression).[23] In summary the case and the decision of the ECtHR was as follows:

> Head of the Press Department of the Prosecutor General's Office, Mr. Iacob Guja was dismissed in 2003 for publishing letters from the deputy minister of interior and a parliamentarian asking to relax prosecution against four police officers accused of illegal detention and ill-treatment. National Courts confirmed the dismissal. The ECtHR reiterates that Article 10 applies also to the workplace, and that civil servants, such as the applicant, enjoy the right to freedom of expression. "At the same time, the Court is mindful that employees have a duty of loyalty, reserve and discretion to their employer. This is particularly so in the case of civil servants since the very nature of civil service requires that a civil servant is bound by a duty of loyalty and discretion (see *Vogt*, cited above, § 53; *Ahmed and Others*, cited above, § 55; and *De Diego Nafría v. Spain*, no. 46833/99, § 37, 14 March 2002)". Since the mission of civil servants in a democratic society is to assist the government in discharging its functions and since the public has a right to expect that they will help and not hinder the democratically elected government,

[22] *Bucur and Toma v. Romania* - **40238/02** Judgment of 8.1.2013 [Section III]. At: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-7395%22]}

[23] Case *Guja v Moldova*: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20GUJA%20v.%20MOLDOVA\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-85016%22]}

the duty of loyalty and reserve assumes special significance for them (see, *mutatis mutandis*, *Ahmed and Others*, cited above, § 53.) In addition, in view of the very nature of their position, civil servants often have access to information which the government, for various legitimate reasons, may have an interest in keeping confidential or secret. Therefore, the duty of discretion owed by civil servants will also generally be a strong one.

To date, however, the Court has not had to deal with cases where a civil servant publicly disclosed internal information. To that extent the present case raises a new issue which can be distinguished from that raised in *Stoll v. Switzerland* ([GC], no. 69698/01, ECHR 2007-V), where the disclosure took place without the intervention of a civil servant. In this respect the Court notes that **a civil servant, in the course of his work, may become aware of in-house information, including secret information, whose divulgation or publication corresponds to a strong public interest**. The Court thus considers that the signalling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection. This may be called for where the employee or civil servant concerned is the only person, or part of a small category of persons, aware of what is happening at work and is thus best placed to act in the public interest by alerting the employer or the public at large. In this context, the Court has had regard to the following statement from the Explanatory Report to the Council of Europe's Civil Law Convention on Corruption (see paragraph 46 above): "In practice corruption cases are difficult to detect and investigate and employees or colleagues (whether public or private) of the persons involved are often the first persons who find out or suspect that something is wrong."

In determining the proportionality of an interference with a civil servant's freedom of expression in such a case, the Court must also have regard to several other factors. In the first place, particular attention shall be paid to the public interest involved in the disclosed information. The Court reiterates that there is little scope under Article 10 § 2 of the Convention for restrictions on debate on questions of public interest (see, among other authorities, *Sürek v. Turkey (no. 1)* [GC], no. 26682/95, § 61, ECHR 1999-IV). In a democratic system, the acts or omissions of government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the media and public opinion. The interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence (see *Fressoz and Roire v. France* [GC], no. 29183/95, ECHR 1999-I, and *Radio Twist, a.s. v. Slovakia*, no. 62202/00, ECHR 2006-XV).

The motive behind the actions of the reporting employee is another determinant factor in deciding whether a particular disclosure should be protected or not. For instance, an act motivated by a personal grievance or a personal antagonism or the expectation of personal advantage, including pecuniary gain, would not justify a particularly strong level of protection (ibid.). It is important to establish that, in making the disclosure, the individual acted in good faith and in the belief that the information was true, that it was in the public interest to disclose it and that no other, more discreet, means of remedying the wrongdoing was available to him or her.

The ECtHR concluded that: Being mindful of the importance of the right to freedom of expression on matters of general interest, the right of civil servants and other employees to report illegal conduct and wrongdoing at their place of work, the duties and responsibilities of employees towards their employers, and the right of employers to manage their staff – and having weighed up the other different interests involved in the present case – the Court comes to the conclusion that the interference with the applicant's right to freedom of expression, in particular his right to impart information, was not "necessary in a democratic society". Accordingly, there has been a violation of Article 10 of the Convention.

a) International European Law does not Protect Whistle-blowers in the Defence and Security Sector

Whistle-blowers in the defence sector are excluded from legal protection by the European Directive of 2019, while at the same time they will most probably be subject to heavy criminal charges regulated in the domestic penal codes of their own country. So far only the ECtHR is protecting these military whistle-blowers.

In arguing for their own exoneration, military and intelligence whistle-blowers have traditionally pursued a line of defence that revolves around two closely related concepts: higher necessity (including the public interest protection) and a conflict of duties. In recent times, this has taken on an added variation: the whistle-blower points out that they were obliged to break domestic laws in order to reveal violations of international law, especially human rights and humanitarian law as well as the law of war. "Law of war is that part of international law dealing with the inception, conduct, and termination of warfare. Its aim is to limit the suffering caused to combatants and, more particularly, to those who may be described as the victims of war—that is, non-combatant civilians and those no longer able to take part in hostilities. Thus, the wounded, the sick, the shipwrecked, and prisoners of war also require protection by law".[24]

Few countries, if any, have legislation protecting adequately whistleblowing in the defence and security sectors. Some of them (e.g. Canada, UK), require that the whistle-blower produces evidence that he/she acted for the benefit of the public interest. The US Military Whistle-blower protection Act of 1988, as amended several times, has produced more victims than it has helped, but its reform in 2013 was a major improvement, according to Tom Devine, Director of the Government Accountability Project, while stating that "*military whistle-blowers will still have second-class rights compared to civilian employees, even in the restricted circumstances where dissent is legal. They still will face rigged standards in burdens of proof that stack the legal deck against their chances of victory, and they do not have access to judicial review of military service administrative rulings. This is a major step forward, but our coalition will redouble our efforts next year to finish what we started*".[25]

Domestic courts have shown a variety of nuanced reactions to the military whistle-blowers' defence based on **law violations**, **conflict of duties** and **higher necessity** to protect public interest. Nevertheless, some tentative jurisdictional trends may be observed.[26] We bring about some cases of whistle-blowers in the military and security services of various countries:

Higher necessity

The cases of whistle-blowers Mordechai Vanunu (Israel) and Ryszard Kuklinski (Poland) are similar in that they both invoked their acting out of higher necessity to justify their reporting. Each of them ended up being handled opposite judicial outcomes. Katharine Gun (UK) invoked higher necessity (to prevent the second war in Iraq and save lives) for her to become a whistle-blower, while she was not aware that she was reporting a violation of the Vienna convention on diplomatic relations by the British and US governments in 2003. [27]

Vanunu, an Israeli citizen, was employed as a nuclear technician at Israel's Negev Nuclear Research Centre (also known as the "Dimona facility"), where he was bound by a confidentiality agreement, in the early 1980s. Sometime after commencing work at the Dimona facility, Vanunu became a peace activist, opposing all weapons of mass destruction. Serendipitously, this change of sentiment coincided with his realization, based on the production processes at his workplace, that Israel was manufacturing nuclear weapons. In early 1985, Vanunu took nearly 60 photos inside the Dimona facility before leaving Israel and eventually selling the photos to two British newspapers in 1986. Before the story was published Israeli intelligence agents abducted Vanunu in Italy and returned him to Israel, where he was convicted by the Jerusalem District Court of treason and aggravated espionage under the Israeli Penal Code. When Vanunu appealed to the Supreme Court in 1990, the Court rejected his argument that he had been serving a *higher goal* (the democratic character of the State), which overrode his duty to maintain secrecy,

[24] Peter John Rowe: TITLE Law of war PUBLISHER Encyclopædia Britannica DATE PUBLISHED September 26, 2018 URL https://www.britannica.com/topic/law-of-war ACCESS DATE October 19, 2020

[25] https://whistleblower.org/press/senate-approves-military-whistleblower-protection-act-makeover/

[26] Fuller, Roslyn. (2014). *A Matter of National Security: Whistleblowing in the Military and the Collision of Duties as a Defence.* San Diego International Law Journal. 15 (2): 249. At https://www.researchgate.net/publication/270795055_A_Matter_of_National_Security_Whistleblowing_in_the_Military_and_the_Collision_of_Duties_as_a_Defence

[27] https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf

endorsing the view expressed earlier in the case by the District Court that ideology could not be taken into consideration, as ideology could be made to justify any action. Vanunu ultimately spent 18 years in prison, 11 of them in solitary confinement.[28] He lives now in Marrakech, Morocco.

