LAWS AND REGULATIONS GOVERNING CYBERSECURITY

Co-funded by the Erasmus+ Programme of the European Union

Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA.

LECTURES

1. Introduction to the subject, system of law, legal norm, law and internet

2. Responsibility in cyberspace

3. Legal basis of ISP (internet service provider) activity

4. Cybersecurity and its legal regulation

5. ISMS

6. Protection of personal data in cyberspace

7. Privacy and security in ICT, data protection in cyberspace

WORKSHOPS

1. Defining the scope of law in cyberspace (limits, possibilities, etc.)

2. Private and public liability for the actions of the user or company in the online environment

3. Characteristics and definition of individual ISPs and their rights and obligations in relation to cybersecurity

4. ISMS and the relationship to cybersecurity law

5. Acquisition of basic rights and obligations for individual subjects from Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, also from national legislation.

6. Application of rights and obligations arising from GDPR in cyberspace

7. Practical analysis of contractual conditions with ISPs in relation to privacy protection

Table of contents

1. Introduction to the subject, system of law, legal norm, law and internet 1.1. Legal norm
1.2. The relationship between the law and cyberspace

2. Responsibility in cyberspace
2.1. Cyberspace
2.2. Scope of the law in Cyberspace
2.3. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

3. Legal basis of ISP (internet service provider) activity
3.1. Regulation of ISP activities in the Czech Republic
3.2. Regulation of ISP activities in Poland
3.3. Regulation of ISP activities in Portugal
3.4. Possibilities of legal liability of a user for actions in cyberspace
3.5. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

4. Cybersecurity and its legal regulation
4.1. EU/EC documents used to harmonise legislation in addressing cybersecurity 4.2. Cybersecurity Legislation in the Czech Republic
4.3. Cybersecurity Legislation in Poland
4.4. Cybersecurity Legislation in Portugal

5. Information Security Management System
5.1. ISMS framework
5.2. Risk management
5.3. Security policy
5.4. Organisational security
5.5. Asset management
5.6. Security of human resources
5.7. Business continuity management
5.8. Technical measures
5.9. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

6. Protection of personal data in cyberspace
6.1. Excursion into the rights and obligations arising from certain legal norms 6.2. GDPR
6.3. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

7. Privacy and security in ICT, data protection in cyberspace
7.1. Digital footprint
7.2. Terms of Service (EULA)
7.3. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

8. Conclusion

9. List of sources used

1. Introduction to the subject, system of law, legal norm, law and internet

The law is one of the most important instruments for stabilising social relations and regulating society.

The law is necessary and currently irreplaceable because, where there is a society, there is law. Society is not able to endure without order and rules. As such, law significantly reduces the degree of chaos (entropy) in society and stabilises relations.

All of the above is true, but only if the law is respected and the law itself is stable (at least relatively).

The law, like society, is evolving and changing.

The law is a set of generally binding rules of conduct accepted by society, defined by a state or bodies authorised by the state. For the law to be sustainable, it must be enforceable. The law without the condition of enforceability is still law, but in reality it is rather a set of recommendations that everyone decides for themselves whether to respect or not.

In order for a citizen or an entity that is subject to a law to be able to exercise its rights or protect them effectively and to be aware of their own responsibilities, which are closely linked to the rights, they need to have at least minimal knowledge of the basic provisions of the legal system.

In today's society, the law can be characterised as a relatively well-defined system of legal norms, ensured by state power and protected by state enforcement. In order for a natural or legal person to be able to exercise or effectively protect his/her/its rights, as well as to be aware of his/her/its obligations under these rights, it is essential that he/she/it has at least minimal knowledge of the basic provisions of the legal system.

The actual concept of the law is relatively difficult to define as it is a multidisciplinary phenomenon and cannot be defined by a single definition:

- **natural law** *(ius naturale)*. It exists independently of the state. It originates and develops in society. In general, it comprises a set of principles that correspond to the achieved level of society's development.

- **positive law** *(ius pozitivum)*. This law is laid down by a state or a system of power. Positive law is therefore predetermined. It consists of predictable rules that are enforced, i.e. where infringement is punished.

- **law** We understand the law (or objective law) as a set of legal norms as generally binding rules of conduct established or recognised and enforced by the state.

- **right** "Right" means the possibility of conduct of legal entities guaranteed by a legal norm. A right usually corresponds to a legal obligation of another legal entity. An entity's statement that "it is my right" corresponds to the law in this sense, for example.

1.1. Legal norm

A legal norm is an essential element of a state based on the rule of law.

A legal norm represents a generally binding rule of conduct that regulates the rights and obligations of entities. This rule of conduct is expressed in a special legal form recognised by the state (or the European Union), and its observance is ensured by state enforcement.

The above definition of a legal norm results in two obligatory features, which are further specified. These features are:

1. Formal

From the point of view of fulfilling the formal feature of a legal norm, it is necessary that a legal norm be issued by an authorised entity, and at the same time, the legally prescribed method of publication is satisfied.

2. Material

The material features of a legal norm include:

- regulation – regulates social relations,
- legally binding – the rule of conduct regulates social relations with binding effects,
- generality – in terms of the subject of legislation, as well as the object of the legal norm,
- enforceability by state power – "state enforcement" in the event that the law is not respected.

The standard **structure of a legal norm consists of three parts**, which are **hypothesis, disposition** and **sanction**.

The hypothesis sets out the conditions under which a legal norm is implemented. The hypothesis, in particular, defines legal facts, entities and objects of a norm to which rights and obligations relate.

The disposition represents its own rule of conduct as it determines and concretises what rights and obligations arise and to whom in the event that the conditions stated in the hypothesis occur.

The sanction is an expression of the consequences of a breach of a legal obligation arising from the disposition of a legal norm.

Division of legal norms

Legal norms can be divided according to various criteria. These are specifically:

1. *The nature of the rules laid down by the legal norm.* According to the nature of the rules, legal norms are divided into:

- Dispositive. A dispositive legal norm does not stipulate a fundamental rule of conduct at all, or it stipulates it only as a possibility. It is left to the addressees to set the rules themselves. If the addressees do not do so, the provisions in the standard serve as a guide for the judge to know how to decide. Dispositive norms are mostly applied in civil law or in civil law relations, which allow greater variability in the solution of various situations (self-regulation).
- Cogent (categorical). A cogent legal norm stipulates a binding rule of conduct. It does not leave room for the will of the addressee.

2. *Wording.* According to wording, legal norms are divided into:

- Entitling. These legal norms explicitly formulate only entitlements.
- Binding. These legal norms explicitly formulate an obligation, either in the form of an order or a prohibition.

3. *Status of entities.* According to the status of entities, legal norms are divided into:

- Public. These legal norms apply where public power is exercised. Public power is exercised by the state through the offices of legislative, executive and judicial power. We view public law as the area of law in which relations are based on the inequalities of the parties involved, where one represents the public power acting against private persons with orders, prohibitions and enforcement.
- Private. These legal norms apply in the field of private law, i.e. where entities act in an equal position, and neither of them can authoritatively decide on the rights and obligations of the other. Entities regulate their mutual rights and obligations through contracts and agreements.

4. *Subject of regulation.* According to the subject of regulation, legal norms are divided into:

- International. These legal norms regulate relations between states or their inhabitants, possibly at the level of the European Union.
- National. National legal norms regulate relations between entities within a jurisdiction of a particular state or usually within its territory.

5. *Method of legislation.* According to the method of legislation, legal norms are divided into:

- Substantive law. These legal norms define legal relations in general and set out the rights and obligations of entities.
- Procedural law. These legal norms regulate the procedure of public authorities in the application of substantive law norms, which may result in the issuance of a public act.

6. *Scope of legislation.* According to the scope of legislation, legal norms are divided into:

- General. These legal norms affect an entire territory of a state or the European Union. Furthermore, they apply to all entities without limit to their temporal scope.

- Special. These legal norms operate only in a certain territory. Otherwise, they only apply to a certain category of entities or for a certain period of time.

Effectiveness of legal norms

The effectiveness of a legal norm means that the addressees in question have rights and obligations arising from it. The prerequisite for effectiveness of a legal norm is its validity. This means that a legal norm can enter into force at the earliest on the day of its validity. However, a legal norm may enter into force later. Thus, a certain period may elapse between the day when a legal regulation becomes valid and the day when it entered into force (the so-called *vacatio legis*). This period is intended to enable the addressees of a legal norm to become acquainted with the legal norm and to adapt to it. The date of entry into force is usually stated in the last provision of the legal norm.

Examples of the law around us:

- Purchase contract
- Contract for work
- Loan agreement
- Employment contract / work contract / contract for work
- Contract for the provision of consulting services
- Licence agreement
- Management contract
- Confidentiality agreement
- Agreement on the sale of a business share
- Civil torts (defamation, breach of contract)
- Crimes (e.g. theft, fraud, copyright infringement, etc.)

1.2. The relationship between the law and cyberspace

Much has been published about the relationship between the law and new technologies, especially the Internet, including its changes and transformations. But many key issues remain unresolved, and many other problems are only in the phase of their identification or analysis. Nevertheless, although the search for reasonable solutions is on the right track in the better cases, sometimes there is no solution in sight. The Internet is undoubtedly a *sui generis* phenomenon. As such, it does not stand alone but is directed mainly through the regulation of the conduct of its users.

The law is one of its possible regulations in the form of imperfect normative constructions, where it applies more so than elsewhere that between conduct in reality, i.e. what is actually carried out in the Internet environment, and normative conduct, i.e. what should be (by the will of the regulator and ours), do not match up. The reality of the Internet and its normative regulations are therefore two relatively separate categories. This assumption will not be challenged in this publication either. On the contrary, it will be one of its mainstays.

Most legal problems related to the Internet must be considered in the overall legal and technological context, not only from the perspective of established formulas or from the perspective of individual legal disciplines *per se*.[1]

---

[1] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Prague: CZ.NIC, 2013. ISBN 978-80-904248-7-6 p. 25

2. Responsibility in cyberspace

Cyberspace

Scope of the law in cyberspace

2.1. Cyberspace

"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."

William Gibson: Neuromancer (1984)

Cyberspace is a metaphorical sandbox where we move, but it is also a key element in the definition of cybersecurity. In order to be able to define cyberspace, it is essential to define the concept of the Internet, which pertains directly to it.

The global beginnings of the Internet, which is a necessary material foundation of cyberspace, date back to the 1950s. At that time, networks of interconnected computers were built and tested, primarily for scientific research and military purposes. Although the Internet was built on the foundations of the ARPANET and NSFNET[1] networks, no one currently owns the Internet, and there is no central authority or institution to manage it. *"Nevertheless, there are institutions that play a significant role in the operation and further development of the Internet. First, let's mention the Internet Society (ISOC), which brings together Internet users. ISOC has two main components: the Internet Activities Board (IAB) and the Internet Engineering Task Force (IETF). Both of these components work with the most important computer companies to create the standards needed for the further development of the Internet."*[2]

ICANN[3] (Internet Corporation for Assigned Names and Numbers) has a sovereign position within the Internet. The scope of activities of this association includes setting rules for the operation of the domain name system. Nowadays, however, ISPs are gaining more and more prominence, and they are playing a bigger role.[4]

The material foundation of the Internet is its backbone network, which conducts a signal (data) through air, cables or other transmission media. In technical terms, it means the worldwide distributed computer network composed of individual smaller networks that are interconnected using internet protocols (IPs) and thus enable communication, data transfer, information and provision of services between entities. This actually creates a dynamic, ever-changing and evolving system tied to hardware, but at the same time, it creates a hard-to-define and virtually unlimited cyberspace. It can be said that cyberspace is a virtual reality that is effectively boundless. However, this virtual reality is completely dependent on the material foundation, i.e. the technologies found in the real world. This creates an interesting paradox that allows the existence of intangible media (cyberspace) able, due to the distribution of tangible media (network elements, individual computer systems, cloud storage, interconnected services, etc.) to adapt and change in case of damage to material media, but in the event of a complete collapse of material medium (or all its components), irreversible damage or extinction of cyberspace as such will occur.

Cyberspace can also be defined as a space of cybernetic activities, or as a space created by information and communication technologies where a virtual world (or space) parallel to real space is created.

The concept of cyberspace began to become more widely known after the declaration of John Barlow (founder of the Electronic Frontier Foundation): „A Declaration of the Independence of Cyberspace":

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland
February 8, 1996[5]

Even almost twenty years after the publication of this declaration, its text remains undeniably relevant. Today's society is trying to respond to the huge expansion of information and communication technologies, their intertwining and interconnection, the emergence of new trends, etc. However, this reaction is often primarily based on enforcement and restriction, rather than understanding and educating users.

Cyberspace, in contrast to the real world, is very specific, and it is certainly wrong to assume that the same rules will work in it as "offline". In general, it can be stated that standard criteria can be applied to cyberspace, and they are valid in relation to the actual physical location of data or information. The second possibility is the creation of new criteria for the application of the principle of local jurisdiction. (This is a virtual localisation of legal relations.)[6]

It is characteristic of cyberspace that a large part of society is connected to it (the estimated involvement of around 3.6 billion people from a global population of around 7.4 billion people).[7] At the same time, it must be stated that the mass involvement of society began only about 15–20 years ago.

Features of cyberspace include its decentralisation, globality, openness, richness of information (including information in the form of "information smog", utter nonsense, half-truths and lies), interactivity and the ability to influence opinions through users (avatars[8]). The essential character of cyberspace is that technology and related services play a primary role in it. Recently, it has become increasingly clear that the manifestation of the virtual world can and does have implications in the real world.

The speed and especially the availability of transmitted data is becoming a key element of today. As a rule, users do not want or do not try to find out where and how the data they entered into information networks are transmitted. They are also not interested in where the recipient of the transmitted data is located or where the data are retained, thus content is dematerialised from the physical structure of information networks.

On the one hand, it is possible to observe a situation **where social relations are delocalised in cyberspace**[9], which entails problems in terms of law enforcement, but on the other hand, this delocalisation allows users to communicate, send, store and change data freely (and without restrictions in the form of borders).

Features of cyberspace include its **decentralisation, globality, openness, richness of information, interactivity** and the ability to influence opinions through a user. An essential attribute of cyberspace is that technology and related services play a primary role in it. Recently, it has become increasingly clear that the manifestation of the virtual world can and does have implications in the real world.

As for a legal definition of cyberspace, it is possible to use, for example, the wording of Section 2 (a) of Act No. 181/2014 Coll., on Cybersecurity[10], where it is stated that "*cyberspace is a digital environment enabling the creation, processing and exchange of information, consisting of information systems, and electronic communications services and networks*."

In our opinion, one of the more effective definitions of cyberspace is in Cyberspace Operations: Concept Capability Plan 2016–2028, which defines **cyberspace as a space composed of three layers:**[11]

1. **physical**,
2. **logical** and
3. **social**.

These layers then consist of a total of five components.

Ad 1) Physical layer

This layer includes the term "**geographic component**" and the term **physical network components**. The term "geographic component" means the exact location of network elements in the physical world. The term physical network components includes the infrastructure in the form of cables, network control elements (switch, router) and other devices.

This division of the physical layer has its own logic. While geopolitical borders between states can be easily crossed in cyberspace, in the real world there are still limitations that stem from the nature of our physical world.

Translating this idea into a world of cyberattacks and incidents means that, as an attacker, I can damage a physical layer element either remotely, for example, by knowing its specific vulnerability that can be remotely attacked, or I can damage it directly in the real world if I can get to it physically and attack it, for example, using physical force. The impact in cyberspace will be the same, but the execution of the attack itself is quite different.

Ad 2) Logical layer

This layer contains **logical network components**, which means logical connections between network nodes. These are implemented via network communication protocols. Nodes can be computers, telephones and other network devices.

Ad 3) Social layer

This layer consists of components called "**cyber personality**" and **personality**.

The "cyber personality" component includes the identification of a person on the network, such as email address, IP address, telephone number and more. The personality component consists of real people connected to the network. One individual can then have multiple "cyber personalities", such as different emails on different devices, and one "cyber personality" can actually be multiple different real people, using, for example, a single shared account.

Cyberspace can also be defined according to the availability and traceability of data for an average user. According to this division, cyberspace can be divided into services and data available via the Internet, services and data available only within specific networks and devices, and services and data intentionally hidden and accessible using special tools.

Typically, the following names are used for these categories:

1. **Surface Web**,
2. **Deep Web** and
3. **Dark Web**.

The Deep and Dark Web are also collectively referred to as **D4rkN3ts – Darknets**. All these components together create the real cyberspace.[12]

Unfortunately, the terminology where the term *web* is used to divide cyberspace has been influenced by the fact that the following simple equation holds true for most of the general public:

CYBERSPACE = INTERNET = **WEB**

However, cyberspace is not just about websites but all the computer systems, services, users and data of this space.

---

[1] Cf. *Internet History of 1980s.* [online]. [cit. 07/06/2016]. Available from:

http://www.computerhistory.org/internethistory/1980s/

[2] *Internet, připojení k němu a možný rozvoj (Část 2 – Historie a vývoj Internetu).* [online]. [cit.10/02/2008]. Available from: http://www.internetprovsechny.cz/clanek.php?cid=163

[3] For more details, see https://www.icann.org/

[4] ISP – Internet Service Provider.

[5] BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit.23/09/2014]. Available from: https://www.eff.org/cyberspace-independence.

[6] For more details see REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, p. 218

[7] See e.g. *World Internet Users and 2015 Population Stats.* [online]. [cit.09/08/2015]. Available from: http://www.internetworldstats.com/stats.htm

[8] I use the term avatar here intentionally because it is an expression of a virtual identity created by a real individual.

The term avatar originally comes from Hinduism, where the term referred to the embodiment of God or the liberated soul in bodily form on earth (the earthly incarnation of a spiritual being).

Currently, this term is used as a visual representation (icon or character) of a user in the virtual world (in a game, blog, forum, Internet, etc.), i.e. in cyberspace.

[9] *Delokalizace právních vztahů na internetu* [online]. [cit.15/04/2012]. Available from: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

[10] Hereinafter referred to as the CSA

[11] TRADOC. Cyberspace Operations: Concept Capability Plan 2016–2028. [online]. [cit. 18/02/2018], pp. 8–9 Available from: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

[12] Cf. E.g. *The dark Web explained.* [online]. [cit. 20/07/2016]. Available from: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html

or

Surface Web, Deep Web, Dark Web – What's the Difference. [online]. [cit. 20/07/2016]. Available from: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

2.2. Scope of the law in Cyberspace

Cyberspace is open and easily accessible to all, ***"... there are no special laws, and it is necessary to follow generally binding standards."***[1]

The indisputable fact is that the implementation of an ever-increasing number of social as well as economic relations is moving into the environment of information networks. Thus, the need for a certain legal regulation of such conduct arises. Due to the delocalisation of legal entities in different countries around the world, the question is what legal system (if any) will apply to any acts (or offences) committed on the Internet.

It is therefore necessary to primarily address two issues. Firstly, whether the law applies on the Internet and, if so, what legal norms apply. Secondly, how this right can be exercised, including possible sanctions or other measures. An example of a difficult application of the law is a case in 2005, when a player of an online game "*The Legend of Mir 3*" **killed another player** in China **for stealing a virtual weapon**. There is a trade in virtual commodities among the players of this game, as well as a loan system. This is especially evident when some players are friends, but it is not a condition that they know each other from the real world. It was a loan that caused the murder. A player named Qui Chengwei lent a virtual sabre, the "*Dragon sabre*", to his virtual friend Zhu Caoyuan. However, Zhu succumbed to the allure of easy money and sold the weapon for 7,200 yuan (which is about 19,000–20,000 CZK) at an online auction. After Qui learned of the sale, he turned to the police and reported the theft of the virtual sabre. The police refused to handle the case, stating that virtual property (of essentially non-existent items) is not covered by law. Qui lost patience, attacked Zhu at his house and stabbed him to death.[2]

It is obvious that this is a very extreme case, but it appropriately demonstrates that the virtual world is not detached from the real world. Therefore, the issue of legal liability in it must be addressed.[3] In fact, since the beginning of the development of the Internet, there has been a conflict between the technical and legal worlds. From a technical perspective, the Internet is logically designed with a clear hierarchy and structure. However, the law, especially local law, has often injected "chaos" into this logic. The term "chaos" perhaps most aptly describes the efforts of legislation to regulate this purely technical world because, in cyberspace, a user has a wide range of options to "circumvent" a certain ban or restriction. In the following examples, I will try to demonstrate the interaction of the real and virtual world.

LICRA vs. Yahoo

One of the first cases relating to the applicability of the law on the Internet occurred in France in 2000. In February 2000, Marc Knobel (a French Jew who dedicated his life to fighting Nazism) visited the auction site www.yahoo.com and found that the server offered a number of Nazi-related items or items related to the German armed forces from World War II on its websites. After this discovery, Marc Knobel turned to Yahoo! Inc. requesting to block this site. Yahoo! Inc., however, did not comply with his request. On 11 April 2000, Marc Knobel, through LICRA (Ligue Internationale Contre Le Racisme et l'Antisémitisme) brought an action against Yahoo! Inc. in a French court for violating French law since the promotion and support of Nazism on television, on radio and in writing is prohibited in France. Yahoo! Inc. defended itself by claiming that the servers on which the auction portal operates are physically located in the United States, so French law cannot be applied to hardware and websites operated in the United States. The defence further argued that the content of the websites is primarily intended for US residents, to whom the First Amendment guarantees freedom of expression. Any attempt to remove this website would then be inconsistent with this amendment.

However, LICRA pointed out that, if Yahoo! Inc. does business in France, it has to respect the laws of France, and the Internet is no exception. Yahoo! Inc. responded to this argument that it is not able to determine where their customers are logging in to the auction portal. Therefore, if they removed the websites in question, not only would they not respect the First Amendment, but they would prevent access for all users, regardless of borders. This would make French law de facto global law. On 22 May, 2000, Judge Jean-Jacques Gomez ordered the company to block French users from accessing US auction websites with Nazi memorials. He justified his decision, inter alia, by saying that Yahoo! Inc. can identify French users so well that they can place advertisements in French on the websites they visit. The judge gave Yahoo! Inc. 90 days to install keyword-based filtering system on the Yahoo! Inc. French websites. *"Judge Gomez stated in the reasoning that it is possible to block up to ninety percent of French users from accessing the websites in question. The technical solution that Yahoo! has to come up with on the basis of the judgment will be assessed by a three-member international panel. His earlier finding states that up to 70 percent of users can be unblocked by their Internet Service Provider (ISP) designation and another 20 percent by tracking search engine keywords on Yahoo!."*[4]

Greg Wrenn, Yahoo! Inc. lawyer, said: *"Whenever the word Hitler is mentioned on a page commemorating Holocaust victims, the page will be closed automatically. It is not possible to talk about an effective judgment at all because in fact it is not possible to meet it."*

The technical problems at that time were, and still are to this day, in that only what can be clearly defined can be filtered (words such as Nazi, Heil Hitler, etc.). But the filter is not able to detect all possible versions of unwanted material (e.g. N_A_Z_I, H3II HiT_L3R, etc.). These differences can be recognised by natural persons (e.g. employees of a particular ISP), who then delete the page; however, an operator of a reprehensible forum or auction can simply change the address and continue its activities.

Yahoo! Inc. waived its appeal against the French court's judgment and began blocking French users from websites offering objectionable content. However, Yahoo! Inc. also applied to the court[5] with local jurisdiction in the United States for a declaratory judgment that would exclude the jurisdiction of the French court over the American company. That court upheld the view of Yahoo! Inc. that the enforcement of the French decision in the United States was unconstitutional. LICRA appealed against that judgment. The US Court of Appeals responded by denying its jurisdiction over LICRA organisations. In 2006, the case went to the US Supreme Court[6], which refused to consider the case in the end. Thus, US court rulings were more in favour of Yahoo! Inc. However, it eventually voluntarily decided to completely remove websites offering Nazi-themed items from its servers, not only in France.

Gutnick vs. Dow Jones

Joseph Gutnick (an Australian diamond businessman) read an article about himself in an online edition of *Barron's*[7] newspaper in 2000, which he considered defamatory. Gutnick filed a defamation lawsuit against Dow Jones in an Australian court. Dow Jones used similar arguments as Yahoo! Inc. in its dispute with LICRA. The argument was based primarily on the fact that the printed version of the newspaper is primarily intended for the US market, so the case cannot be covered by Australian law.

Despite this argument, the Australian court ruled[8] in 2002[9] as follows: *"Since the material (article) is also available in Australia, the place where Gutnick is best known, the defamation can do him the most harm. Dow Jones is required to pay Gutnick compensation."* The court said it would not consider whether the Internet has boundaries or not, taking into account in particular where the content was available, not where it was published. The court also stated that everyone has the right to legal protection against similar conduct or other attacks. In its judgment, the Australian court also noted the reality of the cross-border nature of the Internet, which corresponds to the extensive exercise of jurisdiction.

GoDaddy

GoDaddy[10] is the US majority registrar of Internet domains. In 2016, it manages more than 61 million Internet domains, making GoDaddy the largest domain registrar. Registering a domain with this ISP is very simple and affordable. At the same time, due to the company's location in the US, users are provided with legal protection for their personal data and data listed on a domain registered under GoDaddy, provided that users do not violate US law. For this reason, domains registered with GoDaddy are very often used by, for example, extremist, racist and other groups or users. These users then depend on US constitutional law and the First Amendment to the US Constitution:

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[11]

The problem in addressing cybercrime with the above content is to prove the reality of the threat or crime so that it is not a violation of the First Amendment to the Constitution.

Second Life (and "child" porn).

Second Life is a 3D virtual environment developed by Linden Lab. This environment allows you to create your own avatars and use them to interact with others, with the possibility to generate profit. Second Life is divided into two virtual worlds according to the age of a user.[12] Users are able to change their identity and modify the appearance of the avatar according to their ideas. In 2007, the German station ARD and subsequently CNN drew attention to the existence of a "paedophile island."[13]

This report points to the fact that some MainGrid users (i.e. users over the age of 18) created avatars in the form of a child and others pretended to be adults. As part of the mutual interaction, avatars of children were abused by adult avatars. Law enforcement authorities in Germany launched an investigation because possession of virtual child pornography is a criminal offence under German criminal law.[14] Linden Lab cooperated with the German authorities in identifying the users and owners of the virtual plots on which the virtual child pornography took place. In the Federal Republic of Germany and the United Kingdom, the conduct in question was punishable by criminal law, but in the United States such conduct was not prosecutable.

At present, there is no state in the world that would waive the right to punish an infringement that affects the interests it protects.

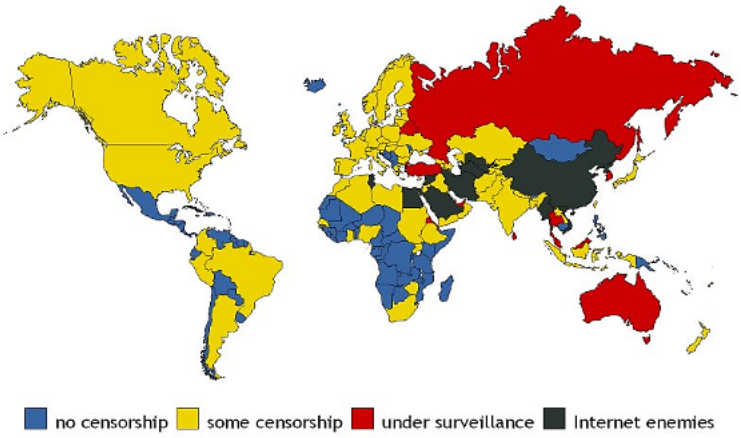


Figure 1 – Division of states according to Internet censorship

In addition to the above cases, there are a number of other examples of Internet regulation and Internet services provided by organisations or states. This regulation then necessarily entails problems with the applicability and enforcement of the law.
The map presented (see Figure 1)[15] shows that most countries in the world have adopted legal instruments that affect the Internet or the services provided.

From a user's point of view, it must be stated that the principle of territoriality in connection with the Internet loses its meaning because he/she can be located anywhere in the world at any time, without a user having to know where the server with which he/she is communicating is located. From this point of view, the Internet is global and knows no boundaries.

"It is true that a physical location of certain information can be traced at any given time – but the location is often random, very short-term and usually completely irrelevant to the information as such and its legal effect."[16]

The law should keep pace with the virtual world, but unfortunately this does not always work as states (closed in fixed territories) often lack the means to effectively enforce law within cyberspace.[17] Basically, there are two ways to address this problem. One possibility is to respect the principles of territoriality of states as they are set today. This approach would then essentially mean that, if someone interfered with the rights that the state guaranteed to protect, it would have to wait until the attacker is in the physical jurisdiction of the state[18], or the attacker would have to use international legal aid.

The second option is to create special legislation, the so-called Internet jurisdiction, which would apply to the online world. The question is how this new right would be adopted by individual countries. Personally, I believe that, under the current conditions, it is not possible to unite all branches of law worldwide (civil, commercial, criminal, administrative, etc.), in which the Internet intervenes in some way. I base my assertion on the fact that the

Convention on Cybercrime, which defines the basic groups of crimes that should be prosecuted in cyberspace, was adopted in 2001, but as of 1 August 2016, only 49 countries had ratified it.

Given the global nature of the Internet, it also seems to be problematic to **determine**:

1. **applicable law** (under which state's law the potential litigation will be decided),

2. **authority empowered to issue a decision**,

3. **authority which may enforce or directly execute a decision**.[19]

In addition to classical legal norms, *defining authorities* participate in the creation of the law or rules on the Internet by creating *defining standards*.

---

[1] SMEJKAL, Vladimír. *Internet a §§§.* 2nd updat. and ext. ed. Prague: Grada, 2001, p. 32

[2]Cf. HAINES, Lester. *Online gamer stabbed over "stolen" cybersword.* [online]. [cit.03/10/2006]. Available from: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

[3] Cf. Decision of the Supreme Court 4 Tz 265/2000, as of 16/01/2001. [online]. [cit.13/03/2008]. Available from: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

[4] ŠTOČEK, Milan. *V Hitlerově duchu proti Hitlerovi.* [online]. [cit.10/07/2016]. Available from: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

[5] United States District Court for the Northern District of California in San Jose

[6] United States Supreme Court

[7] http://online.barrons.com

[8] High Court of Australia

[9] Judgement [2002] HCA 56 as at 10 December 2002, [online]. [cit.24/03/2014]. Available from:

http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html

[10] https://uk.godaddy.com/

[11] *First Amendment.* [online]. [cit.10/07/2016]. Available from: https://www.law.cornell.edu/constitution/first_amendment Author's translation

[12] **MainGrid** – intended for users from the age of 18; **TeenGrid** – intended for the age group from 13 to 18.

[13] For more details see: *CNN on pedophile sex in Second Life.* [online]. [cit.18/06/2009]. Available from: http://www.youtube.com/watch?v=AQM-SiiaipE

[14] *Second Life 'child abuse' claim.* [online]. [cit. 16/06/2009]. Available from:

http://news.bbc.co.uk/2/hi/technology/6638331.stm

[15] *Internet censorship.* [online]. [cit.10/08/2016]. Available from: http://www.deliveringdata.com/2010_10_01_archive.html

[16] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 7

[17] Cf. statements in the framework of the **Declaration of the Independence of Cyberspace**.

