The Accountability of Intelligence and Law Enforcement Agencies in Information Search Activities

Pál Vadász, Zsolt Ződi

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

Pál Vadász [0000-0003-3848-6096] and Zsolt Ződi [0000-0003-3978-5493]

National University of Public Service, Information Society Research Institute Budapest, Hungary
pal.vadasz@uni-nke.hu

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 based intelligent search require a reassessment of the legal barriers to their operations. On the one hand, law enforcement agencies and security services demand increasing access to these technologies to come up to the social expectations in the field of security. On the other hand, civil rights organizations require an ever-stronger oversight of law enforcement agencies and security services to avoid their possible abuse of the most advanced technologies. The paper argues that 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 and technical methods to perform this task are examined. The corresponding EU legal framework is analyzed.

Keywords: Accountability, law enforcement agencies, security services, whistleblowers, targeted search, bulk search, log analysis.

1 Introduction: the freedom versus security dilemma

Citizens' confidence in law enforcement agencies and the security services or intelligence community (henceforth LEA and IC organizations or just organizations if it is contextually evident) is a relative concept that varies in time and space. In the deep layers of the consciousness of Central- and Central-Eastern-European 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. People 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.

Networks involved in organized crime, terrorism, child pornography, illegal arms and drug trades, and human trafficking take advantage of the most modern information and communication technology (henceforth ICT) 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 within strict legal boundaries to avoid unnecessary intrusion into the privacy of citizens and violations of human rights.

Various publications strongly argue either for or against the increased legal limitations, without showing a way out of this dilemma. This paper accepts the arguments of both sides, however, as a new approach, endeavors to cut the Gordian knot by highlighting the importance of the substantially improved accountability both organizationally and, as a new dimension due to the enhanced artificial intelligence (henceforth AI) and natural language processing (henceforth NLP) technologies, technically.

The purpose of this paper is threefold, as follows. To identify the key information search technologies whose use limitation artificially weakens the effectiveness of such organizations. To examine the means and methods by which the conflict between freedom and security could be resolved or at least reduced. To 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.

2 Background and challenges

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 organizations' activities [2-4].

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.

There is an abundant literature on the overwhelming secrecy of LEA and IC organizations, on the lack of transparency, insufficient oversight, and poor accountability. Such is the Carnivore case [5], the hot dispute involving the British Investigatory Powers Bill (the so-called snoopers' charter) [6], the BND[1] practice in 2016 [7] that was again curtailed in Germany in 2020 [8], or GCHQ[2], held responsible for breaching privacy rights [9]. The quintessence of these studies is that they directly or implicitly demand a strict legal framework to limit the technical capabilities of these organizations.

Much less is publicized by the LEA and IC organizations about their demands and the need for loosening control. Seminal work was published by David Anderson Q.C.

[1] Bundesnachrichtendienst, the foreign intelligence agency of Germany

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

[10] that examined both sides of the coin by interviewing all UK LEA and IC organizations as well as civil rights groups with particular focus on the targeted versus bulk search dilemma. This report is one of the very few that elaborates on the specific need and practices of the organizations in their everyday activities. Anderson found that bulk search is not only extremely useful but inevitable in certain cases. He states that stored data provide essential input for AI applications without which they just cannot function. Also, his team cautiously indicates that superficial bulk search followed by focus only on strong suspects is less intrusive, than a deep drill-down into the private life of someone who, at the end of the day, turns out to be innocent.

3 Major technological breakthroughs

In information search, the basic requirements are novelty, timeliness, degree of processing, authenticity, and availability [11]. The most widely used information search within LEA and IC organizations is either open-source intelligence (OSINT) or enterprise content search run on internally stored data. 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. The development of text mining technologies on an exponentially growing amount of data is evident. The reliability of video and image recognition has reached 98% or above. The proliferation of non-relational database technologies has become 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 so-called question and answering (Q&A) and predictive analytic capabilities.