Colonel Ryszard Kuklinski desired to avert the consequences of armed conflict, in his case the outbreak of hostilities between the USA and USSR during the Cold War. A high-ranking strategy officer in the Polish army, Kuklinski had good reason to fear that should hostilities erupt between the Soviet Union and NATO States, Poland would be destroyed in a short-range nuclear war. To save his country from this fate he contacted the US Embassy in Bonn and leaked approximately 35 000 pages of classified Soviet military information to the CIA between 1972 and 1981. Following his escape to the USA in 1981, Kuklinski's activity was discovered and in May 1984 he was sentenced to death *in absentia* by unanimous decision of the Warsaw District Military Tribunal, which stated that he had caused immeasurable damage to the state security of the entire Eastern Bloc through the crimes of betrayal and desertion. After the end of the Soviet Union, the Polish Supreme Court reversed his death sentence in 1995, deciding that whether Kuklinski was acting under a "*higher necessity*" and for the "sovereignty and independence of the country inspired by his ideology" should influence his exculpation. The case was thus referred back to the Military Prosecutor, who on 2 September 1997 cancelled the case, because Kuklinski had acted out of "higher necessity". Kuklinski died in Tampa, Florida, in 2004. Yet he was not welcomed home as a hero in the newly democratic Poland and instead found that many Poles, particularly in military and intelligence circles, remained deeply ambivalent about his actions. Late in his life, he was finally able to return to Poland, but some Poles still felt he had betrayed Poland, not just a ruthless Communist regime.[29] It is alleged that this decision was taken under pressure from the US (apparently it was a precondition for Poland joining NATO). This is possible – the Americans were very public in their desire to have Kuklinski legally exonerated at the time envisaged for Poland to join NATO. However, it does not change the fact that Poland's Supreme Court authorized the possibility of exculpating breaches of State security on the grounds of acting out of higher necessity, even in cases of directly aiding the enemy, as Kuklinski did.

Katharine Gun was employed in 2003 as a translator at the government intelligence agency, GCHQ, in Cheltenham. She was 27.[30] The country, at the time, was being drummed into war by the Blair government, desperate to achieve the United Nations' sanction for the imminent American-led invasion of Iraq. In January that year, Katharine Gun was copied into a classified memo sent to GCHQ by a senior figure in the NSA, its US equivalent. The memo was a top-secret request to monitor the private communication of UN delegates for scraps of information, personal or otherwise, that could be used to "give the US an edge" in leveraging support for the invasion. Katharine Gun leaked that memo to the *Observer*, in the belief that the revelation of the proposed bugging and blackmail tactics might be enough to stop the war. The *Observer* published the dirty tricks memo as a front-page splash just over two weeks before the invasion. She was arrested and charged with breach of the Official Secrets Act. It was in a police cell that she uttered those two sentences that now seem to define the person she was and is. Gun was asked by Special Branch officers why she had chosen to act as she had. "You work for the British government," her interrogator said, with a sneer. "No," Gun replied, steadily. "I work for the British people. I do not gather intelligence so the government can lie to the British people."[31] The legal case against Gun was eventually dropped by the British government in 2004, after her lawyer, Ben Emmerson QC, threatened to use disclosure to put the legal basis of the war itself on trial. Gun had, of course, been forced to abandon her career in the civil service and finally, struggling for work, left Britain altogether.

Conflict of duties (between abiding by the text of the law and serving the general interest)

The basic argument used by Vanunu and Kuklinski was taken up, in a somewhat different variant, by Matthew Diaz, a US Navy Judge Advocate stationed from 2004-2005 at the detention facility in Guantanamo Bay (GTMO). In December 2004, GTMO received a request from Barbara Olshansky, a lawyer working for the Center for Constitutional Rights in New York, for information about the prisoners

[28] https://www.theguardian.com/world/2018/mar/28/mordechai-vanunu-israel-spying-nuclear-1988
[29] https://www.nytimes.com/2004/02/12/world/ryszard-kuklinski-73-spy-in-poland-in-cold-war-dies.html
[30] A film, "Official Secrets" (2019), was produced on her story. https://www.ifcfilms.com/films/official-secrets
[31] https://www.theguardian.com/film/2019/sep/22/katharine-gun-whistleblower-iraq-official-secrets-film-keira-knightley

detained there. The request was ultimately rejected by GTMO's military lawyers in January 2005. Despite this decision, Diaz accessed the military computer systems and printed out the names and some details regarding the identity (e.g. ethnicity, citizenship) of the detainees, as well as details regarding the interrogation team assigned to each detainee, all of which was considered to be classified information. He secretly mailed the information to Olshansky. When his actions were discovered, Diaz was charged with violating a general order, communicating classified information and removing classified material. He was also charged of "Conduct Unbecoming an Officer and a Gentleman". He was sentenced by court-martial to six months confinement and dismissal from the Navy. Diaz appealed his conviction to the US Court of Appeals for the Armed Forces (CAAF), relying in his defence on an alleged *conflict of duties* within the domestic legal system: "on the one hand, his duty as a naval officer and an officer of the court to uphold the Constitution and the rulings of the Supreme Court and the district court in the habeas cases, and on the other hand, his duty as a Naval officer to maintain the confidentiality of information that his superiors should have authorized for release but did not".[32]

While the CAAF did not agree that Diaz had a legal duty as an officer of the court to release the information, it agreed that ethical motives could be relevant in exculpating the appellant. Thus, while the CAAF found that Diaz did not have a legal duty to disclose the information, it admitted the theoretical possibility of such a duty existing in other circumstances and that motive could play a role in at least some delicts concerning the release of classified information. Furthermore, the Court explicitly stated that *it is possible for the conduct to be honourable even if it is illegal* and that the fact that Diaz acted furtively in committing the actions in question, instead of, i.e. openly, was significant.

The case of the Danish Major, Frank Grevil, can also be classified as one of conflicting duties between serving the democracy and the people (the public interest) and serving the government of the day. Frank Søholm Grevil is a Danish former intelligence agent. He was a chemical engineer and language officer within the armed forces. He held the rank of major in *Forsvarets Efterretningstjeneste* (FET), the Danish military intelligence agency. When he heard Danish prime minister Anders Fogh Rasmussen at the Danish Parliament, declaring that intelligence proved that Saddam Hussein possessed weapons of mass destruction, Frank Grevil was shocked. He had taken part in gathering and communicating that intelligence, to which the prime minister referred. And it did not support what the prime minister was claiming. Grevil felt that the prime minister had misled both the parliament and the Danish people in claiming that Saddam Hussein had weapons of mass destruction. And to make matters worse, he was knowingly lying. His declaration was the most important reason for the Danish participation in the coalition of the invasion of Iraq. But Grevil had taken part in writing the reports, which the prime minister used as documentation to make his point. And the reports said nothing certain about the presence of weapons of mass destruction in Iraq. Furthermore, Grevil was offended that the reports, which FET presented to the prime minister and to the Parliament's Committee of Foreign Affairs as their own findings, were allegedly just translations of reports from the US Central Intelligence Agency, CIA. Grevil got a rough deal. Not only did things from his past suddenly surface in the newspapers. He was also charged and convicted to six months in prison for having leaked the classified information. Frank Grevil was an active member of the prime minister's own political party, *Venstre*. The appellate court reduced the sentence to four months imprisonment. "One thing must be understood about Frank Grevil - the man who leaked secret documents about the basis of the Iraq war: Frank Grevil was not against the Iraq war. He was for the war. He leaked the documents because the government, led by Anders Fogh Rasmussen, in his opinion lied to the Folketing (parliament) and the population. What the government lied about - namely the basis of the Iraq war - was in principle subordinate"[33].

The city court (first instance) in Grevil's verdict stated that the opposition in the Folketing had a great interest in gaining insight into the leaked threat assessments, but that did not give Grevil the right to pass on the secret information according to the court. Grevil's defender, lawyer Jakob Lund Poulsen, found this very strange: "He called the verdict "rather regrettable" and said the court had looked too legally rigorously at the possibility of disclosing information in the public interest. - It is difficult to understand that the court on the one hand finds that half of the Folketing had a clear interest in obtaining the information, but that on the other hand it does not influence the verdict. The city court has used a very,

[32] United States v Diaz, 69 M.J. 127, C.A.A.F. 2010, At: https://cite.case.law/mj/69/127/

[33] https://jyllands-posten.dk/premium/indblik/Indland/ECE8989822/danmarks-mest-kendte-whistleblower-vi-var-stadig-i-den-kolde-krig-da-11-september-ramte-os/

very narrow consideration, said Jakob Lund Poulsen about the rejection that Grevil acted in the public interest.

After Grevil went to the media in 2004 with confidential documents with FETs assessment of Saddam Hussein's weapons of mass destruction, there were no more jobs for the Danish chemical engineer and language officer within the Armed Forces. Today, Frank Grevil earns his living as a translator and takes care of technically complicated and legally heavy texts in German, English, Swedish and Dutch.[34] "Grevil believes it to be extremely destructive of democracy when national leaders deceive the citizens' representatives, whether in Parliament or Congress, into voting for what the Nuremberg Tribunal called the "supreme international crime" — a war of aggression. He thought it essential that Danish citizens learn that their political leaders had not told the truth. And so, he gave to the press documents that exposed this, fully aware that, in doing so, he ran the risk of going to prison".[35]

The case of Clive Ponting, a British civil servant deceased on 28 July 2020, is interesting because his acquittal by a jury, despite the manipulations of the trial presiding judge, led to a fundamental legal change in the UK. In accordance with the Official Secrets Act of 1911, it was permitted to release government confidential information if it was in the "interests of the state" to do so. This clause led to the acquittal of Ponting. Subsequently the Official Secrets Act was amended in 1989. As a result of the 1989 modification, the whistle-blower defence based on the protection of the public interest was taken off the law. (In)Famously, the presiding judge in the trial attempted to persuade the jury that "'*public interest' is what the government of the day says it is*".[36] Ponting was a whistle-blower on the sinking by the British army of the Argentinian General Belgrano warship during the Falklands war in 1982, in which more than 400 persons died, despite that the Argentinian warship did not represent any actual threat for the British islands (therefore its sinking was a British aggression).[37] He also reported in 1985 on the Operation Cauldron, a 1952 set of secret biological warfare trials that had led to a trawler being accidentally doused with plague bacteria off the Hebrides, that had not been destroyed. Ponting confidentially told *The Observer* newspaper about it.

b) Is the Domestic Military Justice Fit to Judge Military Whistleblowing?

