ANTI-SPAM LEGISLATION IN CONSIDERATION OF PERSONAL DATA PROTECTION AND OTHER LEGAL INSTRUMENTS[1]

Ján Matejka*

Abstract: *The contribution deals with the possibilities of legal protection from an undesirable phenomenon called spam or, more precisely, spamming, pursuant to the Czech and European laws. In particular, the legal forms of protection of personal data, privacy, and personal rights are described in detail along with unfair competition and the law of obligations in tort. Attention is also paid to effective means that fall outside direct legal regulation, in particular, the technological and Community forms of protection against spam and other issues relating to this phenomenon. The author thoroughly deals not only with the terminological problems but also, for example, with the issue of identification and proving of related legal facts, including the issue of governing law.*

Keywords: *Spam, Personal data protection, E-marketing, Computer privacy, unsolicited commercial communication*

1. SPAM CONCEPT AND ROOTS OF EXISTENCE

One of the current problems associated with the use of modern means of communication is a phenomenon called spam. The significance of this phenomenon is on the rise, despite the enhanced efficiency of a wide range of tools, whether legal or technological, aimed at its prevention.

No clear definition of the term 'spam' as such can be found anywhere and there is no unambiguous consensus as to its content either. By its nature, the term is broad in many respects, is unspecific and has considerably vague borders overlapping numerous spheres and technologies not restricted to the Internet environment. However, at a general level, it may be defined as an act consisting of the collective distribution of messages having a negative impact on the infrastructure of the network via which such distribution takes place (*quantitative criterion*) or, possibly, as an act which may be perceived by the addressee of such message as intrusive (*qualitative criterion*) due to its negligible informational value or obvious uselessness (ballast). Therefore, the stated definition criteria always emphasise, to a certain extent, both the widespread distribution of such messages and their evidently intrusive nature.

Spam or, more precisely, spamming constitutes conduct that is undesirable for various reasons, whether technological, moral or legal. From this perspective, spam is often the subject of legislative or application technological deliberations, differing from one another not only when it comes to their conclusions on the level of threat posed by such messaging but also with respect to the impact on the information society and a particular individual or, more precisely, the intended target of protection (for example, addressee of such message, etc.). Particularly from this perspective, the quantitative and qualitative criteria are

[1] The research reported in this article was supported by the Czech Science Foundation (GA ČR) under grant No. 16-26910S Biometric Data and Their Specific Legal Protection.

* JUDr. Ján Matejka, Ph.D., Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic

variously combined in practice and the legislators of individual states frequently use them as the basic definition criteria for various types of legal regulation of such undesirable conduct. The other criteria usually[2] comprise the following:

- purpose of distribution of a message (commercial, advertising, political, religious, charitable, and others);
- wrong or fraudulent nature of a message (in particular, phishing, malware, Trojan horse, and others);
- absence of certain technical elements of a message (for example, no indication of the actual sender, and others);
- localization of the sender, etc.

The legislations of individual states then work with these criteria further and apply various legal limitations to the individual segments of spam, usually across the entire legal order, that is, including private, administrative and criminal laws. These regulations usually have a clear objective and purpose (for example, protection of infrastructure or the addressee of a message, etc.). However, it is essential, in particular, to set transparent conditions of such distribution in the form of legislative limitations. For this reason, balancing the need for communicating or, more precisely, distributing (beneficial) information in the form of an unambiguous definition on one side and the need for sanctioning its undesirable forms on the other is often difficult.

Nevertheless, although there is no clear definition of spam, it is obvious that, in this respect, the basic elements include a) the specific nature of a message and its capability of negatively influencing the network infrastructure, b) collective nature of the distribution of the message and c) absence of moral or objective reasons for the distribution of the message.

Hence, at a general level, spam or spamming can be defined as the misuse of functioning distribution mechanisms originally established for purposes other than those for which they have been developed or are operated. Spamming is the collective distribution of unsolicited messages (containing both texts and also, for example, various attachments) which is initiated unilaterally, pursues solely unilateral interests, is foisted on other persons, often even despite their clear disagreement, and uses the collective method of funding, that is, makes others who have not initiated such activities and usually disagree with them bear the cost of unilaterally advantageous activities. In this respect, electronic spamming significantly differs from the distribution of unsolicited shipments by general mail (where all cost is borne solely by the initiator of such a campaign).

Due to the absence of a clear and, in particular, functional definition, spam rather contributes to constituting a popular and attractive tool of extraordinary market significance. The reasons are obvious and ensue already from the low-cost essence of most information society services typical of enabling easy communication with an almost unlimited number of addressees. Although the issue of spamming is usually connected only with e-mails, its

[2] For the definition elements or the etymology of spam see, for example, POLČÁK, R. *Právo na internetu: spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 107, or, possibly, PETERKA, J. *Z historie spammingu* [online]. 11 April 2009. Available at http://www.earchiv.cz/a801s600/a801s602.php3.

efficient use is not restricted to this service, but includes many other services, such as blogs, discussions, comments[3], social networks, telecommunication services, etc. It is not easy to arrive at unambiguous conclusions as to the efficiency of spam, although it is obvious that spam as a tool works, which is evidenced, alongside its existence as such, by numerous studies confirming the efficiency of spam at both theoretical (empirical) and practical levels[4].

2. DEFINITION OF SPAM IN THE EU AND NATIONAL LAW

While in the general sense of the word, spam is defined considerably heterogeneously, that is, has basically no unambiguous definition, its meaning in the legal sense of the word must be clear. For this reason, the legislation must be sufficiently defined; otherwise, it cannot be applied and enforced efficiently. Therefore, the absence of a clear definition would result in the possibility of releasing oneself from the impacts of such legislation with reference to the impreciseness of such legislation, which, thus, would become useless.

As already stated above, spamming has an overall negative impact on both the network infrastructure and its users. Thus, it is obvious that this issue is the subject of legal regulation. For such regulation to be efficient, it must stem from certain proportionality of rights where, on one side, there are the rights and freedoms of an individual (or interests of a state) which shall be limited by such regulation and the real threat to the technical, economic and social functioning of the information society which such regulation tries to prevent, on the other. Spam is then defined, in particular, from these perspectives, including issues of specific factual (for example, commercial but not religious spam) and formal (for example, e-mail but not SMS) extents where attention is paid, among other things, to issues relating to the legal presumption of consent (opt-in or opt-out) or the selected type of legal responsibility of the sender (subjective/objective).

One of the first steps made to deal with the issue of spam in the EU was the Directive of the European Parliament and the Council **2000/31/EC** of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on Electronic Commerce"). The key provision was Article 2 (f) which identified spam as a commercial communication defined as follows: *all forms of communication intended for direct or indirect support of goods or services or image of an undertaking, organization or person active in the sphere of trade, industry, or crafts or performing a regulated profession; the data stated below shall not, as such, constitute a form of commercial communication:*

- *purpose of distribution of a message (commercial, advertising, political, religious, charitable, and others);*

[3] For the issue of commentary spam and its solutions see PROKEŠ, J. *Člověk a počítač aneb svítání digitální kultury.* Tišnov: SURSUM 2000, p. 28.