Cf. THOMAS, Douglas. *Criminality on the Electronic Frontier.* In Cybercrime. London: Routledge, 2003, p. 17 et seq.

Cf. JOHNSON, David R. and David POST. *The Rise of Law in Cyberspace.* [online]. [cit.10/07/2016]. Available from: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067

[18] An example of this approach may be the case where a user from the Czech Republic, for example, will publicly and repeatedly attack a country on the Internet (e.g. for non-compliance with human rights in said country, etc.), or will carry out other activities that are illegal in the targeted country (though it is not illegal in the Czech Republic). If such a user decides at any time in the future to visit the country against which he/she has acted against, the country's territorial law may apply to him/her when crossing the borders into that country.

[19] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 7

2.3. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

ℹ️

- To understand the issues of laws and regulations governing cybersecurity, at least the basic principles of the functioning of law, its division and implementation are needed. The first two chapters present the general framework of the applicability of the law in cyberspace.
- A legal norm represents a generally binding rule of conduct that regulates the rights and obligations of entities. This rule of conduct is expressed in a special legal form recognised by the state (or the European Union), and its observance is ensured by state enforcement.
- The law is one of its possible regulations in the form of imperfect normative constructions, where it applies more so than elsewhere that between conduct in reality, i.e. what is actually carried out in the Internet environment, and normative conduct, i.e. what should be (by the will of the regulator and ours), do not match up. The reality of the Internet and its normative regulations are therefore two relatively separate categories. This assumption will not be challenged in this publication either. On the contrary, it will be one of its mainstays.
- Cyberspace is:
  - a space of cybernetic activities, or a space created by information and communication technologies where a virtual world (or space) parallel to real space is created.
  - a digital environment enabling the creation, processing and exchange of information, consisting of information systems, and electronic communications services and networks.
  - space composed of three layers: physical, logical and social.
- Examples of the application of the law in cyberspace were presented in individual case studies.

🔑

KEY WORDS TO REMEMBER

- law
- legal norm
- cyberspace

❓

KNOWLEDGE CHECK

Questions

1. What is the law?
2. What is a legal norm, and how is it divided?
3. What is cyberspace?
4. What layers does cyberspace consist of?
5. Does the law apply in cyberspace, and if so, what legal norms apply?
6. How can the law be applied in cyberspace, including possible sanctions or other measures?
7. Give some examples of the application of the law in cyberspace.

3. Legal basis of ISP (internet service provider) activity

Defining authorities participate in the creation of the law on the Internet, in the restriction or expansion of its activities, by creating *defining standards*. In order to understand the question of a possible liability of information society service providers, I must first characterise the defining standards and the defining authority.

Defining standards are created and implemented by entities that are authorised to define the information network environment. These are in practice *sui generis* standards that define information networks as such. They occur in layers that are interdependent. *"Defining standards are created by telecommunication operators, office software producers but also, for example, creators or operators of online games, or anyone who opens a blog or has an email box. (A defining standard created by a user of this box is a filter that automatically performs a set inbox operation)."* [1]

Defining authorities are the creators of defining standards. It is an entity that, through its operation, creates rules for the functioning of the logical system in which the authority operates. As mentioned earlier, ICANN has an executive position among these authorities since it is responsible for assigning, administering and laying down rules for the domain name system.[2] Another defining authority is, for example, the IETF.[3] Although defining authorities may appear to be unrestricted administrators of cyberspace, they are still subject to the law of a state.[4]

The specificity of the **Internet** is that it **exists only thanks to defining authorities**. **It is composed of them. No operation will take place without the participation** (execution or mediation of the operation) **of the defining authority**.

Lawrence Lessig states in his book Code and Other Laws of Cyberspace (Code v. 2): *"We can build, design or encode*[5] *(program) cyberspace to protect the values we consider fundamental. But we can also design or program it by letting these values disappear. There is no middle ground, everything in cyberspace is built in some way. We never discover the code, we always create it."*[6]

Following the statement above and my experience with cyberspace, I dare say that the greatest **defining authority**, even if it is not the entity that creates the rules of operation of the logical system, **is a user as such**. Its defining role acts indirectly. A user of services provided by each ISP directly or indirectly influences what will be successful in cyberspace and what will not. If a sufficiently large group of users decides to actively stop using any of services provided by an ISP, such a service will be forced to change its "conduct" based on user demand, or in the worst case, will cease to exist. It is a question of how large a group of people would have to stop using services such as Google, Microsoft, Facebook, etc., so that it is not marginal for these companies. However, it is cyberspace where users have the opportunity to directly influence the operation or non-operation of individual services.

The following conclusions can therefore be drawn:

§ **Cyberspace is formed by the will of defining authorities.**

§ **All information society service providers are defining authorities.**

§ **Every service provider, like any other body of law, is legally responsible for its actions.**

The issue of liability of information society service providers (ISPs) under the Act on Certain Information Society Services is mentioned here intentionally as it is directly related to the issue of cybercrime, user liability, and finding and securing information relevant to criminal proceedings. *"In general, the principle is that if information is illegal and an ISP has no knowledge of its creation or communication, the ISP is exempted from liability by law."*[7]

In addition to the above-mentioned law, the term service provider is also defined, for example, in the Convention on Cybercrime, specifically in Article 1 (c) where it is stated that service provider is:

§ any public or private entity **that provides to users of its service the ability to communicate by means of a computer system**, and

§ any other entity **that processes or stores computer data on behalf of such communication service or users of such a service**.

---

[1] Cf. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 42 et seq., p. 88 et seq.

RFC (*Request For Comments*) can also be included in the defining standards. Although these are documents with the nature of recommendations rather than standards, they are respected by users as if they were standards. RFCs are freely available at http://www.ietf.org/rfc.html.

[2] The domain name is used to denote the "class" of computer systems connected to the Internet. They are characterised by a certain geographical and organisational unity: e.g. all computers in the **.cz** domain are located in the Czech Republic. All computers in the domain (subdomain) **nic.cz** are computers under the administration of the CZ.NIC association. The names of the main domains (based on geography) are strictly separated.

Regarding domain names, Polčák states, among other things, that: "A form of **virtual reality** can be a domain name. It is a record in DNS databases. **If the domain authority decides to delete the domain name, this virtual reality will cease to exist.** It doesn't matter if it is a domain name such as: www.tondovy_stranky.cz or www.google.com.

[3] IETF – The Internet Engineering Task Force. For more details, see https://www.ietf.org/.

[4] It is always a natural or legal person that has its registered office or permanent residence. Therefore, they are subject to the law as any other entity. In some countries (e.g. **China**), the defining authority is the state itself.

[5] Lessig refers to the **defining standard** as **code**.

[6] Cf. LESSIG, Lawrence. *Code v. 2. p.* 6 Available in full (Eng) [online]. [cit.13/03/2008]. Available from: http://pdf.codev2.cc/Lessig-Codev2.pdf

[7] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 55

3.1. Regulation of ISP activities in the Czech Republic

The basic legal norm characterising the ISP activities in the Czech Republic is Act No. 480/2004 Coll., on Certain Information Society Services[1]. This act is an implementation of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.[2]

The Czech Act on Certain Information Society Services recognises the following three service providers, stipulating that a service provider is any natural or legal person who provides any of the information society services:[3]

1. **Providers of services based on the transmission of information provided by a user** (Mere Conduit or Access Provider).
2. **Providers of services based on the automatic intermediate storage of information provided by a user** (so-called caching).
3. **Providers of services based on the storage of information provided by a user** (so-called storage or hosting).

No person is excluded from the above definition. (It does not have to be, for example, a person doing business under another legal regulation.) However, if other special regulations apply to a provider (see e.g. one of the connection providers), they must also follow them.

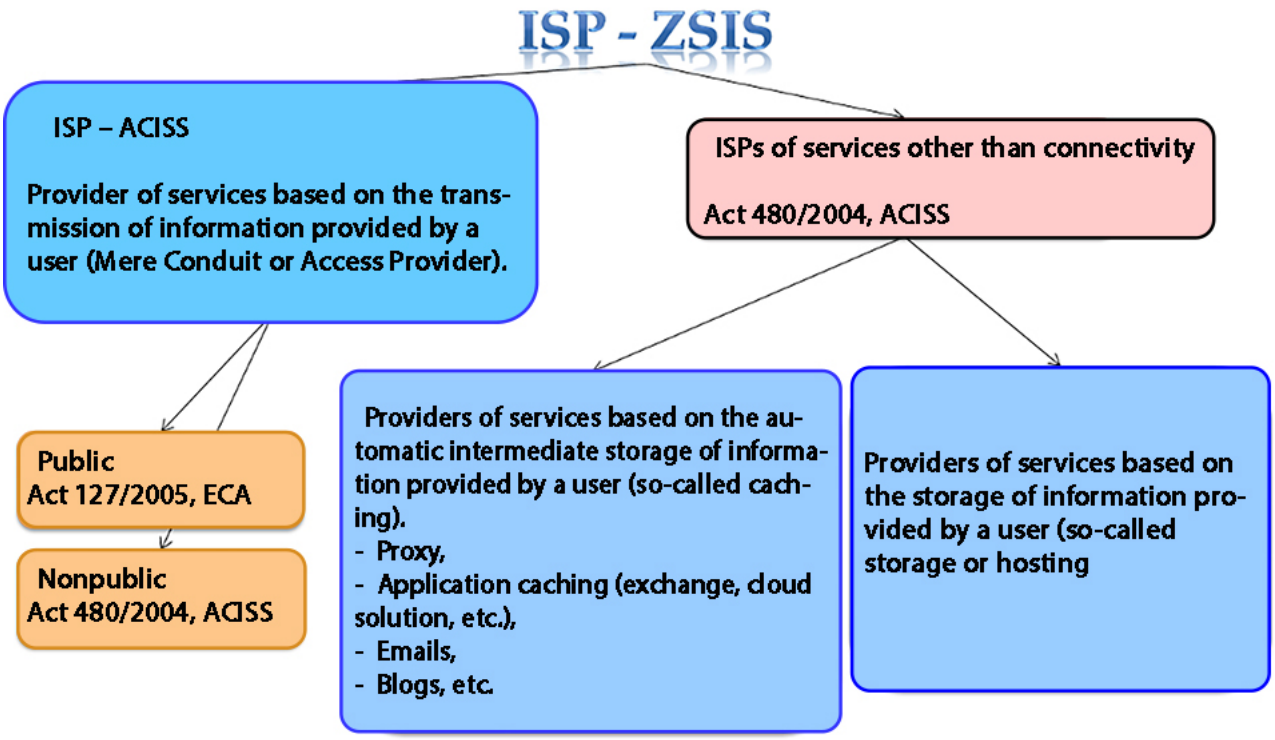
---

[1] Hereinafter referred to as the Act on Certain Information Society Services or ACISS

[2] Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535&qid=1624364501265

[3] See Section 2 (d) of ACISS

Graphically, it is possible to show the listed providers (and the binding by individual legal regulations) as follows:



A recipient of an information society service is a user who can be any natural or legal person using the information society service, in particular for the purpose of seeking information or making it accessible.[1]

According to the Act on Certain Information Society Services, **information society service** means *"any service provided by electronic means at the individual request of a user submitted by electronic means, normally provided for remuneration. A service shall be provided by electronic means if it is sent via an electronic communication network and collected by the user from electronic equipment for the storage of data."*[2]

The definition given in the Czech legislation is then directly based on Directive (EU) 2015/1535 of the European Parliament and of the Council [Article 1 (b)], which states that a service is *"any information society service, i.e. any service normally provided* ***for remuneration, remotely, by electronic means and at the individual request of a recipient of services."***

Four basic features of a service follow from this definition:

- it is provided by electronic means,
- it is provided at the individual request of a user,
- it is normally provided for remuneration,

- it is provided remotely (at a distance).

The concept of provision by **electronic means** is set out in Directive (EU) 2015/1535 of the European Parliament and of the Council in Article 1 (b) (ii), where it is defined as a service that is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data. This service is entirely transmitted, conveyed and received by wire, radio, optical or other electromagnetic means. The Czech regulation uses a demonstrative list that states that it is mainly a network of electronic channels, electronic communication equipment, automatic calling and communication systems, telecommunications terminal equipment and electronic mail.[3]

An **individual user request** means that it must be an active activity by a user. Husovec states that it concerns cases where, for example, a user enters an address into the browser field (IE, Firefox, Chrome, etc.), thereby formulating a request to open the relevant page, or writes an SMS message. According to Husovec, a typical example of a service that is provided without an individual request is, for example, television broadcasting.[4]

The most problematic criterion for defining an information society service is that a **service is provided for remuneration**. The Czech regulation also copies the international regulation on this point and contains a provision "*normally for remuneration*". In the environment of the Internet or other computer networks, there are a number of services that are provided "for free". Husovec quite rightly argues that, under the term remuneration, it is possible to imagine a number of facts different from purely monetary performance.[5] It can be a performance that will take the form of a non-monetary nature, where an ISP obtains information about users in the form of personal, technical and other data, time spent using the service, offers a user advertising for other products, etc. However, even this condition should be interpreted more extensively according to Husovec, meaning that a *potentially economic* activity is carried out.[6]

Due to the fact that the term remuneration can mean really different possibilities (e.g. a thanks, visit to a site or link, financial or other payment) and due to the wording of the Act on Certain Information Society Services (see *"normally for remuneration"*), a conclusion can be reached that the activities of an information society service provider may also be provided free of charge.

The term **remotely** is defined by Directive (EU) 2015/1535 of the European Parliament and of the Council as a service that is provided without the parties being simultaneously present.[7]

In his monograph, Husovec also gives examples that demonstrate what can be considered an information society service. According to Directive 2000/31/EC of the European Parliament and of the Council, a number of activities that take place in the online world must be included under this concept. It can be online sales of goods, services that provide online information, commercial communication, or services providing tools for searching, accessing and retrieving data, services providing information transmission through a communication network, etc.

"The judicature of the Court of Justice of the EU has already directly or indirectly recognised, for example, the AdWords service (advertising service in Google search engine)[8]*, motor vehicle insurance services via the Internet****[9]****, online sales of contact lenses*[10]*, Internet connection*[11]*, hotel reservations via email****[12]****, travel agency services via email*[13]*, eBay auction server*[14] *and traditional Google search."* [15]

---

[1] See Section 2 (e) of ACISS

[2] See Section 2 (a) of ACISS

[3] See Section 2 (c) of ACISS

[4] For more details see HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Prague: CZ.NIC, 2014, p. 100

[5] Ibidem, p. 98.

[6] Ibidem, p. 99.

[7] See Article 1 (b) (i) of this Directive.

[8] Decision *Google France* C-236/08 to C-238/08.

[9] Decision *Bundesverband* C-298/07.

[10] Decision *Ker-Optika* C-108/09.

[11] Decision *Promusicae* C-275/06 and *Tele 2*. C-557/07

[12] Decision *Alpenhof* C-144/09.

[13] Decision *Pammer* C-585/08.

[14] Decision *L'Oreal v. Ebay* 324/09.

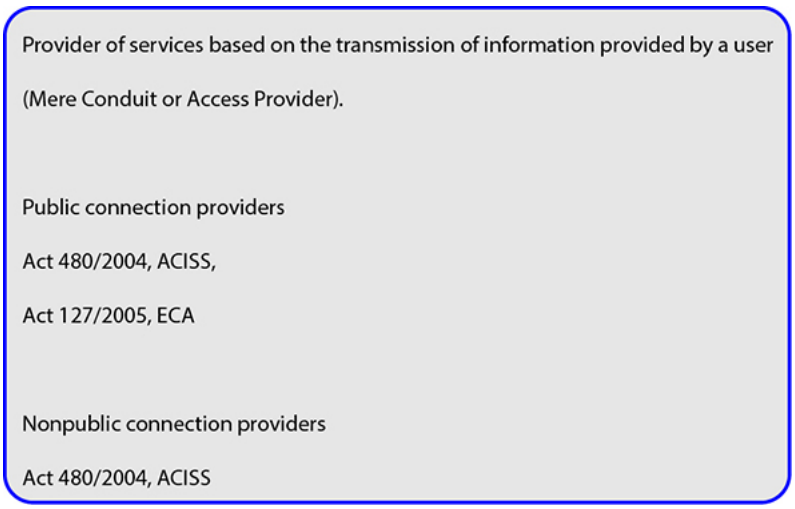
[15] HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Prague: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, pp. 101–102.

3.1.1 Providers of services based on the transmission of information provided by a user (Mere Conduit or Access Provider)

From the point of view of the Act on Certain Information Society Services, such a provider may be any natural or legal person who is able to provide other entities (natural or legal persons) with the service of transmitting information (provided by users) via electronic communications networks or arranging access to electronic communications networks for the purpose of transmitting information.

Such a provider will not only be persons doing business in the field of connecting others to computer networks or the Internet (typically they will be persons registered in the *Register of Entrepreneurs in Electronic Communications under the general authorisation*)[1], but it will be any person providing or mediating transmission of information via electronic communications networks. It is therefore possible to imagine a situation where a connection provider according to this law will be a person who establishes and makes available to others, for example, Wi-Fi connection within a restaurant, apartment building, household, etc. This category will also include, for example, schools (typically universities that provide their students and teachers with connectivity within their network or to the Internet.). However, services based on the transfer of information also include, for example, the Skype application, ICQ, etc. We can very simply describe these providers as **connection providers**.

However, in order to define the individual rights and obligations of connection providers, these providers need to be divided into two groups, **public and non-public**. Both groups of connection providers are covered by the Act on Certain Information Society Services, but public connection providers are also covered by the Electronic Communications Act, which sets out further rights and obligations for these providers. The above-mentioned *Register of Entrepreneurs in Electronic Communications according to the general authorisation* administered by the Czech Telecommunication Office will help to determine whether the provider is included in which group.



[1] The database of entrepreneurs in electronic communications according to the general authorisation is available online: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

3.1.1.1 Rights and obligations of the provider of services based on the transmission of information provided by a user according to ACISS

The Act on Certain Information Society Services in the case of a connection provider limits as much as possible the responsibility of this entity for the transmitted information. However, special requirements and conditions are set for operators of electronic communications services. These conditions are set out in the Electronic Communications Act. Provisions of Article 12 of Directive 2000/31/EC allows Member States to order a provider to suspend the provision of services through which information is transmitted where said services unduly interfere with the rights of another. This option is one means of preventing infringements. The order to suspend the provision of services is usually issued by a court.

A **connection** provider can only **be held responsible for the content of information** if:

§ it initiates such a transmission,

§ it selects the user of transmitted information, **or**

§ it selects or changes the content of transmitted information.[1]

Pursuant to Section 6 of ACISS, a **connection provider is not obliged** to supervise the content of transmitted information or to actively ascertain the illegality of transmitted information. A provider cannot be held responsible for the quality of information (which cannot be attributed to it), even if it is aware of the illegality of transmitted information.[2]

3.1.1.2 Rights and obligations of the provider of services based on the transmission of information provided by a user according to Act No. 127/2005 Coll.

Public connection providers are also governed by Act No. 127/2005 Coll., on Electronic Communications[3]. This law defines some terms that it further uses. For the purposes of this monograph, these are in particular:

§ **Electronic communications service** [Section 2 (n) of ECA[4]]. According to Section 2 (n) ECA, this term means a service that is usually provided for a remuneration and is based on (wholly or mainly) the transmission of signals via electronic communications networks. This service does not include services offering content via electronic communications networks and services or exercising editorial supervision over content transmitted by networks and provided by electronic communications services. Furthermore, this service does not include information society services that are not based wholly or mainly on the transmission of signals over electronic communications networks.

§ **Publicly available electronic communications service** [Section 2 (o) of ECA]. This service is an electronic communications service that no one is excluded from using beforehand.

Non-exclusion means the possibility of entering into a contract with a business entity providing a publicly available electronic communications service. It is important that this service is open to a wide range of people, none of whom is excluded beforehand. The opposite of such a service can be, for example, membership in various associations, chambers, or, for example, the status of a school student.

§ **A business entity** providing or authorised to provide a public communications network or associated facilities is referred to by this act as an **operator** [Section 2 (e) of ECA].

§ **Subscriber** [Section 2 (a) of ECA] is anyone who entered into a contract for the supply of such service with a business entity providing publicly available electronic communications services. **User** [Section 2 letter n) ZoEK] is anyone who uses or requests a publicly available electronic communications service.

The Electronic Communications Act introduced, on the basis of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, *on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* [5], the obligation to preventively retain **traffic and location data**[6] on electronic communications. This obligation only applies to a business entity providing or authorised to provide a public communications network or associated facilities.

The purpose of the Data Retention Directive was to **harmonise Member States' rules on the obligation of providers of publicly available electronic communications services or public communications networks** to retain traffic and location data so that they can be provided to Member States' competent authorities for **prevention, investigation, detection and prosecution of serious crime, such as terrorism and organised crime**.

The scope of the directive has been defined in the area of traffic and location data on legal and natural persons and on related data that are necessary to identify the subscriber or registered user.

This directive did not apply to the content of electronic communications or to information required when using an electronic communications network.

Under the directive, the **Member States were required to ensure that telecommunications data were retained for a minimum of six months and a maximum of two years from the date of communication**. The directive has been transposed in various forms into the legal systems of the EU Member States. However, since its inception, there have been conflicts of opinion on the directive as such. Opponents argued that the directive disproportionately interferes with fundamental human rights and freedoms, in particular by essentially mandating the widespread collection of information on individual users. It was further argued that the directive (in such a general form) would not be able to pass the proportionality test.

The **proportionality test** is a standard legal instrument of both international courts and constitutional (national) courts when assessing the conflict of provisions of the legal order seeking to protect a constitutionally guaranteed right or public interest with another fundamental right or freedom. The proportionality test includes three criteria for assessing the admissibility of an intervention:

1. The **principle of suitability** (fitness for purpose), according to which the **measure in question must be capable of achieving the intended objective** in general, which is the protection of another fundamental right or public good.

2. The **principle of necessity**, which stipulates the **use of only the most environmentally friendly means to achieve the desired purpose** (interference with fundamental rights and freedoms) **from several possible means**.
3. The **principle of proportionality** (in the narrower sense), which seeks to prevent **harm to a fundamental right disproportionate to the intended objective**, i.e. measures restricting fundamental human rights and freedoms must not, in the event of a conflict between a fundamental right or freedom and the public interest, exceed, by their negative consequences, the positives of the public interest in these measures.

The Data Retention Directive and its national transposition have become the subject of constitutional lawsuits in some EU countries. The decisions especially of the constitutional courts of Romania (2009), Germany (2010) and the Czech Republic (2011) must be mentioned among the most crucial. I will focus on court decisions in Germany and the Czech Republic.

The Federal Constitutional Court of Germany resolved a conflict between freedom and security (based on the Data Retention Directive) and ruled in favour of individual freedom. On 2 March 2010, the court ruled that the mass retention of data on telephone and data transmissions was unconstitutional in Germany.

The court responded to a mass complaint from 35,000 citizens seeking the repeal of a 2008 law ordering telecommunications companies to archive records of telephone calls and email communications for six months for investigative purposes. The Federal Constitutional Court repealed the contested regulations on the grounds that they were unconstitutional. It further stated that the obligation to retain data to the specified extent is not entirely unconstitutional from the outset, but there is no legal regulation corresponding to the principle of proportionality. According to the court, the contested regulations were not in line with constitutional requirements for data security, the purpose of the use of the data (and the transparency of the use of the data) was not clearly defined, and legal protection was not sufficiently ensured.

The court stated that *"the exercise of the fundamental rights and freedoms of citizens (here the secrecy of messages transmitted by electronic means of communication) must not be completely monitored, documented and registered by the state; this belongs to the constitutional legal identity of the Federal Republic of Germany, the preservation of which the republic must stand in at European and international level."*[7]

In the Czech Republic, the Data Retention Directive was implemented before its entry into force within the EU. (In the EU, it was implemented on 15 March 2007, with a requirement for transposition by 15 September 2007. In the Czech Republic, it was implemented in Section 97/3 of ECA, with effect from 1 May 2005.) A constitutional complaint was also filed in the Czech Republic, specifically by the association Iuricum Remedium, which was supported by a group of 51 deputies. This complaint was filed with the Constitutional Court in March 2010. In 2011, the Constitutional Court ruled and fully granted the petition for complete annulment of the relevant passages of the Electronic Communications Act (specifically Section 97 (3) and (4) and Implementing Decree No. 485/2005 Coll., on the Extent of Traffic and Location Data and the repeal of the provisions of the Criminal Procedure Code.[8] The Court stated as follows: *"The Constitutional Court found that the contested legislation violates constitutional limits because it does not meet the requirements of the rule of law and contravenes the requirements of restricting the fundamental right to privacy in the form of the right to informational self-determination within the meaning of Art. 10 (3) and Art. 13 of the Charter, which follow from the principle of proportionality."*

Legislators in the Czech Republic responded to the objections of the Constitutional Court of the Czech Republic, and **new legislation** that continues to allow widespread retention of traffic and location data in the Czech Republic was adopted as it respects the aforementioned **proportionality test**, in particular by clearly declaring the range of entities (authorised to request traffic and location data) and the purpose for which the data may be requested.

At the same time, measures have been taken ordering business entities to adopt such rules under the Electronic Communications Act to ensure that traffic and location data are of the same quality and subject to the same security and protection against unauthorised access, alteration, destruction, loss or theft or other unauthorised processing or use as data according to Section 88 of ECA.[9]

The maximum length for which these data can be retained has also **been set. It is currently 6 months.** After expiration of this period, a legal or natural person who retains traffic and location data is obliged to delete them, unless they have been provided to authorities authorised to use them under special legislation or unless otherwise provided by law (Section 90 of ECA). Furthermore, an **obligation was established to ensure that the content of messages is not retained and further handed over during the retention of traffic and location data** (Section 97 (3) of ECA).

At the same time, the Criminal Procedure Code emphasises the **principle of subsidiarity** (especially Sections 88 and 88a of Act No. 141/1961 Coll., on Criminal Court Proceedings: *"if the intended purpose cannot be achieved otherwise or if its achievement would be significantly more difficult"*). The guarantee of minimum inteference with the fundamental human rights in these cases is given, among other things, by the fact that the order to issue traffic and location data is issued by a judge on the proposal of the public prosecutor.

Who is therefore entitled to request the release of traffic and location data and under what conditions in the Czech Republic? Pursuant to Section 97 (3) of ECA, a legal entity or natural person who retains traffic and location data shall make them available without delay upon request to:

a) **the law enforcement authorities** for the purposes and in compliance with the conditions stipulated by a special legal regulation[10],

b) **the Police of the Czech Republic** for the purposes of **initiating a search for a specific wanted or missing person, identifying a person of unknown identity or the identity of a found corpse, preventing or detecting specific threats in terrorism or screening a protected person** and if the conditions stipulated by a special legal regulation are met[11],

c) **the Security Information Service** for the purposes and in compliance with the conditions stipulated by a special legal regulation[12],

d) **Military Intelligence** for the purposes and in compliance with the conditions stipulated by a special legal regulation[13],

e) **the Czech National Bank** for the purposes and in compliance with the conditions stipulated by special legislation[61)][14].

Within the European Union, the Court of Justice of the EU (on 8 April 2014) issued a verdict following the previous opinion of [15]its Advocate General Pedro Cruz Villalón[16], in which **it annulled the relevant Data Retention Directive (2006/24/EC)**.

"By today's judgment, the Court of Justice declares the directive invalid."

"As the Court of Justice has not limited the temporal effects of the judgment, the declaration of invalidity is effective from the date on which the directive enters into force."

In particular, the Court of Justice of the EU criticised the fact that *"the EU legislature has exceeded the limits set by the requirement of compliance with the principle of proportionality by adopting the Data Retention Directive."*

The decision to maintain or repeal the existing legislation governing the retention of traffic and location data in the EU Member States is entirely up to the relevant national authorities, and the European Union itself does not intend to recommend or provide any guidance on how to act.[17]

How to approach the widespread retention of traffic and location data? Personally, I believe that, in cyberspace, it is not possible to reconstruct events that have taken place in the past other than by retention of traffic and location data. Cyberspace and ICT, which allow a very fast change in the topology of the network, services, etc. technologies that allow the acquisition of several different identities within seconds, in fact, do not allow any other option.

I am aware that the widespread retention of traffic and location data interferes with my fundamental rights and freedoms. However, by adopting the concept of a social contract and relinquishing part of my rights and freedoms in favour of an authority (in our case the state) to protect myself and my rights, I have, in fact, no other choice. I believe that, if we want to effectively check and investigate cybercrime, cyberattacks and other negative phenomena that are taking place in cyberspace, we cannot do that without this tool. The issue we should address should not be: *"How to limit the collection of data and information about people in cyberspace (because this happens at completely different levels) and thus limit the state's ability to address negative phenomena in cyberspace?"* The issues that are completely legitimate and that should be addressed are: *"How to set the rules, to whom and under what conditions to allow access to the data, what happens to the data, for what purposes they can be used, etc."*

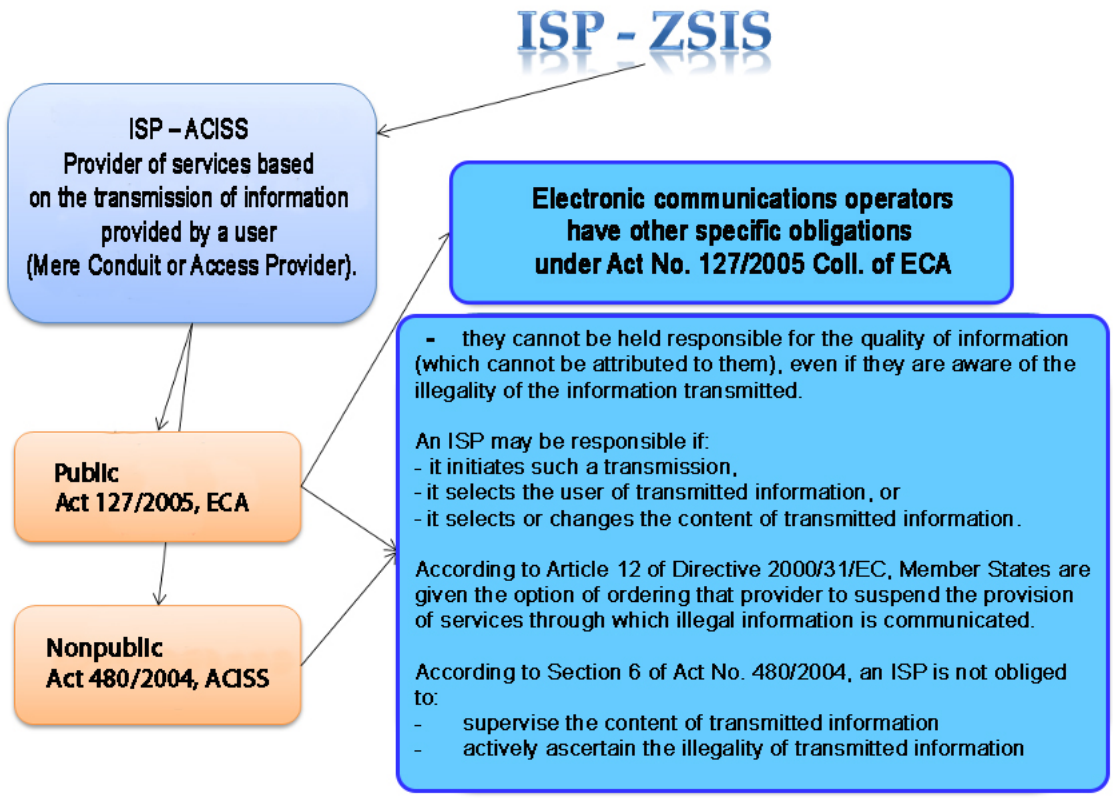
Personally, I believe that similar data should not only be retained by public service providers but by all ISPs that provide a service. My opinion is grounded on the following reasons.