The notion of crimes strictly military and those service-connected, including the enforcement of military discipline, as a basis to attribute jurisdiction to military courts is vague. This elusive conceptual construction contributes to sapping the very rationale for a special military justice separate from the ordinary one. It is considered by many observers as a "privilege" rather than a necessity, especially as the modern "constitutionalism" develops and strengthens.

This is of special relevance when it comes to judging military whistle-blowers. In these cases, the impartiality of the martial court is a stake. The impartiality and independence of the court is imposed by article 6 of the European Convention of Human Rights. In order to judge military whistle-blowers military courts shall be independent, which may hardly be the case when it comes to judging a whistle-blower who has disclosed information affecting military secrets or who put into question the commanders' behaviour. The case is even harder in institutional environments where military whistle-blowers are seen as disloyal or traitors deserving retaliation. The military court may most probably have an interest in the outcome of the trial, usually to the detriment of the whistle-blower's rights. Real-life cases abound of negative predisposition of military judges against defendants who have blown the whistle to signal wrongdoing within the military or security institutions.

For example, the trial of Chelsea (former Bradley) Manning in 2012-2013 where the trial presiding judge, Colonel Denise Lind, refused almost all procedural motions sustained by the Manning's defence. The context of the prosecution is what the *New York Times* called the "emergence of "a national-

[34] https://www.euroman.dk/politik/whistlebloweren-det-gor-man-kun-en-gang-i-livet
[35] Statement justifying the award to Grevil of the ***Sam Adams Associates for Integrity in Intelligence.*** At: http://samadamsaward.ch/frank-grevil/
[36] A good summary in Ponting's obituary of the Guardian newspaper : https://www.theguardian.com/politics/2020/aug/06/clive-ponting-obituary
[37] Ponting published *The Right to Know: The Inside Story of the Belgrano Affair* (1985), Sphere Books

security apparatus that has metastasized into a vast and largely unchecked exercise of government secrecy and the overzealous prosecution of those who breach it. Bizarrely, as many as 4.2 million state employees and contractors are sufficiently part of this apparatus to have clearance to view the sort of material Manning released and many of the 92 million documents the state classifies every year".[38]

The case of the Spanish Lt. Luis Gonzalo Segura also illustrates the point of how counterproductive military justice in fighting corruption may be. "After 13 years of serving his country, Lt Luis Gonzalo Segura had had enough. Everywhere he looked in the Spanish military, he saw corruption, abuse, harassment, and inherited privilege. The top brass, meanwhile, were happy to look the other way. Segura began to document the scams, false invoices, and accounting discrepancies he came across. When he reported what he had discovered to his superiors, Segura says, they advised him to look the other way. He might get a promotion or a medal in exchange for his silence, they said, and he would put himself at risk if he continued denouncing his comrades-in-arms. But Segura refused to become an accomplice. Rather than be deterred, he insisted on reporting to his superiors each crime he encountered within the barracks. His complaints were never answered. In 2012, military courts dismissed his allegations without an investigation or audit. Prosecutors did not even ask him for evidence. Eventually, his frustration exploded into a book. In 2014, he published *Un Paso al Frente* (A Step Forward), a collection of his experiences as a military man. The book depicts a gloomy world where impunity, corruption, abuse, embezzlement, and labour and sexual harassment flourish, where the troops forced to deal with this environment are helpless. In response to the book, military police arrested Segura on charges of "indiscipline." He was held in custody, without trial, for 139 days. To protest his detention, Segura went on a 22-day hunger strike. While in prison, he began writing up memories of his service. His second book, a novel entitled *Código Rojo* (Code Red), portrayed a set of characters solving several crimes—many of which were based on his experiences in the barracks. A day after the book's publication, he was expelled from the army with a dishonourable discharge".[39]

The consideration of the subjection of the military to civil justice, this latter understood as ordinary justice, as opposed to special justice imparted by martial courts, is almost absent from any elaboration of standards to assess the effectiveness of the civilian control over the military. In Norway, the civilianisation of the military justice is part and parcel of the process of subordination of the military to the civilian control.[40]

Some European countries (Austria, Germany, Belgium, Denmark, Estonia, France, Netherlands, Norway, Portugal, Slovenia, Sweden…) have totally or partially abolished their military justice apparatuses (at least in peacetime) and progressively subsumed the jurisdiction of military courts into the one of the ordinary justice. The UN has recurrently advocated for the military justice to be an integral part of the general judicial system. We could understand that full-fledged democracies like the USA, Canada, Spain, the UK or Australia conserve their military courts, but they are becoming more exceptional cases than regular ones among developed countries.

Human rights concerns have entered fully in the elaboration of standards for the democratisation of the impartment of justice in the armed forces (especially with regards to fair trial concerns) and to evaluate their accountability to prevent impunity of gross violations of human rights perpetrated by military personnel, but the protection of those who report these violations is generally overlooked in generating standards of military justice. The factoring in of the respect to human rights into the military justice standards is a positive development, but on the one hand it does not necessarily contribute to the civilian control of the military and, on the other, it does not ensure that citizens will know about the wrongdoings of the military personnel either.

It is often argued that non-military judges cannot understand the specificities of military life and constraints and therefore civilian judges should not be called to judge the behaviour of military men/women. Therefore, the Military Penal Code should be enforced preferably by military judges. This

[38] https://www.irishtimes.com/news/world/us/united-states-v-manning-1.1481894
[39] https://www.opensocietyfoundations.org/voices/how-eu-failing-whistleblowers
[40] Arne Willy Dahl (2011): Presentation at the University of Oslo (international law lunch meeting) on 23 November 2011. At: https://www.generaladvokaten.no/uploads/AS66Wsh5/_2011_11_international_trends_in_military_justice.pdf

argument is weak. We should argue that a well-drafted Penal Military Code can perfectly be enforced by ordinary court civilian judges, in the same way as they enforce other pieces of legislation.

According to Dahl, "it serves the long-term interest of the armed forces to have independent bodies to investigate, prosecute and adjudicate cases, especially when they are of certain gravity. There are, however, also downsides. If independence means distance – in organisation, geography and mentality – one may find oneself in a situation where the independent bodies lack understanding of military affairs. If such lack of understanding leads to unwarranted sentences or acquittals, it is time to pull the brakes… The important question that many countries struggle with is whether military commanders should give up their control of military justice in order to have a system that is perceived as fair by the general public". [41]

In any case, it is worth considering whether the aim to protect the public interest value of military whistle-blowers will be better served by the civilian or the military justice, knowing that, given the elusive nature of the notion of public interest, the occurrence of this latter in every particular disclosure of wrongdoing is to be gauged by judges who are usually imbued with their military mindset or "judicial idiosyncrasy", so adding uncertainty to the trial outcomes for military whistle-blowers as well as representing a deterrent to would-be whistle-blowers.[42]

6. National Security as Justification for Secrecy

The basic conceptual assumption is that open government and free access to information on the one hand and restricting that access on the other benefit the public interest. The internationally accepted general principle is that the 'right to know' shall be promoted by governments while putting reasonable limits to it in order to protect the confidentiality of certain public information if the state action in certain domains, particularly in those concerned with national security and defence, is to be effective. [43]

The main problem of this topic is to determine when and how restrictions to public access to information are legitimate. It is an aspirational goal of healthy democracies to ensure proper public access to information while drawing legitimate boundaries to that access. However, establishing adequate balances between these two goals is very much dependent on national histories, societal values and cultural factors. This is a reason why it is elusive inquiring on whether international standards exist to reach the right balance (Transparency International UK, 2014).[44] In practice they do not exist, although intellectual debates and attempts to establish some principles have been numerous in recent years.[45]

If left unchecked, the practice to ensure confidentiality becomes expansive. Certain state services dealing with national security, defence, criminal investigations, intelligence gathering or counterterrorism have a tendency to cover with secrecy everything they do, even if that results in thwarting the citizens' right to know what the government is doing. Apart from skyrocketing costs in keeping the "machinery of secret" working, this expansive feature of confidentiality tends to undermine public confidence in governmental institutions and ultimately in democracy as a political regime. Too

[41] Arne Willy Dahl (2015), "*Military Justice and Self-Interest in Accountability*", in Morten Bergsmo and SONG Tianying (editors), Military Self-Interest in Accountability for Core International Crimes, FICHL Publication Series No. 25 (2015), Torkel Opsahl Academic EPublisher, Brussels, ISBN 978-82-93081-81-4. First published on 29 May 2015, pages 26 and 33. At https://www.legal-tools.org/doc/6e9fb5/pdf/

[42] Boot, E.R. The Feasibility of a Public Interest Defense for Whistleblowing. *Law and Philos* **39,** 1–34 (2020). https://doi.org/10.1007/s10982-019-09359-1

[43] See CIDS Norway Good Governance Guides # 6 (2018): *Balancing Openness and Confidentiality in the Defence Sector: Lessons from International Good Practice*. At: https://cids.no/wp-content/uploads/2018/06/9062-DSS-GGG-6-eng-4k.pdf

[44] Transparency International UK (2014): Classified Information: A Review of 15 Countries. Available at: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

[45] For all, see The Tshwane Principles (2013): https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

much secrecy also tends to produce more mistakes than public scrutiny in the performance of the government and it often threatens national security more than openness does.