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 and mass data collection, data retention, the interconnectivity of data bases and profiling. Most legal boundaries can be grouped into these four categories.

The confinement of search by purpose limitation (targeted search) or, in other words the prohibition of mass data collection (bulk, dragnet or strategic search) is one of the most controversial issues. To illustrate the problem, one should imagine the unnatural situation in which drug finder dogs are only allowed to sniff those bags that have been authorized by a judge beforehand, and not all of them at the airport arrival hall [10].

The data retention confinement prohibits the storage of collected data over a certain date, i.e., these must be permanently deleted. The technical consequence is that the training data for enrichment evaporates, thus paralyzing the AI search applications [10].

The limitation of interconnecting databases means that relevant information in one database cannot be freely matched with that in another. For example, the fact that a local report that a student pilot is only interested in taking off but not in landing

techniques is not compared to the FBI database of terrorists, can lead to 11/9/2001. The problem is topical in the EU [12].

And finally, the limitation of profiling, particularly by AI-based face-recognition is again one of the controversial topics of the day. This means that the recognition and following of terrorists is made substantially more difficult.

There is no room in this paper to discuss the consequences of AI biases.

4 Examples of abuses of LEA and IC organizations

Several cases of abuse by secret services are well known. Reference can be made to the Echelon system [13] or the Snowden files [14]. There are countless publications on the Orwellian dystopias arising from the abuse of human rights by the NSA[3] or GCHQ 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 in 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 [15].

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 [16];
- observation of members of their own or allied parties, such as in the Watergate case [17];
- action against civil persons or organizations, such as in the Politovskaya case [18];
- monitoring of journalists, for example, the monitoring of French journalists for their sources [19];
- action against inside informants (whistleblowers), such as in the case of Mordechai Vanunu [20];
- disclosure of classified information, such as in the Valerie Plame case [21].

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[4], which infiltrated West-German society after World War II.

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

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

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

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 [22].

Outsourcing of tasks to private organizations is not unknown within LEA and IC circles [23]. 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 [24].

5 Organizational methods to support accountability

5.1 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 [25]. 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 [15].

5.2 Remedies to enhance oversight

Some of the tools and institutions considered by the literature as a method of checks and balances are as follows.

- 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.
- 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.

5.3 Whistle-blowers

Whistle-blowers have received particular attention recently. As 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 verdict on whistle-blowers is ambiguous. Civil society considers them heroes, or even martyrs, while their employers regard them as traitors. Edward Snowden, one of the best-known whistle-blower, 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.

6 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. [15].

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.

6.1 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 logfile 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.

6.2 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.

7 Legal instruments of accountability

7.1 EU legal framework – data protection

The EU's data protection regulation is aware of and articulates the dilemma of freedom versus security. The current EU legislation on the processing of personal data is based on the GDPR [26] while the rules concerning the law enforcement agencies are in

Directive 2016/680 (Law Enforcement Directive — LED) [27]. The LED regulates data protection only in the field of law enforcement agencies and does not concern the activities of national security services; the regulation of the secret service and its data protection aspects are currently within the competence of the member states.

The LED was adopted with the GDPR. The logic of regulation is that the GDPR should be used as a background norm, with the exceptions defined in the GDPR itself. 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 therefore not apply to processing activities carried out for those purposes."

The main difference between the GDPR and the LED is, of course, the legal basis for data processing: whereas the most common legal basis for data processing in the GDPR is the data subject's consent, in LED it is either "public interest", or "performance of official authority". The principles for data processing are very similar in the two norms. According to 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*" [27]. 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, the Article 29 Working Party [28] published an opinion on the subject [29]. The opinion deals with a wide range of issues, including processing special categories of personal data, automated decision-making, profiling, data subjects' rights, and the powers of the data protection authority in the context of LED. In relation to purpose limitation, the document states that the core problem lies in prevention issues. "*The question whether certain data have served their purpose and are no longer necessary, arises particularly when data storage is allowed for preventive purposes*" [30]. The document sees the solution in the combination of an overall maximum time limit and periodic reviews. It recommends that the storage of data should be based on a risk assessment. It refers to the solutions contained in the judgments of the European Court of Human Rights and the European Court of Justice as regards specific period-limitations, and other solutions [27].