Firstly, I believe that services other than those based on the provision of connections are and will continue to be the majority of services in cyberspace. A user thus stops addressing the issue of who connects him/her and how and is primarily engaged in services that may, for example, take the form of a virtual connection to various virtual environments. Thus, it is not the physical connection itself what will be significant but the connection between the individual services.

The second reason is the fact that the vast majority of providers of these services already retain not only traffic and location data but a number of other data that users allow them to retain on the basis of the Terms of Service agreed by an end user with regards to an ISP.

The last reason is an ISP's own protection from users. A service provider must respect the law, and it is in its best interest to retain data that could potentially exempt it from liability, for example, for damage or other harm.

An Advocate General has recently commented on the retention of traffic and location data[18]. He noted that data retention is in many cases the only effective tool for dealing with security risks and serious crime. At the same time, he formulated requirements for its proportional implementation in the legal systems of the Member States.



Graphical representation of the division of connection providers and some of their rights and obligations

---

[1] These three options make a connection provider essentially liable only if it is such an entity that actively sends or otherwise manipulates transmitted information.

[2] Cf. Article 12 of Directive 2000/31/EC and the provisions of Section 3 (1), (2) of Act No. 480/2004 Coll.

[3] Hereinafter referred to as the ECA

[4] Hereinafter referred to as the ECA

[5] Hereinafter referred to as the **Data Retention Directive.** The term data retention means the widespread storage of traffic and location data at connection providers (in the Czech Republic at providers under the Electronic Communications Act).

[6] See Section 97 (4) of ECA.

Traffic and location data are mainly **data leading to the tracing and identification of the source and recipient of a communication,** as well as **data leading to the determination of the date, time, method and duration of the communication.**

The scope of traffic and location data, the form and manner of their transmission to bodies authorised for use pursuant to a special legal regulation (see Section 97 (3) of ECA) and the manner of their deletion shall be determined by a statutory legal instrument. The statutory instrument is **Decree No. 357/2012 Coll., on the retention, transfer and deletion of traffic and location data.**

[7] *German Federal Constitutional Court rejects data retention law.* [online]. [cit.16/07/2016]. Available from: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/

See also e.g.:

National legal challenges to the Data Retention Directive. [online]. [cit.16/07/2016]. Available from: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html

Data retention unconstitutional in its present form. [online]. [cit.16/07/2016]. Available from: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

German Bundestag Passes New Data Retention Law. [online]. [cit.16/07/2016]. Available from: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

[8] See Constitutional Court ruling Pl. ÚS 41/11, as at 22/03/2011. *Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu.* [online]. [cit. 24/08/2016]. Available from: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=4&typ=result

[9] For more details see Section 88a of ECA

[10] Act No. 141/1961 Coll., on Criminal Court Proceedings (Criminal Code), as amended.

[11] Act No. 273/2008 Coll., on the Police of the Czech Republic, as amended.

Act No. 137/2001 Coll., on Special Protection of a Witness and Other Persons in Connection with Criminal Proceedings and on Amendments to Act No. 99/1963 Coll., the Code of Civil Procedure, as amended.

[12] Sections 6 to 8 of Act No. 154/1994 Coll., on the Security Information Service, as amended.

[13] Sections 9 and 10 of Act No. 289/2005 Coll., on Military Intelligence.

[14] Act No. 15/1998 Coll., on Supervision in the Area of the Capital Market and on Amendments to Other Acts, as amended.

[15]Opinion of Advocate General Pedro Cruz Villalón Case C-293/12 and C-594/12. [online]. [cit.15/07/2016]. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

[16] The Court of Justice of the European Union. Press release No. 54/14, dated 8 April 2014. **Judgment in joined cases C-293/12 and C-594/12**. [online]. [cited 15/07/2016]. Available from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

[17] PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10/11/2015]. Available from: http://www.earchiv.cz/b14/b0428001.php3

[18] Opinion of the Advocate General SAUGMANDSGAARD ØE, from 19/07/2016. In joined cases C-203/15 and C-698/15. [online]. [cited 10/8/2016]. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

3.1.2 Providers of services based on the automatic intermediate storage of information provided by a user (so-called caching)

Caching is based on the transfer of information, during which it is automatically temporarily stored. Subsequently, this information is transmitted to the recipients of the service at their request.

"Caching is basically a special arrangement of the mere conduit service as it also includes transmission with temporary intermediate storage of information. The only difference in which the caching service could deviate from the scope of a broadly conceived mere conduit is that storage during transmission is performed for a "period longer than is reasonably necessary for transmission".[1]

Husovec also very aptly describes caching services on the example of a proxy server or caching browser, which speed up the loading of web pages. A recipient of the service is an owner of a daily news website (so-called primary recipient), whose images are saved by a caching provider on a geographically closer computer (e.g. in Europe) so that he does not have to constantly access the computer where the original website is stored (e.g. Africa). Consequently, the overall page load (in Europe) is sped up. A user who visits the website and is another recipient of the service (so-called secondary recipient), thus, on the basis of an individual request addressed to the caching service provider, obtains an image from its computer and is not forced to "travel" to the original computer.[2]

Caching providers are not relieved of responsibility for the quality of information if they violate the standard or agreed technical conditions of caching.[3]

According to Section 4 of ACISS, a caching provider is responsible if it:

a) changes the content of information,

b) does not meet the conditions for access to information,

c) does not comply with the rules on updating information that are generally recognised and used in the sector concerned,

d) exceeds the permitted use of technology generally recognised and used in the industry to obtain usage data; or

e) shall not take immediate action to remove or deny access to information it stores as soon as it finds that the information has been removed from or accessed from the network at the point of transmission or has been ordered by a court to withdraw or deny access to it.

A caching provider is not obliged to actively search for facts and circumstances pointing to the illegal content of information or to supervise the content of information transmitted or stored by it.

---

[1] see HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Prague: CZ.NIC, 2014, p. 133

[2] Ibidem, p. 133.

[3] Cf. Article 13 of Directive 2000/31/EC and the provisions of Section 4 of ACISS

Cf. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 58

3.1.3 Providers of services based on the storage of information provided by a user (so-called storage or hosting)

Providing storage or hosting means making storage (space) available to a user so that he/she can place data there. Storing information or data, unlike mere conduit or caching, is not only temporary. Hosting services include:

a) Webhosting (Active 24, Ignum, Zoner, etc.)

b) Cloud storage enabling storage of any files and data (Dropbox, iCloud, Microsoft OneDrive, ownCloud, etc.)

c) File storage (Rapidshare, DropBox, etc.)

d) Video storage (YouTube, etc.)

e) Audio file storage (iTunes, etc.)

f) Internet auction services (eBay, etc.)

g) Blogs, forums, discussion chats, etc.

h) Social media (Facebook, Twitter, etc.).

The above list is not final. A number of other services can be provided within a hosting.

For hosting providers, the situation with their possible legal liability is the most complicated.[1] Again, it is based on the provisions of Directive No. 2000/31/EC, the recommendations of which were adopted by the Czech legislator in Section 5 of ACISS. This provision stipulates at least a provider's unintentional negligence[2] in relation to an unlawful content of information stored by the provider. However, **the legislator does not oblige providers to actively search for illegal information of users**[3] (because in many cases it would in effect be an interference with the fundamental rights and freedoms guaranteed by the Charter – e.g. Article 13) or to supervise the content of transmitted or stored information.

According to Section 5 (1) of ACISS, a hosting provider shall be responsible if it:

a) ***could, with regard to the subject of its activity and the circumstances and nature of the case, know that the contents of the information stored or action of the user are illegal****, or*

b) ***having demonstrably obtained knowledge of an illegal nature of the information stored or illegal action of the user,*** *failed to take, without delay, all measures, that could be required, to remove or disable access to such information.*

A hosting provider shall always be responsible for the content of the information stored if it exerts, directly or indirectly, decisive influence on the user's activity.[4]

For the purposes of this monograph, only certain aspects related to information society service providers have been selected, in particular with regard to the usability of information in the detection and investigation of cybercrime and cyberattacks.

---

[1] Cf. Article 14 of Directive 2000/31/EC and the provisions of Section 5 of ACISS

[2] Cf. provisions of Section 16 (1) (b) of the Criminal Code.

[3] Cf. Article 15 of Directive 2000/31/EC and the provisions of Section 6 of ACISS

[4] Section 5 (2) of ACISS

3.2. Regulation of ISP activities in Poland

In Poland, the law that regulates the Act of 18 July 2002 on the provision of electronic services (Journal Of Laws of 2002 No. 144, item 1204), which greatly limits cases when an ISP can be held liable:

Art. 12. 1. The service provider who provides services by electronic means, including the transmission of data transmitted by the recipient of the service in the telecommunications network or the provision of access to the telecommunications network within the meaning of the Act of 16 July 2004 - Telecommunications Law, shall not be liable for the content of these data, if:

1) is not the initiator of the data transfer;

2) does not select the recipient of the data transfer;

3) does not select or modify the information contained in the message.

2. The exclusion of liability referred to in par. 1 also includes automatic and short-term indirect storage of the transmitted data, if this activity is solely for the purpose of transmitting and the data is not stored longer than normally necessary to effect the transmission.

Art. 13. 1. The person who transmits the data and provides automatic and short-term intermediate storage of this data in order to speed up the re-access to it on the basis of Art. request of another entity:

1) does not modify the data;

2) uses IT techniques recognized and usually used in this type of activity, which define the technical parameters of access to data and updating them, and

3) does not interfere with the use of IT techniques recognized and usually used in this type of activity in the field of collecting information on the use of collected data.

2. The person who, under the conditions referred to in para. 1, will immediately delete the data or prevent access to the stored data, when it obtains the message that the data have been removed from the original transmission source or access to them has been rendered impossible, or where a court or other competent authority has ordered the data to be deleted or prevented from being accessed. Art. 14. 1. No liability for the stored data shall be borne by anyone who, while providing the resources of the ICT system for the purpose of storing data by the service recipient, does not know about the unlawful nature of the data or related activities, and in the event of receiving a government notification or obtaining reliable information about the unlawful nature of the data or related activities will immediately prevent access to this data.

2. The service provider who has received an official notification of the unlawful nature of the stored data provided by the recipient and has prevented access to this data, is not responsible for this recipient for damage resulting from preventing access to this data.

3. The service provider who has obtained credible information about the unlawful nature of the stored data provided by the service recipient and has prevented access to this data, is not liable to this service recipient for damage resulting from preventing access to this data, if he immediately notified the recipient of the intention to prevent access to them.

4. The provisions of para. 1-3 shall not apply if the service provider has taken control of the recipient within the meaning of the provisions on competition and consumer protection.

Art. 15. The entity that provides the services specified in Art. 12-14, is not obliged to check the transferred, stored or made available by him the data referred to in article 1. 12–14

3.3. Regulation of ISP activities in Portugal

Fix me

3.4. Possibilities of legal liability of a user for actions in cyberspace

Many users of information and communication systems are unaware of their potential responsibility for the misuse of these technologies.[1] Information and communication systems are a thing, and the person who handles them is obliged to **act in such a way that there is no unjustified damage to the freedom, life, health or property of another**.[2]

If a tortfeasor causes damage to an injured party, intentionally violating good morals, he/she is obliged to compensate said party; however, if he/she exercises his/her right, the tortfeasor is obliged to compensate the damage only if he/she observed the damage of another as the main purpose.[3]

This wording of the Civil Code clearly implies both the obligation to properly manage information and communication systems, as well as the obligation to prevent damage that could arise from its activities (i.e. the use of ICT in the Internet environment).

Many ordinary users underestimate the protection and security of the ICT resources at their disposal, either negligently or intentionally.

Determining the form of fault in actions of an end user is crucial for possible civil or criminal liability. This statement can be demonstrated in three illustrative real-world cases.

A personal computer user was using an illegal copy of the Windows 7 operating system and intentionally did not update the system. The user intentionally installed programs on the computer that allowed third parties to manipulate the computer without his further assistance.

The purpose of the activity of the user described above was to free himself from any criminal liability for an attack carried out by another person on such a prepared computer (e.g. the computer is intentionally part of a botnet network).

In practice, it is possible to encounter such attackers who base their defence on the fact that they were not the person who carried out a specific attack through a computer.

Avoiding blame based on the claim that the person is not a direct attacker and his actions did not cause a specific attack is not, in my opinion, legitimate, or it is not valid to accept this claim absolutely.

From the point of view of criminal law, at least the application of the institution of participation and the principle of access to participation could be considered[4] since the actions of a person who aided and abetted a criminal offence by another (in particular by **providing the means, removing of barriers**, eliciting the aggrieved person to the crime scene, keeping watch while an act was committed, providing advice, encouraging the resolve or promising to participate in a criminal offence) are possible to subsume under the provisions on an accessory.[5] In this case, providing the means would also mean making a computer system, or part of it, available for committing an intentional criminal offence.

If a higher degree of direct participation of a user in the infringement of another person were proved, it would be possible to consider such a user as an accessory[6] in a criminal offence. The decisive factor would be the level of knowing about the use of the given computer for an illegal act and further understanding that this activity may violate or endanger the interests protected by criminal law.[7]

From the point of view of civil law, the actions of such a user could be subsumed under Section 2909 of the Civil Code, or it would be possible to use Section 2915 of the Civil Code, which regulates the case where the damage is caused by several persons. This provision stipulates that: *"if several tortfeasors are obliged to provide compensation, they shall do so jointly and severally; if any of the tortfeasors has the duty under another statute to provide compensation only up to a certain limit, he/she is obliged jointly and severally with the other tortfeasors to that extent.* ***This also applies where several persons have committed separate unlawful acts, each of whom may have caused a harmful consequence with a high degree of certainty and if the person who caused the damage cannot be identified.***" It is the second sentence of Section 2915 (1) that can be, in my opinion, applied very well to the case described above.

A personal computer user was using an illegal copy of the Windows 7 operating system and intentionally did not update the system. He had a number of games and other applications installed on his computer, in which copyright infringement was committed, in particular by circumventing or suppressing elements of their protection and by using keygens or cracks[8] *that contained malware from other attackers. The user was not aware of the fact that his computer was being used by other users.*

In practice, this is the most common case in which a computer is misused without the knowledge of its authorised user, even if such a user, through his/her wrongdoing (especially copyright infringement) or simple ignorance of computer technology, caused his/her computer to be misused to attack third parties.

From the point of view of criminal law, it is not possible to use the institution of participation and the principle of accessory participation in this case because the actions of the person who enabled or facilitated the committing of a criminal offence by another person were not intentional and therefore did not aim to help the main offender.

From the point of view of culpability, it would be possible to apply the unwanton negligence provisions to the user of such an infected computer as the offender did not know that his/her conduct may cause such violation or endangering although he/she could and should have been aware of it considering the circumstances and the personal relations.[9]

Due to the fact that there is no negligent factual nature of the crime in the Criminal Code according to Section 230: *Unauthorised Access to Computer Systems and Information Media*, it will not be possible to use criminal law institutes in this particular case.

From the point of view of civil law, the conduct of such a user could then be subsumed under Section 2912 (1) of the Civil Code: *"If a tortfeasor acts in a manner different from what can be reasonably expected in private dealings from a person of average qualities, he/she is presumed to be acting negligently."* In this connection, it should be recalled that the person who caused the damage (tortfeasor) is obliged to compensate the damage, regardless of his fault in cases provided by law.[10]

A user adequately "looks after" his/her computer (has legal software, updates it, etc.) and reasonably secures it (uses antivirus, antispam and anti-malware protection and checks), yet this computer has been attacked from the outside (e.g. connected to a botnet) and subsequently used to attack another.

I consider that, from the point of view of fault, it would not be possible in this case for the users of such an infected computer to be subject to even the provisions relating to unwanton negligence. Due to the proactive activity of such a user, the application of Section 232 of the Criminal Code is also out of the question: *Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence* as gross negligence is required in this provision.[11]

From the point of view of civil law, then, the conduct of such a user would not be, in my opinion, possible to subsume under the previously mentioned Section 2912 (1) of the Civil Code, for in this case the user acted as justifiably required of him/her. However, this needs to be understood more broadly because, if a user learns that his/her ICT resources are being misused to attack another, he/she is obliged to notify such a person who may be harmed as a result of this fact without undue delay[12] and to warn such a person of the possible consequences. If he/she fulfils the notification obligation, the injured party is not entitled to compensation for the damage that he/she could have prevented after the notification.[13]

In a specific case, it will always depend on all the circumstances of the case, and only to the court is entitled to stipulate the obligation to pay damages.

On the other hand, if a user does not "look after" his/her computer (i.e. does not secure it, does not perform maintenance, etc.) and it is subsequently misused, it is realistic that the court in damages proceedings imposes an obligation on such a user in part or in full (e.g. to use the computing power of one data center) to compensate the injured party for damage caused to him/her by the user's computer.

---

[1] For this part of the text, theses were used that were partially published in the article: KOLOUCH, Jan and Andrea KROPÁČOVÁ. Liability for Own Device and Data and Applications Stored therein. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14)*. [B.m.], c2014, pp. 321–324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

[2] Section 2900 of the Civil code

[3] Section 2909 et seq. of the Civil Code

[4] This is the principle of dependence of the criminal liability and criminality of the participant (see Section 24 of the Criminal Code) on the criminal liability and criminality of the main offender (see Section 22 of the Criminal Code), provided that the main offender has at least attempted to commit a criminal offence in which the participant took part.

[5] Under the condition of an agreement between the participant and the main offender. See Section 24 (1) (c) of the Criminal Code

[6] See Section 23 of the Criminal Code

[7] See Section 15 (1) (b) of the Criminal Code

[8] These are interventions in programs by other persons for the purpose of modification aimed at easier launching (keygens), paralysing the program protections that prevent its copying or launching under predetermined conditions (cracks) and further reworking of these programs for subsequent use or distribution to other persons.

[9] See Section 16 (1) (b) of the Criminal Code

[10] See Section 2895 of the Civil Code

[11] See Section 16 (2) of the Criminal Code: *"A criminal offence is committed out of gross negligence if an offender's approach to the requirements for due diligence shows evident irresponsibility of the offender regarding the interests protected by the Criminal Code."*

[12] The question is whether it is possible to realistically identify such a person at a given moment (moment of attack).

[13] See Section 2092 of the Civil Code

3.5. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

ℹ️

- Defining authorities participate in the creation of the law on the Internet, in the restriction or expansion of its activities, by creating defining standards.
- Defining standards are created and implemented by entities that are authorised to define the information network environment. These are in practice *sui generis* standards that define information networks as such. They occur in layers that are interdependent. *"Defining standards are created by telecommunication operators, office software producers but also, for example, creators or operators of online games, or anyone who opens a blog or has an email box, (A defining standard created by a user of this box is a filter that automatically performs a set inbox operation.)"*
- Defining authorities are the creators of defining standards. It is an entity that, through its operation, creates rules for the functioning of the logical system in which the authority operates. As mentioned earlier, ICANN has an executive position among these authorities since it is responsible for assigning, administering and laying down rules for the domain name system. Another defining authority is, for example, the IETF. Although defining authorities may appear to be unrestricted administrators of cyberspace, they are still subject to the law of a state.
- The Internet exists only thanks to defining authorities. It is composed of them. No operation will take place without the participation (execution or mediation of the operation) of the defining authority.
- Cyberspace is formed by the will of defining authorities.
- All information society service providers are defining authorities.
- Every service provider, like any other body of law, is legally responsible for its actions.
- The term ISP is also defined in the Convention on Cybercrime, specifically in Article 1 (c) where it is stated that service provider is:
  - any public or private entity that provides to users of its service the ability to communicate by means of a computer system and
  - any other entity that processes or stores computer data on behalf of such communication service or users of such service.
- The Czech Act on Certain Information Society Services recognises the following three service providers, stipulating that a service provider is any natural or legal person who provides any of the information society services:[1]
  - Providers of services based on the transmission of information provided by a user (Mere Conduit or Access Provider).
  - Providers of services based on the automatic intermediate storage of information provided by a user (so-called caching).
  - Providers of services based on the storage of information provided by a user (so-called storage or hosting).

🔑

KEY WORDS TO REMEMBER

- ISP
- Defining authority
- Defining standard
- Mere Conduit or Access Provider
- Cashing provider
- Hosting provider
- Data retention

❓

KNOWLEDGE CHECK QUESTIONS

- Define ISP.
- How are ISPs divided? According to what criteria?
- What are the responsibilities of ISPs?
- What is a definition standard?
- Who is a defining authority, and what is its role?
- What is data retention?

---

[1] See Section 2 (d) of ACISS

4. Cybersecurity and its legal regulation

Efforts to address cybersecurity can be seen in effect from the very beginning of the use of information and communication technologies. Gradually, recommendations, standards or technical norms were adopted in this area, which usually defined minimum requirements guaranteeing a certain level of security.

There are many reasons for the introduction and implementation of cybersecurity. The most common include, for example, negative economic consequences in the case of a successful cyberattack where sensitive data are stolen. A successful cyberattack can also compromise an organisation's own operations and functioning, for example, by restricting access to computer systems or data through ransomware. Another reason for the introduction of cybersecurity may also be the loss of credibility of an attacked organisation, etc.

The last but no least important reason for the implementation of cybersecurity is to abide by legal regulations as well as the rights and obligations arising from these regulations. This legislative reason for many subjects stems from the Cybersecurity Act, but it is wrong to assume that this is the only legal norm related to the issue of cybersecurity.

In recent years, especially, there has been a massive increase in primarily international legislation that specifically focuses on the activities of entities (individuals, legal entities or states and other organisations) in cyberspace.

The field of cybersecurity differs significantly from other areas where standard security principles are applied in the real world. The difference lies mainly in the possibility of dynamic development and immediate change of cyberattacks and threats (most threats in the real world remain relatively constant), which can entail certain problems in relation to legislation. Legal regulation in this area must, on the one hand, be sufficiently general to enable it to respond effectively to partial negative cyber phenomena without the need for their detailed specification, but on the other hand, it must not be too vague in order not to infringe on the rights and legitimate interests of individuals to a greater extent than is strictly necessary.

Before the actual analysis of existing valid and effective legislation in the field of cybersecurity, it should be noted that, within the European Union and beyond, there is a clear effort to implement more effective legal instruments that would increase the quality of cybersecurity and allow adequate response to cyber threats and attacks. At present, inconsistencies and shortcomings in the legal norms of EU Member States and other states that have decided to actively participate in the creation of cybersecurity are gradually being eliminated.

"Methods of protection of data and information systems are the subject of many scientific studies today. However, without a legal basis, the technical protection of these systems and data may be ineffective due to the unclear definition of how far it is possible to go with such protection. *In this context, the inconsistency of the legal regulations of individual states with the legal regulations of other states is fully manifested. Due to the development of computer and information technologies, which illustrate the international nature of cybercrime, effective protection of computer systems and data is unthinkable without the existence of an international or transnational legal framework, both among EU Member States and worldwide."*[1]

This chapter will address the legislative framework for cybersecurity in the EU and the partner countries participating in the Erasmus+ project.

---

[1] KOLOUCH, Jan and Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Prague: Police Academy of the Czech Republic in Prague, 2013, p. 65

4.1. EU/EC documents used to harmonise legislation in addressing cybersecurity

Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the European Union.

Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the European Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.[1]

In particular, due to the specific borderless nature of cyberspace and the need for effective international cooperation, the EU seeks to approximate the legislation of individual Member States so that cybersecurity can be tackled effectively.

Regulations, directives, framework decisions and other EU/EC documents are primarily a means of approximating the laws of individual EU countries. In terms of cybersecurity, the most important documents are the following:

EU primary law

§ Charter of Fundamental Rights of the European Union

Directives of the European Parliament and of the Council

§ 91/250/EEC on the legal protection of computer programs

§ 98/34/EC on the procedure for the provision of information in the field of technical standards and regulations, as amended by Directive 98/48/EC

§ 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

§ 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

§ 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive)

§ 2002/20/EC on the authorisation of electronic communications networks and services (Authorisation Directive), as amended by Directive 2009/140/EC

§ 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC

§ 2002/22/EC on universal service and user rights relating to electronic communications networks and services (Universal Service Directive)

§ 2002/58/EC on processing of personal data and protection of privacy in electronic communications sector

§ 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks

§ 2008/114/EC on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

§ 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA

§ 2013/11/EU on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on alternative dispute resolution for consumer disputes)

§ 2013/40/EU on attacks on information systems and replacing Council Framework Decision 2005/222/JHA

§ 2015/1535 on the procedure for the provision of information in the field of technical regulations and rules on information society services

§ 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC ("revised Payment Services Directive")

§ 2016/680 on the protection of individuals with regard to the processing of personal data by the competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data and repealing Council Framework Decision 2008/977/JHA

§ **2016/1148 on measures for a high common level of security of network and information systems across the European Union (NIS)**

Regulations of the European Parliament and of the Council

§ 460/2004/EC establishing the European Network and Information Security Agency as amended by Regulation No 1007/2008

§ 1077/2011/EC establishing a European Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice

§ 526/2013 on the European Union Agency for Network and Information Security (**ENISA**) and repealing Regulation (EC) No 460/2004 Text with EEA relevance

§ 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (**eIDAS**[2])

§ 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation – **GDPR**)

Council Decisions

§ 92/242/EEC in the field the security of information systems

§ **2005/222/JHA on attacks against information systems**

§ 2011/292/EU on the security rules for protecting EU classified information

Other documents

§ Council of Europe Convention No. 185 on Cybercrime

§ Council of Europe Additional Protocol No. 189 to the Convention on Cybercrime

§ Council of Europe Convention No. 196 on the Prevention of Terrorism

§ Commission Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

International standards

§ ISMS series ISO/IEC 27000

§ in the Czech Republic ČSN ISO/IEC 27001:2014

Currently, the most important document of the European Union related to the issue of cybersecurity is DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the European Union.[3]

This directive is currently being revised, and the NIS2 directive is being prepared. The first EU-wide law on cybersecurity, the NIS Directive, came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation in the last years, the time has come to refresh it.

The changes to the revised directive are appropriately presented in the European Commission document[4]:

NIS

NIS 2

Greater capabilities

EU Member States improve their cybersecurity capabilities.

More stringent supervision measures and enforcement are introduced.

A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established.

Cooperation

Increased EU-level cooperation.

Establishment of European Cyber crises liaison organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level

Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation Group.

Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established.

Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, cybersecurity testing, and the effective use of encryption.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

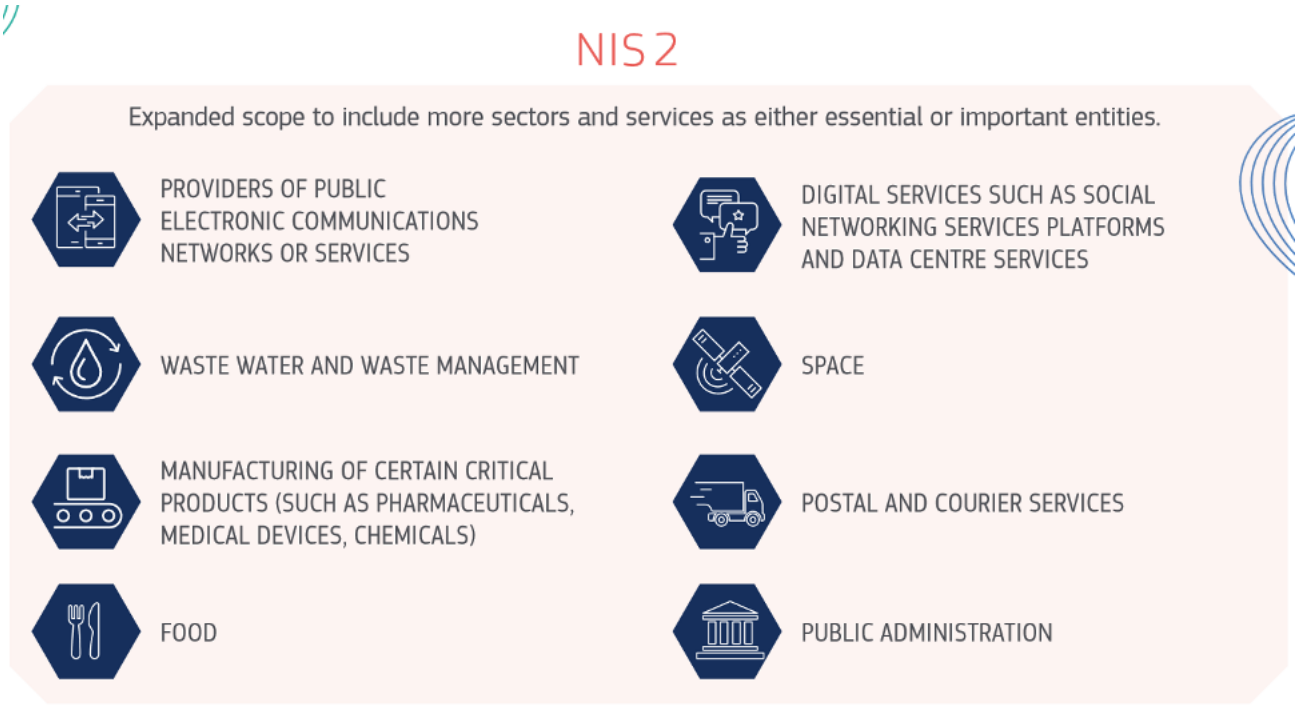
Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

SECTORS COVERED BY THE NIS DIRECTIVE

NIS

- HEALTHCARE
- TRANSPORT
- BANKING AND FINANCIAL MARKET INFRASTRUCTURE
- DIGITAL INFRASTRUCTURE
- WATER SUPPLY
- ENERGY
- DIGITAL SERVICE PROVIDERS



[1] https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[2] Hereinafter referred to as the **eIDAS**

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=CS

[4] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72155

4.2. Cybersecurity Legislation in the Czech Republic

In **2000**, the state started to systematically address the issue of cybersecurity.