As some public officials argue, in certain countries, such as the United States, too much secrecy "has become an unwarranted obstacle to information-sharing inside and outside the government, to the detriment of public policy" (Aftergood, 2008, page 400), which points out at a problem of over-classification, i.e. information-holding services tend to classify information to an extent going well beyond what is actually needed.[46]

The purpose of any classification system is to prevent disclosure of information that could endanger national security, but the vagueness of notions such as "national security", "danger", the difficulty to distinguish between information on facts and information on opinions, makes it very difficult to establish criteria for sound classification of information.

Sound classification of information is also a very difficult notion, but we could conceptually agree that a "sound" classification is the one which is reasonable (proportional) and departs less from the democratic values of openness, transparency and free access to information. In other words, we could agree that a reasonable limitation to transparency is the one that is exceptional and protects critically national security. This entails acknowledging that there is information whose concealment is not critical for the national security and therefore it should be totally or partially disclosed.

There are still prevailing traditional approaches in some democratic countries whereby transparency merely is a citizens' demand whereas secrecy for the sake of national security represents the public interest. For example, Mr. Jean-Marc Sauvé, deputy president of the French State Council, said in an address to the National Assembly of France (low chamber of the French parliament) on 5 July 2011: "*this is the way ahead for drawing the dividing line between the legitimate public interests claiming secrecy and the transparency claimed by the citizens"* (Sauvé, 2011, page 6).[47] This entails the assumption that preserving secrecy protects the public interests, whereas transparency is not in the public interest, but it is a mere claim driven by the curiosity of citizens and journalists. On the contrary, experience shows that promoting transparency is one of the best ways to protect the public interests, because it helps keeping public authorities accountable to the public and other control bodies. Transparency, not secrecy, is believed to bridge "a gap that arises naturally between the state and its public" (Fenster, 2010, page 619).[48]

There is international consensus on that transparency of the acts of public authorities shall be the general rule whereas secrecy must be the exception. Exceptions shall be justified: they can be justified only if they are legitimate. They are legitimate only if they can be proven to be established for the sake of genuine national security interests.

Distinguishing legitimate from illegitimate secrecy calls for some control by authorities which are independent from the classifier, be them the courts or other public bodies, in order to establish whether the national security invoked to classify information is genuine. Otherwise, decisions on classifying information become exclusively discretionary and most probably arbitrary. However, historically courts have played and are playing a role excessively deferential to the withholding of information by security

[46] Aftergood, Steven (2009):"*Reducing Government Secrecy: Finding What Works*," in Yale Law & Policy Review Vol. 27, No. 2 (Spring, 2009), pp. 399-416. Available at: https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

[47] Sauvé, Jean-Marc (2011) : *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général*, discours à l'Assemblée Nationale le mardi 5 juillet 2011 au colloque organisé par Transparence Internationale France. Disponible à : http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

[48] Fenster, Mark (2010): *Seeing the State: Transparency as Metaphor*, in Administrative Law Review, pages 617-672, available at http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

or intelligence agencies. To our knowledge, only the European Court to Human Rights has so far stood up against the immunity of crimes this arbitrary concealment may be conducive to (see above).

Nevertheless, full transparency is not conceptually possible. The state will always have obscure areas. As Fenster (2010, page 623) points out, there exists something in between secrecy and transparency, which makes that secrecy is not necessarily the opposite of transparency. There could be no secrecy and not transparency either, because secrecy and transparency require institutionalisations which are structurally different (Riese, 2014, page 14).[49]

In addition, as said, the notion of "national security" is extremely elusive, as it can mean different things in different national contexts. In many of the European countries surveyed by Jacobsen (2013), national security encompasses international relations and domestic security threats as well.[50]

In order to establish whether or not government secrecy is legitimate, Afterwood (2009, page 402-403) proposes three practical categories of secrecy, while acknowledging that the enduring public policy problem is to disentangle the legitimate from the illegitimate secrecy by preserving the former and exposing the latter:

1. *Genuine national security secrecy*: it works to protect information that would pose an identifiable threat to the security of the nation by compromising its defence or the conduct of its foreign relations. The withholding of such information is not controversial because it is the rationale of any classification systems and the public interest is best served when this type of information remains secret.

2. *Bureaucratic secrecy*: it reflects the tendency of bureaucrats to stockpile information whether out of convenience or a dim suspicion that disclosure is intrinsically riskier for bureaucrats than not disclosure. This bureaucratic tendency usually leads to an inertia of over-classification of information and results in unnecessarily classified information. It also multiplies the budgetary costs of secrecy and plays on the hands of the "secrecy industry".

3. *Political secrecy*: it uses the classification authority for political advantage. This form of secrecy is the most objectionable because it exploits the accepted legitimacy of genuine national security interests in order to advance a self-serving agenda, to evade political controversy or to thwart accountability. In extreme cases, political secrecy conceals breaches of law, human rights violations, corruption or mismanagement and threatens the integrity of the political process.

a) Weak role played by the judicial review in controlling classification systems

Except for the ECtHR (see above), the courts have traditionally been, and still are, quite deferential, to the classifying agencies and their so-called "state secrets executive privilege". Judicial deference has helped to cement the idea that national security is too sensitive to be disclosed even to courts (Setty, 2012), especially in the United States since the cool war hallmark case *United States vs. Reynolds*. [51]

[49] Riese, Dorothée (2014): *Secrecy and Transparency*, paper resented at the ECPR Conference in Glasgow, September 3-6, 2014. Available at: https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf
[50] Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. Available at: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

[51] Setty, Sudha (2012): *The Rise of National Security Secrets*, in Connecticut Law Review, volume 44, number 5, July 2012, pages 1563-1582.

The deferential tendency of the courts towards the executive has been heightened since the September 11 of 2001 terrorist attacks in the USA. Government claims on national security have consistently prevailed in court over principles of accountability, transparency and open government. The cases in the United States, UK, France and elsewhere in the democratic world, let alone in less democratic countries, reflect a judicial adherence to a narrow view of the judicial role concerning the review of security-related executive decisions, to the detriment of the protection of fundamental rights, the rule of law and genuine security interests.

The "state secrets executive privilege" (USA) or the "public interest immunity certificate" (UK) or the "*secret-défense*" (France) are invoked very frequently by classifying executive authorities to pre-empt or difficult judicial review. This exception to openness is regularly accepted by courts even if sometimes courts vaguely state that the privilege should be limited to instances of genuine national security. This quite spread judicial stance generally reveals "a judicial disregard of the notion of checks and balances, an abdication of judicial responsibility and a disdain of the structural need to preserve an avenue for plaintiffs to seek redress against government overreaching" (Setty, 2012, page 1573).

Fuchs (2006, page 168) in an outstanding study on the role of courts found that "given the significant values fostered by the right to access to government information, this right should only be sacrificed when a legitimate need for secrecy exists… Neither parliaments nor the public on its own are able to challenge excessive secrecy. Independent review constitutes a part of the judiciary responsibility to ensure that government action is properly authorised". The courts are the only ones independent enough to play that role of challenging excessive secrecy, but seemingly, Fuchs notes, they have refused to accept that role.[52]

In nearly all the European countries surveyed by Jacobsen (2013), the courts have the authority to examine classified information that the government seeks to keep secret on national security grounds. Notably, however, in some countries, only certain courts or judges with special clearance may examine classified information. In Germany, only the Federal Administrative Court can examine classified information. In Spain, although the Official Secrets Act does not contemplate access for judges, as it does for Congress and the Senate, the Spanish Supreme Court has determined that it, and only it, has the power to review the classification of information by the Government. The one country in which courts do not ever have the authority to directly examine classified information is France (Sartre and Ferlet, 2010).[53] It seems to be impossible for a French judge directly to examine classified information. In France, in order to limit the effect of this prohibition, a law of 1998 created the CSDN (*Commission du secret défense nationale*), an independent commission, which can access classified information requested by the judge in order to evaluate whether it could be reasonable to declassify it. As in the USA, in most European countries, judges normally defer to the public authority's assessment that disclosure would harm national security (Jacobsen 2013).

b) Classification and Declassification Criteria

The classification levels have been standardised in a way that the various levels of classification can be found in many OECD countries. Among OECD countries, a good example of treating state secrets is New Zealand. In New Zealand, official information is protected in accordance with criteria based on a strict definition of the necessity to protect official information: Information is to be protected to the extent consistent with the public interest and the preservation of personal privacy. The classification of information attempts to grade information on the basis of the damage that would result from

[52] Fuchs, Meredith (2006): *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, in Administrative Law Review, Volume 58, Number 1, Winter 2006, pages 131-176.
[53] Sartre, Patrice & Ferlet, Philippe (2010*) : Le secret de défense en France* in Revue Études 2010/2, Tome 412, février, pages 165-175. At : https://www.cairn.info/revue-etudes-2010-2-page-165.htm

unauthorised disclosure and to specify the protective measures to be applied.[54] According to the New Zealand guidelines, in themselves, classifications do not allow official information to be withheld; rather the information must be considered in its merits using the criteria set up by the law.[55] The security classification system of Australia is also interesting, as it provides clear guidelines on classification and declassification of information. [56] The levels of classification in New Zealand, which follows a quite spread international practice, are as follows, depending on the public good to be protected:

a) The **national security** (disclosure would put at risk the security, defence or international relations of the country or those of friendly governments): on this criterion, the information can be classified as Top Secret, Secret, Confidential or Restricted.

b) The **government's policy** and/or **individuals' privacy** (disclosure would endanger the functions of the government or cause loss to a person). On this criterion the information can be classified as Sensitive and Restricted or In Confidence.