[4] See, for example, FRIEDER, L., ZITTRAIN, J. *Spam Works: Evidence from Stock Touts and Corresponding Market Activity* (March 14, 2007). Berkman Centre Research Publication No. 2006-11; Harvard Public Law Working Paper number 135; Oxford Legal Studies Research Paper; available at http://papers.ssrn.com/sol3/papers.cfm?%20abstract-id=920553.

- *information enabling direct access to the activity of an undertaking, organization or person, in particular, a domain name or an e-mail address;*
- *communication relating to goods, services or image of an undertaking, organization or person obtained independently and, in particular, provided without financial counter-performance."*

The motives leading to the adoption of this Directive were declared within the EU in a manner such that sending of unsolicited commercial communications by electronic mail was disadvantageous for consumers and information society service providers and capable of intervening in the proper functioning of interactive networks. The issue of a user's consent to certain forms of unsolicited commercial communications was not the subject of this Directive but is already regulated, in particular, in Directives 97/7/EC and 97/66/EC. The Member States which allow the sending of unsolicited commercial communications through electronic mail should further and facilitate the introduction of devices enabling the proper filtering of these communications. Alongside this, unsolicited commercial communications must be distinguishable so that transparency can be enhanced and the functioning of these devices introduced by undertakings facilitated. No unsolicited commercial communication sent by electronic mail must constitute any additional expenditure for users.

Article 7 of this Directive (column: Unsolicited Commercial Communications) contains the basic rules, which shall be incorporated in the legislations of the Member States of the European Communities. Alongside other EC requirements, the Member States which allow the distribution of unsolicited commercial communications by electronic mail are obliged to make sure that a user is able to clearly and unambiguously distinguish these commercial communications of a service provider located on their territories after their receipt [Article 7(1)]. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, the Member States shall adopt measures to ensure the service providers who send unsolicited commercial communications by electronic mail regularly consult the lists in which natural persons who do not wish to be sent such information are entered and respect such lists.

The crucial EU directive regulating this issue is the Directive of the European Parliament and the Council **2002/58/EC** of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications). This Directive relates not only to spam but, in general, to the protection of individuals from unauthorized interventions in their private lives through information society services. A key provision is Article 13 of this Directive which stipulates the basic standard for regulating spam within the EU which should be incorporated in the specific legislations pertaining to this sphere in the individual Member States of the EU. Therefore, the Directive constitutes a crucial harmonization tool of this sector. The Member States shall be bound by the Directive only within the meaning of its objectives or regulated issues rather than within the meaning of any specific formulations. It is possible to derive from these objectives the individual requirements which, despite their generality, ensue for the Member States from such regulation:

- requirement for the unsolicited and commercial nature of spam to be the key criterion of the regulation (that is, the regulation shall not affect charitable, religious, political or other spam);

- requirement for applying the opt-in principle (that is, on the basis of an actively provided consent to the sending of communications or, more precisely, to the handover of contact details);
- requirement for the contextual side of spam (possibility to unsubscribe, statement of true details of the sender's identity, information on the commercial nature of communications);
- requirement for considering the qualitative aspects of spam, rather than quantitative in the form of collectiveness which, as such, is irrelevant (is not a defining element), and suchlike.

The **regulatory framework stated above was transposed into the Czech law through Act No. 480/2004 Coll., on Certain Information Society Services** and on the Amendments to Certain Acts (Certain Information Society Services Act), which regulates, alongside the issue of spam conceived as an unsolicited commercial communication, some other spheres, for example, the provider's liability. Pursuant to Section 10 of the Act, the supervision over the observance of this Act is carried out by the Office for Personal Data Protection ("Office"), which is the supervisory and contact authority in the sphere of unsolicited commercial communications and is responsible for dealing with related administrative delicts and offences. However, the stated competence has no impact on the distribution of commercial communications through the information system of data boxes (ISDB), which, pursuant to Section 26c of Act No. 300/2008 Coll., on Electronic Acts and Authorized Conversion of Documents, as amended, falls within the competence of the Ministry of the Interior of the Czech Republic. Alongside this competence, the Office performs supervision over unsolicited advertising distributed via electronic means within the meaning of the Advertising Regulation Act. Such solution is not unusual in the European context. This competence is usually vested either in the supervisory body for the protection of personal data or in the supervisory body in the sphere of (electronic) communications. The vesting of supervisory competencies in the sphere of unsolicited commercial communications sent via electronic means in the Office is meaningful also because in compliance with Section 5(5) through (9) of the Personal Data Protection Act, the Office performs supervision over the sending of commercial communications in the classical manner or, more precisely, over the processing of personal data to this effect. Thus, the unification of both stated competences leads to the unification of the practical attitude to marketing in the entire sphere concerned.

The Information Society Services Act defines the concept of a commercial communication as *"all forms of communication, including advertising and the invitation to visit websites, intended for direct or indirect furtherance of goods or services or the image of an undertaking of a person who is an entrepreneur or pursues a regulated activity"* (Section 2 f) of the Act). Hence, this provision defines the key concept for applying the relevant legislation Section 7(1) of the same Act, which stipulates that a commercial communication can be distributed via electronic means only under the conditions stipulated in the Act. For this reason, the definition element of a commercial communication must be a communication:

- **sent through an information society service** (that is, in particular, electronic mail, short message service system, ICQ, Skype, and suchlike);

- **intended for direct or indirect furtherance of goods or services or the image of a particular undertaking**

This definition was taken, in its original wording, from Article 2 f) of Directive No. 2000/31/EC stated above; nevertheless, with effect from 2012, it was partially modified, by which some deficiencies of the original legislation, which, among other things, did not allow imposing sanctions on natural persons-non-entrepreneurs because the addressee of the relevant legislation was, in this original wording, an entrepreneur or an entity pursuing a regulated activity (for example, vendor, attorney-at-law, physician, tax advisor, etc.), were eliminated. This element indirectly ensued from the factual applicability of the Act, which did not allow imposing sanctions on entities other than legal entities and natural persons-entrepreneurs acting within their entrepreneurial activities or in connection with them (see Sections 11 and 12 of the Act). This original concept reducing the regulation of the use of information society services only to entrepreneurs or persons pursuing regulated activities was taken from Directive No. 2000/31/EC.[5] However, the current concept has eliminated this deficiency by the Act giving preference to the qualitative or, more precisely, contextual, side of such communication while the legal nature of an entity is irrelevant (see Section 10a and Section 11 of the Act specifically regulating the sanctions for legal entities and natural persons collectively or repeatedly distributing commercial communications via electronic means).[6]

Therefore, to consider whether or not it concerns a commercial communication, it will be necessary to evaluate its factual contents, that is, qualitative side, in the context of the message as a whole. If a message contains information about a particular product or offered goods or services and its objective is to promote them, whether directly by referring to their properties, price or advantages or indirectly, for example, by means of personal evaluation or recommendation, it concerns the commercial communication within the meaning of that provision.[7]

A frequent bad habit is also the sending of commercial communications containing a request for consent to the sending of commercial communications or, for example, a name of a domain from which it is obvious what the subject of the offer[8] is. Despite the contradicting opinions on the interpretation in the current legal doctrine[9], it is possible,

[5] The recitals of this Directive and the explanatory memorandum of the Certain Information Society Services Act state no reason for such limitation of the application. Therefore, it can only be assumed that the European and, subsequently, Czech legislators decided to adopt such application obviously because entrepreneurs and persons pursuing regulated activities usually have to resale their goods or services to other clients and their activities are generally focused on the achievement of profit. For this reason, the legislator found it necessary to limit the use of unsolicited commercial communications by these entities.