Government Resolution No. 205 was adopted to **address cybersecurity issues in the Czech Republic** in 2010.[1] This resolution established the MICR (Ministry of the Interior of the Czech Republic) as the manager of the issue of cybersecurity and at the same time the national authority for this area. The Minister of the Interior was further instructed to:

1. coordinate the activities of other state institutions in the field of ensuring cybersecurity,

2. coordinate the representation of the Czech Republic in matters of cybersecurity in international forums, including the participation of state bodies in the activities of relevant international organisations,

3. submit the statute of the Interministerial Coordinating Council for Cyber Security to the government for approval by 30 April 2010,

4. submit a cybersecurity strategy to the government by 15 December 2010,

5. start ensuring the operation of the government workplace of the CSIRT (Computer Security Incident Response Team) no later than 31 December 2010.

On **19 October 2011**, the Government of the Czech Republic adopted Resolution No. 781 on the establishment of the National Security Authority (in Czech: Národní bezpečnostní úřad, NBU) as the custodian of cybersecurity issues and at the same time the national authority in this area.[2] Concurrently with this resolution, the Government of the Czech Republic established the **Council for Cyber Security**[3] and approved the establishment of the **National Center for Cyber Security** (as part of the NBU).

In **2011**, the **Strategy for Cybersecurity of the Czech Republic for the period from 2011 to 2015**[4] and an **action plan for this strategy** were adopted. However, given the transfer of responsibility from the Ministry of Interior to the NBU, this strategy is more often referred to as: **Strategy for the area of cybersecurity of the Czech Republic for the period from 2012 to 2015.**[5]

The presented strategic goals and measures were set in the presented strategy:

- creation of a legislative framework,
- creation of the National Centre for Cybersecurity and the CERT government office,
- protection of critical information infrastructures,
- strengthening the cybersecurity of public administration information and communication systems,
- streamlining the fight against crime in cyberspace,
- coordination of activities to ensure cybersecurity in Europe,
- use of reliable and trustworthy information technologies,
- raising awareness of cybersecurity,
- response to cyberattacks.

On 28 June 2013, the NBU submitted a draft law on cybersecurity to the Government of the Czech Republic. The subsequent legislative process took place without any significant comments and **Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts** (Cyber Security Act) entered into force on 29 August 2014 with effect from **1 January 2015**.

Simultaneously with the law, statutory legal instruments were drawn up, namely:

- Decree No. 316/2014, on security measures, cybersecurity incidents, reactive measures and on the determination of the requirements for filing in the field of cybersecurity (**Decree on Cybersecurity**);
- Decree No. 317/2014, **which sets out important information systems and their defining criteria**;
- Decree No. 315/2014, amendment to Government Decree No. 432/2010 Coll., **on criteria for determining the element of critical infrastructure**.

All statutory instruments came into force at the same time as the Cyber Security Act.

In August 2015, the operator of the National CERT Team was selected on the basis of the requirements set out in the CSA. The CZ.NIC association became this operator.[6] On 18 December 2015, the Public Contract on Securing the Activities of the National CERT and on Cooperation in the Field of Cybersecurity was signed.[7] This contract was entered into for an indefinite period.

The Cyber Security Act has undergone two significant amendments since 2015, when it entered into force.

The first amendment was made by Act No. 104/2017 Coll.,[8] with effect from 1 July 2017 and Act No. 205/2017 Coll. with effect from 1 August 2017. This amendment extended the circle of obligors falling under the CSA to include information system operators and further amended certain sanctions.

The second content-significant amendment was made by Act No. 205/2017 Coll.,[9] with effect from 1 August 2017. This amendment implemented **Directive 2004/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of networks and information systems in the European Union (NIS)** into the CSA and at the same time the **National Office for Cyber and Information Security (NUKIB)** was established. It took over rights and obligations in the field of cybersecurity from the NBU, including protection of classified information in information and communication systems and cryptographic protection. NUKIB is the central administrative body in the above areas.

At present, the issue of cybersecurity is specifically addressed by the Cybersecurity Act. However, partial aspects of the protection of the Czech Republic against cyberattacks can be found in other legal regulations. In terms of cybersecurity, the most important documents are the following:

Constitutional acts

- Constitutional Act No. 1/1993 Coll., the Constitution of the Czech Republic, as amended
- Constitutional Act No. 2/1993 Coll., Charter of Fundamental Rights and Freedoms, as amended[10]
- Constitutional Act No. 110/1998 Coll., on the Security of the Czech Republic

Acts

- Act No. 106/1999 Coll., on Free Access to Information, as amended
- Act No. 101/2000 Coll., on the Protection of Personal Data and Amendment to Some Acts, as amended[11]
- Act No. 121/2000 Coll., on Copyright, on Rights Related to Copyright and on Amendments to Certain Acts (Copyright Act), as amended
- Act No. 240/2000 Coll., on Crisis Management and Amendments to Certain Acts (Crisis Act), as amended
- Act No. 365/2000 Coll., on Public Administration Information Systems, as amended
- Act No. 480/2004 Coll., on Certain Information Society Services and on Amendments to Certain Acts (Act on Certain Information Society Services), as amended[12]
- Act No. 127/2005 Coll., on Electronic Communications, as amended[13]
- Act No. 412/2005 Coll., on the Protection of Classified Information and on Security Clearance, as amended[14]
- Act No. 69/2006 Coll., on the Imposing of International Sanctions, as amended
- Act No. 300/2008 Coll., on Electronic Acts and Authorised Conversion of Documents, as amended
- Act No. 40/2009 Coll., Criminal Code, as amended[15]
- Act No. 111/2009 Coll., on Basic Registers, as amended
- Act No. 418/2011 Coll., on the Criminal Liability of Legal Persons and Proceedings against Them
- Act No. 89/2012 Coll., the Civil Code
- **Act No. 181/2014 Coll., on Cybersecurity and on Amendments to Related Acts (Cybersecurity Act)**
- Act No. 297/2016 Coll., on Services Creating Trust for Electronic Transactions

Statutory Instruments

- Government Decree No. 522/2005 Coll., which lays down lists of classified information, as amended
- Decree No. 523/2005 Coll., on the security of information and communication systems and other electronic devices handling classified information and on the certification of screening chambers, as amended
- Decree No. 529/2006 Coll., on requirements for the structure and content of the information concept and operational documentation and on requirements for the management of security and quality of public administration information systems (Decree on long-term management of public administration information systems)
- **Government Regulation No. 432/2010 Coll., on criteria for determining the element of critical infrastructure**
- Decree No. 357/2012 Coll., on the retention, transfer and deletion of traffic and location data
- **Decree No. 317/2014 Coll., on important information systems and their defining criteria**
- **Decree No. 437/2017 Coll., on the criteria for determining the operator of the basic service**
- **Decree No. 82/2018 Coll.**, on security measures, cybersecurity incidents, reactive measures, requirements for filing in the field of cybersecurity and data disposal (**Decree on Cybersecurity**)

---

[1] *RESOLUTION OF THE GOVERNMENT OF THE CZECH REPUBLIC of 15 March 2010 No. 205 addressing the issue of cybersecurity of the Czech Republic.* [online]. Available from: https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ

[2] *RESOLUTION OF THE GOVERNMENT OF THE CZECH REPUBLIC of 19 October 2011 No. 781 on the establishment of the National Security Authority as the custodian of cybersecurity issues and at the same time the national authority in this area.* [online]. Available from: https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E

[3] This council is an advisory body to the Prime Minister in the field of cybersecurity.

[4] *Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015.* [online]. Available from: https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura

[5] *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015.* [online]. Available from: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf

[6] See https://www.nic.cz/page/351/

[7] For more details see [online]. Available from: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf

[8] Act No. 104/2017 Coll., amending Act No. 365/2000 Coll., **on Public Administration Information Systems** and amending certain other acts, as amended, Act No. 181/2014 Coll., on Cybersecurity and Change of Related Acts (Cybersecurity Act) and some other acts. [online]. Available from: https://www.zakonyprolidi.cz/cs/2017-104

[9] Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on Cybersecurity and Amending Related Acts (Cybersecurity Act), as amended by Act No. 104/2017 Coll. and Certain Other Acts.[online]. Available from: https://www.zakonyprolidi.cz/cs/2017-205

[10] Hereinafter referred to as the Charter of Fundamental Rights and Freedoms or **Charter**.

[11] Hereinafter referred to as the Personal Data Protection Act or the **PDPA**. In connection with the effectiveness of the GDPR, this act will be recodified and is expected to be replaced by the Personal Data Processing Act. For more details, see e.g. [online]. Available from: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

[12] Hereinafter referred to as the Act on Certain Information Society Services or **ACISS.**

[13] Hereinafter referred to as the **ECA**

[14] Hereinafter referred to as the **PCIA**

[15] Hereinafter referred to as the Criminal Code or **CC**.

4.3. Cybersecurity Legislation in Poland

Taking into account the Polish legal circumstances in the field of computer crime, it should be stated that virtually all crimes included in Chapter XXXIII of the Penal Code can be committed with the use of a computer. They will then become computer crimes. In some cases, the use of a computer constitutes a circumstance that exacerbates criminal liability, e.g. Art. 268 § 2 and 3 of the Penal Code, while in other situations the perpetrator, committing a crime with the use of a computer, will be treated in the same way as the perpetrator acting in a different way, e.g. art. 265 of the Penal Code, Art. 266 of the Penal Code. Currently, as part of the aforementioned chapter of the Penal Code, the legislator has penalised such behaviours as:

- illegal access to information or an IT system and related to them (Article 267 of the Penal Code)

- acts consisting in destroying, damaging, removing, replacing essential information or similar activities (Article 268 of the Penal Code),

- actions consisting in destroying, damaging, deleting, changing or obstructing access to IT data, or significantly disrupting or preventing the automatic processing, collection or transfer of such data (Article 268a of the Penal Code),

- acts involving the so-called IT sabotage (Article 269 of the Penal Code), also known as IT diversion,

- acts consisting in a significant disruption of the operation of a computer system or teleinformation network (Article 269a of the Penal Code)

- acts consisting in the unlawful production (or similar activities) of computer devices or programs adapted to commit specific crimes, computer passwords, access codes or other data (Article 269b of the Penal Code).

In addition to the above-mentioned chapter, the legislator regulated separately the crime of computer fraud (Article 287 of the Penal Code), theft of a computer program (Article 278 § 2 of the Penal Code) and the handling of a computer program (Article 293 of the Penal Code). All offences included in Chapter XXXIII belong to the category of common offences, with the exception of Art. 269 of the Penal Code, Art. 269a of the Penal Code and art. 269b of the Penal Code. They are of an application nature.

The solutions adopted in Chapter XXXIII of the Penal Code are a consequence of Poland's signing on 23 November 2001 of the Council of Europe Convention No. 185 on Cybercrime and Council Framework Decision 2005/222 / JHA on attacks against information systems.

Article 267 of the Penal Code constitutes the criminal law protection of the privacy of Internet users. In art. 267 § 1 of the Penal Code it penalises actions aimed at obtaining illegal access to information not intended for the perpetrator. From the point of view of the criminal record of the perpetrator's behaviour, it does not matter where the information is stored, whether on the hard drive or on an external server in the network. This means that this provision protects the broadly understood subjective right to dispose of information. The conduct of the perpetrator of the offence specified in art. 267 § 1 of the Penal Code it may consist in opening a closed letter, connecting to a telecommunications network or breaking or bypassing electronic, magnetic, IT or other special security measures. The content of the provision indicates that the legislator penalises the activities indicated in the dispositive part, regardless of whether the perpetrator has read the content of the information. This means that the features of a crime under Art. 267 of the Penal Code will also be filled in by a person who will gain access to information not intended for him, even in a situation where he did not intend to read its content. The privacy of Internet users can also be violated by breaking or bypassing existing security measures and thus breaking into the victim's computer. The broad term in Art. 267 § 1 of the Penal Code types of security, the breaking or bypassing of which is punishable by law, means that securing a file with a password will meet the conditions of secured information.

The perpetrator's actions aimed at gaining access to all or part of the IT system constitute an offence under Art. 267 § 2 of the Penal Code Referring to the subject-matter of the act, attention is drawn to the term "telecommunications network" used by the legislator, which has not been defined in the Penal Code. Therefore, it seems necessary to refer to Art. 2 points 35 of the Act of 16 July 2004 Telecommunications Law, which defines the telecommunications network as transmission systems and switching or redirecting devices, as well as other resources, including inactive network elements that enable the transmission, reception or transmission of signals via wires, radio waves, optical or other means using electromagnetic energy, whatever their type. The analysis of the above definition shows that a telecommunications network can be both the existing cable infrastructure and a wireless network.

Also, the concept of an IT system has not been defined in the Penal Code, its definition is provided in Art. 7 point 2a of the Act of August 29, 1997 on the Protection of Personal Data, which states that "an IT system is a set of devices, programs, information processing procedures and software tools used to process data cooperating with each other". This term also appears in Art. 1 lit. and Council Framework Decision No. 2005/222 / JHA of 24 February 2005, which specifies that an IT system is any device or group of connected or related devices, of which at least one carries out automatic processing of computer data in accordance with the software, as well as data stored, processed, retrieved or provided by them for the purposes of their operation, use, protection or maintenance. Another definition of an IT system is contained in the Council of Europe Convention No. 185 on Cybercrime. Pursuant to Art. 1 lit. and of the Convention, an information system is any device or group of interconnected or related devices, one or more of which, according to the program, performs automatic data processing. Due to the fact that the concept of an IT system plays an important role in determining responsibility for cybercrime, the literature describes an IT system as a set of cooperating hardware and software elements that are used to enter, process and read information. The IT system therefore does not include data transmission facilities.

It is worth noting that the legislator in Art. 267 § 2 of the Penal Code did not define the method of the perpetrator's action, but only its effect. The above requires that any behaviour consisting in unauthorised access to an IT system is penalised, regardless of whether there has been any breach of computer or system security.

In art. 267 § 3 of the Penal Code the legislator sanctions another prohibited act consisting in installing or using a listening device, visual device or other device or software in order to obtain information to which he is not entitled. The condition for liability under this provision is not obtaining information, it is sufficient for the perpetrator to take specific actions. However, these actions must be taken for a specific purpose, i.e. to obtain information to which the perpetrator is not entitled.

In art. 267 § 4 of the Penal Code the legislator penalises the disclosure of information obtained to another person in the manner specified in § 1-3.

Another art. 268 of the Penal Code sanctions the perpetrator's behaviour aimed at violating the integrity of IT data. According to the provisions of the act, this breach may take the form of destroying, damaging, deleting or changing the record of essential information.

In art. 268 § 2 of the Penal Code The legislator covered the situation when the perpetrator's act concerns recording on an IT data carrier, e.g. a hard drive or a CD. It is noted that the subject of protection of Art. 268 of the Penal Code is the availability of information, and the purpose of the perpetrator's action is to prevent or significantly impede the access to the relevant information by the authorised person. The necessity of the occurrence of an effect in the form of frustrating or significantly impeding access to information means that an offence consisting in destroying, damaging, deleting, replacing essential information or similar activities falls into the category of consequential offences. Such a qualification is consistent with the well-established view of the literature. The legislator in Art. 268 of the Penal Code uses the concept of "material information" without indicating the features that the information must have in order to be material within the meaning of this provision. Therefore, the assessment of the nature of the information in question must be made on a case-by-case basis on the basis of both objective and subjective criteria.

The subject of protection of art. 268a of the Penal Code, as opposed to Art. 268 of the Penal Code, has been broadly defined and it is the security and availability of IT data, which do not have to meet the significance characteristics. The signs of an offence under Art. 268a of the Penal Code are destroying, damaging, deleting, changing or obstructing access to IT data. Penalised in art. 268a of the Penal Code the behaviour may also consist in significantly disrupting or preventing the automatic processing, collection or transfer of IT data. The second set of prohibited behaviour must be of significance, which should be related to the degree of disruption or prevention of automatic processing, collection or transmission of IT data, and not to the extent of data modified by the perpetrator. We speak of the importance of actions taken by the perpetrator when these actions are characterised by a sufficiently high degree of intensity. The subject of protection of art. 268a of the Penal Code is the security of information stored, transmitted and processed in systems based on IT data.

On the basis of the Polish legal system, the term "IT data" has not been defined, and it plays an important role. Therefore, it is necessary to refer to international law - in accordance with the content of Art. 1 letter b of the Council of Europe Convention No. 185 on Cybercrime. According to the cited provision, this term means "any representation of facts, information or concepts in a form suitable for processing in a computer system, including an appropriate program causing the performance of a function by an IT system".

The definition of IT data is also included in Art. 1 letter b of the Council Framework Decision 2005/222 / JHA of 24/02/2005 on attacks against information systems and means "any representation of facts, information or ideas in a form suitable for processing in an information system, including a program suitable to cause the performance of a function by the system".

The presented definitions indicate that IT data are all data that is an information carrier, as well as computer programs used both by individually defined persons and used in ICT networks by an undefined number of people.

In art. 269 of the Penal Code the legislator penalised the behaviour of the so-called IT sabotage. The essence of this crime is the destruction, damage, deletion or alteration of IT data of particular importance for the country's defence, security in communication, the functioning of the government administration, other state body or state institution or local government, as well as disrupting or preventing the automatic processing, collection or transfer of such data.

In art. 269 § 2 of the Penal Code the legislator indicated that the crime of sabotage may consist in destroying or replacing an IT data carrier or destroying or damaging a device used for automatic processing, collection or transmission of IT data. As follows from the content of the provision in question, the subject of protection are IT data of particular importance for the country's defence, security in communication, the functioning of the government administration, other state body or local government administration, and the system of automatic processing, collection or transfer of such information. IT sabotage is considered to be a qualified type in relation to the crimes under Art. 268 § 2 of the Penal Code, Art. 268a of the Penal Code and 269a of the Penal Code. The qualifying hallmark here is the type of protected data, i.e. data of particular importance to the values listed in Art. 269 of the Penal Code. The legislator divided the penalised behaviour of the perpetrator into two groups. The first of them are activities aimed at destroying, damaging, deleting or changing computer data of particular importance for the values protected by the regulation. The subject of protection of this part of the provision is the integrity of data belonging to a specific category. The second group of features are activities consisting in disrupting or preventing the automatic processing, collection or transfer of IT data of particular importance for the country's defence, security in communication, the functioning of the government administration, other state body or state institution or local government. In this case, the subject of protection is the availability of data specified in the aforementioned provision.

In art. 269 § 2 of the Penal Code the legislator, protecting the goods specified in § 1, sanctioned the actions of the perpetrator consisting in destroying or replacing an IT data carrier or destroying or damaging devices used for automatic processing, collection or transmission of IT data. These activities may consist in the physical destruction, damage, replacement of e.g. hard drives, as well as hindering or preventing their processing by e.g. damaging network devices. Due to the material nature of the crime of IT sabotage, for assigning the perpetrator an act under Art. 269 of the Penal Code it is necessary to have a specific effect in the form of the destruction or damage to the specified computer data or to disrupt or prevent their automatic processing or transmission.

Another provision regulating the criminal liability of cybercrime is Art. 269a of the Polish Penal Code. The essence of this provision is the protection of the operational security of a computer system or ICT network. The concept of a computer system is identified in the literature with the concept of an information system. Criminal liability under this provision will be imposed on a person who, without the right, significantly interferes with the operation of a computer system or teleinformation network by transmission, destruction, removal, damage, obstruction of access or change of IT data. The methods of action penalised by the act have been enumerated in the provision and, as a rule, should not raise any interpretation doubts. The exception is the term "transmission", which has not been defined by the legislator. In the literature, this term means the transfer of information from one place in a computer system to another, e.g. from operating memory to disk, from disk to printer, from one computer in a network to another network computer. The sanctioned transmission of IT data at a distance is to take place in an encoded form, not on external media such as a CD.

Article 269b of the Penal Code sanctions the production, acquisition, sale or making available to other persons of computer devices or programs adapted to commit the enumerated crimes. It is noteworthy that the features of this crime include a number of preparatory activities that may be related to the commission of crimes indicated in the dispositive part of the provision. Criminalisation covers activities consisting in the creation and adaptation of devices or programs for committing crimes under Art. 165 § 1 point 4, art. 267 § 3, art. 268a § 1 or § 2 in connection with § 1, art. 269 § 2 or article. 269a, their sharing and obtaining, as well as breaking computer passwords, access codes or other data enabling access to information stored in a

computer system or ICT network. The subject of protection is the security of information processed electronically in all aspects, i.e. confidentiality, integrity and availability of IT data and systems. Although the legislator uses the plural for sanctioned activities, a single behaviour, for example the sale of only one program, will be punishable by law. Such a view is established both in the doctrine and in jurisprudence.

In art. 287 of the Penal Code the legislator regulated the crime of computer fraud. This offence is included in Chapter XXXV, "Offences against Property". The subject of protection of this article are IT data together with the information contained therein. These data can be stored both in the computer memory and on a CD or server. Penalised behaviour of the perpetrator consists in influencing without authorisation the automatic processing, collection or transmission of information or the change, deletion or introduction of a new record on IT data. The described behaviour of the perpetrator must be aimed at gaining financial gain or causing harm to another person. The literature indicates that the perpetrator's action aimed at influencing the automatic processing, collection or transmission of information takes the form of unlawful interference by an external entity in the course of automatic processes, which causes that after the perpetrator's influence ends its course, in particular processing, collection or transmission, will be different than if the perpetrator's act had not been performed. Computer fraud is a criminal offence. This means that the offence under Art. 287 § 1 of the Penal Code is made at the time of introducing changes or other interference with the device or system for collecting, processing or transmitting information by means of computer technology, as described in this provision. The necessity of the damage is not one of its hallmarks.

In art. 287 § 2 of the Penal Code the legislator defined the privileged type due to a minor case. The offence under Art. 287 of the Penal Code, as a rule, it has a public prosecution character. However, in the event that it was committed to the detriment of the closest person, it causes, in accordance with the provisions of § 3, to change the mode of prosecution to the application.

The above analysis of the provisions regulating criminal liability in respect of cybercrimes indicates that the fundamental object of protection for the criminalisation of computer crimes is the traditional freedom and privacy of individuals, although viewed from a computer perspective. However, also the data collected in the systems are protected, as well as the systems themselves and their integrity, the violation of which may often have very serious social consequences. At the same time, it should be mentioned that the criminal law regulation of cybercrime will encounter two fundamental problems. The first is related to the principle of jurisdiction. Computer crime committed on the Internet is very often of a cross-border, and sometimes even territorial, nature in the sense that it is often committed in isolation from the territory of a given jurisdiction. The second problem is the very rapid development of new forms of cybercrime, which lawmakers usually do not keep up with.

Nevertheless, taking into account the presented criminal law aspects, the seriousness of the threat posed by cybercrime and the need for an appropriate response to it, in particular through regulations in the field of criminal law, cannot raise any doubts.

4.4. Cybersecurity Legislation in Portugal

Fix me

5. Information Security Management System

Information Security Management System

5.1. ISMS framework

The **Information Security Management System** (**ISMS**)[1] **is a set of rules** designed to maintain the confidentiality, integrity and availability of information by applying a risk management process and providing assurance to stakeholders that risks are being adequately managed.[2]

Within the ISMS, assets are protected, information security risks are managed and measures already in place are checked.

Information security management system means such a part of the management system that is based on the approach to risks of the information and communication system. This part of the management system defines how to establish, implement, operate, monitor, review, maintain and improve the security of information and data.

It is also clear from the above definition that the **ISMS is a part of processes and the overall management system of an organisation as well as being integrated into these systems**.

ISMS can be applied to an organisation as a whole, as well as to an organisational unit within the organisation, or to a specifically designed information and communication system, or part thereof.

"ISMS can be implemented and used in an organisation with ten employees, as well as in a large holding company that can have thousands of employees. Simply put, there is only one ISMS, the one described in ISO/IEC 27001. However, the interpretation and implementation of individual recommendations can vary significantly depending on the scope of the system, the number of users, the way data are processed, their value and especially according to real security risks, etc. The ISMS strategy in small and medium-sized companies is not described in as much detail as is customary in large, especially multinational organisations.

The ISMS does not only apply to industrial enterprises and private organisations, the ISMS applies to all organisations, including public law institutions and state bodies. This is demonstrated by the existence of many national governmental and departmental resolutions recommending or requiring the implementation of ISMS in organisations managed and established by the state."[3]

Many ISMS standards are designed to help organisations of all types and sizes implement and operate ISMS. It consists of the following international standards, collectively referred to as (*Information Technology – Security Technologies*[4] (listed below in numerical order):

ISO/IEC 27000	Information security management systems – Overview and vocabulary
ISO/IEC 27001	Information Security Management Systems – Requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Information security management systems – Guidance
ISO/IEC 27004	Information security management – Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC TR 27008	Guidelines for auditors on information security controls
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications
ISO/IEC 27011	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations
ISO/IEC 27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014	Governance of information security
ISO/IEC TR 27015	Information security management guidelines for financial services
ISO/IEC TR 27016	Information security management — Organisational economics
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

International Standards, which are not listed under this common name but are also part of a series of ISMS standards, are listed below:

ISO 27799	*Health informatics — Information security management in health using ISO/IEC 27002*[5]

The ISMS solution requires a systemic and comprehensive approach, respecting the principles and elements of the entire cybersecurity lifecycle. The ISMS management system is based on the Deming cycle, or also on the **PDCA cycle** (**P**lan-**D**o-**C**heck-**A**ct).

The PDCA cycle is one of the basic management principles based on the gradual improvement of the quality of processes, services, data, products, etc. thanks to the constant repetition of its four basic activities: Plan-Do-Check-Act.

There are currently a number of variants of the PDCA cycle[6], and one of the suitable modifications of this cycle, which is also applicable in the field of cybersecurity, is the **OPDCA** variant, which extends the original model by the **Observe** phase **preceding** the Plan phase.

The PDCA cycle, or some of its modifications, can be applied to all ISMS processes. The simplest way to display this model is a never-ending circle:

Figure: PDCA model[7]

The PDCA model was also expressed in ISO/IEC 27001: 2005 and illustrated how the ISMS accepts information security requirements and stakeholder expectations as an input and uses information and processes to generate information security outputs that meet those requirements and expectations.

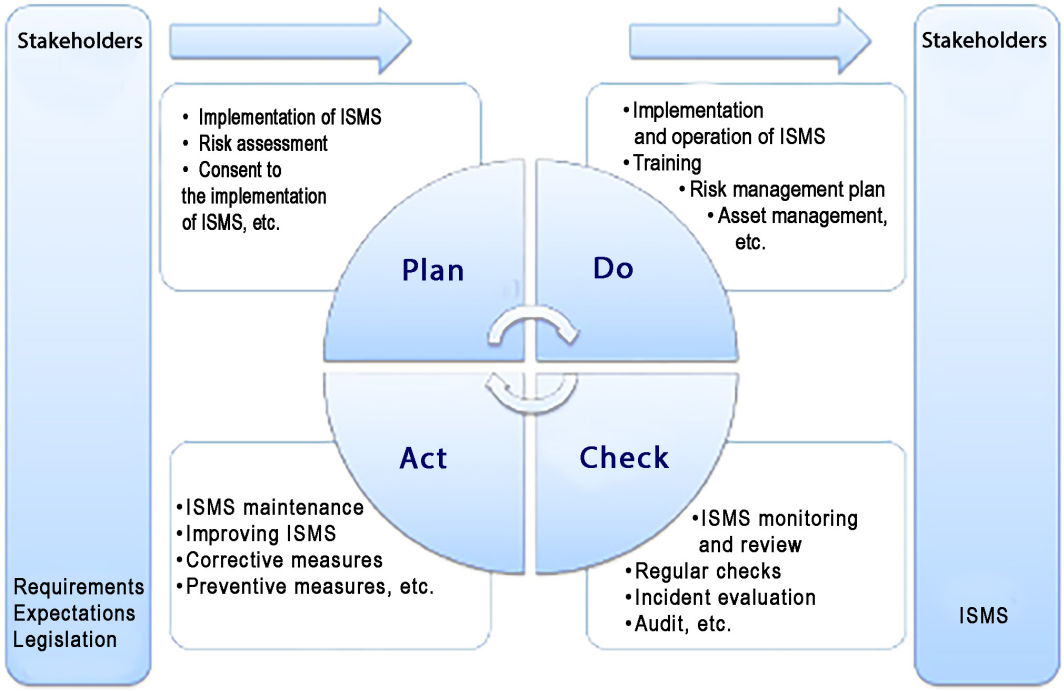


Figure: PDCA model applied to ISMS processes[8]

Plan (ISMS establishment)	Establishment of ISMS policy, goals, processes and procedures related to risk management and information security to provide results consistent with the organisation's overall policy and objectives.
Do (implementation and operation of ISMS)	Implementation and use of the ISMS policy, measures, processes and procedures.
Check (ISMS monitoring and review)	Assess, where possible, process performance measurement against the ISMS policy, objectives and practical experience and reporting results to organisation's management for review.
Act (maintaining and improving ISMS)	Take corrective and preventive actions based on the results of the ISMS internal audit and review of the management system by organisation's management to ensure continuous improvement of ISMS.

The ISO/IEC 27001 standard promotes the adoption of a process approach for **establishing, implementing, operating, monitoring, maintaining and improving ISMS** in an organisation. Emphasis is placed especially on:

- understanding of an organisation's information security requirements and the need to set information security policies and objectives,

- introduction and operation of measures for information security management in the context of managing the overall risks of an organisation's activities,
- monitoring and reviewing the performance and efficiency of ISMS,
- continuous improvement based on objective measurement.

"For ISMS within an organisation, the management organisation, responsibility for information security of managers at all levels, professional bodies and roles in the information security system must be clearly described.

In the organisational structure of an organisation, information security must be taken into account so as to cover the activities and cooperation of management, persons responsible for application systems, operational services, end users and persons responsible for individual activities. Information security presupposes close cooperation of all mentioned groups of employees and provision of training in the field of information security, so that in addition to those responsible for information and other security in the organisation, information management staff and all users of information technology also have a basic knowledge of information security."[9]

With regard to the above, it is possible to define standard goals of ISMS within an organisation:

- ensuring the security of information and communication systems and services,
- ensuring the continuity of operation of information and communication systems and services,
- data and information protection,
- protection of other assets,
- handling threats, events and incidents, including prevention,
- increasing the security of information and communication systems and services,
- raising the general awareness of users about security and security threats (education),
- sharing experiences with other entities.

However, the **implementation of ISMS** in an organisation **cannot ensure the complete security of the organisation's assets**. However, the implementation of ISMS can significantly reduce the risks of asset encroachment to an acceptable level. The whole system is as strong as its weakest link. In this case, the weakest link, and the greatest danger to information security, is a person.