Similar markings and criteria for classifying information may be found across many OECD countries. Even in Turkey, where classification rules are not publicly available, certain classification levels are known to exist (Jacobsen 2013). Sweden was the only country which responded to the survey analysed by Jacobsen (2013) that the law does not specify levels of classification of information, because in Sweden classification serves a purely administrative function. Other aspects (e.g. classification procedures, marking requirements, classification authority, duty to give reasons to classifying, accountability for improper classification, oversight bodies, etc.) related to classification of information vary quite significantly across European countries (see Jacobsen 2013 and Transparency International UK, 2014).

In European countries the declassification of information is shaped by three main criteria: time limits, trigger event, or mandatory review period to prevent perpetual classification of information. However, it is not rare to find countries where no criteria for declassification are provided in legislation or administrative practice. The median time limit, according to Jacobsen (2013) calculations, is 30 years among European countries, with specific time limits ranging from 10 years in the Netherlands to 100 years in Romania to indefinite time limits like in Spain and Turkey, which is quite exceptional in Europe.

The most common period for mandatory review of classified information is 5 years. In Sweden there is no pre-established mandatory review, but the classification of any kind of information must be reviewed whenever a request for information disclosure is made. Automatic declassification (trigger event) varies across countries, but in most of them it depends on the occurrence of a governmental discretionary decision to declassify information. This decision can also be the consequence of an Access to Information Act procedure undertaken by a citizen or institution.

c) Keeping Secrecy under Control: Harm Test and Balancing Test

According to *Right2INFO.org*, an NGO promoting good law and practice, the so-called harm and public interest tests flow from the requirement that restrictions on the right of access to information must be proportionate and necessary. [57] OECD-SIGMA (2010) provided an extensive and deep conceptual approach to the notions of harm test and balancing test flowing from a distinction between absolute

[54] New Zealand's Official Information Act of 1982
[55] New Zealand's Guidelines for Protection of Official Information. See https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/
[56] Australia (2014): Information Security Management Guidelines. Australian Government Classification System. At https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf
[57] http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

restrictions and relative restrictions to access to information. Among the former those having to do with the defence and national security are generally included.[58]

The Harm Test

Pursuant, the harm test, a public authority must demonstrate that a disclosure threatens to cause harm to a protected interest to justify information withholding. The harm test requires that the state shows a risk of a substantial and demonstrable harm to the legitimate interest. It must be demonstrated that the limitation is related to the identified legitimate aim, the disclosure would cause substantial harm to the aim and harm is sufficiently specific, concrete, imminent and direct and not speculative or remote.

Balancing test

The proportionality also requires a balancing act, whereby the harm of disclosure is weighed against the public interest. The explicit and detailed public interest overrides are offered under national laws. The mandatory public interest override in case of information related to human rights violations or crimes against humanity is recognized under many models, including European, Inter-American and African systems. The balancing test requires that a public authority, or oversight body, weighs the harm that disclosure would cause to the protected interest against the public interest served by disclosure of the information.

The definition of what constitutes a public interest varies across countries and often requires a case-by-case assessment. In general terms, public interest issues favouring disclosure usually involve matters of public debate, public participation in political debate, accountability for public funds and public safety. The issues related to safety and environment, significant threats to health and information relating to grave human rights violations are subject to mandatory public interest override.

Some countries have issued guidelines for civil servants. For example, in New South Wales, Australia, when deciding whether to release information, staff must apply the public interest balancing test. This means, they must weigh the factors in favour of disclosure against the public interest factors against disclosure.[59] According to these guidelines, the public interest test involves three steps:

1. Identify the relevant public interest considerations in favour of disclosure
2. Identify the relevant public interest considerations against disclosure
3. Determine the weight of the public interest considerations in favour of and against disclosure and where the balance between those interests lies.

Despite the clear stance of the Australian legislation in favour of the disclosure of information the provincial laws on access to information establish several situations where the presumption is in favour of withholding the information and keeping the secrecy. The most prominent is the information subject to an overriding secrecy law (26 Acts are specifically named). This follows a general tendency affecting many OECD countries whereby Freedom of Information Acts (FOIAs) have stopped at the doorstep of traditional legislation on state secrets. States secrets are consistently kept out of the scope of freedom of access to information legislation. In addition, there has generally been little effort in most countries in trying to harmonise the traditional state secrets legislation with the new one on freedom to access information. Consequently, whistleblowing on state secrets remains unprotected in many OECD countries.

The fact that many FOIAs have left national security-related secrecy virtually untouched means that legislation and recourse to courts are hardly effective instruments for reducing the universal trend towards multiplying confidentiality and secrecy in the workings of security and intelligence agencies.

[58] OECD (2010), "*The Right to Open Public Administrations in Europe: Emerging Legal Standards*", SIGMA Papers, No. 46, OECD Publishing, Paris. At: http://dx.doi.org/10.1787/5km4g0zfqt27-en
[59] http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

Their traditional, opaque way of dealing with confidential information remains basically unaltered despite international movements in favour of more transparency and social demands for the "right to know".

In fact, enacting general legislation which is effective in balancing secrecy and openness is challenging both conceptually and practically. One reason is that public bodies or agencies that are more likely to classify information have quite different purposes and motivation in their workings, a fact which fosters different security-related cultures. For example, military bodies tend to focus primarily on the security of weapons technology and operational plans, intelligence agencies on the protection of sources and operating methods, diplomats are concerned with the international consequences of the classification and declassification of information, the police is eager to protect their snitches and operating plans. This leads each agency to develop its own classification guidelines and protocols, which remain in force for years, unscrutinised. It is understandable that within an agency people tend to play on the safe side, which leads to over-classification (Aftergood, 2009).

In the face of it, informed observers and practitioners suggest that, even if the classification should be done by the relevant agency, the declassification authority should lie outside such agency. This is the best way to nullify agency self-interest and purge it from the classification excesses (Aftergood, 2009, page 412). Some somehow successful attempts in doing so have been carried out in the USA, as for example through the *Interagency Security Classification Appeal Panel* (ISCAP)[60] and *the Fundamental Classification Policy Reviews* (FCPR)[61], or in France with the CSDN (see above). These American experiences, described by Aftergood (2009), in essence show that "if one agency cannot successfully explain to and convince a senior official or panel from other agencies why the national security requires that a certain item is classified, then there is reason to doubt the necessity of its continued secrecy".

7. Standing Up Against Unlawfulness in Defence and Security Sectors

a) Political Loyalty and Professional Autonomy of the Military and the Police

Typically, one of the main focus of research in public administration is the tensions between politics and professional knowledge and expertise, represented both by the civil bureaucracy and by the professional military or the security forces. A central aspect of this topic is the balance between political control and direction on the one hand and the professional autonomy on the other.[62]

Elected politicians should be able to govern the professional civil servants, the military and the security forces. In democratic militaries there is a universal doctrine known as the "imperative for civilian democratic control over the military", which reflects this political supremacy in a field where the outwitting of the civilian elected representatives by the soldiers may lead to the demise of democracy itself altogether.

However, civil servants and the professional military (or police) need to have significant freedom based on their professional competence. Professional knowledge and experience form the backbone of any

[60] https://www.archives.gov/declassification/iscap

[61] https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf :See also the 1994 pioneering review in the Energy Department at: https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html

[62] See for example: Tom Christensen (1991): *Bureaucratic Roles: Political Loyalty and Professional Autonomy*, in Scandinavian Political Studies nº 14 (4), December 1991, Pages: 303-320. At https://doi.org/10.1111/j.1467-9477.1991.tb00121.x

public organisation. In addition, they shape the kernel of the permanent capacity and capability of the state to deliver public services, including security and defence. Politicians come and go, but civil servants and military or police cadres remain and are expected to serve any governments. Hence the required political neutrality expected from civil, security and military personnel. The striking of such a balance between loyalty and autonomy is an issue that remains complex and it is still unsettled in many countries around the world.

With the growth of complexity in contemporary societies, governments are increasingly relying on expertise and science in policymaking to the point that some backlashes are happening against experts in recent times amidst populist political, generally conservative, bigoted or reactionary haughtiness.[63]

This phenomenon is happening ensuing the assumptions put forward by the New Public Management (NPM) movement of the 1980s and 1990s whereby policymaking should be isolated as much as possible from politics and entrusted to "neutral and objective" expert bodies (agencies) such as Central Banks for economic and financial policies, to doctors to manage hospitals and design health policies or to generals to run ministries of defence, and so forth.

Yet this approach has shown its limitations from a democracy point of view, even if it must be recognised that popular vote per se does not always ensure good policies.[64] However, the central, unsolved question remains to reconcile expert-given scientific (and often ambiguous) reassurances with political accountability in policymaking, and consequently how the legitimacy of public action is to be assessed. This unsolved question has shown its sharpest actuality on the occasion of the current coronavirus crisis affecting the whole world.

Especially, military whistle-blowers are often considered disloyal for raising a concern, even though their motivation is to expose illegality, or simply to correct wrongdoing and malpractice. Being seen as disloyal can result in severe retaliation not only from superiors but also from colleagues, friends and even the wider society. This may stem, in part, from the unique nature of military organisations where commitment to service is built on a sense of shared purpose. Blowing the whistle is then perceived as a rejection of a shared way of life and a betrayal.