[6] For more see HRÁDEK, J. Directive of the European Parliament and the Council No. 200/31/EC. *Právní rádce*. 2001, No. 9, pp. 5–8.

[7] It will also be necessary to consider as a commercial communication every message aimed at strengthening the image of a particular entity, that is, strengthening the awareness of its name and brand or improving its media picture, etc., although it does not contain a link to any specific goods or services.

[8] For more, for example, the Judgment of the Municipal Court in Prague 5 Ca/286/2008 of 18 March 2011. Available online at https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=5731.

[9] See, for example, the opposing opinion of POLČÁK, R. *Právo na internetu: spam a odpovědnost ISP.* Brno: Computer Press, 2007, p. 124.

in compliance with administrative practice, to arrive at the conclusion that this form or, more precisely, method of communication meets all definition elements of the concept of a commercial communication. The thing is that its nature points, at least, to the indirect furtherance of goods or services without the existence of a prior consent, that is, a criterion presumed by the Act. Moreover, it is obvious that the actual objective is to obtain the consent to the sending of commercial communications (that is, for the purpose of direct furtherance of goods or services) and to the concurrent promotion of awareness of the sender and, usually, his business activity since such request is not sent without at least a minimum clarification of the sender's scope of business.

However, even, for example, Christmas or Easter wishes and information of charitable activities or other publicly beneficial activities of a particular entrepreneur entity will have to be considered as commercial communications within the meaning of the stated Act if the message itself or the sender details show which entity has sent the message.

Conversely, links in an e-mail message, for example, to the sender's website or the website of his project shall not be considered as commercial communications if used as part of the sender's signature within usual electronic communication with clients or suppliers and the primary purpose of such communication is not advertising or marketing. Therefore, they concern cases when the electronic communication between an entrepreneur and an addressee would take place anyway.

3. LEGAL CONDITIONS OF SPAM DISTRIBUTION IN THE CZECH REPUBLIC

The Czech law regulates the conditions for distributing commercial communications, in particular, in Section 7 et seq. of the Information Society Services Act. Although this Act is based on the respect towards the opt-in principle, it provides commercial communication senders with the possibility to proceed without a risk of administrative sanction if they comply with all of these conditions. The stated clause stipulates as follows:

Section 7

(1) Any commercial communications may be distributed via electronic means only under the conditions stipulated in this Act.

(2) Details of an electronic contact may be used, for the purpose of distributing a commercial communication via electronic means, only in relation to the users who have granted their prior consent thereto.

(3) Notwithstanding paragraph 2, if a natural person or a legal entity obtains details of his customer's electronic contact for electronic mail from such customer in relation to the sale of a product or service according to the requirements for protecting personal data regulated by a special law 5), the natural person or legal entity may use these electronic contact details to distribute commercial communications relating to his own similar products or services provided that the customer has a clear possibility to easily, free of charge, or on the account of such natural person or legal entity refuse his consent to such use of his electronic contact even in the sending of every individual message, unless he has originally refused such use.

(4) The sending of electronic mail for the purpose of distributing commercial communications shall be prohibited if:

a) it is not clearly identified as commercial communication;

b) it conceals or hides the identity of the sender on behalf of whom the communication takes places; or

c) it is sent without a valid address to which the addressee could directly and effectively send the information that he does not wish to be sent commercial information by the sender

5) Act No. 101/2000 Coll., on Personal Data Protection and on the Amendments to Certain Acts, as amended.

The provision stated above anchors the clear general obligation to observe the laws [Section 7(1)] in the distribution of commercial communications via electronic means and regulates other conditions when the electronic contact [Section 7(2) and (3)] and the elements of a commercial communication as such [Section 7(4)] may be used for sending commercial communications.

However, the legislative structure of the facts constituting the unpermitted distribution of spam (Section 7 of the Information Society Act) and the commission of administrative delicts applicable as a result of such conduct (Sections 10a and 11) is intentionally regulated differently. This means that the **possibility of imposing an administrative sanction** is not tied to the (standard) breach of Section 7 of the Information Society Act (that is, the mere unlawfulness lying in an existing conflict with the laws) but rather to the unlawfulness based, alongside the qualitative criteria (Section 7 of the Information Society Act), **on the qualitative criteria in the form of the qualified requirement for the collectiveness or repetition of such conduct** (Section 10a and Section 11 first sentence of the Information Society Act).

This non-uniformity is a direct consequence of the amendment to Act No. 468/2011 Coll., on Information Society, the purpose of which was most likely to limit the very broad factual (sanction) applicability of this Act to any, however small, breach of the Act. As stated in the explanatory memorandum of this amendment, the legislator focused, in particular, on sanctioning collective or recurring sending of unsolicited commercial communications. This means that, in practice, it happened quite often that a sanction was imposed on an action as a consequence of a trivial omission or mistake (negligent conduct of minor significance). Moreover, within an administrative procedure, all suspicions of unlawful sending of commercial communications had to be investigated and, concurrently, the delict had to be examined for compliance with all data protection principles within the meaning of the Personal Data Protection Act.

Nevertheless, a completely essential issue is that of obtaining the electronic contact (usually e-mail) necessary to distribute commercial communications where the Act counts on two possibilities of using such contact:

- **on the basis of a sufficiently definite prior consent** to the distribution of such communications [Section 7(2)];
- **without an express consent** provided that it concerns an electronic mail contact obtained from a customer in relation to the sale of products or services [Section 7(3)].

The first of the options stated above is clearly based on the opt-in principle, that is, a situation when a customer provides his prior consent to the distribution of such communications and, to this effect, also provides an electronic contact detail. In this respect, such detail may be not only an e-mail address but, in fact, any contact information allowing the sending of commercial communications to a particular user. It will most often concern an e-mail address, a phone number, or a user profile address on a social network if messages can be sent to such address. A contact address may not only relate to a particular natural person but also be a general contact address of a legal entity or any other entity. It will be possible to use such contact information if its user has consented to it prior to being sent commercial communications.