---

[1] Hereinafter referred to as the **ISMS**

[2] Cf. introduction ČSN ISO/IEC 27001

[3] POŽÁR, Josef and Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Prague: AFCEA, 2011. ISBN 978-80-7251-364-2, p. 5, or: POŽÁR, Josef and Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Available from: https://www.cybersecurity.cz/data/srib.pdf p. 1

[4] The common name *"Information technology – Security techniques"* indicates that these international standards have been prepared by the joint technical committee ISO/IEC JTC 1 *Information Technologies*, subcommittee SC 27 *IT Security Techniques*

[5] For an overview of standards, see: ČSN EN ISO/IEC 27000 (369790) – Information technologies – Security techniques – Information security management systems – Overview and vocabulary

[6] ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cit. 06/07/2018]. Available from: https://www.allaboutlean.com/pdca-variants/

[7] *PDCA cycle.* [online]. [cit. 06/07/2018]. Available from: https://www.creativesafetysupply.com/glossary/pdca-cycle/

[8] Modified and supplemented PDCA model. The original model was introduced in ISO/IEC 27001: 2005 p. 7

[9] POŽÁR, Josef and Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Prague: AFCEA, 2011. ISBN 978-80-7251-364-2, pp. 7–8, or: POŽÁR, Josef and Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Available from: https://www.cybersecurity.cz/data/srib.pdf p. 2

5.2. Risk management

According to Article According to Article 7 of the NIS, each Member State is to adopt a national strategy for network and information systems security, setting out strategic objectives and relevant policy and regulatory measures to achieve and maintain a high level of network and information systems security. The subject of the national strategy for the security of networks and information systems includes mainly the following objectives and measures:

a) the objectives and priorities of the national strategy for network and information security;

b) the administrative framework for meeting the objectives and priorities of the national strategy for the security of networks and information systems, including the role and responsibilities of governments and other relevant entities;

c) identification of preparedness, response and recovery measures, including public-private cooperation;

d) definition of education, information and training programs related to the national strategy for the security of networks and information systems;

e) definition of research and development plans related to the national strategy for network and information systems security;

f) risk assessment plan for risk identification;

g) a list of the various entities involved in the implementation of the national strategy for network and information systems security.

According to Czech legislation, **risk assessment** means the **overall process of risk identification, analysis and evaluation**.

The risk assessment process is addressed, for example, by ISO/IEC 27005, where this process is demonstrated.

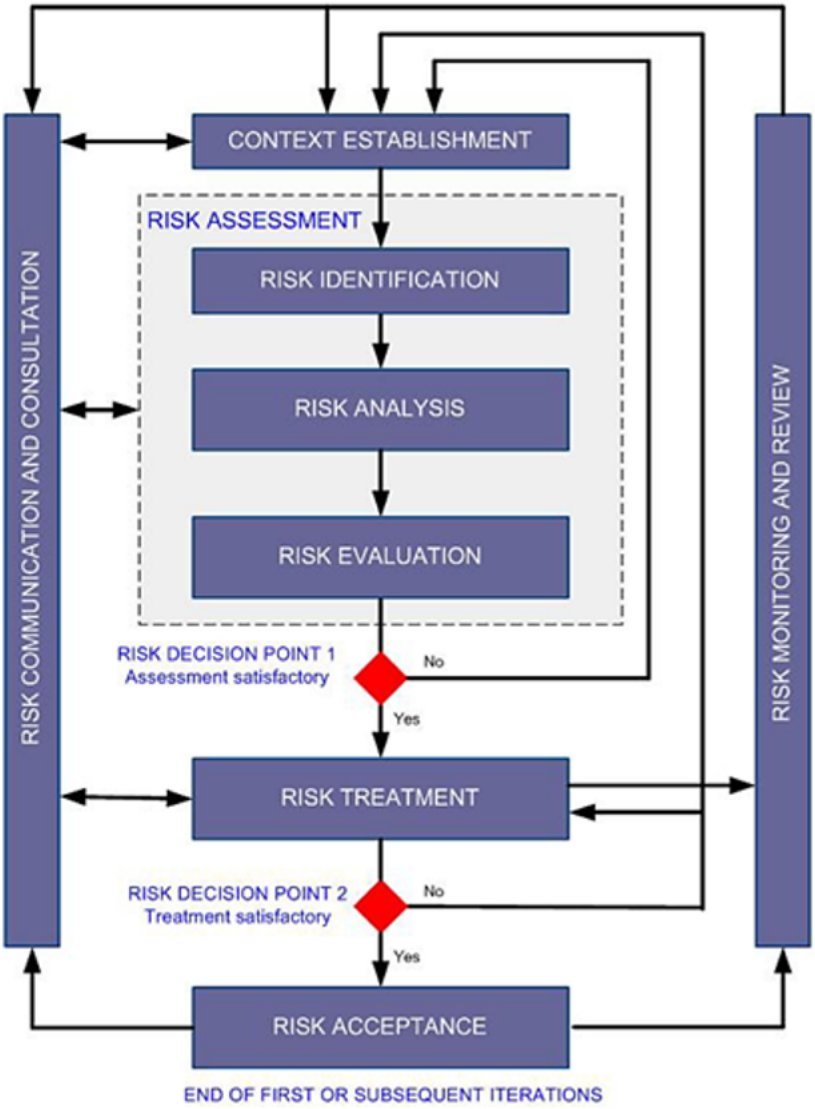


Figure: Demonstration of risk assessment in ISMS[1]

The PDCA model must also be respected in the risk assessment process, but it is adapted for risk assessment.[2]

ISMS process	Risk assessment process in ISMS
Plan	Creating a context Risk assessment Development of a risk management plan Risk acceptance
Do	Implementation of the risk management plan
Check	Continuous monitoring and review of risks
Act	Maintaining and improving the risk assessment and management process Management process

As for the risk management itself, it is possible to graphically illustrate this process as follows:

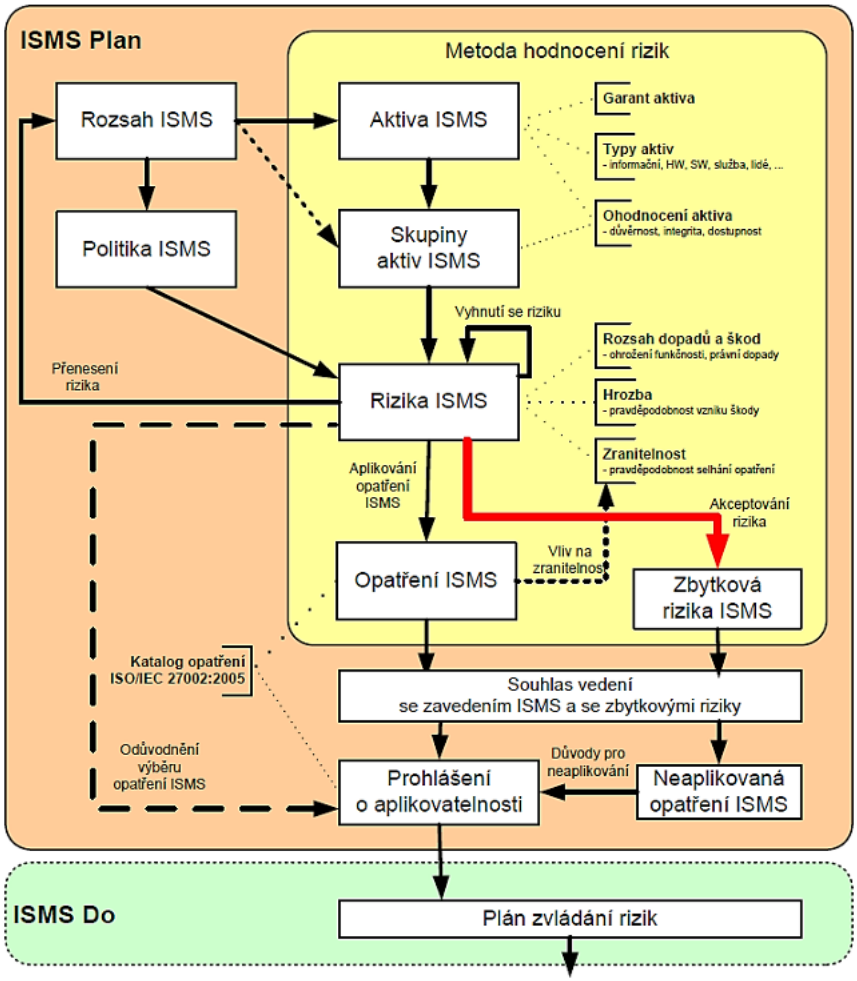


Figure: Risk management in the ISMS process[3]

ISMS Plan	**ISMS Plan**
Rozsah ISMS	ISMS scope
Politika ISMS	ISMS policy
Přenesení rizika	Risk transfer
Katalog opatření ISO/IEC 27002:2005	Catalogue of measures ISO/IEC 27002:2005
Odůvodnění výběru opatření ISMS	Justification for the choice of ISMS measures
Souhlas vedení se zavedením ISMS a se zbytkovými riziky	Management's approval of ISMS implementation and residual risks
Prohlášení a aplikovatelnosti	Declaration and applicability
Důvody pro neaplikování	Reasons for not applying
Neaplikovaná opatření ISMS	Unapplied ISMS measures
Metoda hodnocení rizik	Risk assessment method
Aktiva ISMS	ISMS assets
Garant aktiva	Asset guarantor
Typy aktiv - informační, HW, SW, služba, lidé, ...	Types of assets - information, HW, SW, service, people, ...
Ohodnocení aktiva - důvěrnost, integrita, dostupnost	Asset valuation - confidentiality, integrity, availability
Skupiny aktiv ISMS	ISMS asset groups

Vyhnutí se riziku	Risk avoidance
Rozsah dopadů a škod - ohrožení funkčnosti, právní dopady	Extent of impacts and damages - endangerment of functionality, legal consequences
Hrozba - pravděpodobnost vzniku škody	Threat - probability of damage
Zranitelnost - pravděpodobnost selhání opatření	Vulnerability - probability of failure of a measure
Rizika ISMS	ISMS risks
Aplikování opatření ISMS	Application of ISMS measures
Akceptování rizika	Risk acceptance
Opatření ISMS	ISMS measures
Vliv na zranitelnost	Impact on vulnerability
Zbytková rizika ISMS	Residual ISMS risks
ISMS Do	**ISMS Do**
Plán zvládání rizik	Risk management plan

The value of risk is most often expressed as a function affected by impact, threat and vulnerability. For example, the following function can be used for self-assessment of risk:

Risk = impact * threat * vulnerability

If an obligor uses a risk assessment method that does not differentiate between threat and vulnerability assessments, the threat and vulnerability assessment scales may be combined. The merging of scales should not lead to a loss of the ability to distinguish between levels of threat and vulnerability. For this purpose, for example, a comment can be used that clearly expresses both the level of threat and the level of vulnerability. The same applies in cases where the obligor uses a different number of levels to assess impacts, threats, vulnerabilities and risks.[4]

Appendix 3 to the CSD further lists the scales used to assess threats, vulnerabilities and risks.

Level	Description
Low	Threat does not exist or is unlikely. The expected threat attempt is **not more frequent than once every 5 years**.
Medium	Threat is unlikely to likely. The expected threat attempt is in the range **from 1 year to 5 years**.
High	Threat is likely to very likely. The expected threat attempt is in the range from **1 month to 1 year**.
Critical	Threat is very likely or more or less certain. The expected threat attempt **is more frequent than once a month**.

Figure: Threat assessment scale

Level	Description
Low	**Vulnerability does not exist or** is **unlikely** to be exploited. Security measures are in place that are able to detect possible vulnerabilities or possible attempts to exploit them in a timely manner.
Medium	**Vulnerability exploitation is unlikely to likely.** Security measures are in place, the effectiveness of which is regularly checked. The ability of security measures to detect possible vulnerabilities in time or possible attempts to overcome measures is limited. There are no known successful attempts to overcome security measures.
High	**Vulnerability exploitation is likely to very likely**. Security measures are in place, but their effectiveness does not cover all the necessary aspects and is not regularly checked. There have been some partial successful attempts to overcome security measures.

Critical	**Vulnerability exploitation is very likely or more or less certain.** Security measures are not implemented or their effectiveness is severely limited. The effectiveness of security measures is not checked. Successful attempts to overcome security measures are known.

Figure: Vulnerability assessment scale

Level	Description
Low	**Risk is** considered **acceptable**.
Medium	**Risk can be reduced by less demanding measures** or in case of higher intensity of measures the risk is acceptable.
High	**Risk is unacceptable in the long run,** and systematic steps must be taken to eliminate it.
Critical	**Risk is unacceptable,** and steps must be taken to eliminate it immediately.

Figure: Scale for risk assessment

---

[1] ISO/IEC 27005 p. 8

[2] ISO/IEC 27005 p. 9

[3] POŽÁR, Josef and Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Prague: AFCEA, 2011. ISBN 978-80-7251-364-2, p. 12, or: POŽÁR, Josef and Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Available from: https://www.cybersecurity.cz/data/srib.pdf p. 5

[4] See Appendix 3 (5) to the CSD (Cybersecurity Decree)

5.3. Security policy

A security policy is **a set of policies and rules that determine how to ensure the protection of assets.**

By default, a security policy rests on the fact that the designated entities are obliged, with regard to the information security management system, to:

a) establish a security policy and **maintain security documentation** covering the following policy areas:[1]

- information security management system,
- asset management,
- organisational security,
- supplier management,
- security of human resources,
- traffic and communication management,
- access control,
- safe user behaviour,
- backup and recovery and long-term storage,
- secure transmission and exchange of information,
- management of technical vulnerabilities,
- safe use of mobile devices,
- acquisitions, development and maintenance,
- protection of personal data,
- physical security,
- security of the communication network,
- protection against malicious code,
- deployment and use of a tool for detection of cybersecurity events,
- secure use of cryptographic protection,
- change management,
- cybersecurity incident management,
- business continuity management.

The **content of the security documentation** is also specified. It must include:

- cybersecurity audit report,
- report on the review of the information security management system,
- methodology for asset identification and evaluation and for risk assessment,
- asset and risk assessment report,
- declaration of applicability,
- risk management plan,
- security awareness development plan,
- records of changes,
- reported contact details,
- an overview of generally binding legal regulations, internal regulations and other regulations and contractual obligations,
- other recommended documentation (e.g. infrastructure topology, overview of network devices).

b) regularly review the security policy and **security documentation,**

c) ensure that the security policy and security documentation are up to date.

The security policy and security documentation must be:

- available in printed or electronic form,
- communicated as part of an obligor,
- reasonably available to the parties concerned,
- managed,
- protected in terms of confidentiality, integrity and availability,
- maintained in such a way that the information contained therein is complete, legible, easily identifiable and easily searchable.

---

[1] For more details, see Appendix 5 to the CSD

5.4. Organisational security

Defining organisational security and especially anchoring cyber or ICT security within the already functioning structures of an organisation is of the utmost importance for the possible management of cyber threats or attacks.

Security issues should be addressed within an organisation at the operational, tactical and strategic level from the perspective of the organisation's management.

From a security point of view, it is important that the cybersecurity department is separated from the department that provides ICT operations.[1]

```
Example: The author met with a network administrator who was required by his employer to become a security manager at the same time.
In practice, this would mean that the
administrator would draw up directives to be followed, while at the same time checking for himself the compliance and enforcing it.
The absurdity of this
situation is obvious at first glance.
```

By default, organisational security rests on the fact that the designated entities are obliged, with regard to the information security management system, to:

- **ensure that the security policy and objectives of the ISMS** are set in such a way that they are compatible with the strategic direction of the obligor,
- **ensure the integration of the ISMS** into the processes of the obligor,
- **ensure the availability** of resources needed **for the ISMS**,
- **inform employees of the importance of the ISMS** and the importance of achieving compliance with its requirements with all parties concerned,
- **provide support** to achieve the intended **ISMS** outputs,
- **lead employees to develop the efficiency of the ISMS** and support them in this development,
- **promote continuous improvement of the ISMS**,
- **support those holding security roles** in promoting cybersecurity in their areas of responsibility,
- **ensure the establishment of rules for the designation of administrators and persons who will hold security roles**,

  Security roles include:

  - Cybersecurity **Manager**,
  - Cybersecurity **Architect**,
  - **Asset Guarantor**,
  - Cybersecurity **Auditor.**
- **ensure that the confidentiality** of administrators and security officers is maintained,
- **provide persons with security roles with the appropriate powers** and resources, including budgetary allocations to fulfil their roles and perform related tasks,
- **ensure testing of business continuity plans, recovery and cybersecurity incident management processes**.

To assign and display (within a table) the responsibilities of individual persons (security roles according to CSD) within an organisation, use of the **RACI responsibility matrix** (**RACI matrix) is recommended.** RACI is an acronym of:

R – Responsible	who is responsible for performing the assigned task (given activity)
A – Accountable (or Approver)	who is responsible for the whole task, or for the fact that the given process is performed as predefined
C – Consulted	who can provide valuable advice or consultation for the task but does not take responsibility for the performance of the process
I – Informed	who should be informed about the progress of the task or decisions in the task

The rule is that only one person has overall responsibility (A – Accountability) for a given task, the people involved (R – Responsibility) should be proportionate to the given task. The RACI method is a simple form of a competency model.[2]

Processes:	**Roles:**	**CS Committee**	**CS Manager**	**CS Architect**	**CS Auditor**	**Asset guarantor**
Overall management and development of CS		**A**	**R**	**R**		**C**
Information security management system		**A**	**R**	**C**		**C**
Proposal of security measures		**C**	**A**	**R**		**C**
Implementation of security measures		**C**	**A**	**R**		**C**
Ensuring development, use and security assets			**A**	**C**		**R**

CS audit	**I**	**C**	**C**	**A/R**	**C**

Figure: RACI matrix[3]

[1] Cf. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21/08/2018]. Available from: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf p. 3

[2] For more details see e.g. *Matice odpovědnosti RACI (RACI Responsibility Matrix).* [online]. [cit. 21/08/2018]. Available from: https://managementmania.com/cs/matice-odpovednosti-raci or *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21/08/2018]. Available from: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf p. 6

[3] The RACI matrix in the description of basic processes associated with security roles. The relationships of individual security roles and processes may vary depending on the organisation. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21/08/2018]. Available from: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf p. 7

5.5. Asset management

An asset is anything that has a certain value for a person, organisation or state.

An asset can be a **tangible** thing (building, computer system, networks, energy, goods, etc.) or an **intangible** one (information, knowledge, data, programs, etc.) from the point of view of civil law.

However, an asset can also be a **quality** (e.g. availability and functionality of the system and data, etc.) or a **good name**, reputation, etc. **People** (users, administrators, etc.), along with their knowledge and experience, are also an asset from the point of view of cybersecurity.

An **ancillary asset** is a technical asset, employees and suppliers involved in the operation, development, administration or security of the information and communication system.

A **primary asset** is information or a service processed or provided by an information and communication system.

"As part of sound information security management, it is important to have an overview of the links and dependencies between primary and ancillary assets."[1]

As part of asset management, entities are required to:

- **establish a methodology for identifying assets**,
- establish a methodology for **valuing assets**,
- **identify and record assets**,
- **determine** and record **asset guarantors**,
- **assess and record primary assets** in terms of confidentiality, integrity and availability and classify them into individual asset levels,
- **determine and record the links between primary and ancillary assets** and assess the consequences of the dependencies between primary and ancillary assets,
- **assess ancillary assets** and take into account the interdependencies between primary and ancillary assets,
- establish and **implement the protection rules** necessary to secure the **various levels of assets**,
- lay down permissible uses for the assets and rules for the handling of assets with regard to the level of assets, including rules for the secure electronic sharing and physical transfer of assets,
- determine the method of disposal of data, operational data, information and their copies or disposal of technical data carriers with regard to the level of assets.

In assessing the significance of primary assets, it is mandatory to consider:

- scope and importance of personal data, special categories of personal data or trade secrets,
- scope of legal obligations or other obligations in question,
- scope of breach of internal management and inspection activities,
- damage to public, commercial or economic interests and possible financial losses,
- impacts on the provision of important services,
- scope of the disruption of normal activities,
- impacts on the maintenance of goodwill or the protection of reputation,
- impacts on the safety and health of persons,
- impacts on international relations,
- impacts on users of the information and communication system.

---

[1] MAISNER, Martin and Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Prague: Wolters Kluwer, 2015. p. 85

5.6. Security of human resources

Entities are also obliged to pay attention to the security of human resources within the ISMS as one of the assets. As mentioned earlier, people are usually the weakest link in cybersecurity. In particular, these entities are obliged to:

- **establish a security awareness development plan** to ensure adequate security awareness education and improvement,
- This plan contains the form, content and scope of
  - instruction of users, administrators, security officers and suppliers about their responsibilities and security policy;
  - necessary theoretical and practical training for users, administrators and security officers.
- **designate the persons responsible** for the implementation of the individual activities set out in the plan,
- **provide guidance** to users, administrators, security officers and suppliers on their responsibilities and security policy through initial and regular trainings,
- **provide regular professional trainings for persons holding security roles**,
- ensure **regular training sessions** and checking of security awareness of employees in accordance with their job description,
- ensure **check of compliance with the security policy by users**, administrators and persons holding security roles,
- in the event of termination of the contractual relationship with administrators and persons holding security roles, **ensure the transfer of responsibilities**,
- **assess the effectiveness of the security awareness development plan**, the training provided and other activities related to improving security awareness,
- **determine rules and procedures for dealing with breaches of established security rules** by users, administrators and persons holding security roles.

It is obligatory to keep overviews of the above-mentioned training sessions that contain the subject of the training and a list of persons who have completed the training.

```
Example:
Because the standard training, which is the only one users are required to complete, proves to be ineffective, some organisations
also approach methods to
verify a true understanding of the information provided in their own training. This could be, for example, sending out phishing
messages to users after training focused on this area. The organisation then monitors how many users
responded incorrectly to the attack. However, it should be noted that such tests must be well thought out, and a lawyer to assess
whether the test used
will not, for example, infringe on the privacy of employees should not be absent.
```

5.7. Business continuity management

Business **C**ontinuity **M**anagement (**BCM**) is a process based on identifying key elements (systems and processes) in an organisation and then setting up processes and procedures to ensure continuity or renewal of these elements, at a predefined level at which it will still be possible to perform basic tasks of the organisation.

In the case of business continuity management, a risk assessment and analysis of existing information and communication systems and services should be carried out and on the basis of the data thus obtained determined:

- **the minimum level of services provided**, which is acceptable for the use, operation and management of the information and communication system,
- **the time of restoration of operation**, during which the minimum level of provided information and communication system services will be restored after a cybersecurity incident,
- **that data recovery point** as the time period for which data must be recovered after a cybersecurity incident or failure.

The obligor also within the framework of business continuity management shall:

- **set out the rights and obligations** of administrators and **persons** holding security roles,
- assess and **document possible impacts of cybersecurity incidents and assess possible risks** related to threats to business continuity through risk assessment and impact analysis,
- **set out a policy of business continuity management**,
- **develop, update and regularly test business continuity plans and emergency plans** related to the operation of the information and communication system and related services,
- **implement measures to increase the resilience of the information and communication system** to cybersecurity incidents and restrictions on availability.

5.8. Technical measures

Technical measures together with organisational measures are the basic elements of security measures. While organisational measures are primarily focused on setting rules and policies in an organisation, technical measures are primarily focused on rules for setting up information and communication systems and services.

Within individual technical measures, possible open source tools applicable to the given measure will also be demonstrated.

5.8.1 Physical security

Physical security is primarily focused on the protection of the technical assets of a given entity. Regarding physical security, Maisner states that "*the aim of this measure is primarily to prevent unauthorised access to individual elements of infrastructure, server rooms, system administrators' workplaces, etc. The effort is to prevent theft of property directly and indirectly related to the information system, or to prevent damage to tangible and intangible equipment or equipment of spaces. Last but not least, it tries to prevent a leakage of information and data.*"[1].

Within the scope of physical security, the obligor shall

- **prevent damage**, theft or misuse of assets or interruption of the provision of information and communication system services,
- determine a **physical security perimeter** demarcating the area in which information is stored and processed and where the technical assets of the information and communication system are located,
- **apply means of physical security** to the physical perimeter:
  - **to prevent unauthorised entry,**
  - **to prevent damage and unauthorised interference**,
  - **to provide protection at the building level and within buildings.**

The term physical **security perimeter** delineates a designated space or the boundaries of this space. Such a space can be, for example, a set of premises, the premises itself or part of a premises.

The premises is a building or other confined space. The **boundary of the premises** means a building envelope, a physical barrier (fencing) or another visibly defined boundary of the area. A **secured area** means a space in a building that is structurally or otherwise visibly delineated.

Means of physical security may include:

- **mechanical means of restraint** (e.g. locks, doors, grilles, foils, glass and other security structural and building elements, cabinet safes, safe doors and chamber safes,
- **secure area access inspection system** [alarm and electronic security systems, detectors (motion, glass breakage, etc.) determination of conditions for entry: identification element, PIN, biometrics (or a combination thereof)],
- **electrical security signalling equipment** (alarm security and emergency systems – electrical security signalling control panels, electrical security signalling detectors, shock detectors, perimeter detection systems, emergency systems, etc.),
- **special television systems** (**camera systems**, CCTV surveillance systems, etc.),
- **fire detection and fire alarm systems** (connection to the control and alarm equipment, or to the electrical security alarm control panel),
- **equipment limiting the effects of fires and natural events** (alarm systems, smoke detectors, automatic fire extinguishing systems, etc.),
- **equipment to ensure protection against failure of the power supply** (backup power supplies – UPS, diesel generators, etc.).

It is also possible to implement, for example:

- **equipment against passive and active eavesdropping.**[2].

Areas where entry/access should be limited or regulated from the point of view of security of information and communication systems, include mainly **server rooms** (primary, backup), **spaces with network elements** (router, switch, etc.), **data storages** (filing rooms, NAS storages, etc.), **premises of ICT administrators**, etc.

```
Example:
Physical security is one of the areas where organisational rules are typically violated and where periodic audits are required.
While most of the other
activities in the organisation are performed by administrators, the management of physical access is entrusted to a less qualified
workforce after security
deployment, for example, for cost-benefit reasons. This workforce may not be cognisant of particular security issues.
```

```
The author experienced several situations where, after a certain period of time, a person responsible for managing
physical access began to grant access to persons who should not have had access to the areas (e.g. server rooms), for example only
because a senior manager
requested access to the protected area, although he did not have sufficient privileges to be approved.
```

As part of physical security, it is also possible to use open source tools. In particular, these will involve cases of *"implementation of central security counters, including camera surveillance systems. For this purpose, tools designed for monitoring network elements (**Icinga, Nagios** and others) can be used, supplemented by an interface for corresponding sensors, connected to programs for the transmission and capture of video signals from security cameras."*[3].

5.8.2 Tool for protecting the integrity of communication networks

Within the scope of physical security, some administrators are required to:

- **ensure segmentation** of the communication **network**,
- ensure the management of communication within the communication network and the perimeter of the communication network (i.e. **manage secure access between the internal and external network**),
- **use cryptography to ensure the confidentiality and integrity of data during remote access**, remote **administration or access** to the communication **network using wireless technologies** (i.e. use cryptography to ensure e.g. VPN, ICT connection to Wi-Fi, etc.),
- **actively block unwanted communication** (e.g. spam filters, etc.),
- to ensure the segmentation of the network and to manage the communication between its segments, use a tool that ensures the protection of the integrity of the communication network.

*"The tool for protecting the integrity of communication networks here means a **suitably designed network topology**, including the use of network elements enabling the required network segmentation and filtering of traffic between individual elements. The equipment used to achieve these requirements are Ethernet switches, routers and firewalls. If it is not possible to ensure network segmentation using a VLAN on an editable switch, it is possible to secure it using several smaller non-manageable switches, each of which implements one physical LAN.*

When segmenting some networks, it is possible to use, for example, Turris routers (https://www.turris.cz/cs/), where high security is guaranteed (among other things due to the firmware, which was designed with regard to and achieving the maximum possible security) and also low power consumption.

*Software **routers/firewalls**: www.ipcop.org/; https://www.ipfire.org/*

*Ethernet **switch** for virtualised environment: http://www.openvswitch.org/".*[4]

5.8.3 Tool for user identity verification

As part of physical security, some administrators are required to use a tool to manage and verify the identity of users, administrators and information and communication system applications.

This tool is currently in effect a component of all commonly used operating systems (Linux, iOS, Windows). According to CSD, this tool should ensure

- **personal identity verification** (before starting activities in the information and communication system),
- **management of the number** of possible failed **login attempts**,
- **resilience** of stored or transmitted **authentication data against unauthorised theft and misuse**,
- **storage of authentication** data in a form resistant to offline attacks,
- **re-verification of identity** after a specified period of inactivity,
- **observance of the confidentiality of authentication data** when restoring access,
- **centralised identity management.**

To verify the identity of users, administrators and applications, the obligor uses:

- an **authentication mechanism** that is not **based** solely on the use of an account identifier and password but **on multi-factor authentication, with at least two different types of factors**,
- a tool for verifying the identity of users, administrators and applications, to use **cryptographic key authentication** and guarantee a similar level of security[5],
- a tool for identity verification of users, administrators and applications that uses an **account identifier and password for authentication**.[6]

If an account and password are used for authentication, the following conditions must be met:

- minimum password length:
  - **12 characters for users** and
  - **17 characters for administrators and applications**.
- **possibility to enter a password of at least 64 characters,**
- possibility to use **lowercase and uppercase letters, numbers and special characters** in a password,
- **possibility to change a password**, while **the time between two password changes must not be less than 30 minutes**,
- **not allow users and administrators to:**
  - **choose the most frequently used passwords,**
  - **create passwords based on** multiple repetitive characters, login name, email, system name or similar,
  - reuse previously used passwords with a **memory of at least 12 previous passwords**.
- **mandatory change of a password at intervals of a maximum of 18 months**, while this rule does not apply to accounts used to recover the system in the event of a disaster,
- **force the default password to be changed immediately after its first use,**
- **immediately revoke a password used to restore access after its first use or after a maximum of 60 minutes from its creation**,
- **include rules for creating secure passwords in the security awareness development plan.**

```
Example:
We recommend using practical demonstrations for training users. For example, CEWL or CUPP tools. Both can be found, for example, in
the Linux distribution
Kali. The CEWL tool can create a dictionary for a dictionary attack tailored to a specific organisation, based on the content of its
website. The CUPP tool can
then create a dictionary tailored to a specific user. According to the authors' experience, these practical examples are very
beneficial for users as they
practically see that their password used so far, consisting of, for example, the date of birth and the name of the family dog, can
actually be generated if
the attacker has enough information about them.
```

"For practical user authentication, the open source community offers plenty of software compatible with its commercial counterparts. These are, for example:

FreeRADIUS - http://freeradius.org/ /RADIUS

OpenLDAP - http://www.openldap.org/ /Microsoft AD, Oracle Internet Directory

Kerberos - https://www.gnu.org/software/shishi/

OpenDiameter - https://sourceforge.net/projects/diameter/

All of these tools provide means to enforce the specified password complexity, as well as other attributes required by CSA, either by themselves through login.conf*, or by using external mechanisms such as cracklib and dictionaries of popular "passwords".*[7]

5.8.4 Access permission management tool

Within the scope of physical security, some administrators are required to use a centralised access permission management tool.

The term **permission** means the right to access any of the assets (typically an information or communication system, applications, etc.). In practice, it is a tool for "user and group management" and a tool for setting permissions on files and directories. These tools are a proprietary component of all standard operating systems.

