The accountability of intelligence and law enforcement agencies in information search activities

Abstract. The development of technology has challenged legislation in several areas during the last decade. The increase in the amount of data and computer performance, and new software solutions such as artificial intelligence and computer linguistics require a reassessment of the legal barriers to their operations. On the one hand, law enforcement agencies and national security services demand increasing access to these technologies. On the other hand, civil rights organizations require a strong oversight of law enforcement agencies and national security services to avoid their possible abuse of the most advanced technologies. The only way to resolve this dilemma is to improve the accountability of law enforcement agencies and national security services, thereby increasing public trust. Procedural, legal, and technical methods, and tools to perform this task are examined.

Keywords: Accountability, LEA, IC, whistleblowers, targeted search, bulk search, log analysis.

1 Introduction: the freedom versus security dilemma

Citizens' confidence in national law enforcement agencies and the intelligence community (henceforth LEA[1] and IC[2] organizations) is a relative concept that varies in time and space. Today's Central- and Central-Eastern-European generation is more likely to only be familiar with the idea of early dawn raids from films and literature, and certainly from family stories. In the deep layers of the consciousness of these nations the state has, for centuries, been more a repressive organization serving an elite than a group of civil servants working for citizens and providing security as a service from the taxes they pay. The memories of the secret services of the most recent repressive regimes (Gestapo[3], NKVD[4]/KGB[5], Stasi[6], StB[7], ÁVH[8], Securitate[9],

[1] Law Enforcement Agency
[2] Intelligence Community
[3] *Geheime Staatspolizei*, Secret State Police, secret police of Nazi Germany
[4] *Naródnyy komissariát vnútrennikh del*, People's Commissariat for Internal Affairs, secret police of the Soviet Union between 1917 and 1930 and 1934 and 1946
[5] *Komitet Gosudarstvennoy Bezopasnosti*, Committee for State Security, the main security service of the Soviet Union between 1954 and 1991
[6] *Ministerium für Staatssicherheit,* Ministry for State Security, the security service of East Germany
[7] CZ: *Státní bezpečnost*, SK: *Štátna bezpečnos*, State Security, the secret police of Checholsovakia between 1945 and 1989
[8] Államvédelmi Hatóság, State Protection Authority, the secret police of Hungary between 1945 and 1956

etc.) have not diminished in the region. Although trust has increased in countries in the region - albeit to varying degrees - since the change of regime in '89, the "*not over the telephone*" attitude has remained to some extent, and in some countries has not necessarily decreased in recent years.

Citizens do not feel the same way everywhere. In Switzerland, a referendum [1] recently decided that LEA and IC organizations should be able to legally listen to telephone conversations, and carry out online searches, because Swiss citizens are less afraid of the state than of terrorists or organized crime and expect that state organizations use all available means to protect their personal security.

Organizations involved in organized crime, terrorism, child pornography, the illegal arms and drug trades, and human trafficking take advantage of the most modern ICT[10] arsenal available without being too worried about legal hurdles. The complexity of data generated by these activities presents LEA and IC organizations a virtually impossible task unless they keep up with the most modern technologies.

On the one hand, LEA and IC organizations are therefore seeking to make full use of the arsenal available to them. On the other hand, civil rights organizations have a legitimate expectation that these activities are carried out with the maximum oversight to avoid unnecessary intrusion into the privacy of citizens and violation of human rights.

For thousands of years, the conflicting demands of freedom and security have been a concern for thinkers, lawyers, politicians, writers, and philosophers. The question, "*Who will guard the guards?*" originally comes from Decimus Junius Juvenal's 6th satire (the Satire against Women) not in the context we are using today, but in that of declining feminine virtues. The control of the responsible state is a topic that has been repeatedly raised, from Plato's The State to Dan Brown's Digital Fortress, throughout the centuries.

We are aware of several cases of abuse by secret services. Reference can be made to the Echelon system [2] or the Snowden files [3]. There are countless publications on the Orwellian dystopias arising from the abuse of human rights by the NSA[11] or GCHQ[12] and the like. But there are also strong arguments to support the use of modern technologies by LEA and IC organizations. This debate has resulted a process of rethinking the legal framework in several advanced democracies, including the USA, the UK and, within the EU, Germany, France, the Netherlands, and Sweden [4,5].