The Information Society Act does not regulate the elements of the consent to the sending of commercial communications, but the essential elements of such consent ensue from Act No. 89/2012 Coll., the Civil Code, and Act No. 101/2000 Coll., on Personal Data Protection, as, in the event of an electronic contact ascribable to a natural person, it also concerns processing of data in the form of storage and use of the electronic contact. This consent to the use of an electronic contact must be, in particular:

- **free and serious;**
- **expressed intelligibly;**
- **sufficiently definite; and demonstrable**

Anyone obtaining an electronic contact and intending to process it for the purpose of sending commercial communications should also provide the electronic contact user with at least basic information (on themselves, the purpose of processing the electronic contact, etc.) and should obtain the user's consent so that it is demonstrable throughout the process in case of dispute with the user or investigation on the part of the Office. If a business communication is sent to a legal entity's electronic contact which does not constitute personal data, the consent to such contact being used must be provided by the authorized person.[10]

With regard to the fact that in these cases, such consent is usually obtained in the environment of electronic trade, the administrator should have at his disposal, to prove the consent, at least the exact time when the consent was granted and the IP address from which it was granted. For greater certainty, it is also advisable, after the consent is granted, to send first an information message to the used electronic contact address stating that consent to the sending of commercial communications has been provided in relation to this address (or, possibly, an instruction how to proceed if the address has been misused and how to unsubscribe from receiving commercial communications). Conversely, it is inadvisable to obtain such consent, for example, by phone since the subsequent demonstrability of such consent is very complicated.[11]

[10] For more information see, for example, PECHÁČEK, M. Temná strana e-mailu. *Ad notam: Časopis českého notářství*. 2014, No. 4, pp. 18–21.

[11] For more information see, for example, NONNEMAN, F. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, p. 9.

The second of the options of using an electronic contact stated above is tied solely to the provision of a contact in the form of electronic mail, that is, not any other forms of contact (see above). However, this is the only lawful possibility when commercial communications can be sent through electronic contacts without prior consent as the Act does not require it if the sender has obtained the respective electronic addresses directly from his customers in relation to the implementation of a particular business transaction (usually by selling these customers goods or providing them with services). In such case, the quite opposite opt-out procedure shall apply rather than the envisaged opt-in regime. The stated legal structure has probably been chosen because it is not purposeful to require from the sender's standard customers to provide him with special consents to receiving commercial communications when, conversely, it is obvious that they have already shown interest in the sender's goods or services or, more precisely, implemented business transactions with the sender in the past and, thus, their interest or consent is expectable. However, the application of this legal entitlement to send commercial communications is conditional upon the simultaneous fulfilment of several **conditions** being as follows:

- The electronic contact to which commercial communications are sent must be obtained by the sender from the user of such contact, being a customer of his, in relation to an implemented business transaction, for example, after the user having signed up to an e-shop in the purchase of goods and having agreed with the business conditions containing the consent to receiving commercial offers with the possibility to refuse it (*a customer is any entity, whether a natural person or a legal entity, with whom the sender implemented business or civil contractual relationship in the past, within which the sender sold, or rented to, the customer a certain product or provided the customer with a certain service*)[12].
- The sender has obtained an electronic contact or an electronic contact detail from the user in compliance with a special law, whether it concerns the Personal Data Protection Act or the Civil Code (*in other words, it must not concern the obtaining of a contact for any other purpose, for example, contact details of employees or through an unlawful activity in the form of theft of data*).
- The sent commercial communication may be used only for the purpose of offering one's own products and services which, on top of that, must be similar to those which the addressee of the commercial communication purchased from the sender in the past (*hence, it is prohibited to send offers to the benefit of a third party; conversely, they must concern offers of similar products or services which the addressee purchased from the sender in the past*).
- In the sending of every individual message, the addressee of a commercial communication must have the possibility to refuse their further receipt free of charge or on the sender's account (*the communication must contain information on how the consent to such electronic contact being used can be refused; such refusal must not burden the addressee financially, for example, by the addressee having to make the refusal by calling a paid phone number or sending a paid short text message*).

[12] The stated facts do not, of course, rule out sending a particular answer to an offer; however, the contact so obtained cannot be used for purposes of other offers of goods or services.

- A customer, as an addressee of the respective commercial communication, has not refused to provide his prior consent to his electronic contact being used (*the sender is not obliged to inform the customer about this possibility; nevertheless, if the customer refuses to be sent commercial communications, the sender is obliged to respect it*).

The fulfilment of the conditions of distribution of commercial communications or, more precisely, the conditions of use of electronic contacts as stated above constitutes only the fulfilment of the basic legal prerequisite for distributing commercial communications as a certain alternative to the obtaining of prior consent. For a distribution of commercial communications to be lawful, it must meet a number of other contextual formal elements applicable to every commercial communication sent via electronic means, that is, both to communications sent to a sender's customers [Section 7(3)] and to communications sent on the basis of an addressee's prior consent [Section 7(2)]. These contextual formal elements of commercial communications are stipulated in Section 7(4) of the Act, which, concurrently, **prohibits** the distribution of commercial communications that do not meet the elements stated below:

- A communication is not intelligibly and clearly identified as a business communication.
- A communication hides or conceals the identity of the sender on behalf of whom it is made.
- A communication is sent without a valid address to which the addressee could directly and effectively send the information that he does not wish to be sent commercial information by the sender.

Therefore, a commercial communication must be, in particular, visibly and clearly identified as a commercial communication so that the addressee cannot confuse it with a document of a different nature. The identification does not need to contain directly and only the words 'commercial communication' in the subject of a message (if sent by electronic mail), but the text of such communication must visibly and unambiguously state that it is a business offer.

A commercial communication must contain a valid (that is, technically functional) address through which the addressee can directly and effectively express his dissent to receiving any other commercial communications. It may concern an e-mail address to which the addressee can send a message, expressing his dissent to receiving any other commercial communications from the given sender, or a website address after the loading of which the addressee is automatically unsubscribed from the sending of commercial communications. However, in any case, this address must lead directly to the implementation of this action, that is, the termination of the sending of commercial communications, and must be effective, that is, continuously functional and current. It would concern the breach of this Act, for example, if an addressee of a commercial communication sent an e-mail message to the stated address for de-registration, stating that he no longer wishes to receive commercial communications, and the message could not be delivered due to reasons on the recipient's part (full or non-functional e-mail box).

The prohibition to conceal or hide an entity's identity is only a supplement to the principles stated above. An addressee of a commercial communication must always be able to identify by whom or on behalf of whom the commercial communication was sent. Only in this way will the addressee be able to assert, for example, his legal rights.

The sent message must meet all elements of a commercial communication required by the laws simultaneously. In other words, even breach of one of them means breach of the Act.

4. OTHER LAWS OF THE CZECH REPUBLIC PERTAINING TO SPAM

Despite its relatively separate regulation in the Information Society Act, the issue of spam is rather fragmented. The roots of this regulation need to be looked for in the regulations across the entire legal order, including European.

The crucial law is, of course, **Act No. 480/2004 Coll., on Certain Services of Information Society** and on the Amendments to Certain Acts (Certain Information Society Services Act), which regulates, alongside the issue of distribution of commercial communications, in particular, the liability, rights and obligations of persons providing information society services.

Another regulation is **Act No. 101/2000 Coll., on Personal Data Protection** and on the Amendments to Certain Acts, as amended, which regulates, for the purpose of providing everyone with protection from unauthorized intervention in privacy, the rights and obligations in the processing of personal data and sets the conditions under which personal data may be handed over to other states.