A centralised access permission management tool is intended to ensure the management of permissions:

- for access to individual assets of the information and communication system and
- for reading data, writing data and changing permissions.

It is advisable to apply tools for centralised management of access rights **that will communicate with a central AAA** (**A**uthentication, **A**uthorisation, **A**ccounting) **server**.

Example:
It is important to keep in mind the management of access permissions when designing software. The author knows of an application that had very general
permissions, and in fact only the roles of administrator and user existed in it. The administrator was authorised to add additional users and
administrators, and the user was authorised to perform other activities. However, this application stored important information about the organisation's
customers. Because this application did not allow any granularity of permissions, all users, regardless of their actual business needs, were allowed
to access any part of the customer information. This situation eventually resulted in a leak of data related to a specific customer.

5.8.5 Malware protection tool

As part of physical security, some administrators are required to set up protection against malicious code by:

- **ensuring** (given the importance of assets) **the use of a tool for continuous automatic protection of**
  - terminal stations,
  - mobile devices,
  - servers,
  - data storages and removable data carriers,
  - communication networks and elements of the communication network,
  - similar devices.
- **monitoring and managing the use of removable devices and data carriers,**
- **monitoring and managing the use of** removable devices and data carriers,
- **managing permissions to run code,**
- **performing a regular and effective update** of an anti-malware tool.

"Protection against malicious software distributed via email. *An open source email proxy solution that provides protection against malicious software is the ASSP project (AntiSpam SMTP Proxy, https://sourceforge.net/projects/assp/), which enables comprehensive configuration of mail proxy behaviour via a web interface.*

Protection against malicious software distributed via web. *A suitable solution is, for example, the HTTP AntiVirus Proxy project (http://www.havp.org/) or www.cacheguard.com. Here, too, it is necessary to ensure adequate protection for end workstations, as encrypted traffic cannot be scanned in real time in the 'man in the middle' position.*

Blocking its network traffic, both at the level of the data infrastructure and at the level of 'personal firewalls' of end stations. Network communication rules should be set 'in a paranoid way', i.e. to allow only traffic necessary for legitimate software to work and ban everything else. However, a measure of a server, proxy server or network infrastructure element in no way fully replaces protection against malware on endpoint workstations, especially as it may not always be able to intercept encrypted traffic that is decrypted only on the client program."[8]

5.8.6 Tool for detection of cybersecurity events

Within the scope of physical security, some administrators are required to implement, within a communication network that includes an information and communication system, a tool for detection of cybersecurity events that ensures:

- **verification and check of transmitted data within the communication network** and between communication networks,
- **verification and check of transmitted data on the perimeter** of the communication network and
- **blocking of unwanted communication**.

"Outputs from many software tools can be used to detect cybersecurity events, including log analysers, such as Logwatch (https://sourceforge.net/projects/logwatch/files/), Epylog (https://fedoraproject.org/wiki/Infrastructure/Fedorahosted-retirement), intrusion detection systems, such as OpenVAS (http://openvas.org/), Suricata (https://suricata-ids.org/), Snort (https://www.snort.org/) or Samhain (la-samhna.de/Samoin)."[9]

5.8.7 Tool for collecting and evaluating cybersecurity events

Within the scope of physical security, some administrators are required to use a **tool to collect and continuously evaluate cybersecurity events.** It allows

- **the collection and evaluation of events**,
- **search for and grouping related records,**
- **provision of information for designated security roles** on detected cybersecurity events,
- **evaluation of cybersecurity incidents** in order to identify cybersecurity incidents, including early warning of identified security roles,
- reduction of cases of incorrect evaluation of events by regular updating of rule settings for:
  - evaluation of cybersecurity events,
  - early warning,
- use of information obtained by a tool for collecting and evaluating cybersecurity events for optimal setting of security measures of the information and communication system.

The tool for collecting and evaluating cybersecurity events means tools that are referred to as **SIEM** (**S**ecurity **I**ncident and **E**vent **M**anagement).

Within the open source SIEM solution, it is possible to use, for example, OSSIM/USM (https://www.alienvault.com/products/usm-anywhere/try-it-now), OSSEC (www.ossec.net/) or logalyze (www.logalyze.com).[10]

5.8.8 Application security

In the case of application security, attention is paid to applications that are used in information systems (whether within a computer system, mobile device or as a web application). Application security is ensured by, among other things, penetration testing of applications or application firewalls.

As part of physical security, some administrators are required to perform **penetration tests** of the information and communication system, focusing on important assets, namely:

- **before** they **are put into service and**
- **in connection with a significant change**.

Within the scope of application security, an obligor shall also **ensure the permanent protection of applications, information and transactions against:**

unauthorised activity,

denial of the activities performed.

"Application firewalls include, for example, web server security modules (www.modsecurity.org) or OWASP Web Application Firewall. Commercial tools for testing application security include, in particular, the Nessus tool (www.tenable.com/products/nessusvulnerability-scanner). Its open source alternative is the Open-VAS project (www.openvas.org/)."[11]

5.8.9 Cryptographic means

Cryptography (encryption) is a scientific discipline that deals with the conversion of intelligible information into a form incomprehensible to a recipient if the recipient does not own the keys with which it is possible to decrypt the information.

With the transfer of a considerable amount of data and information to ICT systems, it is necessary to pay increased attention to the possibilities of encrypting (confidentiality of content) of transmitted data.

Within the scope of physical security, some administrators are required, to protect information and communication system assets, to:

- use currently robust cryptographic algorithms and cryptographic keys,
- use a key and certificate management system that:
  - ensures the generation, distribution, storage, changes, validity restrictions, revocation of certificates and disposal of keys,
  - enables inspection and audit.
- promote safe handling of cryptographic means,
- take into account the recommendations in the field of cryptographic means issued by the Office (NÚKIB), published on its website.

*"In order to ensure sufficiently robust encryption of network traffic, the OpenSSL libraries (*openssl.org*) are used, but it is necessary to ensure that they are up-to-date and properly configured in order to comply with the terms of this decree. It is necessary to follow current reports on vulnerabilities and upgrade unsatisfactory versions of libraries without delay to variants without known vulnerabilities. In this regard, the bettercrypto project (https://bettercrypto.org/), is recommended to help administrators ensure the best possible security for the services and the cryptography they use."*[12]

5.8.10 Tool for ensuring the level of information availability

Within the scope of physical security, some administrators are required to implement measures to ensure the level of availability to ensure:

- **availability of information and communication system,**
- **resilience of information and communication system** to cybersecurity incidents that could reduce its availability,
- **availability of important technical assets** of information and communication system,
- **redundancy of assets** necessary to ensure the availability of information and communication system.

The implementation of a tool for ensuring the level of information availability fulfils an organisational asset: Business Continuity Management (**BCM**).

"To achieve the prescribed level of availability, cluster and cloud technologies developed as open source (KVM, OpenStack) can be used, or the availability of a replacement asset can be ensured at a specified time through back-up/restore software (https://sourceforge.net/projects/bacula/)." ***[13]***

---

[1] MAISNER, Martin and Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Prague: Wolters Kluwer, 2015. p. 91

[2] The area must be secured against passive and active eavesdropping by sufficiently soundproof walls, doors, floor and ceiling, windows, ventilation openings or air conditioning ducts must be protected by technical means. The area must be protected against eavesdropping from outside the meeting area. No furniture or equipment may be placed in the area unless they have been inspected for the unauthorised use of technical means of obtaining information in the meeting area. The furniture and equipment of the area must be registered (including the type, or serial and inventory number), including the history of movement. It is not desirable to place telephones in the area. If their installation is absolutely necessary, they must be equipped with a disconnector or disconnected manually before the meeting. Mobile phones, any recording equipment, transmitting equipment, any test, measuring and diagnostic equipment and other electronic equipment may not be brought into the area. (This does not apply to equipment used in the course of the inspection with the knowledge of the responsible person or his/her authorised person.) Rules for the registration and movement of persons and facilities must be developed for the area.

[3] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[4] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[5] Provided that the obligor has not yet fulfilled the first of the preferred authentication mechanisms.

[6] Provided that the obligor has not yet fulfilled the second of the preferred authentication mechanisms

[7] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[8] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[9] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[10] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[11] Ibidem

[12] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[13] Ibidem

5.9. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

ℹ️

- There are many reasons for the introduction and implementation of cybersecurity. The most common include, for example, negative economic consequences in the case of a successful cyberattack where sensitive data are stolen. A successful cyberattack can also compromise an organisation's own operations and functioning, for example, by restricting access to computer systems or data through ransomware. Another reason for the introduction of cybersecurity may also the loss of credibility of an attacked organisation.
- Currently, the most important document of the European Union related to the issue of cybersecurity is DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the European Union.
- The Information Security Management System (ISMS) is a set of rules designed to maintain the confidentiality, integrity and availability of information by applying a risk management process and providing assurance to stakeholders that risks are being adequately managed.
- The ISMS solution requires a systemic and comprehensive approach, respecting the principles and elements of the entire cybersecurity lifecycle. The ISMS management system is based on the Deming cycle, or on the PDCA (Plan-Do-Check-Act) cycle too.
- The PDCA cycle is one of the basic management principles based on the gradual improvement of the quality of processes, services, data, products, etc. thanks to the constant repetition of its four basic activities: Plan-Do-Check-Act.
- The value of risk is most often expressed as a function affected by impact, threat and vulnerability. For example, the following function can be used for self-assessment of risk:

Risk = impact * threat * vulnerability

- A security policy is a set of policies and rules that determine how to ensure the protection of assets.
- Defining organisational security and especially anchoring cyber or ICT security within the already functioning structures of an organisation is of the utmost importance for the possible management of cyber threats or attacks.
- An asset is anything that has a certain value for a person, organisation or state.
- An ancillary asset is a technical asset, employees and suppliers involved in the operation, development, administration or security of the information and communication system.
- A primary asset is information or a service processed or provided by an information and communication system.
- Business Continuity Management (BCM) is a process based on identifying key elements (systems and processes) in an organisation and then setting up processes and procedures to ensure continuity or renewal of these elements, at a predefined level at which it will still be possible to perform basic tasks of the organisation.

🗝️

KEY WORDS TO REMEMBER

- NIS directive
- ISMS
- PDCA
- Threat
- Risk
- Impact
- Vulnerability
- Security policy
- Asset
- Physical security
- Business Continuity Management

❓

KNOWLEDGE CHECK QUESTIONS

- Define ISMS.
- What is the PDCA cycle, and how does it apply?
- What components can be included in physical security?
- What is: Business Continuity Management?
- Define threat.
- Define risk.
- Define impact.
- Define vulnerability.
- Define asset.
- What assets do we recognise, and what everything is an asset?

6. Protection of personal data in cyberspace

In the first place, I want to focus on the protection of individuals, specifically the protection of the form and privacy of the individual. Privacy is one of the fundamental human rights enshrined in the Universal Declaration of Human Rights of 1948[1].

---

[1]Available from: http://www.osn.cz/wp-content/uploads/2015/03/vseobecna-deklarace-lidskych-prav.pdf

These rights are primarily enshrined in Articles 12 and 18 of the Universal Declaration of Human Rights.

Article 12: *"**No one shall be subjected to arbitrary interference with his privacy**, family, home **or correspondence**, nor to attacks upon his honour and reputation. **Everyone has the right to the protection of the law against such interference or attacks.**"*

Article 18: *"Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance."*

6.1. Excursion into the rights and obligations arising from certain legal norms

We are absolutely convinced that **it is not appropriate to address the issue of cybersecurity and other areas of security separately** (e.g. protection of personal data, data related to electronic communications and other similar data).

The reason for this belief lies in the growing integration and interconnection of different categories of data with computer systems and applications running on them. This interconnectedness and digitisation of analogue data will only increase in the future.

For this reason, it seems to be a suitable starting point to address the issue of security comprehensively and not only in connection with the rights and obligations arising from the Cyber Security Act or from other legislation.

The goal of organisations or individuals should be to implement such rules, processes, procedures and security measures that will meet the requirements of NIS, as well as, for example, GDRP, ePrivacy, eIDAS, etc. Such a procedure will allow the creation of **integrated security**.[1]

Figure: Demonstration of integrated security solutions[2]

Integrated multidisciplinary security

Řízení rizik a soulad s právními předpisy	**Risk management and compliance with legislation**
Právní poradenství pro bezpečnost	Legal advice for security
Finanční analýza bezpečnostních aspektů	Financial analysis of security aspects
Reakce na bezpečnostní incidenty a řízení incidentů	Security incident response and management
Bezpečnostní audity, soulad s požadavky ZoKB, eIDAS, GDPR, ČNB, PCI DSS, ISO27k	Security audits, compliance with CSA, eIDAS, GDPR, CNB, PCI DSS, ISO27k requirements
Analýza rizik	Risk analysis
Obnova po havárii	Disaster recovery
Řízení informační bezpečnosti	Information security management
Řízení kontinuity činnosti organizace	Business continuity management
Řízení fyzické bezpečnosti	Physical security management
Zabezpečení provozu	**Traffic security**
Forenzní služby	Forensic services

Specializovaná bezpečnostní školení a předávání know-how	Specialised security training and transfer of know-how
Mobilní bezpečnost, MDM, BYOD	Mobile security, MDM, BYOD
Řízení přístupů a identit, Identity-as-a-Service	Access and identity management, Identity-as-a-Service
Pokročilá analytika pro bezpečnost, predikce, predikce, učící se stroje	Advanced analytics for security, prediction, machine learning
Zpravodajství a ochrana kybernetického prostoru	Intelligence and cyberspace protection
Bezpečnost z technologického hlediska	**Security from a technological point of view**
Bezpečnost Cloudů	Cloud security
Bezpečnost datových center a sdílených služeb	Security of data centres and shared services
Posouzení a audit ICS/SCADA systémů	Assessment and audit of ICS/SCADA systems
Zabezpečení průmyslových zařízení a IoT, Průmysl 4.0	Security of industrial facilities and IoT, Industry 4.0
Systémy distribuované důvěry a Blockchain	Distributed trust systems and Blockchain
Post-kvantová kryptografie	Post-quantum cryptography
Zabezpečení platebních a transakčních systémů	Security of payment and transaction systems
Bezpečnostní technologie a integrace (Monitoring, SIEM, SOC, DLP, řízení zranitelnosti)	Security technologies and integration (Monitoring, SIEM, SOC, DLP, vulnerability management)
Bezpečnost Veřejně regulovaných služeb (PRS) a satelitních technologií	Security of Public Regulated Services (PRS) and satellite technologies
Etický hacking	**Ethical hacking**
Bezpečnostní revize kódu	Security code revision
Penetrační testování	Penetration testing
Red Teaming	Red Teaming

[1] For more details, see e.g. GREENFIELD, David. *Integrovaná bezpečnost: Už nastal její čas?* [online]. [cit. 01/03/2018]. Available from: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

[2]*Integrovaná multidisciplinární bezpečnost.* [online]. [cit. 17/02/2018]. Available from: https://www2.deloitte.com/cz/cs/pages/risk/solutions/integrovana-multidisciplinarni-bezpecnost.html

6.2. GDPR

The General Data Protection Regulation (EU) 2016/679 or the GDPR [1]is one of the most important international legal documents that is directly related to the issue of cybersecurity, although it is not primarily aimed at the field of ICT.

> *"**GDPR ≠ IT + software.***
>
> *The new data protection regulation has 778 lines. Only 26 of these directly concern IT security. Do you have any idea what the others contain?"*
>
> Mgr. Eva Škorničková[2]

It is the GDPR and the implementation of the obligations arising from this regulation that can be demonstrated by the fact that it is appropriate to comprehensively address security issues and not artificially isolate the obligations arising from various legal norms (in this case the Cyber Security Act and the GDPR).

The aim of this publication is not to perform a separate and comprehensive analysis of GDPR issues. Only partial terms, rights and obligations arising from the GDPR that at the same time have an overlap in the field of cybersecurity will be defined here.

The GDPR Regulation is a **general legal framework for the protection of personal data** valid and effective throughout the EU and, in certain cases, outside this territory. The main objective of the GDPR is to ensure comprehensive protection of the rights of data subjects against unauthorised treatment of their data and personal data, to strike a balance between the legitimate interests of controllers, processors and data subjects, to create a system of uniform law enforcement and a single sanction mechanism in this area, etc.

The scope of collecting and sharing personal data has increased significantly due to information and communication technologies and services that are linked to them. Information and communication technologies allow both private companies and public authorities to use personal data to an unprecedented extent in carrying out their activities. On the other hand, it is also possible to observe massive voluntary disclosure of personal data by natural persons whose data this applies to.

Information and communication technologies have significantly changed the economy and social life. They should facilitate the free movement of personal data within the European Union and the transfer of such data to third countries and international organisations. At the same time, however, these technologies and the processes associated with them should ensure a high level of protection of personal data.[3]

Due to the above, however, an **interesting paradox arises**, which consists of the following points:

- **natural persons on their own voluntarily publish an ever-increasing amount of data about themselves** (photos, videos, etc.), typically using information society services based on EULA[4] or SLA[5] between a user and a service provider to distribute this data,
- **personal data are mostly published on social media**, which, by the nature of its operation, presupposes such disclosure and enshrines in the Terms of Service the rules on the basis of which such data are treated,
- **when using a number of information society services, natural persons assume, and often expect, the interaction between these technologies and their cyber personality**[6].
- the international community, state and **natural persons** themselves **demand greater security of personal data and the denial of access to this data to other** (usually unauthorised) **entities, all provided that the existence of the first three points of this paradox is maintained**.

The consequence of this paradox is obvious. Information society service providers[7] must therefore make greater efforts to secure the individual services they provide to the end user, to increase the level of security of user-related data, to modify the existing Terms of Service and to introduce additional requirements arising from the GDPR.

6.2.1. Territorial scope of the GDPR

One might think that a way to avoid the GDPR would be to move beyond its reach, that is, outside the territory of the EU. However, the GDPR applies in cases where:

- **a controller or processor is established in the EU**, regardless of whether the processing takes place in the EU,
- **controllers or processors are not established in the EU, but**
- goods or services are offered to data subjects in the EU (regardless of remuneration),
- the conduct of data subjects within the EU is monitored.[8]

Due to the territorial scope thus defined, the GDPR has an extraterritorial impact and will in effect apply to all information society services that can be accessed from the geographical territory of the EU or that monitor the conduct of data subjects within the EU.

6.2.2. Personal data

Pursuant to Article 4 (1) of the GDPR, personal data are "***any information relating to an identified or identifiable natural person***. *An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

According to the GDRP, personal data are **any information** (e.g. pictorial, written, verbal, digital, genetic, medical, etc.) that **is related** (by content – e.g. name, address, job title, email, etc.) **to a data subject**.[9] From this point of view, and in line with the interpretation given in recitals 30, 34, 35 and 38 of the GDPR[10], the following should be considered as personal data:

- name and surname,
- **identification number,**
- birth certificate number,
- **location data (geo-)**,
- age and date of birth,
- gender,
- personal status,
- citizenship,
- **network identifiers**,
  - **IP address**,
  - **cookie identifiers**,
  - radio frequency identification tags, etc.,
- **photography**,
- **elements** of physical, physiological, genetic, mental, economic, **cultural or social identity**,
- personal or work address,
- personal or work telephone number,
- **personal or work email,**
- **verification identification data**,
- identification numbers issued by the state.

Bold personal data are typically related to information and communication technologies as well as the applications that use those technologies. The expansion of the range of data that can be considered personal data significantly affects the issues of cybersecurity and ensuring the protection of data that is managed in the organisation.

If we focus on the **item of network identifiers and authentication identification data, we will find that a number of data enabling the basic functioning of a computer system in a network can and probably will be considered personal data**.

There is a question often discussed in practice – is an IP address personal data?

In this case, in addition to the GDPR, it is appropriate to take into account the case law of the Court of Justice of the EU, which ruled, inter alia, in the case: **Patrick Breyer** versus **Federal Republic of Germany.**[11]

Patrick Breyer demanded in German courts that Germany stop retaining his IP addresses, which it obtained during his "visits" to several publicly accessible websites of the German federal authorities. From the point of view of the activities of the operators of the websites in question, this was a classic logging of the services offered by this ISP[12].

The German courts stayed the proceedings and referred the question to the EU Court of Justice for a preliminary ruling because there was no uniform interpretation of EU law in the present case.

In particular, it is necessary to proceed from an "*objective*" or "*relative*" criterion in order for a single detail to be personal data and thus identify a specific person.

"Objective" criterion means that data such as **IP addresses could be considered as personal data** processed by ISPs of non-connection services (e.g. by a website operator), **even if only a third party would be able to identify a specific user** (typically ISP connection).

"**Relative**" **criterion** means that **IP addresses could be considered personal data for an ISP connection** as they allow it to pinpoint the identity of a user, **but no longer for ISP services that actually only have IP address information and do not know the visitor's name**.

The Court of Justice of the EU stated that **it is indisputable that a dynamic IP address does not constitute information about an "identified person"** as the **address does not directly reveal the identity of the individual** owning the computer from which the website was visited **nor the identity of any other person who may have used the computer**.

On the other hand, the Court (Second Chamber) also stated (and subsequently ruled) that a **dynamic address** of an internet protocol **held by an online media service provider in connection with a person's access to a website** that was made available by that provider to the public **constitutes personal data** for that provider within the meaning of Article 2 (a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, **so long as the provider has legal means at its disposal that enable it to have the data subject identified by means of other information available to that data subject's internet service provider.**

According to this judgment, dated 19 October 2016, a dynamic IP address may in certain circumstances be personal data.

We demonstrate the impact of the fact that an **IP address, as well as other network identifiers, can be personal data** in two examples.

The following figure shows the communication of a PC and individual network elements (AP, DHCP server) and the subsequent connection of the PC to the network.

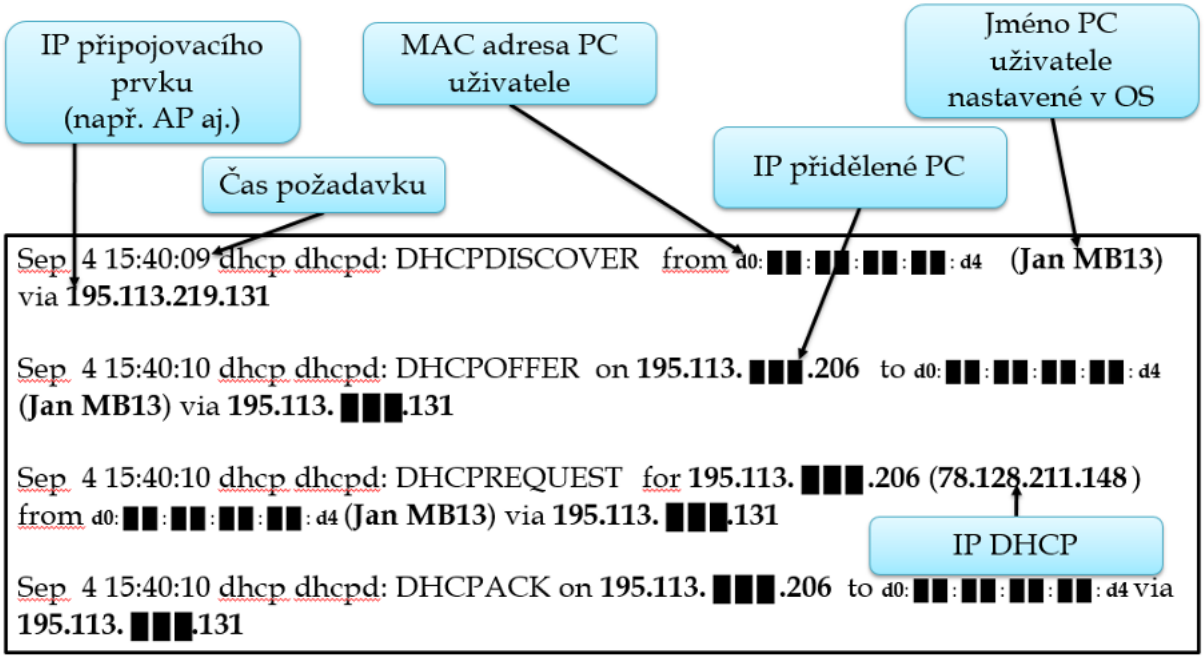


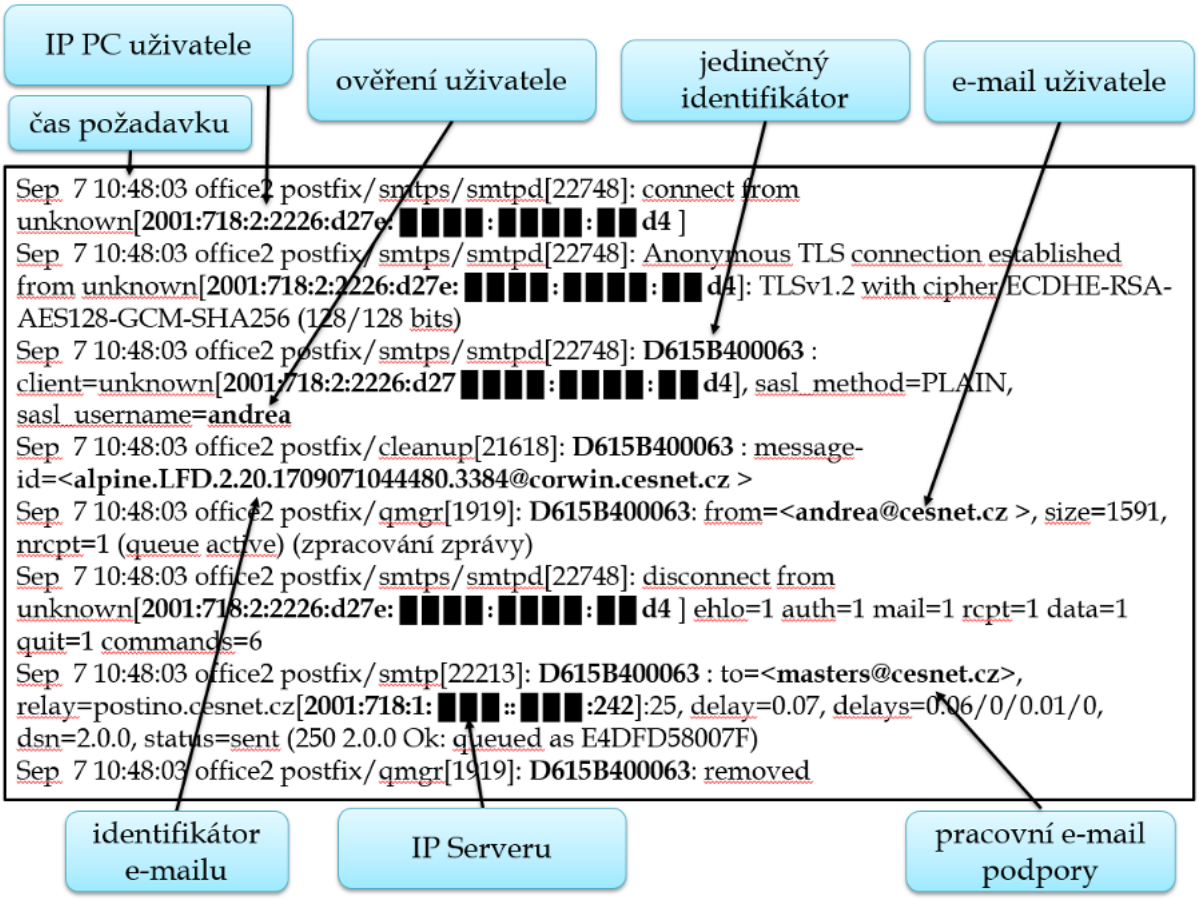
Figure: DHCP

IP připojovacího prvku (např. AP aj.)	IP of the connecting element (e.g. AP, etc.)
Čas požadavku	Request time
MAC adresa PC uživatele	MAC address of the user's PC
IP přidělené PC	IP assigned to the PC
Jméno PC uživatele nastavené v OS	The name of the user's PC set in the OS
IP DHCP	DHCP IP

If we consistently focus on **data** (information) **that are related to the data subject and are able to identify him/her**, then personal data in this case will not only be the IP address of the connecting element and the IP address of the DHCP server.

Theoretically, the time of a request is also personal data as it is a trace that can be used to identify a natural person, especially in combination with unique identifiers and other information that servers obtain.[13] At the same time, this is very important information because without an exact time it is not possible to identify to whom (which computer system) a specific IP address has been assigned.

Another example showing the extent of data processing that can be considered personal data is the processing of personal data when sending email via SMTP.



IP PC uživatele	IP address of a user's PC
čas požadavku	request time
ověření uživatele	user authentication
jedinečný identifikátor	unique identifier
e-mail uživatele	user email
(zpracování zprávy)	(message processing)
identifikátor e-mailu	email identifier
IP Serveru	Server IP
pracovní e-mail podpory	support work email

Figure: SMTP

If we again consistently focus on **data** (information) **that are related to the data subject and are able to identify him/her**, then personal data in this case will not be only the IP address of the connecting element and the IP address of the DHCP server.

The support work email could again be personal data if additional identifiers are assigned to it that are able to identify a natural person.

The key question is whether, in all processes that take place in computer systems (ICT elements) that are managed by an entity (natural or legal person), **we are able to distinguish a situation where data are transferred purely between computer systems without relation to any natural person and when the natural person will already be involved in these processes as a data subject according to the GDPR**.

We believe that, with specific exceptions, we will not be able to single out processes that take place without human interaction. Based on this assertion, the requirements of the GDPR should then be applied to all processes involving the manipulation of information that is relevant to the data subject and capable of identifying him or her. At the same time, it will be necessary to take sufficient security measures to sufficiently protect both the transmission system, computer systems and applications that work with such information and the information (or data) itself.

In addition to the above personal data, the GDPR defines specific categories of personal data that include data on:

- racial or ethnic origin,
- religion,
- political views,
- membership in trade unions or other organisations,
- sexual orientation,

- committing offences (crime/misdemeanour, etc.) and punishing them,
- genetic data (DNA & RNA),
- biometric data,
- health data.