Regarding the special data, (such as health, political opinion, race, etc.) the LED requires that they can only be processed if "*strictly necessary*" ([29], Article 11). The WP 29 recommendation also proposes further risk analysis, the introduction of additional procedural guarantees and technical measures in this area. According to the WP 29, profiling also poses significant risks to the rights and freedoms of individuals and therefore requires adequate protection measures [27]. Another important requirement is that the data subject should always retain the right to obtain human intervention in these cases. A new, additional principle that is becoming increasingly significant is that profiling cannot lead to discrimination [31].

The data subject also has the right regarding data processing under the LED to get information on the data processing in a "*concise, intelligible and easily accessible form, using clear and plain language*" ([27], Article 12 (1)) but there are obviously serious restrictions laid down in Article 15. (e.g., it should not obstruct official or legal inquiries, investigations, or procedures, or prejudice the prevention, detection, investigation, or prosecution of criminal offences.) The scope of the exceptions is so broad that the WP 29 reminds the "*national legislators that any exemptions from the fundamental rights and legitimate interests of the natural person should be applied as the exception rather than the rule and that omitting information may be allowed within an investigation only for as long as such a restriction constitutes a necessary and proportionate measure*" ([29], Article 22).

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: it includes purpose limitation, prohibition of unlimited storage, right of access for the data subject, etc. The data protection regulations of national security services are a matter of national competence, and currently there is no EU standard.

7.2 European Court of Human Rights (ECtHR) case law

The ECtHR has issued several judgments protecting privacy ("Right to respect for private and family life" – Art. 8.) under the European Convention on Human Rights. The second paragraph of Art. 8. states that public authorities are entitled to intervention "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 ECtHR, 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, namely 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 (5493/72 of 7 December 1976) and The Sunday Times vs. United Kingdom. (6538/74 of 6 November 1980). In those rulings, the Court stated that "necessary" means that an intervention is a pressing social need, rather a way of better achieving certain objectives, or making it easier to achieve them. There have also been numerous judgments on proportionality, like S & Marper vs. United Kingdom (30562/04 and 30566/04 (4 December 2008), in which unlimited storage of DNA samples was prohibited by the court. The ECtHR case law regarding the dilemma of mass surveillance (or, as it is called by the Court, "strategic monitoring") versus targeted surveillance is interesting. In the Weber vs. Germany case [32], the ECtHR considered the issue closely and concluded that "strategic monitoring" should have adequate guarantees (i.e., only a higher body can order it with a sufficiently powerful reason, data should be destroyed when it is no longer needed, and should not be transmitted to other authorities). But

overall, strategic monitoring is not in itself a disproportionate interference with private life.

8 Conclusion

The present paper covers the relationship between LEA and IC organizations and the legal framework of data protection in view of recent disruptive technologies. The dilemma between freedom and security still exists today and has even been sharpened by new ICT developments. The paper highlights the key legal boundaries that confine the application of modern technologies by LEA and IC organizations. Instead of arguing either for or against more technological freedom, the paper takes sides for both, but strongly argues for enhanced accountability. Organizational, procedural and - as a barely covered new area - technical methods are presented to improve the accountability of LEA and IC organizations to ensure greater confidence among citizens.