We do not consider it to be task of this paper to take a final position in the debate. Both parties are right up to a certain point because the excesses that exist not only exceed the limits of legality, but also undermine confidence in LEA and IC organizations. In this paper, we attempt to examine the arguments of both sides and to resolve the antagonism by explaining ways in which the range of operations of LEA and IC organizations can be expanded without undermining human rights. As the argument

---

[9] *Departamentul Securității Statului*, Department of State Security, the secret police of Romania between 1948 and 1989

[10] Information and Telecommunication Technology

[11] National Security Agency, the signals intelligence service of the USA

[12] Government Communications Headquarters, the signals intelligence service of the UK

on the subject generally takes a stronger position on one side or on the other, we will try to weight it in a balanced way.

There are two limitations to the subject of the present research. LEA and IC organizations should be treated separately in one sense, since, as outlined below, these are subject to two types of legal regulation. While LEAs are regulated by EU law, the IC is governed at national level. Although ICT technology covers a wide area, including communication interception, encryption etc., the crucial areas are the four principles of data protection laws: purpose limitation, data retention, the interconnectivity of data bases, and mass data collection.

The present study is seeking answers to questions such as what procedural, technical and legal means one can use to monitor the activities of the authorities. There is noa perfect solution. This endless conflict is caused by a lack of trust.

Two trends have been observed since the 2001 terrorist attacks.

- Terrorist organizations and organized criminal groups are using increasingly sophisticated and modern information and communication technologies.
- The legal frameworks of all known countries are accepting – if very slowly – this changing environment and are gradually reducing the restrictions on the use of key technologies.

The purpose of this provision is therefore to:

- identify the key information search technologies whose use limitation artificially weakens the effectiveness of such organizations;
- examine the legal environment in terms of how and to what extent it restricts LEA and IC organizations from using state-of-the-art information search technologies;
- examine the means and methods by which the conflict between freedom and security could be resolved or at least reduced. Thus, increased confidence would lead to both more efficient professional work and a healthier level of public trust.

2 Major technological breakthroughs

In information search, the basic requirements are novelty, timeliness, degree of processing, authenticity, and availability[i] [6]. The most widely used information search within LEA and IC organizations is either open-source intelligence (OSINT)[13] or internal search (enterprise content search, ECS). It is a natural requirement of LEA and IC organizations to obtain data, which is as complete as possible, and to do so as quickly as possible, preferably in real-time, with as few restrictions as possible and bringing to the surface as many hidden data connections as possible.

Over the last decade, new technologies have emerged, the use of which has become paramount for LEA and IC organizations. ICT infrastructure has developed enormously. We have also witnessed exponential developments in data and text mining technologies. These areas include the applicability of multi-layer neural network-based AI[14] technologies. The reliability of video and image recognition has reached 98% or above. The proliferation of non-relational database technologies has become

[13] Open-source intelligence
[14] Artificial intelligence

widespread. Breakthroughs in the application of multi-layer neural networks in semantic language technologies have reached new levels since 2017, in terms of automatic translation, natural language-based Q&A[15] and predictive analytic capabilities.

A widespread use of cryptographic and encryption technologies in terrorist and organized crime circles can be observed. More and more criminal and terrorist groups are using social media for drug and arms trafficking, human trafficking, the communication of pedophile content, the smuggling of weapons of mass destruction or the recruitment of terrorist groups. People who prepare themselves for terrorist acts alone (*lone wolves*) often make statements beforehand on social media. Finally, autocratic regimes that care little about fundamental human rights produce a tsunami of organized fake news to influence the public of democratic nations.

3 Organizational methods for accountability

A full review and analysis of the literature on the accountability of LEA and IC organizations would go far beyond the space available here. Most publications do not, of course, focus on information search only, but rather take a holistic view of LEA and IC activities [7-9].

3.1 Accountability

The problem of accountability can be very simply formulated: how to exercise democratic control over organizations whose functioning is essential for the security of the state, while their operation is essentially secretive. The antagonism is clear: the control mechanisms want to know as much as possible, while LEA and IC organizations want to disclose as little as possible. How do you supervise institutions if you do not see what they do? And how should they function if any leak puts at risk the success of operations, the survival of structures built over a very long time, or even people's lives? This is particularly true of operations which are illegal in a hostile environment. Control is based on the creation of checks and balances. In democracies, there are basically two kinds of solutions to this problem. On the one hand, to balance rights and duties between LEA and IC organizations and the institutions that control them. On the other hand, monitoring mechanisms can be established outside the implementing organizations [10]. It should be noted that democratic control and the freedom of operation of LEA and IC organizations are not mutually exclusive concepts. On the contrary: the freedom of operation of the Dutch secret services is perhaps one of the most extensive within the EU, while the oversight is one of the strongest [11].