The employment status of military personnel is often quite different from that of other public service employees and the consequences of making unauthorised disclosures to the media often much more severe. The way many countries around the world use and classify national security information creates a severe imbalance of power that prevents military personnel from raising concerns. Official secrecy can also frustrate the vital oversight function performed by parliamentarians and external bodies.

It is necessary to consider the theoretical, ethical and legal arguments for whistleblowing, but it is important not to forget the practical consequences of blowing the whistle. The right to disobey an unlawful order, for example, is particularly challenging for rank-and-file military or police personnel who must make quick decisions in conflict situations. How the "right to disobey" is defined depends on the country, and the application of national and international law in such circumstances is by no means straightforward. It is therefore just as important to provide practical guidance as it is to inform military personnel of their legal rights. Guidance can provide clarity on the circumstances in which people may disobey an order and how they can obtain support when they do.[65]

[63] See Tom Nichols (2017): The Death of Expertise: The Campaign against Established Knowledge and Why it Matters. Oxford University Press.
[64] See Christopher H. Achen and Larry M. Bartels (2016): Democracy for Realists: Why Elections Do Not Produce Responsive Government. Princeton University Press.
[65] See Ashley Savage (2016): Leaks, Whistleblowing and the Public Interest: The Law of Unauthorised Disclosures. Edward Edgar Publishing, Cheltenham, UK and Northampton, MA, USA. Especially its chapters 6 (Whistleblowing in the security and intelligence services) and 7 (Whistleblowing in the armed forces).

b) The Effectiveness of the Bureaucracy as Neutrality

The core aim of bureaucratic autonomy is for civil servants or experts to be able to translate their own knowledge into authoritative action without external constraints.[66] Bureaucratic autonomy would be the "fundamental distinguishing characteristic of independent civil service systems: that it 'ties the hands' of rulers for managing civil servants".[67] Bureaucratic autonomy is necessary for professional autonomy of civil servants or the militaries, but it must always be understood as relative, as we will see.

The effectiveness of bureaucracy is increasingly acknowledged as important for democratic stability. The dominating presumption in the literature is that what underlies administrative effectiveness of bureaucracy is the bureaucracy's autonomy in hiring and firing its own staff and in emitting professional advice and judgement.[68]

Andersen and Mikkelsen point to an important omission in this framework of making bureaucracies effective: that the bureaucratic autonomy only contributes to administrative effectiveness if bureaucrats are loyal to the political executive (or government) of the day. Furthermore, if such executive loyalty is not established prior to the bureaucratic autonomy, the government faces a serious problem of political control that may not be solved without conflict. Their analysis suggests that studies of administrative effectiveness should not only consider whether bureaucracies are autonomous in employment-related matters but increase their scope of inquiry to include how bureaucrats handle their freedom from political pressure.[69]

The Weber's idea of civil servants acting as neutral implementers was merely an ideal stereotype. According to Weber, and most scholars within the field of public administration today, there is no such thing as 'neutral competence' in civil or military bureaucracies. When implementing or advising on policies within their own field of responsibility civil servants (or generals) always have 'views' on how the policy should develop, and they bring these 'views' to policy analyses and discussions and to policy propositions.

Nevertheless, professional experts are not necessarily guided only by individual self-interest, but also by some notion of the 'public interest'. The problem is that they rely heavily on their own allegedly scientific knowledge or on whatever their field of expertise might be. Instead of being loyal to their political masters they tend to be loyal to the norms within their own profession and their professional colleagues. When they run into doubts and dilemmas they typically turn to their own profession for guidance. Within their own organization, in national and international arenas, and in publications specialised in their own field they try to find out how their professional colleagues discuss appropriate ways of acting. They feel prouder when commended by their colleagues than when applauded by the politicians or by the media.

However, these discussions go on within an established 'scientific paradigm' held by the profession, and therefore the alternatives the professional experts try out the next time are quite similar to alternatives tried before, at least in the eyes of 'outsiders'. Further, due to their expertise, professional experts feel they have a right to work with a high degree of autonomy within the area in which their

---

[66] Maggetti, M., & Verhoest, K. (2014). *Unexplored aspects of bureaucratic autonomy: A state of the field and ways forward*. International Review of Administrative Sciences, 80(2), 239–256. DOI: 10.1177/0020852314524680

[67] Horn, Murray J. (1995): The Political Economy of Public Administration: Institutional Choice in the Public Sector, New York: Cambridge University Press.

[68] On professional judgement, see Cardona, F (2019): *On the Needs and Functions of Codes of Ethics*, in Good Governance Guides # 8, Ministry of Defence, CIDS, Oslo. At: https://cids.no/wp-content/uploads/pdf/cids/Guide-to-good-governance-no8.pdf

[69] Andersen, D. & Mikkelsen, K. S. (2014). *How State Bureaucracies Become Effective*. Paper presented at the 2014 Annual meeting of the Danish Political Science Association (DPSA), Vejle, Denmark. https://dpsa.dk/papers/How%20bureaucracies%20become%20effective.pdf

expertise is needed. The steering and control from 'outsiders' (read elected politicians) should be limited, since outsiders anyway are generally unable to understand the work assigned to the professional experts.[70]

Consequently, in their quest for legitimacy, democratic regimes find themselves having to balance two values that can be in tension: on the one hand a fair, professional and non-politically partisan professional advice and public service delivery and, on the other hand, the responsiveness of public servants to the policies of the current executive.

Neutrality, in the sense of political non-partisanship in public (civil or military) administration, is of course a precondition for ensuring that, regardless of their political orientation, citizens are treated fairly and in an equitable manner and that the public affairs will be addressed with sound know-how and capability. Operationally it is delivered by emphasising professionalism, merit and competence amongst public servants. These values are important as a significant determinant of how much trust citizens may place in their system of government. At the same time, responsiveness of the administration to the government of the day is key to the effective implementation of government policies, and public servants must be accountable to the government for the effective delivery of its political programme.

c) Does professional autonomy include moral dissent?

This core question refers to the difficult issue of how public officials and, more specifically, members of the security forces or the army should react in front of illegal orders or in front of legal, but morally objectionable orders from the hierarchy. Is moral dissent a sufficient ground for blowing the whistle?

This matter is complex, as the notion of morally objectionable orders is ambiguous and equivocal and may be deemed as being too subjective, too dependent on the personal moral sensitivity of an individual. Samuel Huntington, in his much referred to "*The Soldier and the State*" indicates that a soldier cannot surrender his right to make ultimate moral judgements.[71] Beyond that statement, Huntington leaves the matter blurred, without any clear guidance, which may be interpreted as an indication corroborating the complexity of the problem.

It could be argued that expressing dissent in front of what someone considers a morally objectionable order is a moral imperative, in particular "in a business of violence and death", such as the military, or the police, where to remain silent equates to an immoral act and the acquiescing person accepts responsibility for its potential lethal consequences.[72]

Expressing dissent is often referred to as "speaking truth to power", a formulation that may be useful to enervate negative associations with words such as disloyalty, disobedience, insubordination, indiscipline, etc. Speaking truth to power must be done in appropriate ways though. About the implications of speaking truth to power', it is useful and inspiring to revisit *An Enemy of the People* (*En folkefiende*, 1882) by the Norwegian playwright Henrik Ibsen, where he tells the story of Dr. Stockmann, a medical doctor who dares speak up an unpleasant factual truth, urged by what he feels is a moral imperative stemming from his professional duty.

---

[70] See Sundström, G and Premfors, R (2006): *The Limits of Loyalty: Civil Servants' Role Perception within the Swedish Government Office*. Paper presented at International Political Studies Association (IPSA) World Congress in Fukuoka, 9-13 July 2006. RC27: 'Structure and Organization of Government'. Panel RC27.19: 'Core Executives: Change and Dynamics of Central Government Organization'.

[71] Samuel Huntington (1957): The Soldier and the State: The Theory and Politics of Civil-Military Relations. The Belknap Press, Cambrdige.

[72] Jimmy Drennan (2019): *Bad Ideas Have No Rank: The Moral Imperative of Dissent in the Navy*, in US Naval Institute, July 2019 Proceedings Vol. 145/7/1,397. At: https://www.usni.org/magazines/proceedings/2019/july/bad-ideas-have-no-rank-moral-imperative-dissent-navy

Nevertheless, 'speaking truth to power' is not the same as moral dissent. The former may consist simply of comparing a professional truth with other professional truths or opinions. Moral dissent is a more fundamental opposition to a way of action which an individual deems incompatible with an "ethical midfield": doing what is right at all times, regardless of the circumstances.[73] Yet it is easier said than done and it is subject to still unsettled intellectual controversy. Within such a controversy, it can be useful, given the lack of clear ethical guidance on the topic of dissenting of lawful, but immoral orders to rely on three ethical response frameworks entailing different costs, benefits and degrees of risks to those dissenting and to the robustness of the institutional setup:[74]

1. *Dissent through Voice*: Proponents of this framework represent the traditionalist view that rigid obedience is a core and uncompromising value in the military ethos.[75] They also accept the premise that senior military officers are not morally ''co-responsible'' with their civilian bosses for the final decisions on policy, war, and peace. In other words, once civilians approve a final military decision, the liability for the outcome rests fully on their shoulders and not on those of their uniformed counsellors. The traditionalists also believe that civilian leaders, unlike their senior military advisors, have the "right to be wrong" in the sense that they have the constitutional license to contravene the best military guidance and warnings of senior officers, in pursuit of a higher policy considerations, and choose an immoral, and even disastrous, policy. Traditionalists believe that a senior military advisor serves in the role of a trusted, loyal counsel. The officer provides his best military advice—as well as strident dissent, when necessary—through "voice," but does so—particularly for the latter—with discretion and through the proper chain of command. Traditionalists imply that only internal channels are legitimate to whistleblowing.

