NOTIONES

Intelligence Ethics

Whitepaper

Author: Giulia Venturi, Zanasi & Partners
January 2024

DOI: 10.5281/zenodo.10389801

Table of Contents

Project Introduction: NOTIONES

Novel technologies have presented practitioners with new opportunities to improve the intelligence process, but have also created new challenges and threats. Consequently, the timely identification of emerging technologies and analysis of their potential impact, not only on the intelligence community but also on terrorist or criminal organisations, is crucial.

However, time constraints can prevent intelligence practitioners from being updated on the most recent technologies.

In order to address this challenge NOTIONES will establish a network, connecting researchers and industries with the intelligence community. This network will facilitate exchange on new and emerging technologies but also equip solution providers with insights on the corresponding needs and requirements of practitioners. The so gained findings will be disseminated in periodic reports containing technologic roadmaps and recommendations for future research projects and development activities.

The consortium of NOTIONES includes, among its 29 partners, practitioners from military, civil, financial, judiciary, local, national and international security and intelligence services, coming from 9 EU Members States and 6 Associated Countries. These practitioners, together with the other consortium members, grant a complete coverage of the 4 EU main areas: West Europe (Portugal, Spain, UK, France, Italy, Germany, Austria), North Europe (Finland, Denmark, Sweden, Estonia, Latvia), Mittel Europe (Poland, Slovakia, Ukraine), Middle East (Israel, Turkey, Georgia, Bulgaria, Greece, North Macedonia) for a total of 21 countries, including 12 SMEs with diverse and complementary competences.

Project Objectives

GATHER the needs of intelligence and security practitioners related to contemporary intelligence processes and technologies;

PROMOTE interaction of technology providers and academy with intelligence and security practitioners;

IDENTIFY novel technologies of relevance for practitioners through research monitoring;

PUBLISH a periodic report, summarising key findings in order to orientate future research and development;

ENSURE the commitment and involvement of new organisations in the pan-European NOTIONES network.

Project Introduction: NOTIONES

Project Facts:

Duration: **60 Months** Reference: **101021853**

Programme: **Horizon 2020 SU-GM01-2020 Coordination and Support Action**

Coordinator: **FUNDACION TECNALIA RESERACH & INNOVATION (Spain)**

Scientific Technical Coordinator: **ZANASI ALESSANDRO SRL (Italy)**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101021853.

Coordinator	Scientific Technical Coordinator	Project Security Officer
tecnalia	Zanasi & Partners Security Research and Advisory	

Academic | Think-Tanks | Research

Technology Providers

Practitioners

1. Background and definitions

The Intelligence community has an unquestionable role in pursuing the security of citizens and Nations.

Due to the nature of the profession, intelligence practitioners obtain information using both overt and/or covert operations. They are sometimes encouraged by their agencies to use tactics (e.g. lie, deceive, steal, manipulate…) that could be categorised as "unethical" in an ordinary situation in order to obtain information. Some of these operations breach ethical standards, sometimes even resulting in deliberately violating fundamental human rights. Nevertheless, this can be perceived as ethically acceptable when national security is at risk [1]. Ethical dilemmas are therefore a constant trait of the intelligence profession and can generate much public controversy when certain operations become public – consider as examples mass surveillance of citizens over social networks or torture and inhumane degrading treatment for the purposes of HUMINT intelligence collection [2].

In addition to this, it can happen that an intelligence practitioner comes into possession of information of such seriousness that he or she considers the possibility of disseminating it, for example in the name of democracy or human rights, sometimes leading to scandals even at an international level (e.g. leak of confidential information, as in the Snowden case). Indeed, practitioners should stay within the law and be loyal to their agency, but they should also fight for the truth by keeping integrity [3].

Therefore, everyday Intelligence practitioners have to make choices based on what is wrong and what is right - with respect to law, their conscience, the code of professional conduct, the indications of their agency, the possible consequences of such choices or actions, and many other aspects.

Ethics is the discipline concerned with what is morally good and bad and morally right and wrong [4], that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues [5]. As such, ethics is a branch of philosophy.

The points of contact between ethics and **lawfulness** are various. In human history, however, there have been many cases in which law has not followed morality, as for example in the case of the Nuremberg laws of 1935 in Germany or the Italian racial laws of 1938. On the other hand, there are many cases in which man has refused the right in order to follow his own ethics. This is the case of conscientious objection which appears to be a behaviour with very ancient origins in human history. In fact, Sophocles already underlined the eternal conflict between human law (juridical act) and divine law (reflection of conscience) and how one of the two could dominate the other in its tragedy Antigone in 441 BC [6].