[15] Question and answer, here an interactive AI-based information service application

3.2 Potential abuses of LEA and IC organizations

The fundamental danger, irrespective of the country, is political interference in the operation of LEA and IC organizations, which jeopardizes their professional independence and democratic objectives. Such political meddling can, inter alia, be illustrated by a few examples, as follows:

- influencing opposition political parties or movements, such as in the Öcalan case [12];
- observation of members of their own or allied parties, such as in the Watergate case [13];
- action against civil persons or organizations, such as in the Politovskaya case [14];
- monitoring of journalists, for example, the monitoring of French journalists for their sources [15];
- action against inside informants *(*whistleblowers), such as in the case of Mordechai Vanunu [16];
- disclosure of classified information, such as in the Valerie Plame case [17].

Having considered the legal and organizational mechanisms which ensure the checks and balances cited above, it is obvious that no control mechanism can be effective if the people carrying out the oversight are influenced through an invisible structure such as a party hierarchy, a religious order, a freemason's lodge, or the like. Examples are easy to find. These include Stalin's Soviet system, the National Socialist's capture of the state after 1933, or the ODESSA[16], which infiltrated West-German society after World War II.

3.3 Remedies to enhance oversight

Some of the tools and institutions considered by the literature as a method of checks and balances are the following:

- The services watch each other.
- The appointments of Directors-General are subject to parliamentary approval. Thus, the executive power is subject to personal scrutiny by, for example, the National Security Committee of the National Assembly.
- Compliance audit.
- LEA and IC organization heads report to Parliamentary committees. The depth at which a parliamentary committee can see into an organization's internal affairs differs from country to country. There are countries where this is possible only at a strategic level, while in other countries the committee can investigate specific details. It matters what classified information have member access to.
- Ad hoc parliamentary committees can be appointed by the legislature to investigate specific cases.
- The work of LEA and IC organizations is overseen by a responsible minister whose power may differ from one country to another.

---

[16] *Organization der ehemaligen SS Angehörigen*, organization of persons formerly belonging to the SS,

- In most countries judicial decisions can also allow operations that restrict individual rights, such as data acquisition and processing.
- Any EU citizen can appeal to the European Court of Justice.
- Civil societies can organize protests.
- Think tanks monitor events and influence processes through public forums.
- The free press can reveal abuses.
- Social media can be a platform for free critical expression, even in an anonymous form.
- Committees of respected people with high integrity can investigate matters and formulate independent views.
- Whistle-blowers can call the attention of the public to a particular issue.
- Finally, the data protection authorities may monitor the processing of personal information by LEA and IC organizations.

3.4 Whistle-blowers

Whistle-blowers have received particular attention recently. As we have seen above, in situations where the system of checks and balances function only superficially because the real line of command runs under the surface, the only functioning independent sources of information are whistle-blowers. The judgement of whistle-blowers is ambiguous. Civil society considers them as heroes, or even martyrs, while their employers regard them as traitors. Edward Snowden, one of the best-known whistle-blowers, was honored with statues in New York, Berlin, and Glasgow, while he has a good chance of being sentenced to life imprisonment or even being injected with poison in the United States. Mark Felt, Deep Throat, did not have the courage to reveal until hours before his death that he had informed Bob Woodward and Carl Bernstein of the background to the Watergate affair, which ultimately led to the fall of President Nixon. Perhaps less well-known is the case of Katharine Gun, a translator at GCHQ, who, in 2003, released classified documents related to the UN Security Council's decision-making procedure regarding the existence of Iraq's weapons of mass destruction. The charge was dropped due to a brilliant move by the defense, and she was unexpectedly released.