Although the factual and personal applications of the Personal Data Protection Act do not relate only to spam but are primarily aimed at protecting an individual's personal rights, in particular, his/her personal data, in terms of the issue of spam it concerns one of the most important sources of law in this sphere, particularly because one of the crucial conditions of distribution of spam is the issue of obtaining the details of electronic contacts, which constitutes personal data and, thus, is protected by the Personal Data Protection Act. Another key aspect is the fact that the Office is the sole supervisory body over the distribution of commercial communications. It performs inspection activity, consisting of the investigation of senders of commercial communications on the basis of received complaints or its own findings (stemming, for example, from mass media), and may impose financial sanction on those breaching the relevant provisions of the Certain Information Society Services Act.[13]

The issue of spam is also contained, in the broader sense of the word, in **Act No. 127/2005 Coll., on Electronic Communications,** as amended, which regulates the conditions of entrepreneurship and of performance of public administration, including market regulation, in the sphere of electronic communications. However, the subject of

[13] In this respect, the Office is also competent to receive initiatives and complaints. However, if the person who has received an unsolicited commercial communication or who believes that his or her personal data has been processed contrary to the laws requests an apology or financial compensation, it is necessary, in such case, to have recourse to the court since the Office is not authorized to determine claims of a satisfaction nature.

application of this Act is not the content of services provided through electronic communications networks and, for this reason, its impact on the issue of spam is reduced only to the cases explicitly stipulated therein. The Act does not regulate this issue generally at all, except for two spheres of application relating to the obligation of access to identification and operational data within: identification of malicious or harassing phone calls (Section 67 of the Electronic Communications Act) and misuse of phone numbers for fraudulent purposes (Section 35(3) and Section 90 of the Electronic Communications Act).

Another law regulating the issue of spam, though rather indirectly only, is **Act No. 40/1995 Coll., on the Regulation of Advertising** and **Act No. 89/2012 Coll., the Civil Code**, which is applicable to the issue of spam, in particular, as a tool of protection from spam in the form of intensity of unfair competition (see below) and in relation to the contextual elements of informed consent and the notification obligations (for example, Section 1728(2) of the Civil Code), general legal acts, compensations for property and non-property harm, etc.

The last important law is **Act No. 40/2009 Coll., the Criminal Code**, as amended, the importance of which in terms of spam lies in the possibility of being applied simultaneously with other spam protection tools. They concern, in particular, the issues of publicly committed crime (Section 117 of the Criminal Code), mistake and taking advantage of another person's mistake via technical equipment (Section 120 of the Criminal Code), a crime of unauthorized handling of personal data (Section 181 of the Criminal Code), etc.[14]

5. SANCTIONING SPAM IN THE CZECH REPUBLIC THROUGH ADMINISTRATIVE LAW MEANS

The key and, in fact, only efficient legal tool enabling the imposition of sanctions on spam in the Czech Republic is the administrative regulation in the Information Society Services Act. The sole inspection and supervisory body in the sphere of distribution of commercial communications is the Office for Personal Data Protection. This Office performs investigations on the basis of received complaints or its own findings and regular inspections of senders of commercial communications. It also initiates the administrative procedure and imposes financial sanctions in the event of breach of this Act.

The Office performs its activity ex officio and, within the competence vested in it by the Act, receives and verifies incentives from the public and handles complaints. This competence is anchored in Section 29(1) c) of the Information Society Act. To ensure the efficient handling of the complaints, the Office has issued a simple form through which unlawful spamming may be reported. Alongside the form, the Office has issued detailed instructions on how to complete it, by which it tries to facilitate the reporting of spam for the public and accelerate its subsequent sanction.

[14] With regard to the legislation in this sphere at administrative level and to the high sanctions stated therein, the upper limit of which is CZK 10 million, it can be supposed that the application of criminal law tools will be rather exceptional though it cannot, of course, be ruled out with immediate effect with regard to the nature and intensity of the distribution of spam.

In terms of the structure of liability, the Act stems from the model of sanctioning the actual originator of spam; that is, only the natural person or the legal entity who has distributed spam in a manner contrary to the Act is liable for spamming. Therefore, by its concept, it concerns liability without fault, that is, liability for the result, the prerequisite of which is not fault and which is borne only by the one who has caused such result.

However, Section 12(1) of the Information Society Act permits the so-called **grounds for liberation**. It stipulates that a natural person or a legal entity shall not be liable for an administrative delict if he *"proves that he has made all efforts that could be expected of him to prevent the breach of the legal duty"*. This liberation clause allows a wrongdoer to avoid liability for an administrative delict provided that he has made all efforts that could be generally expected of him to prevent the breach of a legal duty, whereupon the wrongdoer of the administrative delict shall always prove the existence of the grounds for liberation. A typical example when liability can so be avoided is a situation when an employee sends out a defective commercial communication without his or her employer's knowledge despite the fact that such type of communications is expressly prohibited by an internal regulation the observance of which is verified by the employer.

Another possibility of avoiding liability is the expiration of the limitation period. Section 12(3) stipulates that liability for an administrative delict (offence) shall be considered as terminated if the supervisory body has failed to initiate procedure within 1 year of learning about the delict (subjective time-limit), but at the latest within 3 years of its commission (objective time-limit).

Sanctions for breaching the Act are regulated differently for natural persons-non-entrepreneurs and for legal entities. The reason for this is probably the nature of a commercial communication where the legislator obviously presumes, as the previous legislation did, that according to the definition of a commercial communication in Section 2 f) of the Information Society Act, the natural person who is not an entrepreneur or does not pursue a regulated activity cannot send such communication to his benefit. Pursuant to the current legislation, a natural person will commit an offence, in particular, if he, for example, sends a commercial communication to the benefit of another entrepreneur, or to his own benefit but for the purpose of one-time promotion of an isolated business transaction.[15]

The difference in the construction of liability ensues, in particular, from Sections 10a and 11 of the Information Society Act which stipulate that a natural person-non-entrepreneur shall be considered as committing an offence if he **is collectively or repeatedly distributing commercial communications via electronic means without the addressee's consent, for which he may be imposed a fine of up to CZK 100,000**. However, in the event of a natural person-entrepreneur or a legal entity, this construction is conceived completely differently, including the maximum financial sanction. In this respect, Section 11 of the Act stipulates that **a legal entity may be imposed a fine of up to CZK 10 million** if it is collectively or repeatedly distributing, via electronic means, commercial communications:

[15] Only in 2014, the workers of the Office for Personal Data Protection of the Czech Republic dealt with 7,951 incentives relating to unsolicited commercial communications. They handled 2,965 questions and consultations and initiated 144 inspections and 78 administrative procedures (source: Annual Report of the Office for Personal Data Protection for 2014).

- without the addressee's consent;
- not clearly and intelligibly identified as commercial communications;
- hiding or concealing the identity of the sender on behalf of whom the communications have been sent;
- not containing a valid address to which the addressee could send a request for termination of such communication; or
- without providing the addressee with the opportunity to clearly, intelligibly, easily and free of charge or on the sender's account grant or refuse his consent to his electronic contact being used for the purposes of such communication.