The ethical values of law are based above all on **human rights**, i.e. those values given by what are considered right. Human rights began to be talked about extensively after the Second World War, with the *Universal Declaration of Human Rights* (UDHR, 1948). In the European Union, the *Charter of Fundamental Rights of the European Union* (CFR, 2000) depicts the political, social, and economic rights for EU citizens and residents, based on the principles of Dignity, Freedom Equality, Solidarity and Justice.

As stated in the CFR Article 52, *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others"*. Indeed, legislation that allows limitations to fundamental rights needs to strictly comply with the ethical principles of proportionality and necessity.

Necessity is a fundamental principle when assessing the restriction of fundamental rights. Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. **Proportionality** is a general principle of EU law. It restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim. More specifically, proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right. In other

1. Background and definitions

words, the limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure. A pre-condition is that the measure is adequate to achieve the envisaged objective [7].

It is now essential to investigate the concept of national security and to consider its use as a justification for state action, including cases in which, under the banner of alleged national security interests, different purposes are pursued to the detriment of fundamental rights and democracy.

The concept of **security** is used in different contexts where its scope varies depending on the threats in question. It can be distinguished in external security (relative to threats originating outside a Country's territory), internal security (relative to all threats to people's safety in a Country or region), and global security (relative to transnational threats).

The European Council characterises **internal security** as *"protecting people and the values of freedom and democracy, so that everyone can enjoy their daily lives without fear" [8]. The Council lists the main threats to internal security as "terrorism, serious and organised crime, drug trafficking, cybercrime, trafficking in human beings, sexual exploitation of minors and child pornography, economic crime and corruption, trafficking in arms and cross-border crime" as well as "violence itself, natural and man-made disasters" and "other common phenomena which cause concern and pose safety and security threats to people across Europe, for example road traffic accidents".*

National security has a more restricted scope than internal security, covering cases where a Nation's fundamental interests are harmed or threatened in terms of territorial integrity, political, terrorism, violent subversion, but possibly also their sovereignty and ability to police their territory [9].

The concepts of national security, human rights, lawfulness and ethics of Intelligence activities described so far apply to Intelligence practitioners, especially field operatives. But there is another type of practitioners – Intelligence analysts – that deals with another form of ethical dilemma. The core values of Intelligence agencies in the West are strictly related to the concept of **Integrity**, in turn strictly related to honesty, trustworthiness, accountability, transparency, and avoidance of prejudice. Intelligence analysts should therefore adhere to a code of conduct that prescribes to analyse and report information in the most unbiased manner possible, refraining to put personal considerations in their analysis, reporting "bad news" clearly and early despite desiring not to have to, and ultimately telling the truth.

In addition to this, ethical questions in Intelligence analysis may be a matter of **"Right vs Right"**, instead of "Right vs Wrong". If a Military Intelligence analysts sees an IMINT satellite image depicting operational enemy ballistic missiles that threaten National security, there is no ethical dilemma: the information must be passed on to higher authorities. To hide, purposely misinterpret, or ignore the information would be wrong. This is a case of "Right vs Wrong". But if, upon further inspection, one of the missiles appears to be a decoy, the analyst is now faced with an ethical dilemma: are there more decoys? Maybe all missiles are decoys? And why? Should the report be suspended until more detailed information is obtained? How long? This is a case of "Right vs Right" [10]. Some authors argue that intelligence officers are constantly presented with **moral hazard** in their profession [11]: simply put, *"due to power and information asymmetries, intelligence officers are put in position in which actors do not share the same benefits and risks. In other words, intelligence agencies can create negative externalities for which their officers are not held accountable for due to their obligations towards the national interest."* [2]

Additionally, as already mentioned in the beginning, Intelligence practitioners may have to face difficult ethical dilemmas when their code of professional conduct or their agency's indications are in conflict with what they believe in conscience to be right or wrong.

2. Ethical issues in Intelligence activities

Ethical approaches and code(s) of ethics for the Intelligence community

There are four main approaches to studying ethics applied to Intelligence in the current literature: realism, consequentialism, idealism, and the "just intelligence" theory:

- Within the realist approach, intelligence activities are justified if they serve the well-being of the state and rest on the moral duty of the Head of State to protect their citizens. According to this approach, governments are entitled to do anything for the purposes of national security, and when an intelligence officer engages in what is generally considered unethical behaviour these actions are not considered unethical because they are all necessary for national security [1]. *"It was argued by Stansfield Turner, former Director of the Central Intelligence, that "...the overall test of the ethics of ... intelligence activities ... is whether those approving them feel they could defend their actions before the public if the actions became public"* [12].