2. *Resign Quietly*: Advocates for a "quiet resignation" framework assert that senior military (or police) advisors are in fact "co-responsible" for both the decision-making process and its outcomes. Therefore, these military advisors must retain some moral agency over decision-making and are not "mere instruments" of the civilian commander. Dissent should be expressed through "voice" first, but quiet resignation should be used if (and only if) military counsel is not persuasive. In other words, discreet resignation is a last resort. The morality threshold for resignation must be kept remarkably high and mostly limited to weighty decisions to ensure lives are not "wasted" in unnecessary or unwinnable wars, or in state-police promoted violence against the population. "Resignation must be a private affair over principle, not a public affair over primacy. 'Going public' changes the character of the resignation from a matter of principle to a political matter."[76]. Advocates of this quiet voice also seem to imply that only internal channels are legitimate to whistleblowing.

3. *Disobey and Resign Publicly*: Don Snider[77] compares the military profession to others such as medicine, where doctors can refuse medical services that are ''not medically indicated'' regardless of how emphatically the patient may request them. Snider believes that senior officers have their own highly developed internal logic on the proper conduct of the profession

[73] James Mattis (2017): *Memorandum for All Department of Defense Employees*. Subject: *Ethical Standards for All Hands*. Available at https://globalsecurityreview.com/subtext-secretary-mattis-mysterious-memo/ Also at: https://dod.defense.gov/Portals/1/Documents/pubs/Ethical-Standards-for-All-Hands-SecDef-04-Aug-17.pdf

[74] Steven Katz (2020): *Frameworks for Dissent and Principled Resignation in the US Military: A Primer*, in Georgetown Journal of International Affairs. At: https://gjia.georgetown.edu/2020/04/17/frameworks-for-dissent-and-principled-resignation/

[75] The main representative of this line of thought is Richard H. Kohn. His 2009 article summarises this ideology: *Always Salute, Never Resign. How Resignation Threatens Military Professionalism and National Security*, in Foreign Affairs, 10 November 2009. At: https://www.foreignaffairs.com/articles/united-states/2009-11-10/always-salute-never-resign

[76] James M. Dubik (2014): *On principled Resignation: a Response*, in Foreign Policy, 14 October 2914. At: https://foreignpolicy.com/2014/10/14/on-principled-resignation-a-response

[77] Snider, D. M. (2017). *Dissent, Resignation, and the Moral Agency of Senior Military Professionals*, in Armed Forces & Society, 43(1), 5–16. https://doi.org/10.1177/0095327X16657322

of arms. He also believes that acts of disobedience and a public resignation may be required on occasion for the preservation of the profession as a "social trustee," to ensure the military is being used consistently with fundamental societal values and ethical norms. The situations he lists as warranting such measures include civilian leaders directing the military to plan a war of aggression or one that cannot achieve its strategic objectives, thereby needlessly imperilling the lives of civilians and service members. Milburn[78] acknowledges the professional risks associated with disobeying an immoral, but lawful order and complements Snider's position, saying: "*you have to be confident that you are [disobeying] in accordance with the ethics of your profession. And you had better be prepared to face the consequences if you are wrong.*" Milburn provides two examples where he would have refused to obey lawful but immoral orders: 1) the 2003 Coalition Provisional Authority's orders to disband the Iraqi Army and ban former Baathists from employment in the fledgling Iraqi government, and 2) the carrying out of the Bush administration's Enhanced Interrogation Techniques, resembling torture, on suspected terrorists.[79] This stream of thinking seems to advocate for external channels of whistleblowing or, even in some cases, public disclosure of dissent by publicly exposing what one considers wrongdoing.

The United States promulgated regulation DoDI 1325.06 on "Handling Dissent and Protest Activities among Members of the Armed Forces" on 27 November 2009, updated on 22 February 2012. The regulation is aimed at addressing the rights of members of the military to engage in free speech and dissent (i.e. whistleblowing). It spells out the current US military policy on the matter and provides several procedures to be followed regarding dissent and freedom of expression by members of the armed forces. The regulation is rather flawed, as at the end of the day, it makes the right to free expression and dissent depending, in the whole, on the appreciation of individual commanders. This notwithstanding, the fact that a regulation deals with the matter is per se an indication that the issue of dissent and criticism within the armed forces is a growing concern within the military, especially given the high number of former generals that are speaking up once retired.[80]

The mentioned regulation does not seem to be reliable in terms of providing legal protection to dissenters. Lawyers counselling members of the armed forces conclude that "*when planning or considering a particular course of conduct, it is always helpful to consult with a lawyer to find out just what the potential consequences are. We emphasize that what one does is up to the individual, but no one should make decisions rashly or without understanding what risks are being taken. Further, the fact that individual commanders are expected to use their judgment as to what is, or is not, permitted can lead to widely disparate conclusions and policies in different commands*".[81]

Given the unsettled character of these controversies, ministries of defence and of the interior should commission internal reviews to determine how officers serving in their ranks understand obedience, dissent, whistleblowing and principled resignation. Such insight could prove highly informative and valuable on the current state of development of professional autonomy of soldiers and on civil-military relations. Such studies could also shed light on the extent to which human rights are respected and protected by the military and security forces. This would contribute to shaping the "ethical midfield"

[78] Milburn, Andrew (2019): *When do not Obey Orders*, in War on the Rocks, Texas National Security Review; July 8, 2019. https://warontherocks.com/2019/07/when-not-to-obey-orders/

[79] Milburn, Andrew R. (2010): *Breaking Ranks: Dissent and the Military Professional*, at https://www.army.mil/article/47175/breaking_ranks_dissent_and_the_military_professional

[80] Eric A. Hollister (2011): *The Professional Military Ethic and Political Dissent: Has the Line Moved?*, in The Land Warfare Papers nº 83, August 2011. The Institute of Land Warfare. At: https://www.ausa.org/sites/default/files/LWP-83-The-Professional-Military-Ethic-and-Political-Dissent-Has-the-Line-Moved.pdf

[81] NLG Military Law Task Force, 25 May 2017. https://nlgmltf.org/; Article available at: https://couragetoresist.org/lawyers-explain-military-policies-dissent/

mentioned by the Mattis' memorandum. These insights could also serve as a groundwork to future national security decision-making.

More deeply, it is useful here to retrieve the idea that the capacity to resist illegal or unethical orders is an act of civilisation, of human rationality and stems from a rational sense of justice. As Niebuhr, echoing the Kantian moral imperatives, puts it, "growing rationality is a guarantee of man's growing morality".[82]

8. Dealing with Unlawful Superior Orders

a) Mindless obedience is perilous for society

Before going into a more practical discussion, we may want to consider the human nature about obedience as a conceptual framework defining power relationships. The psychological Milgram experiments conducted by American psychologist Stanley Milgram between 1960 and 1963 in coincidence with the Eichmann trial in Jerusalem (and replicated with consistent results several times since, including by Polish researchers in 2016-17) show a strong propensity of ordinary and decent human beings to obey superiors' orders even if those orders imply unjustly harming someone else (i.e. committing a crime).[83]

The Milgram experiment leaders instructed participants to obey an authority figure who ordered them to perform acts conflicting with their personal conscience and moral values. The experiment found that a remarkably high proportion of people were prepared to obey, albeit unwillingly, even if apparently causing serious injury and distress to others. It also showed that only a small proportion of adult humans are ready to resist heroically. Milgram first described his research in 1963 in an article published in the *Journal of Abnormal and Social Psychology*[84] and later discussed his findings in greater depth in his 1974 book, *Obedience to Authority: An Experimental View*.[85]

Milgram summarized the experiment in his 1973 article, "*The Perils of Obedience*", writing: "The legal and philosophic aspects of obedience are of enormous importance, but they say truly little about how most people behave in concrete situations. I set up a simple experiment at Yale University to test how much pain an ordinary citizen would inflict on another person simply because he was ordered to by an experimental scientist. Stark authority was pitted against the subjects' [participants'] strongest moral imperatives against hurting others, and, with the subjects' [participants'] ears ringing with the screams of the victims, authority won more often than not. The extreme willingness of adults to go to almost any lengths on the command of an authority constitutes the chief finding of the study and the fact most urgently demanding explanation. Ordinary people, simply doing their jobs, and without any particular hostility on their part, can become agents in a terrible destructive process. Moreover, even when the destructive effects of their work become patently clear, and they are asked to carry out actions incompatible with fundamental standards of morality, relatively few people have the resources needed to resist authority".[86]

---

[82] Reinhold Niebuhr (1932): Moral Man and Immoral Society. A Study in Ethics and Politics. Westminster John Knox Press, Louisville, Kentucky and London (Page 27).
[83] http://www.spsp.org/news-center/press-releases/milgram-poland-obey
[84] Milgram, Stanley (1963). "*Behavioral Study of Obedience*" in Journal of Abnormal and Social Psychology. 67 (4): 371–8. PMID 14049516. doi:10.1037/h0040525
[85] Milgram, Stanley (1974). Obedience to Authority: An Experimental View. Harpercollins.
[86] Milgram, Stanley (1973): "*The Perils of Obedience*". Harper's Magazine. Available, among others, at https://is.muni.cz/el/1423/podzim2012/PSY268/um/35745578/Milgram_-_perils_of_obediance.pdf

The same line of thought is to be found in some key pieces of Balkan contemporary literature such as the 2004 "*They Would Never Hurt a Fly: War Criminals on Trial in The Hague*" by Slavenka Drakulic where the Croatian journalist cum novelist gives an account, resembling and describing the "banality of evil", as coined by Hanna Arendt, on the personalities of the war criminals on trial in the Hague that destroyed the former Yugoslavia.