A different liability-relevant construction can be found in the event of **legal entities pursing regulated activities** (attorneys-at-law, notaries, tax advisers, etc.). Such a legal entity shall be imposed a penalty of up to **CZK 1,000,000 if the commercial communications do not contain:**

- name of the statute-based professional self-administration chamber with which it is registered;
- reference to the professional rules applied in the member state of the European Union where it has its seat; or
- method of permanent public access to information on the relevant statute-based professional self-administration chamber of which it is a member

Thus, the set upper limits of the possible financial sanction for distributing commercial communications are relatively high – between CZK 1 and 10 million. The Office has relatively broad administrative discretion. The main criteria of such discretion are contained, in particular, in the provisions of Section 12(2) of the Act, which stipulate that in determining a penalty, the following shall be taken into account: gravity of an administrative delict; *method of its commission and its consequences; and circumstances under which it has been committed*[16]. The Office is obligated to consider in its decision all circumstances named therein and, as already stated, is authorized to consider even other aspects which it considers essential.[17]

[16] The Office imposed a penalty of CZK 1,900,000 on Traffic7 s.r.o. for the distribution of unsolicited commercial communications. In 2013 and 2014, this company sent a large amount of unsolicited commercial communications (the penalty was imposed for the distribution of more than 500 unsolicited commercial communications). The decision is final. For more information on penalty stipulation, for example, the Judgment of the Municipal Court in Prague 5, case ref. Ca/286/2008, available online at https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=5731.

[17] The circumstance which is taken into account when the penalty is determined is, in particular, the gravity of an unlawful act as a criterion including the method of committing an administrative delict, its duration and consequences (in particular, the impact on the affected persons' privacy), and the circumstances of its commission. The administrative body must avoid taking into account, in determining the sanction, the circumstances which already constitute the facts of an administrative delict, that is, must not violate the prohibition of double sanction. Compare Judgments of the Supreme Administrative Court number 2 As 47/2009 and number 2 As 58/2007.

6. OVERVIEW OF PRIVATE MEANS OF PROTECTION AGAINST SPAM

Of course, the Information Society Services Act is not the only legal tool of protection against spam. However, it is a tool which is efficient, at least, in the sense that the body of its protection is only a public authority in the form of the Office, that is, not necessarily other persons, for example, those whose rights have been affected in any way. Hence, in this respect these other persons have to pursue no or only minimal activity leading to the filing of a complaint with the Office which is then obliged to act ex officio and only notify these persons of the result of their filing. Moreover, this method of automatic legal protection is precautionary for the Office's next procedure to deter other wrongdoers of similar offences.

Nevertheless, the legal order permits a number of other tools, in particular, private, the consumer protection body of which is the court. To implement this protection, it is necessary that the entity whose rights have been affected seeks remedy by pressing charges. In its essence, it concerns follow-up and reparatory protection where the main activity, including the submission of evidence and the bearing of all costs, rests on a private person. In this respect, the charges should be based on the provisions prohibiting unfair competition, specifically Section 2986 regulating the so-called intrusive conduct, or on the provisions regulating compensation for damages (harm), etc.

These private tools of possible protection against spam are not used regularly under the conditions of either the Czech Republic or other European countries and, therefore, the judicature is, in fact, missing. The reasons for this need to be looked for, in particular, in the nature of spam which, in essence, does not inflict harm significant enough for the affected entities to be motivated towards protecting their subjective rights. However, private ways of dealing with the issue of spam are usually taken in the countries of Anglo-American legal culture where they constitute the principal legal titles of follow-up protection against spam. They concern, in particular: **protection of moral rights or privacy** (e-mail hijacking); **protection of ownership and author's rights** (use of infrastructure for unfair practices); **unfair competition** (an advantage obtained contrary to good morals).[18]

In the environment of the Czech law, it is theoretically possible to consider numerous similar titles although they are likely to be used rather exceptionally, in particular, with regard to the non-triviality, period and overall high cost of legal protection in the Czech Republic, including the problematic issues of legal certainty and the overall enforceability of law in the global Internet environment (for example, application of another governing law, venue of litigation, etc.). In terms of the Czech law tools, the following legal titles may be considered as the possible tools of private protection of subjective rights from spam:

- **unfair competition** pursuant to Section 2976 of the Civil Code;
- **protection of privacy** pursuant to Section 81 at seq. of the Civil Code;
- **liability for breach of law** (Section 2910 of the Civil Code), **etc.**[19]

[18] For more details see POLČÁK, R. *Právo na internetu: spam a odpovědnost ISP.* Brno: Computer Press 2007, p. 132.

[19] The applicable legislation offers, alongside the already mentioned, a number of other law-qualified possibilities aimed at the efficient protection against spam. Once of these possibilities is the relatively broad potential of the institute of self-help defined in Section 14 of the Civil Code stipulating, among other things, that *"anyone may adequately help themselves to enforce their rights if these are at risk and it is obvious that the intervention on the part of public power will come late"*. This provision constitutes a certain exception to the otherwise state monopoly of protection against spam in the form of guarantees of subjective private messages. Concurrently, it probably constitutes one of the most common and, at the same time, least visible possibilities of efficient protection against spam.

The successful use of all the titles stated above is conditional, in particular, upon proving that spam has been distributed by a particular person or upon many other facts lying, for example, in the existence of damages or in the intervention in privacy or property rights of an individual or a corporation. Pursuant to the private law, this burden is usually borne by the one seeking legal protection, that is, the plaintiff. Nevertheless, the issue of provability of these matters is discussed in the following part of this article. For the purpose of facilitating the interpretation, we will suppose that the identity of a spam sender is indisputable (for example, because it has already been proven in another type of proceedings, usually administrative).

7. PROTECTION FROM SPAM THROUGH THE INSTITUTE OF UNFAIR COMPETITION

The first of the possibilities of private protection from spam is unfair competition which is often one of the few tools suitable for sanctioning free-riding when someone intentionally obtains benefit based on an unlawful or immoral procedure. With regard to the nature of the distribution of spam, it can be supposed that such tool will be suitable more likely for the spammer's competitors. Nevertheless, it may also be used by possible addressees or other affected entities.

The unfair competition is regulated in Section 2976(1) of the Civil Code, which defines it as an act within an economic relationship which is contrary to good morals of the competition and is capable of inflicting harm on other competitors or customers. The **general clause of unfair competition** is contained in Section 2976(1) of the Civil Code and consists of three conditions that have to be cumulatively met for a certain action to be qualified as unfair competition:

- **conduct within an economic relationship;**
- **contradiction with good morals of the competition**
- **capability of inflicting harm on other competitors or customers**

It is obvious that the distribution of spam in the form of commercial communications is an act within an economic relationship. Concurrently, it is contrary to good morals of the competition (distorts competition) and is capable of harming other consumers (customers, addressees, etc.). Thus, all elements of unfair competition are fulfilled. A part of the general clause is also a provision stipulating *"unfair competition shall be prohibited"*. This provision expressly prohibiting unfair competition is of significant importance since were it not for it, it would not be possible to apply the sanctions regulated in Sections 2988 and 2989 of the Civil Code.