References

1. Gerny, D.: Das Nachrichtendienstgesetz auf einen Blick. https://www.nzz.ch/schweiz/abstimmung-vom-25-september-das-nachrichtendienstgesetz-auf-einen-blick-ld.111204, last accessed 21/03/2021
2. FRA: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, vol. 1, p. 8., European Union Agency for Fundamental Rights, Vienna (2017)
3. 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)
4. Born, H., Wills, A.: Overseeing Intelligence Services, A toolkit, DCAF, Geneva (2012)
5. Ventura, H.E., Miller, J.M., Deflem, M.: Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power, https://doi.org/10.1007/s10612-004-6167-6, last accessed: 26/05/2021
6. Schafer, B.: Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill, (2016), https://doi.org/10.1007/s11623-016-0664-0, last accessed: 26/05/2021
7. Meyer, D: Spy agency back in court over snooping: You're abusing mass surveillance powers, https://www.zdnet.com/article/spy-agency-back-in-court-youre-abusing-your-mass-surveillance-powers/, last accessed: 24/05/2021
8. Rojszczak, M.: Extraterritorial Bulk Surveillance after the German BND Act Judgment, European Constitutional Law Review, pp 1-25 (2021) https://doi.org/10.1017/S1574019621000055/
9. Goodwin, B.: GCHQ bulk interception programme breached privacy rights, Strasbourg court rules (2021). https://www.computerweekly.com/news/252501356/GCHQ-bulk-interception-programme-breached-privacy-rights-Strasbourg-court-court-rules?utm_campaign=20210526_GCHQ+bulk+interception+programme+breached+privacy+rights%2C+Strasbourg+court+rules&utm_medium=EM&utm_source=EDA&asrc=EM_EDA_163354630
10. Anderson, D.: Report of the Bulk Powers Review, Crown copyright, London (2016)

11. Kahaner, L.: Competitive Intelligence, p. 104., Touchstone-Simon & Schuster, New York (1997)
12. Quintel, T.: Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention**,** University of Luxembourg Law Working Paper No. 002-2018 (2018)
13. Schmid, G.: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 07th 11th European Parliament Session Document A5-0264/20012001, http://cryptome.org/echelon-ep-fin.htm, last accessed 25/03/2021
14. Macaskill, E., Dance, G.: NSA Files: Decoded, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1, last accessed 25/03/2021
15. FRA: Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, vol. 2, European Union Agency for Fundamental Rights, Vienna (2018).
16. Öcalan v. Turkey, http://hudoc.echr.coe.int/eng?i=001-69022, last accessed 25/03/2021
17. 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)
18. Archangelsky, A.: Murder in Moscow: Anna's Legacy. https://doi.org/10.1177/0306422016670350, last accessed 01/06/2021
19. 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
20. Mordechai Vanunu gets 18 years for treason - Archive 1988, https://www.theguardian.com/world/2018/mar/28/mordechai-vanunu-israel-spying-nuclear-1988 (1988)
21. Iley, C.: Valerie Plame Wilson: housewife CIA spy who was a 'fair game' for Bush, 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
22. Ball, J.: US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data, last accessed 25/03/2021
23. Voelz, G. J.: Contractors and Intelligence: The Private Sector in the Intelligence Community, https://doi.org/10.1080/08850600903143106, last accessed 01/06/2021.
24. Shorrock, T.: Spies for hire, , Simon and Schuster Paperbacks, New York (2008)
25. Caparini, M.: Controlling and Overseeing Intelligence Services in Democratic States. In Born H., Caparini M. (eds.) Democratic Control of Intelligence Services, Routledge, New York (2016)
26. 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)
27. 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)
28. Article 29 Working Party was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission. After the entering into force of the GDPR it ended its functioning

29. WP 258: 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
30. Opinion 01/2014 on the WP 211 - Application of the necessity and the proportionality concepts and data protection within the law enforcement sector. (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf, last accessed: 31/05/2021.
31. FRA: Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide. European Union Agency for Fundamental Rights, 2010 https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf, last accessed: 30/05/2021.
32. Weber and Saravia v Germany (2006) http://hudoc.echr.coe.int/eng?i=001-76586, last accessed 01/06/2021.