To protect public employees' ability to resist in situations where they receive an unlawful or unethical order from the superior has been the object of numerous philosophical research since the classical Greek philosophers such as Plato and Aristotle and Latin authors such as Cicero all along the way to the Western Middle Ages through Albert the Great (1200-1280) and Thomas of Aquinas (1225-1274). Their basic idea was that natural law was prevalent over positive law or, otherwise said, that human rationality was prevalent over the whims of a particular ruler.

These ideas gained special importance during the Nuremberg War Crime Trials, [87] the Tokyo trials[88] and the Frankfurt trials[89] when many indicted war criminals invoked compliance with "superior orders" as the excuse in their defence. In the trail of the Nuremberg trials the line of German case law, known as the *Mauershützenprozessen* in the aftermath of the Germany's unification, reiterated the principle that following orders is not a sufficient legal excuse to relieve personal criminal liability. This legal doctrine is also to be found in the Adolf Eichmann trial in Jerusalem (1961). The justification of this doctrine is based on the philosophy of law. It comes from the notion of natural law from Aristotle, Albert the Great and Aquinas and, since the Nuremberg trials, from the well-known Gustav Radbruch above-mentioned formula, which in a nutshell reads: an extremely unjust law is not law. Therefore, such a law is not valid law and is not binding on anyone.

Later on, this line of philosophical reasoning evolved, through an all pervasive human rights development originated in the UN Universal Declaration of Human Rights (UNUDHR), to include the notion of human dignity in the equation: Courts use now the concept of dignity to give meaning to rights, to connect rights, to extend rights, to create new rights and to weigh rights against each other.[90] Dignity has thus become a tool through which courts define, order and extend rights.

From this standpoint, the human right to dignity confers the right to a public employee to refuse compliance with instructions going against his conscience, moral values or ethical convictions. At the same time, from the perspective of causing no harm to others or to the public interest, a public employee has the obligation to refuse compliance with instructions departing from this perspective. This understanding is nowadays part and parcel of widely accepted Western philosophical values.

[87] During the Nuremberg trials, which were conducted in accordance with the rules of the London Charter of the International Military Tribunal, it was found that a superior's order does not relieve officers from criminal responsibility, but that is may be a ground for reduction of sentence. L.C. Green, *Superior Orders in National and International Law*, (A. W. Sijthoff International Publishing Co., 1976.

[88] The International Military Tribunal for the Far East (IMTFE), also known as the Tokyo Trial or the Tokyo War Crimes Tribunal, was a military trial convened on April 29, 1946, to try the leaders of the Empire of Japan for joint conspiracy to start and wage war (categorized as "Class A" crimes), conventional war crimes ("Class B") and crimes against humanity ("Class C").

[89] The Frankfurt Auschwitz trials, known as *der Auschwitz-Prozess*, or *der zweite Auschwitz-Prozess*, i.e. the "second Auschwitz trial", was a series of trials running from 20 December 1963 to 19 August 1965, charging 22 defendants under German criminal law for their roles in the Holocaust as mid- to lower-level officials in the Auschwitz-Birkenau death and concentration camp complex. The German Prosecutor, Fritz Bauer (1903-1968), was instrumental in those trials.

[90] See Christopher McCrudden (2008): *Human Dignity and Judicial Interpretation of Human Rights*, in The European Journal of International Law, Vol. 19 no. 4, pages 655-724. Available at http://www.ejil.org/pdfs/19/4/1658.pdf

b) From values to rules and practice

Although the rules of conduct for acting on superior orders are stated in the civil service legislation and in military and police regulations in many European and OECD countries, they are not easily implemented in practice. While the legislation contains the basic provisions on acting on orders by managers, it is vague and ambiguous as to how to perform in practice in particular situations.

In such situations, civil servants and military personnel are faced with two main dilemmas. The first one relates to the already mentioned fear of the superior's resentment, which may result in getting unfavourable performance assessments, lack of promotion, and even job loss, if the public official does not fulfil the order or the instruction of his/her superior. The second dilemma is reflected in the fear of criminal liability, and therefore being jailed and losing the job if he/she does comply with the order or instruction.

In accordance with many existing legal frameworks, public officials confronted to an illegal (or ethically questionable) order from their superiors, should first warn the superior that the order is unlawful and request a written order. However, it is very unlikely that the superior will easily issue the written order. Therefore, the subordinate may face the dilemma of how to proceed. Without a written order by the superior, subordinates are not protected from disciplinary or criminal liability. Public officials should consider whether fulfilling the order of the superior would constitute a criminal offense in accordance with the national legislation. If the conduct in question contains any elements of a criminal offense, such as, for example, the broadly defined criminal offence of "abuse of office", "torture", "embezzlement" or "murder", public officials should not only refrain from the requested behaviour, but also notify the head of the authority or the judicial institutions about the incident.

It is worth pondering the following question: How a public official and his/her superior, if enmeshed in a situation of confronting illegal orders, should behave? Are there any institutional solutions beyond personal heroic immolation?

The issue of the unlawful superior's order should be addressed as an institutional problem, not merely as an individual one. The reason is that the implementation of the principle of legality, the fundamental loyalty of the public official to the legal order of the country and the respect for human rights are institutional commitments of any public administration ruled by law and democratic, often established in national constitutions and binding international treaties. They are not obligations affecting only the individuals acting within the institution. The whole institution (and the state of which it is a part) is committed to respect legality, ethics standards and human rights, including the respect for dignity.

To ensure that public officials are able to abide by the rule of law, avoid disciplinary liability and provide adequate evidence in case of potential disciplinary or legal proceedings, it would be best (if it is not already provided for in the national legislation) that the senior management at the institutional level adopts guidelines for public officials on how to behave in the event that the immediate superior, or even the senior command, requires them to act in accordance with an order or an instruction that is not in compliance with the regulations or the ethical values. These guidelines could address, for example, the following issues:

1. A public official, civilian or military, in the event that he/she considers that acting in accordance with the instruction or order of the superior would be in breach of regulations or the ethical principles, is under the obligation to request, while putting on hold its fulfilment, that the instruction or the order is submitted to him/her in writing, indicating who and when ordered him/her to act in such a manner. A copy of such written instruction shall be forwarded simultaneously to the HR department (if it does exist) and to the higher command of the institution, along with the comments or critical observations by the incumbent public official.

2. The guidelines should establish a short timeline for the response by the immediate superior or the senior command of the institution to the public official's request (in terms of delivery of the written instruction or order). The exclusive argument of authority should not be admitted in that response, which must be reasoned in terms of facts and law. The reason is that instructions to subordinates shall be non-arbitrary and rational, i.e. based in human reason and because what is precisely questioned is the rationality or legality of the instruction reputed to be unlawful, arbitrary or unethical. A superior must not expect mindless obedience from a subordinate if the human dignity of this latter is to be protected.
3. The guidelines should spell out the obligation of the public official to prepare written records, with the written requests and instructions (if submitted by the superior) attached. The records should contain the signature of the person who wrote the records, in addition to the date and detailed description of the specific situation, indicating the reasons for refusing to act in accordance with the superior's instruction or order.
4. A question may be raised on whether the public official is under the obligation to inform the senior command about his/her refusal to act. In these situations, it would be reasonable that the public official informs the official who is his/her immediate superior's superior about the situation in writing. The regulations should establish that obligation on public officials. This would allow also timely implementation of appropriate measures by the senior command towards the lower-level management that has acted unlawfully in carrying out their duties and powers. However, in some situations, the immediate superior may refer to an order of the senior command, which may be false, so that this solution would ensure also that the head of the institution is notified about the new situation, considering that he/she is responsible for the legality of its operations.
5. In addition, it should be underlined that a difficulty could arise in practice: the insufficient knowledge of the criminal law provisions or of the fundamentals of human rights by public officials. Therefore, it is possible that officials are not aware that their conduct constitutes a criminal offense or may represent a violation of human rights. That is why it is necessary to ensure continuous counselling, education and training of civil servants, police officers and military personnel in democratic values, human rights, ethics, accountability mechanisms and whistleblowing.

Internal guidelines can help addressing the above issues. Commanders should take measures to prevent unlawful activities of their subordinates. That can be facilitated by written guidelines to be followed under their direct control. The written guidelines detailing how to act in specific situations when there is a possibility of unlawfulness would reduce the sharpness of the illegal orders' dilemma for all participants in public administration (managers, subordinates and the external or internal observers of the public behaviour) and military and security settings. Although those guidelines may or may not be legal acts, all public officials can benefit from abiding by them.

A useful approach to this problem of how to deal with illegal instructions or ethically questionable requirements by hierarchical superiors, would be to create a counsel or internal complaints mechanism, which could be established within the Human Resource Management departments, where they exist. The role of these units would be to provide advice, orientation and act as eyewitnesses in case of future legal conflict between the institution and a given public official. These units should also act as a checks and balances instrument to refrain superiors from dictating illegal or ethically dubious instructions to subordinates. Legislation should also foresee, as in the case of retaliation on whistle-blowers, sanctions on those commanders who knowingly dictate illegal orders.