- Within the consequentialist approach - or Utilitarian Approach - the ends are perceived are more important than the means, actually the means are judged based on their consequences. According to the consequentialist approach, Intelligence activities are acceptable if they maximize the "good" through balancing the benefits of increased knowledge against the costs of how it might have been acquired – with obvious considerations about the fact that a single event or fact may be "good" for a certain entity, and "bad" for another one [1]. Under a utilitarianism system, secrecy and deception would pose no barrier to action, provided that the desired outcome was successful. Some may argue that although this system is more applicable to intelligence operations, its application in practice could be used to justify torture, and assassination. *"It is against the Turner Test previously mentions that utilitarian intelligence operations fail"* [12].

- Whitin the idealist approach - also referred to as deontological approach - morality is regarded as an absolute concept, with no exceptions. According to this approach, activities like deception and covert operations are considered morally unethical and should thus be avoided [1]. The inappropriateness of this approach can be demonstrated by considering the case of a government being alleged to have eavesdropped on the telephone calls of a Foreign President's family. If honesty was expected of the intelligence community under this doctrine, then an admission or denial would have been required (based on whichever was accurate).

But the governments' policy is not to comment on intelligence operations because any comments could undermine agencies' ability to conduct effective operations. As such, this case is a simple demonstration where the universalism of the virtue of honesty is not appropriate [12].

- Within the "just intelligence" approach, structured reasoning is used to distinguish between the conditions under which an object can justly be targeted by an intelligence agency and the manner in which intelligence agents and entities conduct themselves thereafter. This approach is the Intelligence parallel of the "just war" approach: in war times, military professions are exempt from ordinary laws as they have the right to use covert methods to obtain information from a national threat and also have the right to kill, but the same actions would be considered illegal and highly unethical in peace times [1].

The just intelligence is commonly accepted as the most reasonable way of addressing the ethics–intelligence dilemma, as resembled also in the related legislation around Intelligence in the EU Countries. Nevertheless, actions driven by just intelligence may be so reprehensible that governments may still need to hide or disguise them so to avoid public backlash, even if, under just intelligence approaches, these actions would be perfectly sound and justifiable [2].

2. Ethical issues in Intelligence activities

Still, apart from legislation, the Intelligence Community also benefits from code(s) of ethics to be followed in their profession. For example, already in the 2000s' the South African Intelligence Services issued the "Five principles of intelligence service professionalism" [13]. These flow directly from the Constitutional provisions and prescribe that Intelligence practitioners:

- do not stand above the law;
- are accountable to the executive and Parliament;
- accept the principle of political non-partisanship;
- owe their loyalty to the Constitution, our people and the state;
- appreciate that they must maintain high standards in the performance of their functions.

Bulgaria also applied the Ethical Code of Behaviour for Civil Servants to members of the intelligence services in 2000.

In 2010, the Geneva Centre for the Democratic Control of Armed Forces (DCAF) reported the *"Compilation of Good Practices for Intelligence Agencies and their Oversight"* [14] to the UN Human Rights Council. The report presented 35 areas of good practice grouped into four different "baskets", namely legal basis, oversight and accountability, substantive human rights compliance and issues relating to specific functions of intelligence agencies.

Bailey & Galich [15] reported in 2012 on the results of a workshop which highlighted the core principles of such code(s) as: integrity, accountability, respect, excellence, loyalty, trustworthiness, truthfulness, objectivity, credibility, self-control, and many others.

The U.S. Office of the Director of National Intelligence (ODNI) issued in 2014 the *"Principles of Professional Ethics for the Intelligence Community"* to serve public-facing and internally-focused purposes [16]. They reflect the core values common to all elements of the Intelligence Community and distinguish the officers and employees of the IC as "intelligence professionals."

The principles – Mission, Truth, Lawfulness, Integrity, Stewardship, Excellence and Diversity – reflect the standard of ethical conduct expected of all Intelligence Community personnel, regardless of individual role or agency affiliation (see Figure 1).

2. Ethical issues in Intelligence activities

MISSION We serve the American people, and understand that our mission requires selfless dedication to the security of our Nation.

TRUTH We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively.

LAWFULNESS We support and defend the Constitution, and comply with the laws of the United States, ensuring that we carry out our mission in a manner that respects privacy, civil liberties, and human rights obligations.

INTEGRITY We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the Intelligence Community at large.