Another theory is that there are essentially three ways to achieve control of organizations by the state [18]. Horizontal control covers control mechanisms that are peer-to-peer but are not subordinate to parent organizations but operated by other organizations within the country. This type of horizontal check is judicial control. 'Vertical' control refers to means of control within the parent organization. These include the Minister of Oversight or the Government, possibly the Head of Government, or the scrutiny of a Parliamentary Committee, but also 'bottom-up' control by NGOs, and indeed all checks which are referred to by the term 'control' in the English language. Finally, the 'third type of control' occurs where the literature refers to a non-system (e.g., an international) organization or other mechanism which controls law enforcement agencies and national security services. This article argues that a new form of the 'third type' of control, 'technological control' based on new technologies, could be

a new means of resolving the dilemmas faced by law enforcement agencies and national security services.

3.5 LEAs and the IC can circumvent the law

The other side of the coin is that some cases and methods publicized by NGOs illustrate the possibility of circumventing the laws which guarantee individual rights. These methods are by their nature less verifiable, but they most certainly cannot be ignored. The essence of the "*one hand washes the other*" model is that what is forbidden in one country is not forbidden in another. This can help to circumvent national laws. The cooperation between the NSA and GCHQ is a striking example. Both are rather limited in monitoring their own nationals, but it is not forbidden to look at nationals of the other country, since, as foreigners they are not subject to national legal restrictions. Data exchange is permitted [19].

Outsourcing of tasks to private organizations is not unknown within LEA and IC circles [20]. It is quite difficult to officially control the activity of a foreign private subcontractor financed through unofficial channels. Such organizations can be entrusted with sensitive tasks that could be unpleasant to report on to a parliamentary committee [21].

4 Technical tools for accountability

Before dealing with the subject of data protection, one must highlight that, apart from legal and organizational-procedural guarantees, there is an alternative to improving accountability, which is less addressed in the literature and which would require greater attention. This is a method involving technical controls. It is worth mentioning that the FRA study strongly criticizes the poor technical background of the oversight bodies in the EU. [22].

The distillates from any system (such as in the two cases outlined below) must be stored in places that are not accessible to internal personnel, and the resulting data must be indelible and unalterable. Obviously, all analytical tools only look at those event logs or records that each individual application environment provides, i.e., ‘they are hooked up’. Permanently or provisionally disconnected proceedings are not recorded, and therefore not analyzed.

4.1 Log analysis

Log analysis consists of analyzing the collection of electronic tracks, log files (audit trails, event logs) of transactions and events generated by the operation of an IT system (network, operating system, applications) with the help of an application designed for this specific purpose. Examples of such events include the opening of a file or a directory, printing, entering, exiting, or copying files without permission. The log file is usually a structured database (the records are structured in the same way, e.g., after normalization a list of telephone calls or credit card numbers), but its size is vast

and therefore cannot be processed by human effort. The log analyst analyzes the log-file using statistical methods and AI to highlight non-routine events, called anomalies (e.g., illegal copying). Log analysis has been used for a long time to detect events which deviate from the norm. Its use is not unknown in public administration and in the private sector for checking compliance or fraud detection, for example, however, not much on the subject can be found in the publications related to LEA and IC accountability.

4.2 Database extraction

Another technology available is the permanent filtering of databases within an organization under appropriate conditions for an engineering and human analysis unit which ensures accountability. The filtering mechanism should ensure that all data relevant to accountability is passed on for verification (even encrypted) and that confidential operational data is not removed from the system unnecessarily.

Appropriate conditions (both human and technical) must be provided in the classified environment. Anyone who receives insight into these system mappings should have the highest security clearance and periodic vetting.

5 Legal instruments for accountability

5.1 The EU legal framework

The EU's data protection regulations are aware of and articulate the dilemma of freedom versus security. The backbone of current EU legislation is the GDPR [23]. However, there are special rules for law enforcement agencies (Directive 2016/680 [24]. *Law Enforcement Directive* — LED). The data protection aspects of national security services and secret services are currently within the responsibility of the member states.

The LED was adopted together with the GDPR. The logic of regulation is that the GDPR is the background regulation, with the exceptions defined in the GDPR itself. Recital 16 says, that the GDPR "*does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security.*" Recital 19 of the GDPR defines the exception for law enforcement agencies: "*The protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council.*"

The main difference between the GDPR and the LED is the legal basis for data processing: whereas the most common legal basis for data processing in the GDPR is the consent of the data subject, in LED this legal ground is not necessary. However, the principles for data management are very similar in the two norms. According to the LED, personal data should be processed 'lawfully and fairly', collected only 'for specified, explicit and legitimate purposes', and 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.' [LED 4. (1) (a) to (f)] It can therefore be concluded that the principles of purpose limitation, data minimization, and storage limitation should also apply to law enforcement organizations.