6.2.3 Processing of personal data

According to Article 4 (2) of the GDRP, the processing of personal data means **any operation** or set of operations that is performed on **personal data** or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The protection of the data subject shall apply to the processing of personal data where such data are stored or entered in a register.[14]

However, according to the GDPR, **processing cannot be understood as any handling of personal data**. **Processing of personal data must be considered as a more sophisticated activity that a controller performs with personal data for a certain purpose and does so systematically from a certain point of view.**[15]

Among other things, **activities performed by a natural person within the framework of a purely personal nature or activities performed exclusively in a household, and thus without any connection with professional or business activities, are excluded** from the processing of personal data according to the GDPR.[16]

Article 5 (1) (a) of the GDPR sets out the principles for the processing of personal data. According to the GDPR, these principles include:

- **lawfulness, fairness and transparency** [Art. 5 (1) (a) of the GDPR] – a controller of personal data is obliged to:
- inform a data subject of the ongoing processing operation and its purposes,
  - inform a data subject about profiling and its consequences,
  - inform a data subject, if personal data are obtained from him/her, whether he/she is obliged to provide these data and about the consequences of their possible non-provision,
  - **prove the existence of at least one legal reason for the processing of personal data**,
  - **document:**
    - what, how, why it processes,
    - consent and legal reason,
    - the time for which it processes,
    - **guarantees and security measures taken**.
- **purpose limitation** [Art. 5 (1) (b) of the GDPR] – personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,
- **data minimisation** [Art. 5 (1) (c) of the GDPR] – personal data must be commensurate and relevant to the purpose for which they are processed,
- **accuracy** [Art. 5 (1) (d) of the GDPR] – personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate with regard to the purposes for which they are processed are erased or rectified without delay,
- **storage limitation** [Art. 5 (1) (e) of the GDPR] – personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which they are processed,
- **integrity and confidentiality** [Art. 5 (1) (f) of the GDPR] – personal data must be **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.**

6.2.4 Security of personal data

One of the areas that the GDPR explicitly addresses is the **issue of security of processing of personal data**.

Article 32 of the GDPR states that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the **controller** (or processor) **shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate:

- **the pseudonymisation and encryption of personal data,**
- **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,**
- **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,**
- **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.**

*"**In assessing the appropriate level of security account shall be taken in particular of the risks** that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."*[17]

In determining the risk, it is necessary to take into account in particular the category of personal data that could be affected by the security breach, the nature of the security breach and the number of data subjects concerned. Higher risk is posed by "more sensitive" personal data (see e.g. special categories of personal data), a larger set of personal data, or data that can cause harm to the data subject or interfere with his or her rights.

According to Article 32 (4) of the GDPR, the controller and the processor shall take measures to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by European Union or Member State law.

6.2.5 Data Protection Impact Assessment (DPIA)

The **D**ata **P**rotection **I**mpact **A**ssessment (**DPIA**) is a tool to be used when a certain type of **processing is likely**, **especially when using new technologies**, taking into account the nature, scope, context and purposes of the processing, **results in a high risk to the rights and freedoms of individuals**. It is a tool that can help controllers identify potential risks of personal data processing and implement appropriate measures.

A data protection impact assessment should be carried out in the following cases:

- a **systematic and comprehensive assessment of personal aspects relating to natural persons, based on automated processing, including profiling** that determines decisions that produce legal effects in relation to natural persons or have a similarly serious impact on natural persons,
- **processing of special categories of personal data** (biometric data or data on criminal convictions and on criminal offences or related security measures),
- extensive systematic monitoring of publicly accessible premises,
- **any other operation where the competent supervisory authority considers that the processing is likely to pose a high risk to the rights and freedoms of data subjects.**

The data protection impact assessment should include:

- description of the intended processing operations,
- assessment of the necessity and adequacy of operations in terms of purpose (**proportionality test**),
- **risk assessment for the rights and freedoms of entities**,
- **planned measures to address these risks, including guarantees, security measures, etc.**

The GDPR itself also contains other institutions (e.g. pseudonymisation, requirements for erasure or portability of personal data, etc.) that may relate to activities carried out within information and communication systems and that require an appropriate level of security and protection.

It is important to identify the influence (impact) of the GDPR on an organisation, on its individual parts and processes. In fact, it is an audit where everywhere in an organisation or for the individual, personal data are processed in relation to the GDPR. Subsequently, the procedure is based on modifying or creating rules and processes (if necessary) both within an organisation and in relation to the data subject. At the same time, all these activities should respect the basic principles of security.

As with the implementation of security rules in general, when implementing the GDPR or other documents and recommendations, it should be kept in mind that there is no single rule, template, tool, solution or procedure applicable to each organisation or each situation.

It is necessary to adopt and implement your own solution in accordance with the GDPR.

It is necessary to individualise...

---

[1] [online]. Available from: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&qid=1488972453767&from=CS

[2] ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10/11/2017]. Available from: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

[3] Cf. recital 6 of the GDPR

[4] **EULA** (**E**nd **U**sers **L**icence **A**greement) means the Terms of Service that allow the use of a service of a service provider. The EULA is a contract that is usually defined unilaterally by a service provider. However, a user is not limited in any way in his/her rights as he/she has the option of not using such unilaterally set terms of service. In the case of consent to the use of such services, it is generally possible to state that private law standards will be applied primarily.

The question is whether a user is really aware of what Terms of Service he/she has agreed to, when they become binding on him/her and what possible (legal) interference with his/her fundamental human rights and freedoms is such consent. Another important fact is that the service provided in this way may affect the rights and legitimate interests (e.g. IT security, trustworthiness of data, etc.) of third parties (e.g. employers, etc.) who have not explicitly agreed to use the service.

The sad fact remains that a very small percentage of users are willing to read the Terms of Service relating to a service provided.

[5] **SLA (S**ervice**-L**evel **A**greement) means an agreement entered into by and between a provider of a service and its user.

[6] **This interaction can be monitored when using location and geolocation services** (e.g. Google Maps, Waze, Map List, etc.) since a natural person assumes that the computer system will be able to locate him/her and display the most convenient route. Likewise, the interaction is expected, for example, **for services enabling the sale and purchase of goods** (e.g. Letgo – see recommended ads by geolocation or already purchased goods), **restaurant and accommodation services** (e.g. Tripadvisor, Booking.com, Airbnb, etc.), etc.

[7] For more details see KOLOUCH, Jan. *CyberCrime*. Prague: CZ.NIC, 2016, p. 78 et seq. and p. 109 et seq.

[8] See Article 3 of the GDPR – Territorial scope

[9] According to Article 4 (1) of the GDPR, **a data subject** is an identified or identifiable **natural person**. **A subject may be identified:**

- **directly,**
- **indirectly (e.g. singling out, etc.).**

[10] The recitals are provisions preceding the actual text of the GDPR and are in some cases an interpretation or, to some extent, an explanatory memorandum to the actual text of the regulation.

[11] For more details see: [online]. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

[12] On the concept of ISP itself, the rights and obligations of individual ISPs, see in more detail, for example, KOLOUCH, Jan. *CyberCrime.* Prague: CZ.NIC, 2016, p. 78 et seq. and p. 109 et seq.

[13] For more details see recital 30 of the GDPR

[14] See recital 15 of the GDPR

[15] For more details see *Základní příručka k GDPR.* [online]. [cit. 07/08/2018]. Available from: *https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938*

[16] See recital 15 of the GDPR

[17] Article 32 (2) of the GDPR

6.3. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

ℹ️

- The GDPR is a general legal framework for the protection of personal data, and it is valid and effective throughout the EU and, in certain cases, outside this territory**.** The main objective of the GDPR is to ensure comprehensive protection of the rights of data subjects against unauthorised treatment of their data and personal data, to strike a balance between the legitimate interests of controllers, processors and data subjects, to create a system of uniform law enforcement and a single sanction mechanism in this area, etc.
- However, the GDPR applies in cases where:
  - a controller or processor is established in the EU, regardless of whether the processing takes place in the EU,
  - controllers or processors are not established in the EU, but
    - goods or services are offered to data subjects in the EU (regardless of remuneration),
    - the conduct of data subjects within the EU is monitored.
- Pursuant to Article 4 (1) of the GDPR, personal data are *"any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*
- According to Article 4 (2) of the GDRP, the processing of personal data means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller (or processor) shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
  - the pseudonymisation and encryption of personal data,
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- The Data Protection Impact Assessment (DPIA) is a tool to be used when a certain type of processing is likely, especially when using new technologies, taking into account the nature, scope, context and purposes of the processing, to result in a high risk to the rights and freedoms of individuals. It is a tool that can help controllers identify potential risks of personal data processing and implement appropriate measures.

🗝️

KEY WORDS TO REMEMBER

- GDPR
- Personal data
- Data controller
- Processing of personal data
- Data Protection

❓

KNOWLEDGE CHECK QUESTIONS

- What is the territorial scope of the GDPR?
- What overall is personal data?
- Is an IP address personal data?
- What are the responsibilities of a personal data controller?
- What is meant by the processing of personal data?
- What does Data Protection Impact Assessment mean?

7. Privacy and security in ICT, data protection in cyberspace

Living in the digital age with the idea or feeling that my actions are anonymous or hidden from the eyes of other users[1] is, in my opinion, naive. With the advent of the digital age, not only its positive but also its negative aspects appear.[2] One such negative aspect is the fact that we are less and less interested in the essence of the functioning of services provided in cyberspace.

Our world, which we increasingly understand as the "world of information" or "world of the Internet", is firmly connected with information and communication technologies that interfere in an individual's life in a very significant way. These technologies facilitate access to information and simplify or speed up mutual communication between individual users, etc. On the other hand, it is important to realise that any publication of information from our private life on the Internet poses the risk of exploitation by anyone in cyberspace.

All applications, whether used in any computer system, web services[3] and especially social media,[4] collect a considerable amount of information about their users. They do not need this information for their operation, but it allows both the ISP in question to provide a service "for free" and to "target" or modify the services it offers. Information that is not necessary by default for the direct functionality of individual services includes, for example, information of a **personal** nature (name, surname, email address, telephone number, address, etc.), **sensitive** nature (e.g. information about the computer operating system used, versions individual applications, cookies, etc.), **location data** (GPS coordinates, information about Wi-Fi, GPRS, etc.), operational data, etc.[5]

The information can be used in a wide variety of ways. According to the information, a service provider may offer, for example, additional services or advertising based on the requirements, interests or hobbies of users. Thanks to them, the police are able to create a framework for the daily activities of a person who, for example, is lost or abducted and thus expedite their own activities in the search for this person. At the same time, however, the information can very easily be misused by criminals, either to establish contact with a victim or to plan a crime.

By providing (even if involuntarily or unwittingly) the data, the user of the service allows other people to obtain important information about their lives (e.g. information about their behaviour during the day, places visited, activities and people with whom he/she is in contact).[6] At this point, **we ourselves become information or a commodity that someone else can trade with**.

Various available statistics[7] indicate that the total population is currently approximately 7,359,244,000 people. Of this number, about 3.6 billion people are active Internet users, and more than 2.1 billion people are active users of social media. Mobile devices are owned by more than 3.6 billion users, and more than 1.7 billion users connect to social media through these devices. Social media is dominated by Facebook with more than 1.59 billion users:[8]

In this section, I will try to draw attention to possible security threats that we are used to accepting or not perceiving in effect and in which most individuals or organisations are not even aware of the possible danger.

---

[1] The term user includes all entities that influence events in cyberspace. It is primarily necessary to include **ISP**s in this group. However, not all ISPs fall under the jurisdiction of Czech law (either for geolocation reasons or rather because their activities are not regulated by the law). Other "users" will undoubtedly be **LEAs** (Law Enforcement Agencies – which are allowed by the norms of individual countries to be one of the most intensive interventions in fundamental human rights and freedoms), **CERT/CSIRT teams**, **IT administrators**, **end users, etc.**

[2] E.g. cybercrime, addictions and, among other things, so-called digital dementia. For more details see: SPITZER, Manfred. *Digitální demence.* Brno: Host, 2014. ISBN 978-80-7294-872-7

[3] See e.g. *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají možnost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit.04/04/2014]. Available from: https://www.google.cz/intl/cs/policies/?fg=1

[4] See *Prohlášení o právech a povinnostech.* [online]. [cit.04/04/2014]. Available from: https://www.facebook.com/legal/terms

[5] **However, some authentication systems also need this additional information to function.**

[6] KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN and Terezie JANÍKOVÁ. neBezpečné chování na Facebooku. In: *Sborník příspěvků ke konferenci: Sociální sítě. Mobilní aplikace.* Plzeň: Západočeská univerzita v Plzni, 2014, pp. 39–47. ISBN 978-80-261-0362-2 p. 40

[7] For more details, see e.g.:

World Internet Users and 2015 Population Stats. [online]. [cit.09/08/2015]. Available from: http://www.internetworldstats.com/stats.htm

Digital, Social & Mobile Worldwide in 2015. [online]. [cit.09/08/2015]. Available from: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

Největší sociální sítě na světě? Facebook je sice jednička, ale... [online]. [cit.10/08/2015]. Available from: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

Current World Population. [online]. [cit.10/08/2015]. Available from: http://www.worldometers.info/world-population/

[8] *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions)* [online]. [cit.10/08/2015]. Available from: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

7.1. Digital footprint

The mentioned threats, or rather risks, very often consist of leaving digital footprints in cyberspace. Digital footprints, based on whether or not they can be influenced by a user, can generally be **divided into footprints that can be influenced (active) and that cannot (passive)**.

Division of digital footprints:

- **Passive digital footprint**
  - Information from a computer system;
  - connection to computer networks, in particular the Internet;
  - use of provided services, etc.
- **Active digital footprint**
  - conscious use of services;
  - voluntary disclosure of information;
  - blogs, forums;
  - social media;
  - email;
  - data storage;
  - cloud services, etc.

In the following section, I will focus on some aspects of individual digital footprints and information contained in them. The purpose is to warn users that their actions in the environment of information and communication systems are not as anonymous as they may think.

In the world of ICT, one rule applies: **whenever you upload, transfer, mediate or put anything into cyberspace, it stays there "forever"**. There will always be a copy (created based on the functionality of a computer system or a copy stored by another user) of your data. And even if you subsequently delete the data, they will not be actually, permanently and irreversibly deleted. It is therefore appropriate to pay attention to your digital footprint and the information or data that we leave behind in the cyberspace environment.

7.1.1 Passive digital footprint

Passive footprints most often arise from the interaction of one computer system with another computer system or from the functionality of a computer system (and associated software). Examples of such traces may be information from the operating system (such as Windows error messages or system information), or other information and data that are stored based on the system's functionality without having to be transmitted (such as a computer system that has never been connected to any network or other computer system).[1] To say completely uncompromisingly that these footprints cannot be influenced would not be entirely correct. If a user is sufficiently experienced, he/she is able to change, mask or suppress a number of "passive" digital footprints (e.g. by a simple anonymous mode of the web browser that turns off cookies). However, a user's movement on the Internet can be monitored in a variety of ways.

IP address

A computer system's connection to the Internet is a typical example of a relatively passive footprint. An IP address or MAC address that are passed along with other ISP information. An IP address is not anonymous by default, and the computer system uses it as one of the identifiers when communicating with other computer systems. IP addresses are assigned hierarchically, with **ICANN** playing a dominant role, dividing the real world into regions managed by regional internet registrars (**RIR** – **Regional Internet Registry**). These registrars have been assigned a range of IP addresses from ICANN, which they assign to LIRs within their region. Regional registrars are divided into the following five territories:

1. "Euro-Asian" region – RIPE NCC: https://www.ripe.net/
2. "Asia Pacific" region – APNIC: https://www.apnic.net/
3. "North American" region – ARIN: https://www.arin.net/
4. "South America" region – LACNIC: http://www.lacnic.net/
5. "African" region – AFRINIC: http://www.afrinic.net/

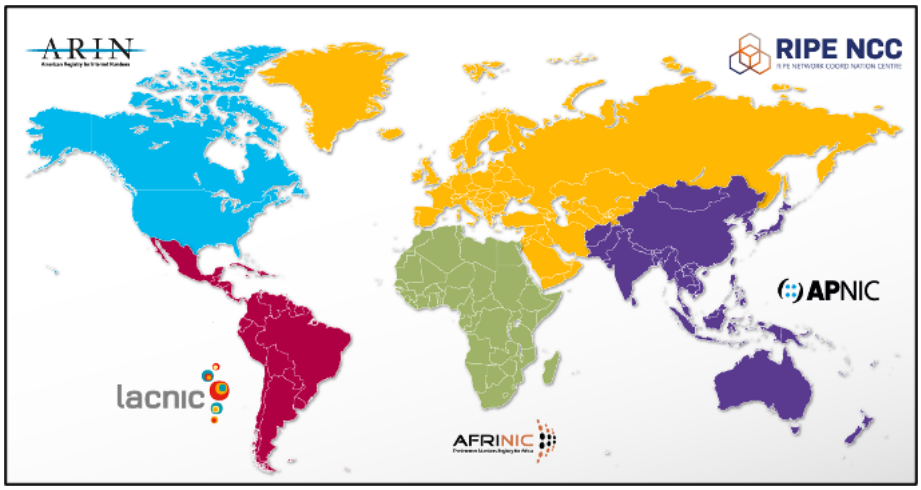


Figure – Division of the world between RIRs

The regional registrars[2] operate the *Whois* service on their websites, which is a name for a database in which data on IP address holders are registered. These databases contain a wide range of information that enables the identification, for example, of a range of public IP addresses used, contact information, abuse contact[3], hierarchically superior connection provider, etc. To determine an "owner" (operator, provider) of a particular IP address, it is often possible to use these freely available databases.[4]

Regional registrars further divide the assigned IP ranges between local internet registrars (**Local Internet Registry – LIR**). A local registrar is usually an ISP (in the Czech Republic, a provider of information society services, specifically a connection provider, whether public or non-public). This registrar can then provide its range of IP addresses to, for example, parts of its organisation or other entities.

```
Responsible organisation: Policejni akademie CR v Praze
Abuse contact info: abuse@polac.cz

inetnum:          195.113.149.160 - 195.113.149.175
organisation:     ORG-PACV1-RIPE
org-name:         Policejni akademie CR v Praze
org-type:         OTHER
address:          Policejni akademie CR v Praze
address:          Lhotecka 559/7
address:          P. O. Box 54
address:          Praha 4
address:          143 01
address:          The Czech Republic
phone:            +420 974 828 551
e-mail:           polac@polac.cz
abuse-mailbox:    abuse@polac.cz

route:            195.113.0.0/16
descr:            CESNET-TCZ
origin:           AS2852
mnt-by:           AS2852-MNT
remarks:          Please report abuse -> abuse@cesnet.cz
created:          1970-01-01T00:00:00Z
last-modified:    2006-06-26T14:36:38Z
source:           RIPE
```

Figure – Information extracted from the RIR database

The abbreviated selection from the RIR database shows the LIR (in this case the CESNET, z. s. p. o. association, using the IP address range: 195.113.0.0/16) and an organisation to which CESNET has assigned part of the public addresses [Police Academy of the Czech Republic with the IP address range 195.113.149.160 – 195.113.149.175. The police academy can again distribute these addresses among other parts of the organisation (e.g. faculties, laboratories, or other sub-networks it manages)]. Depending on the IP address and the exact time, it is possible to determine a specific computer system based on the hierarchical address assignment. Information about a connection of an end computer system (source) to a target computer system (e.g. computer connection to the Internet and displaying the required web page) is stored by individual ISPs throughout the path between the source and the target.

Due to the strict rules defining the management of IP addresses and publicly accessible RIR databases that contain information about the holders of individual address blocks, it is possible to find out very quickly which network a certain IP address belongs to and who operates the network. Thanks to logging information from network traffic, the operator of a given network is then able to identify who (or which computer system) used a particular IP address at a particular time. This determination is a very important source of information in handling security incidents (cyberattacks) and in searching for their source (originator).

Email

Email, as one of the most frequently used services in the Internet environment, is definitely not an anonymous service. A message that is sent from a source to a destination (recipient) typically contains a range of different types of information that can identify both the service provider (email) and the connection provider of the device from which the email was sent. This information is not displayed in the body of the message (i.e. the text we send to a specific person) but in the source code (header) of the message. From this source code, it is possible to find out the path via servers, real sender, source computer name, computer name, time of sending message (including time zone) used by operating system, mail client, etc. Below is an example of a header of forwarded[5] fraudulent email with potentially interesting information marked.

```
From - Wed Aug 19 15:14:52 2015
X-Account-Key: account1
X-UIDL: 7
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Received: from relay.fit.cvut.cz (relay.fit.cvut.cz [147.32.232.237])
    by email-smtpd5.ko.seznam.cz (Seznam SMTPD 1.3.4) with ESMTP;
    Wed, 19 Aug 2015 15:14:16 +0200 (CEST)
Received: from imap.fit.cvut.cz (imap.fit.cvut.cz [IPv6:2001:718:2:2901:0:0:0:238])
    by relay.fit.cvut.cz (8.15.2/8.15.2) with ESMTP id t7JDE1Mm072888
    for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
Received: from PCP[redacted] (cust-178.17.4.174.uvt.cz [178.17.4.174] (may be forged))
        (authenticated bits=0 as user ko[redacted])
        by imap.fit.cvut.cz (8.15.2/8.15.2) with ESMTPSA id t7JDE139012575
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
        for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
X-Authentication-Warning: imap.fit.cvut.cz: Host cust-178.17.4.174.uvt.cz [178.17.4.
From: "JUdr. Jan Kolouch, Ph.D." <jan.kolouch@fit.cvut.cz>
To: <kyber.test@seznam.cz>
References: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
In-Reply-To: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
Subject: =?UTF-8?Q?FW:_Chci=2C_aby_partner_s_v=C3=A1mi_na_?=
    =?UTF-8?Q?tomto_projektu?=
Date: Wed, 19 Aug 2015 15:14:15 +0200
Message-ID: <006901d0da80$f3599db0$da0cd910$@fit.cvut.cz>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_006A_01D0DA91.B6E2BBD0"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQDP5b3kQbONWI2VUUpIa1oprzeNE6AVNk1w
Content-Language: cs
X-FIT-MailScanner-ID: t7JDE1Mm072888
X-FIT-MailScanner: Found to be clean
X-FIT-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-0.381, required 7, autolearn=not spam, RP_MATCHES_RCVD -0.38)
X-FIT-MailScanner-From: jan.kolouch@fit.cvut.cz
X-FIT-MailScanner-Watermark: 1440594843.20583@MBoaO3F9jzMModBIjGdzYg
X-Spam-Status: No
```

Figure – View information from the header of an email message

Web browser

A web browser is another application that by default passes information about a user and his/her computer system to the computer system (server) of a visited site. Within a query from a client, this server then finds out, for example, the referrer (which is the page from which the user comes), the web browser used and operating system (including the exact version), cookies, flash cookies, history, cache, etc.

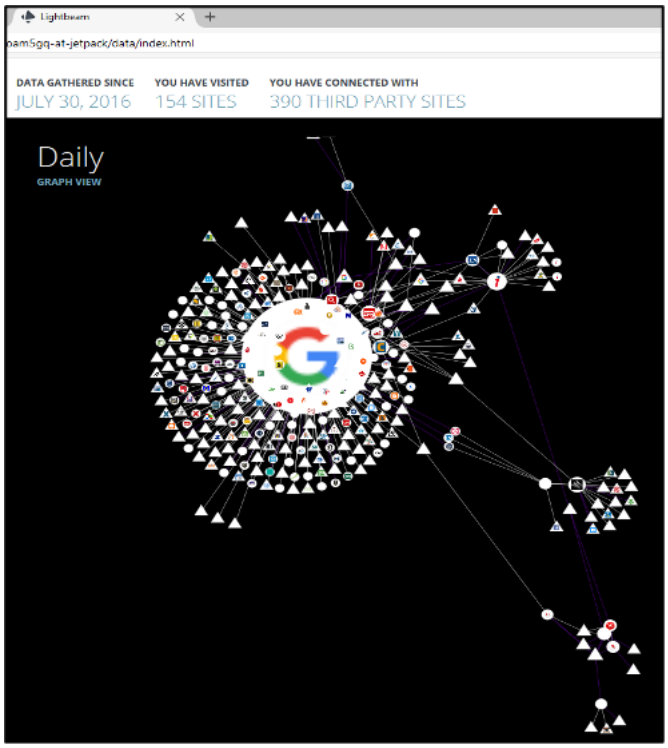
In addition to the IP address, these are, among other things, cookies[6] that help create a "fingerprint" of the user's computer system (computer, smartphone, etc.). This fingerprint allows the specification of a specific computer system[7], even if the user uses a different web browser, or deletes cookies, logs in from a different IP address, etc.

One of the many ways of creating "fingerprinting" currently in use is canvas fingerprinting.[8] Canvas fingerprinting works by having a visited webserver instruct the user's web browser to "draw a hidden image." This image is unique to any web browser and computer system. The drawn image is then converted into an ID code, which is stored on the web server in case the user visits it again.[9]

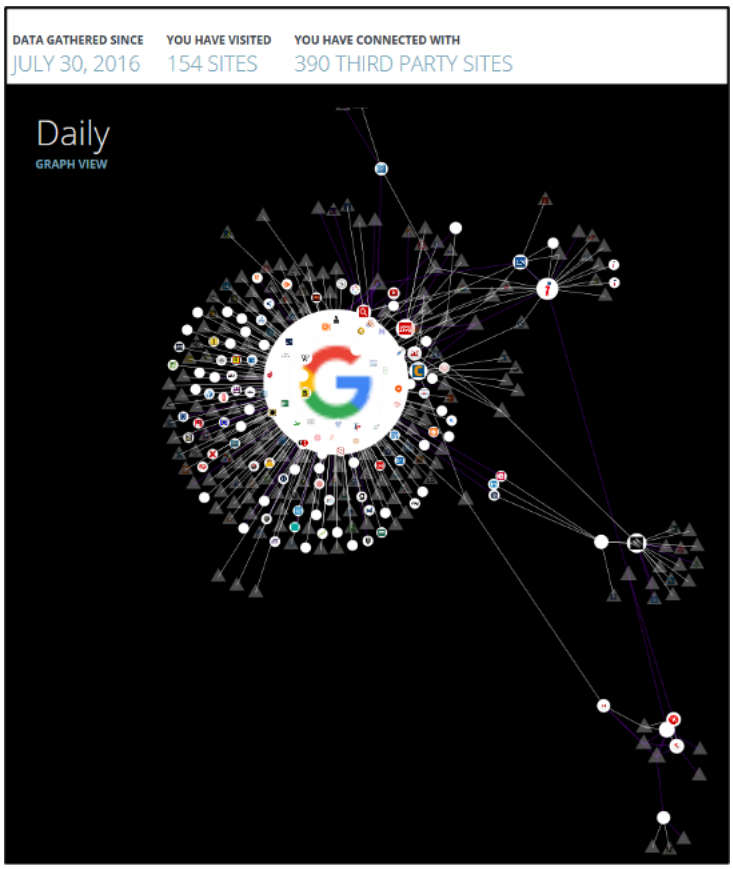
Figure – Example of Canvas Fingerprinting

In addition to fingerprinting, it is also interesting to monitor the transfer of information to third parties (both entities and services that can further use user information) in a web browser. By default, this transfer takes place on the basis of the Terms of Service agreed to with an ISP. For example, each end user can use the Light Beam application[10], which displays all the pages with which a user (often unknowingly) communicates on the website. (Data are passed on to third parties.) Passing information about users to third parties is certainly not exceptional. On the contrary, in the digital world it is a matter of course and a "necessary prerequisite" for the functioning of many ISPs.

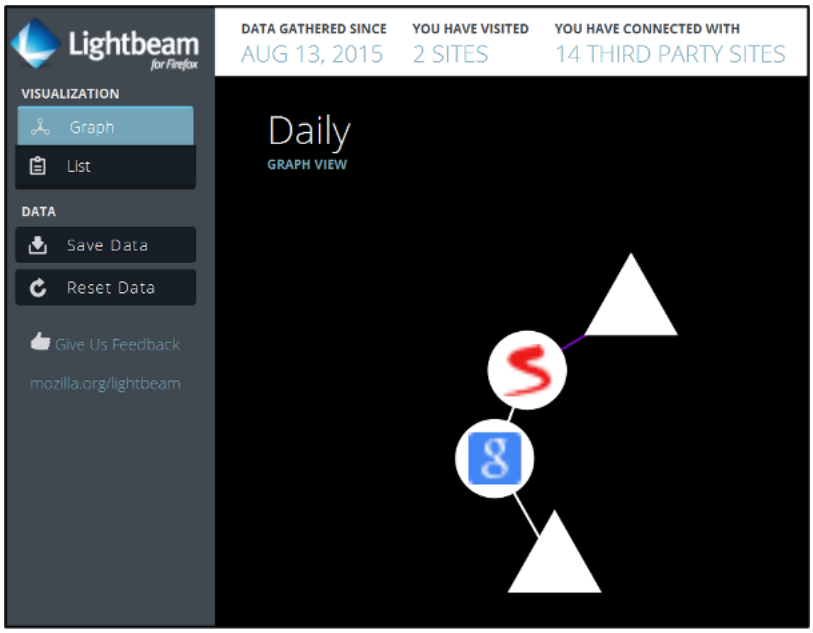
1. The first slide shows Firefox activity for the period from 30 July 2016 to 4 August 2016. During that period, 154 pages were visited, and 390 **third-party pages** were linked.



2. The second print screen displays the same map but filters out third-party pages that are represented by triangles.



3. The last print screen displays the LightBeam application after cleaning and displaying the following pages: www.seznam.cz; www.google.com;



Other applications

In the following part of the text, I will partially focus on smart devices (smartphones, tablets, etc.) and applications associated with "smart devices" activities. I purposefully choose these devices because they are computer systems in which users install probably the largest number of programs (very often unverified, only recommended by a "friend"). It is these devices that, due to contractual terms and conditions among other things, do not have to be under the full control of the user, administrator, etc., that pose a security risk for both the end user and the company (organisation).

The previously mentioned statistical survey[11] shows that on average we spend on the Internet: 4.4 hours (access via computer in the form of a desktop PC or laptop, etc.) and 2.7 hours (access via mobile devices) per day. In the case of a computer, the security of the device is usually ensured, but mobile devices (smartphones, tablets, etc.) usually do not have policies set for possible software installation (either from trusted or untrustworthy sources) and often lack basic protection in the form of an antivirus program.[12]

An end user has the option to primarily install software on the Android OS device, and this software will pass on (to other entities) and store information about its activities, including the storage and transfer of the content of the transmitted information. The Play Store service, which is provided by Google within the Android OS, allows any developer to set rules for what the application should collect, for example, and where to send this data.

Personally, I believe that it is not a mistake to allow developers and application developers to obtain sufficient information about their applications, their functionality, etc. If we regulate the collection of this information, then we will undoubtedly regulate and hamper possible progress and subsequent development of these and other applications. On the other hand, there are attackers who, because Play Store does not authenticate and scan applications, can offer malware-infected applications that, when installed on an end-computer system, can take control of an end-user smartphone, for example.

Identification of a computer system based on information from its components

One of the unique, yet in some circumstances changeable, computer system identifiers is a MAC address, which is tightly bound to a computer system's network card. However, a network card is not the only hardware component that is able to pass on a unique computer system identifier to another computer system.

Researchers at Princeton University have found that a computer system can be identified, for example, by the system's battery information, and web browsers are an essential part of transmitting this information.[13]

In practice, a procedure is used that uses the capabilities of HTML5. This standard includes a function that allows websites (or web servers) to identify a battery level of the computer system that accesses them. (Information is passed on what percentage of the battery remains and how long it approximately takes to discharge or charge.) The idea of web server owners is that a user who is running low on battery will be shown a cost-effective version of a web page. The two scripts described by Princeton University researchers are already actually using battery data, while also collecting additional information – such as an IP address or a canvas fingerprinting. Such combinations can already provide a very accurate identification of a computer system.[14]

7.1.2 Active digital footprint

An active digital footprint that can be influenced represents all information that a user voluntarily transfers about himself/herself to another person (whether natural or legal, or even ISP). Transferring may include a number of activities, such as sending an email, adding a post to a discussion, forum, publishing any media (photo, video, audio, etc.) on social media, etc. The term also includes a registration and use of all conceivable services within cyberspace [e.g. operating systems, emails (including freemail), social media, dating, P2P networks, chats, blogs, bulletin boards, websites, cloud services, data storages, etc.].