STEWARDSHIP We are responsible stewards of the public trust; we use intelligence authorities and resources prudently, protect intelligence sources and methods diligently, report wrongdoing through appropriate channels; and remain accountable to ourselves, our oversight institutions, and through those institutions, ultimately to the American people.

EXCELLENCE We seek to improve our performance and our craft continuously, share information responsibly, collaborate with our colleagues, and demonstrate innovation and agility when meeting new challenges.

DIVERSITY We embrace the diversity of our Nation, promote diversity and inclusion in our work force, and encourage diversity in our thinking.

Figure 1 - Principles of Professional Ethics for the Intelligence Community (ODNI, [16])

In many other Countries, there is no specific code of ethics for intelligence agencies, rather there is a more general code of conduct that the intelligence community adheres to - that of the Public Services. Unfortunately, these codes are generic, tailored for no specific profession, and therefore not entirely appropriate for intelligence personnel.

In some cases, codes exist within the professional registers of Intelligence practitioners, for example the Australian Institute of Professional Intelligence Operators (AIPIO) [17].

The Committee of Ministers of the Council of Europe issued a recommended Code of Conduct for Public Officials in 2000 [18], which in Article 4 states that *"the public official should carry out his or her duties in accordance with the law, and with those lawful instructions and ethical standards which relate to his or her functions"*, but such ethical standards or ethical values are not explicated in the document, or obviously are explicated the specific ethical values appropriate for the Intelligence Community. Indeed, the Code of Conduct for Public Officials could be not effective related to intelligence practitioners.

3. Mass surveillance and OSINT ethical issues

Surveillance is defined as *"the monitoring of the behaviour, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them"* [19], and as such it is a form of Intelligence gathering.

In 2014 Edward Snowden, a National Security Agency (NSA) contractor, released to the public a large amount of confidential data from the NSA and revealed mass surveillance programs conducted by the NSA and its partners over the last years, exploiting mainly Big data analytics techniques[1]. This raised socio-political concerns over the transition of democracies towards surveillance states, and over possible predictive policing and pre-emptive justice [2]:

- big data exploitation generates new inequalities, because there is a disadvantage between the watchers and the watched, limiting the watched' knowledge and autonomy;
- the urgency of protection from mass surveillance leads to enhancement of privacy-by-design technologies, that make legitimate surveillance and intrusion more difficult;
- big data collection and exploitation are mostly run by algorithms that may be trained using biased data, have non transparent computation methods, and in general may not be trusted to be "ethical";
- big data analytics without a proper contextualisation can produce distorted results;
- the data leak did considerable institutional damage, reasonably caused harm to national security, and exposed NSA's methods.

It is important to remember that NSA's actions were not made under a regime of complete illegality, as it has received legal legitimation through the 2008 Amendment Act to the U.S. Foreign Intelligence Surveillance Act. In addition to this, targets may all have been legitimate since they explicitly gave their consent for their information to be shared when they signed up on Facebook, Gmail and similar websites and services, and hence they may have voluntarily give up any right to privacy.

Indeed, another issue is that *"the mere fact that some information is public does not mean privacy concerns should be discarded entirely. Moreover, modern OSINT techniques can aggregate several chunks of information and identify physical persons even when each element comes from anonymous sources (profiling)."* [20]

The evidence seems to suggest that, if this mass surveillance truly had unethical traits, then whistleblowing may represent the last safeguard against it. However, *"in intelligence, this is a behaviour that most likely equates to treason: the lack of possibilities to denounce abuses in intelligence provides then no incentives to curb excesses. This severely damages democratic institutions in terms of accountability"* [2].

As a good thing, Snowden's revelations opened an opportunity and a wake-up call for public discussion on intelligence ethics. It is not a case that soon after, the EU published the General Data Protection Regulation (GDPR) [21] and the Law Enforcement Directive (LED) [22]. The European Commission also announced the adoption of a series of initiatives on artificial intelligence (a branch of Big Data analytics): the High-Level Expert Group on Artificial Intelligence (AI HLEG) was created to develop a set of ethical guidelines, published in April 2019 under the name of Ethics Guidelines for Trustworthy AI [23], and the EU Artificial Intelligence Act (AIA) [24] was proposed in 2021.

[1] This umbrella term encompasses a series of technologies, practices and services that consist in collecting, pre-processing, storing and analysing huge amounts of data – both structured and unstructured – basically in real time. Today's importance of Big Data is made even more disrupting by the daily usage of internet-based technologies, social networks and online retail services, that basically feed on the mentioned data. The amount of actionable intelligence that can be gathered by making use of Big Data related technologies is enormous and the scope of application depends only on the user.