In 2017, in Article 29, the Working Party of the EU Data Protection Advisory Board also issued an opinion on the subject [25]. The document says that in law enforcement agencies "in principle, personal data should be processed until they serve the purpose for which they were collected and when they are no longer necessary for that purpose, they should be deleted, unless subsequent processing is foreseen by law and is deemed relevant for a purpose which is not incompatible with the original purpose for processing." [26] This refers to the solutions contained in the judgments of the European Court of Human Rights and the European Court of Justice as regards specific periods and solutions [27]. Regarding the special data, the LED requires that they can only be handled if "absolutely necessary." [28] The WP 29 recommendation also proposes further risk analysis, and the introduction of additional procedural guarantees and technical measures in this area.

According to the WP 29, profiling "can pose significant risks for individuals' rights and freedoms, and therefore require[s] appropriate safeguards." [29] Another important requirement is that the data subject should always retain the right to request human intervention. A new, additional principle that is found in almost all material today is that profiling cannot lead to discrimination.

An important control solution for the LED is that it declares, that "Member States shall provide for the right of the data subject to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data." The limitations to this rule are laid down in Article 15 (e.g., it cannot obstruct legal inquires, investigations, or proceedings; it does not prejudice prevention, etc.). *The WP 29 recommendation correctly observes that the scope of the exceptions is so broad that Member States can render the right of access virtually meaningless*.

In summary: the logic of EU regulation is that it has created specific regulations for law enforcement organizations which are based on very similar principles to the GDPR: these include purpose limitation, prohibition of unlimited storage, right of access for the data subject, etc. However*, it allows very wide exceptions, with which the Member States can render the Directive meaningless.* The data protection regulations of national security services are a matter of national competence and currently there is no EU standard.

5.2 The ECtHR and EU case law

The ECtHR has made several judgments interpreting the European Convention on Human Rights. The second paragraph of Article 8 of the Convention states that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." The European Court of Human Rights, which is the guardian of the Convention, has contributed to the development of the Convention through specific interpretations of *necessity* and *proportionality*. For example, in the *MM vs. United Kingdom* (24029/07 - 13 November 2012) and *Huvig vs. France* (1105/84 - 24 April 1990) cases, it stated that any intervention must have its domestic legal basis, laid down in a law to which the parties concerned have access, and may adapt their action. Several judgments dealt with what the term 'necessary in a democratic society' meant (e.g., *Handyside vs. United Kingdom* Appl (5493/72 of 7 December 1976) and *The Sunday Times vs. United Kingdom* Appl. (6538/74 of 6 November 1980). In those rulings, the Court stated that 'necessary' means that there is a genuine social need (*a pressing social need*), rather than that it would be better, or easier, to achieve certain objectives with such an intervention. There have also been numerous judgments on proportionality, *S & Marper vs. United Kingdom*, in which unlimited storage of DNA samples was prohibited by the court.

ECtHR case law has also addressed the dilemma arising from the issue of *mass surveillance versus targeted surveillance.* In the *Weber vs. Germany* case [30], the ECtHR considered the issue closely and concluded that if 'strategic monitoring' has adequate guarantees (i.e., only a higher body can provide a sufficiently powerful reason and destroy data when it is no longer needed), *it is not in itself a disproportionate interference with private life.*

The European Court of Justice has, by its very nature, much less case law in this matter. Here, one should highlight the case ECJ, C-291/12, *Schwarz vs. Stadt Bochum*, in which the legality of the use of fingerprints for visas and passports was challenged. The court held that for biometric passports it is legitimate to require fingerprints.

6 Conclusion

The present paper covered the relationship between law enforcement agencies and security services and data protection. The dilemma between freedom and security still exists today and has even been sharpened by new technological developments. One of the most important areas where this dilemma is expressed is the area of mass data collection, which is likely to occur more and more frequently.

Data protection restrictions need to be overhauled.

The main point of this article is that, to ensure greater confidence among citizens, there must be greater freedom for national security services and law enforcement

agencies to use modern technologies and, at the same time, greater accountability must be enhanced by new means and methods.