Active digital footprints are footprints over which users can have relative control, and it is only up to them what information about themselves they intend to make available to others. However, it is necessary to draw attention to the already mentioned premise: any data or information entered into cyberspace will remain in cyberspace.

Theoretically, it would be possible to define a category of **hypothetically active footprints**, which is in a way an oxymoron. However, this category includes certain facts that a user can theoretically influence, i.e. is able to influence them but usually does not because it would in effect significantly limit his/her functioning in the digital world. These footprints could include, for example, the use of the services of the largest ISPs (Microsoft, Apple, Google, Facebook, etc.), for which the use of the service is subject to the agreement of the Terms of Service (EULA) that in turn allow these ISPs to obtain a significant amount of information. Furthermore, it is possible to include in these footprints also footprints that arose, for example, by correlating active and passive footprints; information that other users disclose about us; data that are mirrored; EXIF data[15]

---

[1] This means mainly information that is logged and archived about the activities of users in places to which a user does not have access and does not have them under control [e.g. the user is not able to delete logs proving his/her activity (e.g. access, sending email, etc.) on the mail server]. On their own computer, users can influence the stored data and information. They are entitled to delete (e.g. history, e-mails, etc.), edit, etc.

[2] *Regional internet registries.* [online]. [cit.04/08/2015]. Available from: https://www.nro.net/about-the-nro/regional-internet-registries

[3] This is a contact that a user can get in touch with if he/she is harmed by a given IP address or range of addresses (for example, there is a cyberattack in the form of spam, phishing, etc.). It is the contact closest to the source of the attack.

[4] However, this is not the only database. There are a number of services that offer the same information. I will also mention other databases as an example: http://whois.domaintools.com/; https://www.whois.net/; http://www.nic.cz/whois/; https://whois.smartweb.cz/, etc.

[5] the email was forwarded from: jan.kolouch@fit.cvut.cz to: kyber.test@seznam.cz

[6] In HTTP, the term cookie refers to a small amount of data that a visited webserver (a visited web page) sends to a web browser, which then stores it on the user's computer. This data are then sent back to the web server each time you visit the same server.

[7] If a user wants to learn more about what a web browser reveals about their activity, I recommend the following URLs: http://panopticlick.eff.org, http://browserspy.dk/, http://samy.pl/evercookie.

[8] ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit.10/06/2016]. Available from: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[9] Example of Canvas fingerprinting. A test showing the fingerprint of your web browser can be tested within the article ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit.10/06/2016]. Available from: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[10] The application enables graphical display of interconnection of individual services and transfer of information to third parties. This is a Firefox web browser add-on that is available at: https://www.mozilla.org/en-US/lightbeam/.

[11] *Digital, Social & Mobile Worldwide in 2015.* [online]. [cit.09/08/2015]. Available from: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

[12] It should be noted that, for example, a report issued by Kaspersky Lab shows that there are more than 340,000 types of malware intended primarily for mobile devices. Kaspersky Lab further states that 99% of this malware targets Android devices. It should be noted that this targeting is perfectly understandable as the variability of individual devices and versions of the Android OS is considerable. (Some reports state that more than 24,000 types of different devices use the Android OS.)

For more details, see e.g.:

The very first mobile malware: how Kaspersky Lab discovered Cabir. [online]. [cit.01/08/2016]. Available from: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

See also: *Interesting Statistics On Mobile Strategies for Digital Transformations.* [online]. [cit.15/07/2016]. Available from: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

The fragmentation of Android has new records: 24 000 different devices. [online]. [cit.15/07/2016]. Available from: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

[13] For more details see ENGLEHARDT, Steven and Ardvin NARAYANAN. *Online tracking: A 1-million-site measurement and analysis.* [online]. [cit.05/08/2016]. Available from: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[14] For more details see VOŽENÍLEK, David. *Promazání „sušenek" nepomůže, na internetu vás prozradí i baterie.* [online]. [cit.04/08/2016]. Available from: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

[15] EXIF – *Exchangeable image file format*. It is a format of metadata that is embedded in digital photos by digital cameras. These metadata include, for example:

- Camera brand and model.
- Date and time a picture was taken.
- GPS position.
- Information about the author (the person who registered the camera).
- Camera settings.

- Preview of an image, etc.

7.2. Terms of Service (EULA)

In the next part of this chapter, I will try to describe what information about users is collected by default by the largest ISPs.[1] I specifically chose Google Inc. because I believe there are a tiny number of users who would never use one of Google's products (such as OS Android, the search engine on www.google.com, Gmail, Google Chrome, etc.).[2] My goal is by no means to "attack" Google Inc. or other companies (including their products). The purpose is to present the possible security risks that are associated with the use of certain services provided and with the acceptance of the Terms of Service (EULA – End Users Licence Agreement), to which the use of these services is bound.

The Terms of Service enabling the use of a service of a given service provider are, in essence, nothing more than a generally unilaterally established definition of rights and obligations by the service provider (ISP). However, a user is not limited in any way in his/her rights as he/she has the option of not using such unilaterally set terms of service. In the case of consent to the use of such services, it is generally possible to state that private law standards will be applied primarily.

The question is whether a user is really aware of what Terms of Service he/she has agreed to, when they become binding on him/her and what possible (legal) interference with his/her fundamental human rights and freedoms is such consent. Another important fact is that the service provided in this way may affect the rights and legitimate interests (e.g. IT security, trustworthiness of data, etc.) of third parties (e.g. employers, etc.) who have not explicitly agreed to use the service.

Theoretically, it can be stated that a private law contract with this company for the entire period of its existence has been entered into by almost 3 billion users.[3] The sad fact remains that a very small percentage of users are willing to read the Terms of Service relating to a service provided.[4]

Excerpts from Google Inc. Terms of Service[5]

Google explicitly states that if any user begins to use any Google services, they agree to the applicable terms of service. It further clearly defines the relationship between a user and itself, as a service provider, in the event that the user is obliged to accept other terms of service. This relationship is expressed as follows: *"Our range of services is wide, and some may be subject to additional conditions or requirements (including age restrictions).* ***Additional terms*** *will be available along with applicable services.* ***If you use these services, the additional terms of service become part of the contractual arrangements between the two parties."***

In the introduction to the Terms of Service, Google states that: *"****We may review content***[6] ***to determine whether it is legal and in compliance with our policies*** *and if we believe that it violates our policies or laws, we may remove or prevent the content from appearing. Please note that the* ***above does not mean that we review content****."*

From the point of view of security, in my opinion, an essential part of the Terms of Service is the section dealing with the **protection of personal data and copyright**.[7] In this section, Google defines what information it collects about users and how it handles it. The following information is crucial from a security and "anonymity" perspective. I believe that declaring that the following information is collected *"so that we can provide a better service to all our users – from identifying simple things like the language you speak to more complex things, such as ads that will be most useful to you, the people you are most interested in on the web or which YouTube videos you might like,"* may be commendable but at least startling. The comparison with the already mentioned *Minority Report* in the form of advertising targeting is more than obvious after such a statement. Furthermore, Manfred Spitzer and *Digital Dementia* again spring to mind because, over time, it is no longer me who decides what I will watch or what I will search for (or all the relevant responses may not and are not offered to me).

Google collects user information in basically two ways:

Information disclosed by a user. Typically these are:

Name, email address, phone number or credit card.

Information obtained through the use of Google services. It involves the collecting of information about the services that a user uses, including how they are used (*"for example, when you watch a video on YouTube, visit websites that use our advertising services or watch or respond to our ads and content"*). According to Google, these are:

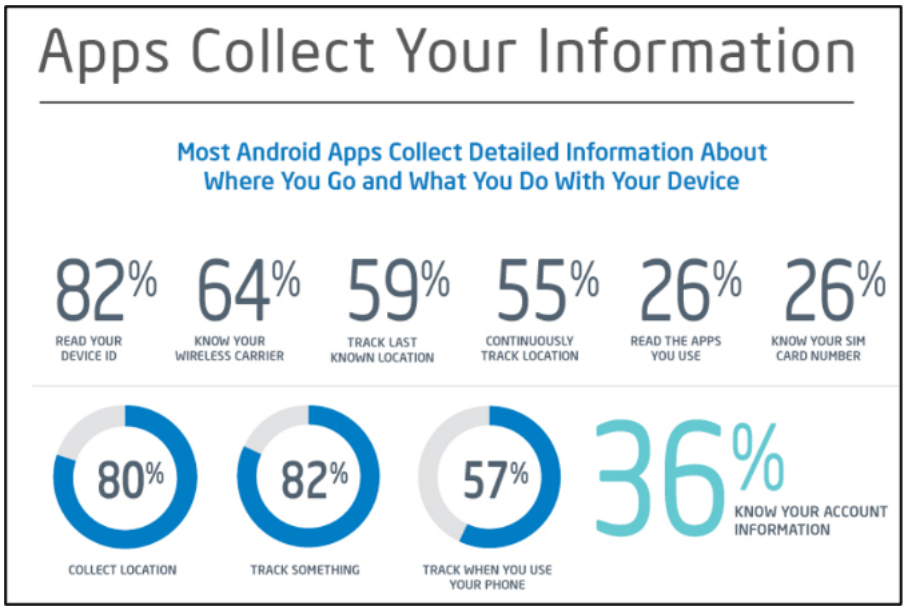
- **Device information** *(e.g., hardware model, operating system version, unique device identifiers*[8] *and mobile network information, including the phone number).* Google reserves the right to assign your device identifiers or your phone number to your Google user account
- ***Protocol information:***
  - *details of how a user used a Google service,*
  - *information from the call protocol (e.g. phone number, caller number, divert numbers, time and date of calls, call duration, SMS routing data and call types),*
  - *Internet Protocol address*
  - *information about device events (e.g., failure, system activity, hardware settings, browser type, browser language, date and time of your request, or referring URL),*
  - *cookies, which can be unique identifiers of your browser or Google account.*
- ***Location information.*** Google may collect and further process information about the actual location of its user. Google can determine your location using a variety of technologies, such as IP address, GPS and other sensors that can provide Google with information about nearby devices, Wi-Fi hotspots and mobile network transmitters.
- ***Unique application numbers.*** **Typically, this is a licence number and type (version) of an applicable installed software product. The Terms of Service** do not imply that unique application numbers are recorded only from devices whose primary operating system is Android. It can therefore be concluded that, if Google services are used, then information about unique application numbers is also collected from other operating systems (iOS, Linux, Windows, etc.).
- ***Local storage.*** **Under the Terms of Service, Google may: "***collect and store information (including personal information) in your device's local storage."* In this case, too, the same conclusion can be reached as for unique application numbers.

In my opinion, the problem is also the fact that nowhere in the General Terms of Service is it precisely defined[9] what location and especially what security will be used by Google. Thus, it is theoretically possible to use the storage as a whole. It is possible to obtain information about files (e.g. their names, location, and even absurdly the hash, which will then be compared, for example, with the database of another service where data are stored – e.g. DropBox, OneDrive, etc.).

In my opinion, the possibility of misuse of such stored data by an attacker is also a threat to users. Information (which is typically packaged on cookies, etc.) stored in a user's local storage can also become an appealing target for an attacker because it is from this information that it is possible to determine, for example, patterns of user behaviour.

- ***Cookies and similar technologies.*** *"When you visit a Google service, we and* ***our partners*** *use a variety of technologies to collect and store information. This may include, but is not limited to, the use of cookies or similar technologies to identify your browser or device. We use these technologies to* ***collect and store information even when you use services we offer to our partners****, such as advertising services or Google features that may appear on other websites."*

What information do apps running on Android OS collect:



[10]

Google may continue to use this information based on the agreed Terms of Service. Among other things, Google is authorised to analyse content (including emails) using automated systems. It is also entitled to combine personal data from one service with information and personal data from another service (using Google).

Handling of the mentioned information then means its sharing, either with the user's consent or without this consent.[11] The Service of Terms enable **sharing for external processing and for legal reasons**:

"We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

"We share personal information with companies, organizations or individuals *outside of Google* ***if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:***

- *meet any applicable law, regulation, legal process, or enforceable governmental request,*
- *enforce the applicable Terms of Service, including investigation of potential violations,*
- *detect, prevent, or otherwise address fraud, security, or technical issues,*
- *protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law."*

However, from a security and anonymity perspective, I consider the following section of the Terms of Service that deals with user content on the services provided by Google to be probably the most problematic:

"By ***uploading, submitting, storing or receiving content to or through our Services, you grant Google*** *(and its partners)* ***a worldwide license to use, host, store, reproduce, modify, create derivative works*** *(for example, those that are of the translation, adaptation or other changes that we make so that your content is better adapted to our Services)*[12]***, communicate, publish, perform or publicly display and distribute of said content****..... This license will remain in effect even when you stop using our Services (e.g. business listing added to Google Maps).* ***Some services allow you to access or remove content that you have submitted to the service....*** *"*

Personally, I believe that at least in this part of the Terms of Service, the imaginary limit defining the adequacy of the information collected about individual users has been exceeded. This section is, in fact, about a "legal use" of any content that Google "interacts with". Personally, I believe that it is the interference with the content of, for example, transmitted information that should be a last possible resort, and not a kind of "matter of course" enshrined in the contract.

[1] For this part of the text, the theses that were used were published in the article: KOLOUCH, Jan. Pseudoanonymita – bezpečnostní riziko pro uživatele Internetu. *DSM – data security management* [online]. 2015. Vol. 19, No. 3, pp. 24–29 ISSN 1211-8737. Available from: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

[2] It should be noted that the following companies have very similar Terms of Service (enabling them to provide information to a comparable extent): Microsoft, Apple, Facebook, etc.

[3] According to the article SMITH, Craig. *By the Numbers: 100 Amazing Google Search Statistics and Facts.* [online]. [cit. 04/08/2016]. Available from: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/, there are 100 billion searches per month through Google search.

[4] And according to one participant in the Security 2015 conference, a normal person would spend about 10–20 years of their life reading all the constantly changing Terms of Service.

[5] Hereinafter referred to as the Google. All excerpts from the Terms of Service were drawn from: *Smluvní podmínky společnosti Google.* [online]. [cit.14/06/2016]. Available from: https://www.google.cz/intl/cs/policies/terms/regional.html

[6] Content means content (data) that does not belong to Google. The entity that published it is responsible for the content.

[7] Specifically then *Zásady ochrany osobních údajů.* [online]. [cit.14/06/2016]. Available from: https://www.google.cz/intl/cs/policies/privacy/

[8] Google definition. *Unique device identifier.* [online]. [cit.14/06/2016]. Available from: https://www.google.cz/intl/cs/policies/privacy/key-terms/#toc-terms-unique-device-id

"A unique device identifier (sometimes called a universally unique ID or UUID) is a string of characters that is encoded into the device by the manufacturer and is used to uniquely identify the device (for example, the IMEI of a mobile phone). Different device identifiers differ depending on whether they are permanent, whether users can reset them and how they can be accessed. A given device can contain several different unique identifiers. Unique device identifiers can be used for a variety of purposes, such as security, fraud detection, synchronisation of services such as inbox, or to store user settings and provide relevant ads."

[9] According to the required function, it will be mainly about storing information and data in the folder of the given browser (web browser), but according to the contractual conditions, it can also be applications other than a web browser.

[10] CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cit.10/04/2015]. Available from: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

[11] E.g. with domain administrators; for external processing or for legal reasons.

[12] It is understandable that Google attempts, for example, to translate works, pages or other content so that even a user who does not know the original language of the work can read it. However, in absurd cases, it is possible to imagine the publication of your private love poem that you sent using one of the Google services, your photo, your brilliant idea for a perpetual-motion machine, etc.

7.3. SUMMARY / MAIN OUTPUTS FROM THE CHAPTER

ℹ️

- All applications, whether used in any computer system, web services and especially social media, collect a considerable amount of information about their users. They do not need this information for their operation, but it allows both the ISP in question to provide a service “for free” and to “target” or modify the services it offers. Information that is not necessary by default for the direct functionality of individual services includes, for example, information of a personal nature (name, surname, email address, telephone number, address, etc.), sensitive nature (e.g. information about the computer operating system used, versions individual applications, cookies, etc.), location data (GPS coordinates, information about Wi-Fi, GPRS, etc.), operational data, etc.
- Digital footprints, based on whether or not they can be influenced by a user, can generally be divided into footprints that can be influenced (active) and those that cannot (passive).
- In the world of ICT, one rule applies: whenever you upload, transfer, mediate or put anything into cyberspace, it stays there “forever”. Passive footprints most often arise from the interaction of one computer system with another computer system or from the functionality of a computer system (and associated software). Examples of such traces may be information from the operating system (such as Windows error messages or system information), or other information and data that are stored based on the system’s functionality without having to be transmitted (such as a computer system that has never been connected to any network or other computer system). To say completely uncompromisingly that these footprints cannot be influenced would not be entirely correct. If a user is sufficiently experienced, he/she is able to change, mask or suppress a number of “passive” digital footprints (e.g. by a simple anonymous mode of the web browser that turns off cookies). However, a user’s movement on the Internet can be monitored in a variety of ways.
- An active digital footprint that can be influenced represents all information that a user voluntarily transfers about himself/herself to another person (whether natural or legal, or even ISP). Transferring may include a number of activities, such as sending an email, adding a post to a discussion, forum, publishing any media (photo, video, audio, etc.) on social media, etc. The term also includes a registration and use of all conceivable services within cyberspace [e.g. operating systems, emails (including freemail), social media, dating, P2P networks, chats, blogs, bulletin boards, websites, cloud services, data storages , etc.].

🗝️

KEY WORDS TO REMEMBER

- Digital footprint
- Passive digital footprint
- Active digital footprint
- EULA

❓

KNOWLEDGE CHECK QUESTIONS

- Define the term “digital footprint”.
- How do digital footprints differ from each other?
- What elements does a passive digital footprint consist of?
- Who is LIR?
- What information about a user does an IP address carry?
- What is the EULA?

8. Conclusion

With the use of information and communication technologies and the ever-increasing volume of data published by users, there have necessarily been requests for the suppression or deletion of data that are out of date or that in some way harm a user.

The vision that the digital world and its users will become anonymous is, in my view, a utopia. The various possibilities of anonymisation in the form of, for example, TOR network services[1], etc. will not change anything in this statement as there will always be interactions with the real world. Moreover, there will always be users in the digital world who are fallible and who make mistakes no matter how well they try to conceal information about their activities. It is also a utopia to think that technology will forget. Data will continue to be collected about users. What will happen will be another technical setting of who will see the data and who will not.

Undoubtedly, the interconnection of individual offered services and the possibility of passing information about users to third parties, as well as the **Internet of Things (IoT)**, contribute to the "deanonymisation" of users.

For example, Facebook came up with an interesting solution for "deanonymisation" of users, developing the **DeepFace** method, which is based on the creation of a 3D model of the face based on defined starting points in a photograph.[2] Based on this method, it is also possible to identify persons who do not have a Facebook account and have only been marked (identified) as a specific person. The DeepFace method is intentionally mentioned here as the possibility of using this method is enshrined in the Facebook Terms of Service and allows, even if a user does not wish to do so (e.g. does not intentionally mark himself/herself under a photo), his/her identification.

As for **IoT**, the intervention of new technologies and our "deanonymisation" is even more apparent. As an example, I will mention a "smart TV"[3], which during the actual installation will again offer the Terms of Service for approval and immediately afterwards "ask" about the possibility of connecting to the Internet. For example, a closer look at the Terms of Service may indicate that this TV is authorised to provide a record of confidential and in-person calls or activities that you "*make at it*", provided you use voice or motion control. As part of the Terms of Service, you will also be notified that the recorded data are passed on to the manufacturer and third parties. The only solution to prevent this information from being passed on is to turn off voice or motion recognition. The question is whether this is really the solution. Personally, I think that the solution would be to turn off or restrict the transfer of data, or to identify the entity with which I am willing to share this personal data.

As for the right to be forgotten, I can imagine a hypothetical situation where a user will request that the company that produced the television or other computer system with similar Terms of Service delete the call record, for example, from 1 March 2016. The court applies the right to "be forgotten" also in this case, but the question is who will actually guarantee the user that his data have been deleted from all data repositories.

Excerpt from Samsung EULA:

Please be aware that, if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

There is no anonymity on the Internet and certainly will not be in the near future. Users often, quite logically, justifiably intensively fight against the intervention of the state in their privacy, but on the other hand, they themselves offer this private information voluntarily and much more willingly to everyone around them (e.g. on social media, cloud services, etc.).

I do not think the gap between the real and digital world is so huge. Maybe that is why I often do not understand the thoughtless behaviour of users when it comes to the services offered by ISPs. Yes, as users, we will receive a service under the Terms of Service we enter into. The question is whether this deal is advantageous and whether the price we pay for this service is reasonable.

Personally, I am fully aware of the fact that my freedom, including a degree of "anonymity" on the Internet, is already a utopia. I believe that in the near future, thanks to IoT and the ever-increasing interconnection of all "services", this utopia will be brought almost into a situation, not unlike the one in the *Minority Report*. On the other hand, I believe, or rather I want to believe, that I am still free and have the right to choose.

This right of my choice then at least lies in my decision whether, or what services I want to use and under what conditions. I think that users should become the real defining authority of the Internet, at least in the form that they show their will and try to gain their rights to the service provider because, in the case of state intervention in their privacy, in many cases they succeed.

After all, to evaluate how "aggressive" the service is, or how much it interferes with your privacy, can be found, for example, on the website: Terms of Service, Didn't Read: https://tosdr.org/. If nothing else (although it is possible to use the analogy of "Digital Dementia"), then at least checking the basic terms on this page can help users to be better informed in the issue.

We live in a time when information and communication technologies are already inextricably linked to every aspect of our being. A certain paradox is that we essentially do not have the opportunity to avoid this penetration and mutual interaction with ICT, which at the same time makes us more vulnerable.

Due to information and communication technologies and interconnected services, we create a reflection of our identity or personality in the virtual world.

Our digital "me" has all the prerequisites to be "much more durable" than our physical body. Information about our activities in cyberspace, our cyber personalities, accounts and digital footprints will live on after our death thanks to the archiving of data and information about us.

As the volume of data and information stored in individual ISPs grows, the issues of their effective security, transfer or deletion are increasingly being addressed, not only on the basis of a contract entered into between the service provider and the end user but also on the basis of emerging legislation.

States, organisations and individuals are increasingly aware that information and data represent significant potential, which is increasingly attacked by cyberattacks, whether with the aim of theft, damage, inaccessibility or deletion of data.

If we want to live in today's society and take advantage of its benefits, it is not possible to get rid of ICT, and it definitely does not make sense to stop using these technologies. It is necessary to start learning how to use these technologies and services and how to avoid, or at least eliminate, the consequences of cyberattacks.

In cyberspace, as in the real world, there is no single type of security or protection that can be universally applied to everyone. If we want to address security, we need to address it comprehensively, and we need to tailor it to each individual.

---

[1] Some cases of TOR network security breaches:

FBI Exploits Flash Vulnerability to Breach Tor Network Security. [online]. [cit.23/07/2016]. Available from: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/

Tor security advisory: "relay early" traffic confirmation attack. [online]. [cit.23/07/2016]. Available from:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

[2] For more details, see e.g.: *Facebook will soon be able to ID you in any photo.* [online]. [cit.09/08/2015]. Available from: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

[3] See also e.g. ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit.09/08/2015]. Available from: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

9. List of sources used

1. ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit.10/06/2016].

2. BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit.23/09/2014]. Available from: https://www.eff.org/cyberspace-independence.

3. CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cit.10/04/2015]. Available from: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

4. ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit.09/08/2015]. Available from: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

5. *CNN on pedophile sex in Second Life.* [online]. [cit.18/06/2009]. Available from: http://www.youtube.com/watch?v=AQM-SiiaipE

6. *Current World Population.* [online]. [cit.10/08/2015]. Available from: http://www.worldometers.info/world-population/

7. See also: *Interesting Statistics On Mobile Strategies for Digital Transformations.* [online]. [cit.15/07/2016]. Available from: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

8. *Data retention unconstitutional in its present form.* [online]. [cit.16/07/2016]. Available from: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

9. *Delokalizace právních vztahů na internetu* [online]. [cit.15/04/2012]. Available from: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

10. *Digital, Social & Mobile Worldwide in 2015.* [online]. [cit.09/08/2015]. Available from: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

11. ENGLEHARDT, Steven and Ardvin NARAYANAN. *Online tracking: A 1-million-site measurement and analysis.* [online]. [cit.05/08/2016]. Available from: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

12. *Facebook will soon be able to ID you in any photo.* [online]. [cit.09/08/2015]. Available from: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

13. *FBI Exploits Flash Vulnerability to Breach Tor Network Security.* [online]. [cit.23/07/2016]. Available from: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/

14. *First Amendment.* [online]. [cit.10/07/2016]. Available from: https://www.law.cornell.edu/constitution/first_amendment

15. *German Bundestag Passes New Data Retention Law.* [online]. [cit.16/07/2016]. Available from: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

16. GREENFIELD, David. *Integrovaná bezpečnost: Už nastal její čas?* [online]. [cit. 01/03/2018]. Available from: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

17. HAINES, Lester. *Online gamer stabbed over "stolen" cybersword.* [online]. [cit.03/10/2006]. Available from: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

18. http://news.bbc.co.uk/2/hi/technology/6638331.stm

19. http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html

20. HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Prague: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, pp. 101–102.

21. *Internet censorship.* [online]. [cit.10/08/2016]. Available from: http://www.deliveringdata.com/2010_10_01_archive.html

22. *Internet History of 1980s.* [online]. [cit. 07/06/2016]. Available from: http://www.computerhistory.org/internethistory/1980s/

23. *Internet, připojení k němu a možný rozvoj (Část 2 – Historie a vývoj Internetu).* [online]. [cit.10/02/2008]. Available from: http://www.internetprovsechny.cz/clanek.php?cid=163

24. JOHNSON, David R. and David POST. *The Rise of Law in Cyberspace.* [online]. [cit.10/07/2016]. Available from: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067

25. KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25/04/2018]. Available from: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

26. KOLOUCH, Jan and Andrea KROPÁČOVÁ. Liability for Own Device and Data and Applications Stored therein. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14).* [B.m.], c2014, pp. 321–324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

27. KOLOUCH, Jan and Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Prague: Police Academy of the Czech Republic in Prague, 2013, p. 65

28. KOLOUCH, Jan. *CyberCrime.* Prague: CZ.NIC, 2016, p. 78 et seq. and p. 109 et seq.

29. KOLOUCH, Jan. Pseudoanonymita – bezpečnostní riziko pro uživatele Internetu. *DSM – data security management* [online]. 2015. Vol. 19, No. 3, pp. 24–29 ISSN 1211-8737. Available from: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

30. *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions)* [online]. [cit.10/08/2015]. Available from: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

31. LESSIG, Lawrence. *Code v. 2. p.* 6 Available in full (Eng) [online]. [cit.13/03/2008]. Available from: http://pdf.codev2.cc/Lessig-Codev2.pdf

32. MAISNER, Martin and Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Prague: Wolters Kluwer, 2015. p. 85

33. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Prague: CZ.NIC, 2013. ISBN 978-80-904248-7-6 p. 25

34. *National legal challenges to the Data Retention Directive.* [online]. [cit.16/07/2016]. Available from: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html

35. *Největší sociální sítě na světě? Facebook je sice jednička, ale...* [online]. [cit.10/08/2015]. Available from: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

36. *PDCA cycle.* [online]. [cit. 06/07/2018]. Available from: https://www.creativesafetysupply.com/glossary/pdca-cycle/

37. PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10/11/2015]. Available from: http://www.earchiv.cz/b14/b0428001.php3

38. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 7

39. POŽÁR, Josef and Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Prague: AFCEA, 2011. ISBN 978-80-7251-364-2, p. 5, or: POŽÁR, Josef and Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 06/07/2018]. Available from: https://www.cybersecurity.cz/data/srib.pdf p. 1

40. REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, p. 218

41. *Regional internet registries.* [online]. [cit.04/08/2015]. Available from: https://www.nro.net/about-the-nro/regional-internet-registries

42. ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cit. 06/07/2018]. Available from: https://www.allaboutlean.com/pdca-variants/

43. ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10/11/2017]. Available from: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

44. SMEJKAL, Vladimír. *Internet a §§§.* 2nd updat. and ext. ed. Prague: Grada, 2001, p. 32

45. SMITH, Craig. *By the Numbers: 100 Amazing Google Search Statistics and Facts.* [online]. [cit. 04/08/2016]. Available from: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/

46. The Court of Justice of the European Union. Press release No. 54/14, dated 8 April 2014. Judgment in joined cases C-293/12 and C-594/12. [online]. [cited 15/07/2016]. Available from: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

47. SPITZER, Manfred. *Digitátlní demence.* Brno: Host, 2014. ISBN 978-80-7294-872-7

48. Opinion of Advocate General Pedro Cruz Villalón. Case C-293/12 and C-594/12. [online]. [cit.15/07/2016]. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

49. Opinion of the Advocate General SAUGMANDSGAARD ØE, from 19/07/2016. In joined cases C-203/15 and C-698/15. [online]. [cited 10/8/2016]. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

50. ŠTOČEK, Milan. *V Hitlerově duchu proti Hitlerovi.* [online]. [cit.10/07/2016]. Available from: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

51. *Surface Web, Deep Web, Dark Web – What's the Difference.* [online]. [cit. 20/07/2016]. Available from: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

52. *The dark Web explained.* [online]. [cit. 20/07/2016]. Available from: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html

53. *The fragmentation of Android has new records: 24 000 different devices.* [online]. [cit.15/07/2016]. Available from: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

54. *The very first mobile malware: how Kaspersky Lab discovered Cabir.* [online]. [cit.01/08/2016]. Available from: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

55. THOMAS, Douglas. *Criminality on the Electronic Frontier.* In Cybercrime. London: Routledge, 2003, p. 17 et seq.

56. *Tor security advisory: "relay early" traffic confirmation attack.* [online]. [cit.23/07/2016]. Available from:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

57. TRADOC. Cyberspace Operations: Concept Capability Plan 2016–2028. [online]. [cit. 18/02/2018], pp. 8–9 Available from: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

58. VOŽENÍLEK, David. *Promazání „sušenek“ nepomůže, na internetu vás prozradí i baterie.* [online]. [cit.04/08/2016]. Available from: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

59. *World Internet Users and 2015 Population Stats.* [online]. [cit.09/08/2015]. Available from: http://www.internetworldstats.com/stats.htm

60. *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají možnost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit.04/04/2014]. Available from: https://www.google.cz/intl/cs/policies/?fg=1