3. Mass surveillance and OSINT ethical issues

In addition to this, the European Union Agency for Fundamental Rights (FRA) issued two volumes in 2017 titled *"Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU"*, and updated them in 2023 [25]. These volumes are more focused on legislative framework and oversight on the activities of national Services, rather than on ethics. Indeed, the 2017 report highlighted that fundamental rights related to the respect for private and family life, the protection of personal data and an effective remedy and a fair trial of the Charter of Fundamental Rights of the European Union should be protected by setting up strong oversight systems and effective remedies open to individuals in the context of surveillance by intelligence services. The 2023 update describes the developments that have taken place since 2017 in intelligence laws in the European Union.

In 2017, FRA concluded that protecting the public from security threats while respecting fundamental rights can be achieved through strong oversight systems and effective remedies open to individuals. This conclusion remains valid in the 2023 report.

These norms should provide high explicitness about what the regulations are about and the ways in which actors understand them. In other words, it should be very few ways to interpret the rules: *"The more precise and detailed the surveillance rules are, the smaller the window for arbitrary official actions is"* [26].

4. Functional guarantees in selected EU countries and National securiaty exceptionalism

As a result of CFR Article 52, in many EU Countries the National Intelligence services benefit from so-called "functional guarantees". These represent the power of special agents to deliberately violate the law in order to get to the result. For example, the Italian law 124/2007 [27] provides for a specific procedure: with the prior authorization of the Italian Prime Minister, the agents of the Intelligence services can be authorized to commit crimes – obviously with limitations. In detail, the agents of the Italian Intelligence Services are not criminally liable provided that their conduct:

- is indispensable and proportionate to the achievement of the objectives of the operation, which cannot be pursued in any other way;
- is the result of a comparison of the public and private interests involved cause the least possible damage to the affected interests;
- does not constitute crimes aimed at endangering or harming the life, physical integrity, individual personality, personal freedom, moral freedom, health or safety of one or more persons, or crimes against the administration of justice, or crimes against constitutional bodies or against regional assemblies, against the political rights of the citizen as well as other crimes expressly provided for by law;
- is not carried out in the offices of political parties represented in Parliament or in a regional assembly or council, in the offices of trade union organizations or in relation to professional journalists.

Similarly, in France the law of July 24, 2015 [28] provides a legal framework for the French intelligence practices. The law aims both to give resources to the intelligence services and to guarantee the protection of public freedoms by subordinating the use of surveillance measures to the authority of political power and to a double control, that of an independent authority, the National Commission for the Control of Intelligence Techniques, and that of the Council of State.

The law provides that the intelligence services may be authorized by the Prime Minister to implement techniques intended to collect information for the purposes exhaustively listed. The techniques implemented can be telephone tapping, image capture in a private place, computer data capture. A specific decision may also authorize the entry into a private place, including the dwelling, in order to install or remove a beaconing or recording device. The purposes that may justify the implementation of these techniques are as follows:

- national independence, territorial integrity and national defence;
- major interests of foreign policy, execution of France's international commitments and prevention of any form of foreign interference;
- major economic, industrial and scientific interests of France;
- prevention of terrorism;
- prevention of attacks on the republican form of institutions, actions aimed at maintaining dissolved groups, prevention of collective violence;
- prevention of organized crime and delinquency;
- preventing the proliferation of weapons of mass destruction.

The law of October 30, 2017 [29] strengthening internal security and the fight against terrorism established a new legal regime for the surveillance

4. Functional guarantees in selected EU countries and National securiaty exceptionalism

of communications. The French intelligence services can intercept and exploit communications using exclusively channels which do not involve the intervention of an electronic communications operator within a legal framework provided with guarantees.

In Spain, the Law 2/2002 [30] states that the Secretary of State Director of the Spanish National Intelligence Center must request to the competent Supreme Court Magistrate the authorization to adopt measures that affect the inviolability of the home and the secrecy of communications, provided that such measures are necessary for the fulfilment of the functions assigned to the Center. The request for authorization must contain the following:

- Specification of the measures requested;
- Facts on which the request is based, purposes that motivate it and reasons that advise the adoption of the requested measures;
- Identification of the person or persons affected by the measures, if known, and designation of the place where they are to be carried out;
- Duration of the measures requested, which may not exceed twenty-four hours in the case of affecting the inviolability of the home and three months for the intervention or interception of postal, telegraphic, telephone or any other type of communication, both periods extendable for successive equal periods if necessary.