1 References

1. Gerny, Daniel: Das Nachrichtendienstgesetz auf einen Blick. Neue Zürcher Zeitung, 18.08.2016 https://www.nzz.ch/schweiz/abstimmung-vom-25-september-das-nachrichtendienstgesetz-auf-einen-blick-ld.111204, last accessed 21/03/2021.
2. Schmid, G.: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 2001. 07th 11th European Parliament Session Document A5-0264/2001 http://cryptome.org/echelon-ep-fin.htm, last accessed 25/03/2021.
3. Macaskill, E.-Dance, G.: NSA Files: *Decoded,* The Guardian 07/11/2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1, last accessed 25/03/2021.
4. FRA: Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union — Volume I.: Mapping Member States' legal frameworks. (henceforth FRA I), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf, last accessed 25/03/2021.
5. FRA: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU — Volume II.: field perspectives and legal update (henceforth FRA II), https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu, last accessed 25/03/2021.
6. Kahaner, L.: Competitive Intelligence, p. 104., New York, Touchstone-Simon & Schuster, (1997).
7. Weber, R.H., Staiger, D.N.: Privacy versus Security. In Kulesza, J., Balleste, R. (eds.): Cybersecurity and Human Rights in the Age of Cybervelliance, Rowman & Littlefield, Lanham, ML, USA (2016).
8. FRA I. p. 8.
9. Born, H., Wills, A.: Overseeing Intelligence Services, A toolkit. DCAF, Geneva (2012).
10. Caparini, M.: Controlling and Overseeing Intelligence Services in Democratic States. In Born H., Caparini M. (eds.) Democratic Control of Intelligence Services, New York, Routledge, (2016).
11. FRA II. p. 95.
12. Öcalan v. Turkey, http://hudoc.echr.coe.int/eng?i=001-69022, last accessed 25/03/2021.
13. Dickinson, W. B., Mercer, C. Polsky, B.: Watergate: Chronology of a crisis, 1., pp. 133.,140.,180.,188. Washington D.C. Congressional Quarterly Inc., (1973)
14. Archangelsky, A.: Murder in Moscow: Anna's Legacy. DOI: 10.1177/0306422016670350.
15. Lichtfield, J.: Sarkozy accused of using security service to spy on journalists, The Independent, (2010), https://www.independent.co.uk/news/world/europe/sarkozy-accused-of-using-security-service-to-spy-on-journalists-2124599.htm, last accessed 25/03/2021.
16. Mordechai Vanunu gets 18 years for treason - Archive 1988,The Guardian (2018), |Mordechai Vanunu gets 18 years for treason – archive, 1988 | Mordechai Vanunu | The Guardian, last accessed 25/03/2021.
17. ILEY, CHRISSY: Valerie Plame Wilson: housewife CIA spy who was a 'fair game' for Bush, 2011, *The Telegraph:* http://www.telegraph.co.uk/culture/film/8318075/Valerie-Plame-

Wilson-the-housewife-CIA-spy-who-was-fair-game-for-Bush.html, last accessed 25/03/2021.

18. Caparini quotes Schedler in Born - Caparini. p. 10.
19. Ball, J.: US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, The Guardian, http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data, last accessed 25/03/2021.
20. Voelz, G. J.: Contractors and Intelligence: The Private Sector in the Intelligence Community, International Journal of Intelligence and Counterintelligence, (22). 4, pp. 586 – 613. (2009).
21. Shorrock, T.: Spies for hire, New York, Simon and Schuster Paperbacks, (2008).
22. FRA II: p. 9.
23. Regulation (EC) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46 (General Data Protection Regulation, GDPR).
24. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection, prosecution, or enforcement of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. (Privacy Policy, LED)
25. Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) adopted on 2017 November 29, https://iapp.org/media/pdf/resource_center/wp258_police_directive-11-2017.pdf, last accessed 25/03/2021.
26. Ibid 4.
27. For details on the question, see further material of WP 29, which was published in 2014: Opinion 01/2014 on the WP 211 *'Application of the necessity and the proportionality concepts and data protection within the law enforcement sector*'. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf
28. For details on the question, see further material of WP 29, which was published in 2014: Opinion 01/2014 on the WP 211 *'Application of the necessity and the proportionality concepts and data protection within the law enforcement sector*'. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf
29. For details on the question, see further material of WP 29, which was published in 2014: Opinion 01/2014 on the WP 211 *'Application of the necessity and the proportionality concepts and data protection within the law enforcement sector*'. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf
30. *Weber and Saravia v Germany* (2006) http://hudoc.echr.coe.int/eng?i=001-76586