8. PROTECTION AGAINST SPAM THROUGH THE INSTITUTE OF PRIVACY PROTECTION

Another possibility of protection against spam pursuant to private law is the **protection of privacy**. However, with regard to the overall scope of spamming, the assertion of this type of protection will be rather exceptional. It is possible to resort to its application, in particular, if any of the moral rights, in particular, privacy rights (including personal data

protection), protection of documents or other written instruments (mail confidentiality), an individual's dignity, respect and other exhibitions of a personal nature, has been violated. Probably the most frequent is the infringement of the right to privacy in the form of an e-mail address forged to distribute spam (that is, sending of spam from an existing person's forged address), or other forms of stolen identity (spamming within social networks, other methods of misuse of a particular person's access or contact details, etc.).

The basis of protection of a natural person's privacy rights ensues from Section 81 of the Civil Code. The protection is broad in many respects and still developing.[20] The substance of this legislation is made up of the so-called general clause (Section 81(2) of the Civil Code) containing positively defined enumeration of protected ideal estates forming partial units of a uniform moral right. This protection is conceived as falling within the so-called general moral rights[21] which pertain to every natural person being a subject of law. The enumeration of the estates (units) protected by these provisions is demonstrative and their importance ensues, among other things, from the application of constitution-compliant interpretation and from the order of these individual units. The uniform nature of moral rights shows that, **in particular, the following shall be subject to protection:**

- *an individual's life and dignity and his/her health and right to live in a favourable living environment;*
- *an individual's respect and honour and exhibitions of a personal nature; other ideal estates specifically unnamed in the Civil Code*[22]

The general clause is further elaborated on and specified in Sections 81 to 117 of the Civil Code. It is also necessary to mention that the protection of moral rights relates solely to natural persons and no legal entity shall be entitled to protection of moral rights as a natural person. However, a legal entity has similar rights[23], such as the right to protection of its name, good reputation, image, etc.

The issue of a natural person's integrity is not associated only with civil law but also closely with numerous other legal branches across the legal order, in particular, with constitutional, administrative, press, telecommunication, criminal, and other laws.

The units of protection of moral rights stated above cannot be considered as separate. The contents of the rights ensuing from these units often overlap since the application of any of these units is often conditional upon the application of another of them. In this respect, we speak about the so-called inseparability of moral rights. The scope of protection

[20] For more information see MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013, p. 135. Available online at https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

[21] Compare the concept of the so-called special moral rights that are attached, conversely, only to selected entities meeting the criteria stipulated by the laws (such as authors, professional artists, invention patent originators or applicants, etc.).

[22] However, the last of the points stated under e) is not stated in the general clause. The protection of these other estates needs to be provided with regard to the nature of a uniform moral right, to the fact that the general clause contains only a demonstrative (exemplary) enumeration of these ideal estates, and to the application of constitution-compliant interpretation.

[23] The aforementioned also ensues from the opinions of the Constitutional Court of the Czech Republic which awards to legal entities only these rights and the rights ensuing from the protection of economic competition or trade secret. Compare III US5/01, volume 22, Resolution 18, p. 369.

of general moral rights may then, in some cases, be contrary to other protected values and estates, in particular, to the freedom of speech (for example, the exercising of the right to express criticism affecting a natural person's honesty), the right to privacy, the right to protection of reputation (for example, the publication of debtors without their consent), the right to information or, possibly, also the right to self-administration of certain institutions.

In terms of protection against spam, it is possible to use, in particular, the parts of protection of moral rights (estates) which relate to respect, dignity, reputation and certain exhibitions of a personal nature. These estates may be interfered with in numerous ways, such as:

- misuse (forging) of another person's e-mail address for the purpose of distributing spam;
- theft and misuse of contact (personal) data;
- theft of identity on social networks and misuse of access details for the purpose of distributing spam;
- distribution of denunciation communications affecting an individual's private sphere;
- specific form of cyberbullying

The **protection of an individual's honour and dignity** follows Article 10 of the Charter of Fundamental Rights and Freedoms, which speaks about human dignity, personal honour, name and good reputation[24] and the objective of which is the protection of the psychological or, more precisely, emotional part of a natural person's comprehensive integrity. The consequences of intervention in a natural person's human dignity, honour, name or reputation are usually apparent in the family and in business, entrepreneurial or other social relationships, that is, both public and private. These rights may be intervened in, for example, by the publication of false data on a particular person (his family, family or private life, etc.), by which such falsity is objectively capable of putting the individual's reputation, name, honour, respect and dignity in the society at risk or affecting his/her private and family life (for example, publication of intimate or family circumstances, taking a child away from his/her parent's care without factual and legal reasons, etc.).

A very significant moral estate is the **right to privacy,** the foundations of which can be found in many international documents, in particular, in the Convention for the Protection of Human Rights and Fundamental Freedoms and others.

The regulation of the **protection of a name or, more precisely, the right to a name,** is considerably fragmented across a number of laws although the dominant legislation is anchored in Section 77 et seq. of the Civil Code. The public protection of a name ensues, in particular, from Section 61 et seq. of **Act No. 301/2000 Coll., on the Registers of Births, Deaths and Marriages and on the Name and the Surname**, as amended, stipulating, among other things, that a citizen shall be both entitled and obliged to use, in dealing with public bodies, the name(s) stated in his/her birth certificate issued by the Registry of Births, Deaths and Marriages. Certain aspects of protection of these rights can be found

[24] That is, not civic honour as in the Civil Code.

in many other regulations although their subject is not the protection of a natural person's moral rights but rather of certain partial and related units.

Exhibitions of a personal nature comprise, on principle, any expressions relating to a natural person, regardless of whether such expression is made verbally, in writing, or by a sound, an image or an audio visual. In particular, the relation to the natural person's integrity or its personal nature rather than the form of such expression is decisive. Hence, the protection applies to all carriers of such expressions, whether traditional paper ones or electronic. The unauthorized intervention in an exhibition of a personal nature lies, in particular, in any unauthorized disposition with this, though isolated, exhibition, ranging from its acquisition, re-disposal (for example, reading, listening, publication or distribution of personal messages, etc.) to its destruction (depreciation, liquidation or shredding).