The Magistrate will decide, by reasoned resolution within a non-extendable period of seventy-two hours, the granting or not of the requested authorization. Said term will be reduced to twenty-four hours, for reasons of urgency duly justified in the request for authorization from the Secretary of State Director of the National Intelligence Center which, in any case, will contain the details previously specified.

The Magistrate will arrange what is appropriate to safeguard the confidentiality of his actions, which will be classified as secret. The Secretary of State Director of the National Intelligence Center will order the immediate destruction of the material related to all information that, obtained through the authorization provided for in this article, is not related to the object or purposes thereof.

In Germany, the Law BND-Gesetz (BNDG) of 1990 [31] regulates the organisation, tasks and powers of the German foreign intelligence service. This law was extensively amended by the law on Foreign-Foreign Telecommunications Intelligence of the Federal Intelligence Service of 2016 [32]. With it, the legal basis for the foreign-foreign telecommunications reconnaissance of the Federal Intelligence Service was specified and new control rights were introduced. On May 19, 2020, the Federal Constitutional Court declared the amendments to the BNDG made by this law to be largely unconstitutional, since they violate the fundamental rights of telecommunications secrecy and freedom of the press.

From these examples throughout the European Union it is evident that in the field of Intelligence the line between what is ethically acceptable and what is not is still the subject of discussion, not only on a philosophical level, but also on a legislative level.

Some of the scandals and case-law originate from the excessively expansive use of the notion of national security, which is the main driver of the "exceptionalism" that is granted to state action. *This "exceptionalism" should not be understood as the ability to suspend the rule of law (and the law itself) so as to preserve a national community, as would be possible under an authoritarian interpretation of the principle that "the safety of the people is the supreme law." It is rather to be understood as the possibility of restricting the scope of certain fundamental rights no more than is necessary to preserve a democratic community (whose preservation includes maintaining*

4. Functional guarantees in selected EU countries and National securiaty exceptionalism

its democratic institutions and the rights of its citizens) from serious risks, and doing so within a legal framework. [33]

Regarding this, a consideration proposed by Cantarella [2], in turn citing Agamben [34], appears particularly suited:

> *"Can exceptions to the law exist? As Giorgio Agamben argued, every constitution envisions clauses for a state of exception. What Agamben argues it that every political systems embeds in its constitution some kind of self-destruct mechanism that enables the same rights expressed in the constitution to be suspended or diminished, in the event of supposed national crisis. This means that, in case of emergencies, legal limits to intelligence are usually circumvented easily.*
>
> *The national interest apparently still takes priority over laws.*
>
> *However, this mechanism is regarded as intrinsically dangerous. As Agamben argues, a prolonged state of exception leads to nothing short of a totalitarian system, an oxymoronic "permanent state of exception". While intelligence agencies have been known to break the law or infringe constitutional rights for the sake of the national interest, it would be insane to assume that intelligence agencies can invoke this clause as much as they want. As we already argued, intelligence is a continuous process: therefore, it cannot operate in a continuous state of exception from the law. Exceptions can take place, but they have to be exceptions, literally. Intelligence needs clear and well-defined boundaries that are always valid. And, still, the existence of exceptions does not make the acts of agencies made under a "state of exception" less morally questionable."*

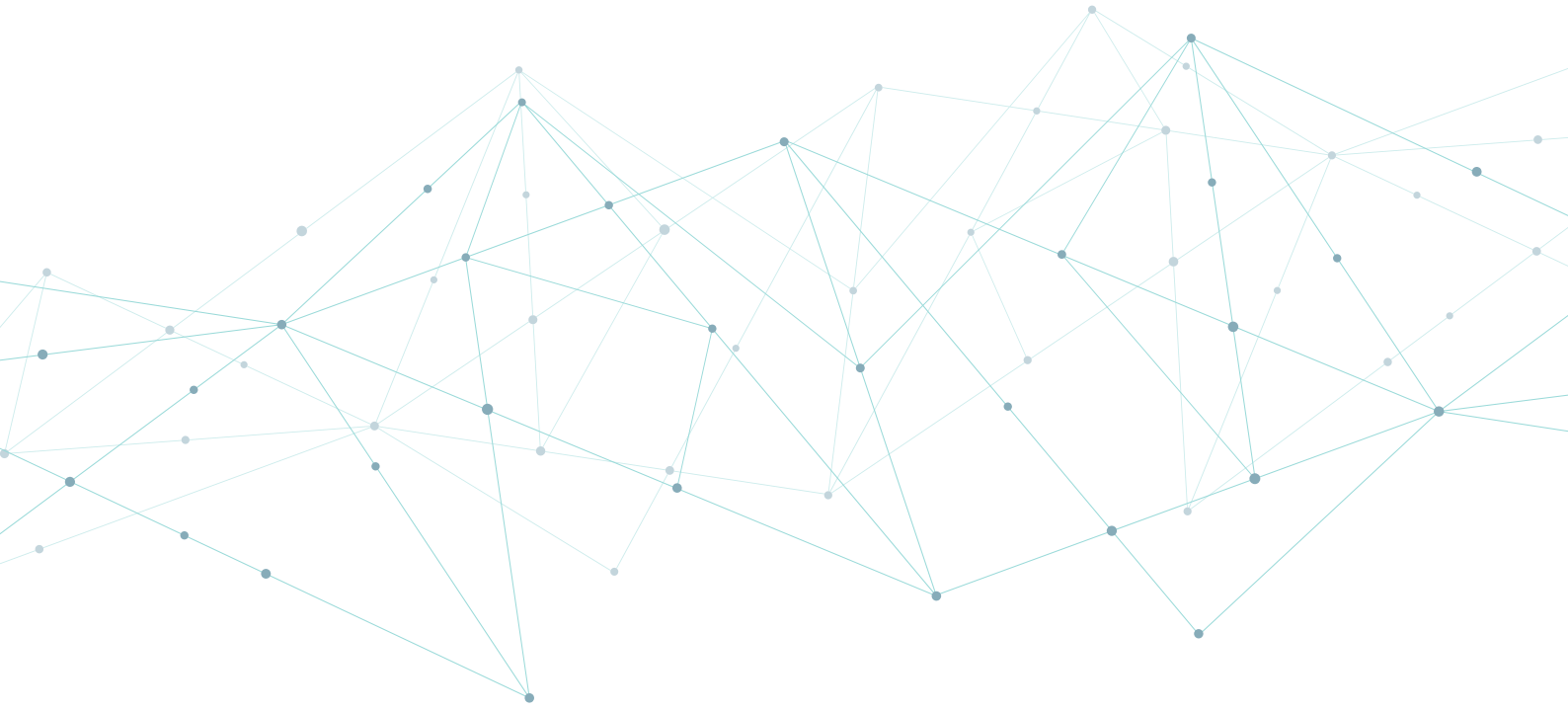
This is exactly the topic addressed by the already mentioned report *"Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU"* by the European Union Agency for Fundamental Rights [25]. Indeed, specific measures need to be put in place in order to ensure that individual rights and democratic principles are not unduly restricted and that secret services are not exempt from all legal constrains.

From the perspective of the EU vision, agencies hold a moral obligation to limit the roughness of their methods to the strictly necessary, and action should be as measured and as less harmful as possible even against legitimate targets. Going past those ethical boundaries would contradict the same national interest that those intelligence services are trying to protect [2].

As a last observation, under the EU vision some kind of non-coercive, non-harming intelligence gathering (such as some forms of mass surveillance and open-source intelligence) could apparently still be permitted, but there is still discussion on whether this kind of intelligence collection is something that violates basic human rights or not. The problem is that this kind of intelligence becoming more technically possible and more invasive thanks to the technological developments, and on the other side, the perception of EU citizens about their privacy is also increasing, and the legislation has also evolved.

5. Conclusions: a code of ethics and conduct for the EU Intelligence Community is needed

The evidence clearly suggests that ethical dilemmas are a constant trait of the intelligence profession, and can generate much public controversy when certain operations become public. Indeed, legislation that allows limitations to fundamental rights needs to strictly comply with the ethical principles of proportionality and necessity. It is noted that the EU is keen on providing rules for protecting the public from security threats while respecting fundamental rights (CFR Article 52), through strong oversight systems and effective remedies open to individuals (2023 FRA Report). It is essential however, for the benefit of all stakeholders, that Intelligence practitioners have access to a code of ethics and conduct to be followed in their activity. Such code should explicate the specific ethical standards and values applicable to the Intelligence Community in order to be effective. It is observed that no such code is available in the EU as a whole or at NATO level - at least not publicly - and that national codes are available only in some Member States.



6. References

[1] J. W. Coyne, P. Bell e S. Merrington, «Exploring ethics in intelligence and the role of leadership,» *International journal of business*, vol. 2, n. 10, pp. 27-37, 2013.

[2] M. Cantarella, «Intelligence Ethics in the Digital Age,» LUISS University - Department of Political Sciences, 2016.

[3] C. E. Bailey, «The Moral-Ethical Domain and the Intelligence Practitioner,» *American Intelligence Journal* , vol. 33, n. 1, pp. 49-58, 2016.

[4] P. Singer, *Ethics*, Aencyclopaedia Britannica , 2023.

[5] M. Velasquez, C. Andre, T. Shanks, S.J. e M. J. Meyer, «What is Ethics?,» *Issues in Ethics*, vol. 1, n. 1, 1987 - revised in 2010.

[6] F. Grandi, *Recenti sviluppi in tema di obiezione di coscienza*, Istituto della Enciclopedia Italiana, 2019.

[7] European Data Protection Supervisor (EDPS), «Necessity & Proportionality,» [Online]. Available: https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. [Consultato il giorno 23 May 2023].

[8] European Council, «Internal security strategy for the European Union Towards a European security model,» Publications Office of the European Union, 2010.

[9] T. Legrand, «National Security and Public Policy: Exceptionalism Versus Accountability,» in *The Palgrave Handbook of National Security*, 2022, pp. 53-72.

[10] P. McGlynn, «Open-source Intelligence,» in *Taking Intelligence Analysis to the Next Level*, CRC Press, 2022, pp. 225-250.

[11] S. D. Omand e M. Phythian, «Ethics and Intelligence: A Debate,» *International Journal of Intelligence and CounterIntelligence*, vol. 26, n. 1, 2013.

[12] N. J. Phillips, «"We're the ones that stand up and tell you the truth": necessity of ethical intelligence services,» *Salus Journal*, vol. 4, n. 2, 2016.

[13] South Africa, *Ministerial Regulations of the Intelligence Services, chapter 1(3)(d), 1(4)(d)*;.

[14] Geneva Centre for the Democratic Control of Armed Forces (DCAF), «Compilation of Good Practices for Intelligence Agencies and their Oversight,» 2010.

[15] C. E. Bailey e M. S. M. Galich, «Codes of Ethics: The Intelligence Community,» *International Journal of Intelligence Ethics*, vol. 3, n. 2, pp. 77-99, 2012.

[16] ODNI, «DNI.gov,» 2014. [Online]. Available: https://www.dni.gov/files/documents/CLPO/Principles%20of%20Professional%20Ethics%20for%20the%20IC.pdf.

[17] Australian Institute of Professional Intelligecne Officers, «AIPIO Code of Ethics,» [Online]. Available: https://www.aipio.asn.au/menu-1/governance/code-of-ethics/.

6. References

[18] Committee of Ministers to Member states, «Recommendation No. R (2000) 10 on codes of conduct for public officials,» 2000.

[19] D. Lyon, Surveillance Studies: An Overview, Cambridge: Polity Press, 2007.

[20] R. Ghioni, M. Taddeo e L. Floridi, «Open source intelligence and AI: a systematic review of the GELSI literature,» *AI & SOCIETY*, pp. 1-16, 2023.

[21] European Union, «Regulation (UE) n. 2016/679 General Data Protection Regulation,» 2016.

[22] European Parliament, «Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016,» 2016.

[23] High-Level Expert Group on AI, «Ethics guidelines for trustworthy AI,» 2019.

[24] European Parliament, «COM/2021/206 final,» 2021.

[25] European Union Agency for Fundamental Rights, «Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update,» May 2023. [Online]. Available: http://fra.europa.eu/en/publication/2023/surveillance-update.

[26] A. Deeks, «An International Legal Framework for Surveillance,» *Virginia Journal of International Law*, vol. 55, p. 291, 2015.

[27] Italy, *Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto Legge 3 agosto 2007*, n. 124, 2007.

[28] France, *LOI n° 2015-912 du 24 juillet 2015 relative au renseignement*, 2015.

[29] France, *Loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*, 2017.

[30] Spain, *Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia*, 2022.

[31] Germany, *BGBl. I S.* 2954, 2979, 1990.

[32] Germany, *BGBl. I S.* 3346, 2016.

[33] Policy Department for Citizen's Rights and Consitutional Affairs, «The impact of Pegasus on fundamental rights and democratic processes,» European Parliament, 2023.

[34] G. Agamben, Stato di eccezione, Torino: Bollati Boringhieri editore, 2013.

NOTIONES

Coordinator	Scientific Technical Coordinator	Project Security Officer
tecnalia	Zanasi & Partners	

Academic | Think-Tanks | Research

Technology Providers

Practitioners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101021853.