As already stated above, a natural person's moral rights are protected across the legal order, that is, not only by the Civil Code and the Labour Code, that is, regulations regulating the contents and scope of moral rights rather generally. Thanks to the principle of subsidiarity, significant space is left for extending such protection by other personal right estates, which also deserve civil protection with regard to their nature or the constitution-compliant arguments. **Therefore, these estates indisputably include, for example, the personal freedom of expression, the right to information, the right to personal secret, the right to good reputation, etc.** The specific means through which the protection of moral rights may be sought and the scopes of specific entitlements are defined in a number of provisions, in particular, in Section 82 of the Civil Code stipulating that an individual whose moral rights have been infringed shall be entitled to seek that the unauthorized intervention stops or its consequence is eliminated. In the event of an intervention in an individual's moral rights, the laws provide a number of efficient means of protection, whether it concerns the call for desistance from infringement, for elimination of consequences, or for rectification or litigation within civil proceedings.[25]

9. PROTECTION AGAINST SPAM THROUGH OBLIGATION TORT LAW

Other possibilities of private protection against spam are represented by the so-called non-contractual liability or **liability in tort**. The basic principle of the obligation tort law is the principle of no harm to anyone or, more precisely, no intervention in another person's rights. Within the obligation tort law, this principle is reflected in two basic provisions of the Civil Code, being:

- liability for intentional violation of good morals (Section 2909)
- liability for intervention in an absolute right and violation of the protective purpose of a standard (Section 2910)

The **intentional violation of good morals** is defined by Section 2909 of the Civil Code which stipulates that *"a wrongdoer who has harmed another person by violating good morals shall be obliged to provide compensation for such harm; however, if the wrongdoer has exercised his right, he shall be liable for damages only if he has pursued another person's*

[25] See HULMÁK, M. et al. *Civil Code VI. Special Part, Commentary.* Praha: C. H. Beck, 2014, p. 2072.

harm as the main purpose". As ensues from the relevant provision, the liability for damages is not explicitly tied to the breach of a legal duty but rather to the 'mere' **breach of the obligation to observe good morals**. The breach of good morals is on a par with the breach of a contractual or legal duty. However, the prerequisite of successful assertion of such right is, in particular, the evidence of damage. In the event of dispute, it is up to the aggrieved party to prove all necessary prerequisites for the obligation to provide compensation for damages to apply – an action contrary to good morals, the occurrence of harm, causal relation, and maliciousness.

The other possibility of protection against spam through the means of obligation tort law is the application of **liability for intervention in an absolute right** (Section 2910 first sentence of the Civil Code) and **breach of the protective purpose of a standard** (Section 2910 second sentence of the Civil Code). In this respect, the Act stipulates that *"a wrongdoer who has breached a legal obligation by fault on his part and has so intervened in the aggrieved party's absolute right shall provide the aggrieved party with compensation for the damages caused. The obligation to provide compensation shall also apply to any wrongdoer who has intervened in another right of the aggrieved party as a consequence of breach of a legal obligation established to protect such right by fault on his part"*.

Pursuant to the provision stated above, the wrongdoer may, on principle, be any person capable of committing a delict, whether a legal entity or a natural person, that is, the one who has actually and directly caused the harm (spammer). However, in certain cases, someone may be ascribed a consequence caused by another person and, even though they have not directly caused the harm themselves, they shall be identified as a wrongdoer.

10. PROVING OF SPAM ORIGINATOR (DISTRIBUTOR)

It seems easy to ascertain to whose benefit spam is distributed. Nevertheless, it is more difficult to ascertain whether the entity to the benefit of which spam is distributed has distributed such spam or has assigned its distribution. However, it can be supposed that the distributor of such communications (spammer) will do his best to prevent or, at least, significantly aggravate the unambiguous identification of his identity. Such identification may be almost impossible in a number of cases. The Internet environment can be considered, with regard to the comparatively old technology on which some of its services are based, as relatively anonymous and, on principle, enables concealment of an identity. In this respect, a sophisticated spammer is able to prevent the communicating persons (for example, recipient) from identifying the counterparty (for example, a particular www server or the original distributor's address) or to disable the unambiguous designation of whether the given message was delivered to the respective addressee in a specific time period (recipient's anonymousness)[26]. With regard to the legal provability of such conduct, it can be stated that this fact considerably aggravates or, in some cases, prevents the identification of a particular spammer, that is, the person who has sent out spam through a computer and a specific IP address.

[26] For more details on the issue of anonymous advertising see BENEŠ, T. Anonymní spojení v prostředí Internetu. *DSM*. 2002, No. 2, pp. 36–38.

A spam originator's IP address or, more precisely, a complete list of such addresses with other accompanying details then form the basic pillars for proving all related legal facts. One of these key proofs is represented by the so-called head of a particular e-mail message (spam), which is its integral part containing information on the sender, the recipient and the route the message has taken on the Internet from a sender to a recipient.

The overall context of these identifiers (as evidentiary means) is then essential for their application. The aforementioned applies, for example, to an IP address, which unambiguously identifies the network interface in the computer network rather than directly a particular person. In this respect, it can be said that an IP address as such represents an imperfect identifier indicating only the point of connection or a network of more computers or one particular computer.

On principle, an IP address as such does not serve for the purpose of identifying a particular person but rather identifies the place where a certain activity is carried out; it is not known whether it concerns mechanical activity (that is, computer) or an activity of a particular person. The thing is that it does not need to be evident at first glance whether at all any person (spammer) sat at a computer and, if so, the IP address itself is not able to identify such person – any person could have sat at the computer at the given moment. An IP address may be aimed, for example, at an undefinable group of these people, that is, not at a particular person. However, the aforementioned is an issue of provability (significant, for example, in criminal proceedings) rather than the fact that an IP address identifies a particular means used by a particular natural person.[27]

The facts stated above can also be demonstrated in the usual procedure of the Police of the Czech Republic which, in proving a crime committed on the Internet, need to know a demonstrable and reliable connection (relationship) between a particular IP address and a particular person. Although it can be said that the obtaining and production of such evidence may be difficult,[28] this cannot, as such, be a reason for excluding the identifier in the form of an IP address from protection provided by the laws with respect to similar identifiers (as personal data). Although it may represent a difficult expert activity, such evidence may be successfully produced on the basis of the context itself in the form of other network operation records or, possibly, on the basis of other proofs showing that a particular natural person worked with the computer having this IP address at a particular time.

The issue of an IP address and of whether, in its case, it may concern personal data was also discussed by the Supreme Administrative Court, which stated in one of its judgments (file number As 90/2008-189) that in considering the nature of an IP address, it was possible to secondarily refer also to the judicature[29] of the European Court of Justice which had stated, among other things, that in the context of the given case, an IP address could

[27] See MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, p. 84. Available online at https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

[28] Report on the workshop of 26 January 2011 held at the Faculty of Law of Masaryk University and titled 'Electronic Means- based Proving'. It was held within the OPVK project 'Law and Technology'. For more information see KINCL, L. IP adresa identifikuje místo připojení, nikoli osobu. *Revue pro právo a technologie*. 2011, No. 3, p. 5. Also available at: http://www.law.muni.cz/dokumenty/12793.

[29] Decision of the European Court of Justice of 29 January 2008, file number C-275/06, in the case of *Productores de Música de España (Promusicae)* vs. *Telefónica de España SAU* (available on http://curia.europa.eu).

be considered as sufficient identifier of an individual (personal data) enabling revelation of the identities of persons who had been provided with Internet connection and whose IP address and the date and time of connection had been known. Therefore, under certain circumstances, an IP address constitutes data based on which it is possible to identify a particular person and, hence, may also serve as a proof in an offence procedure or legal proceedings despite the fact that it will always concern an indirect proof.

In fact, Internet sources and the providers of their contents further work with the IP address of a particular user (that is, his/her public IP address) and process it. Sometimes, they also make it public, for example, within discussion contributions. Thus, every such user leaves behind some sort of electronic trace which, however, is far from standing alone. Instead, it is completed by a wide range of other personal data and often contains a true name (or a pseudonym or nickname), a functional e-mail, an (author's) text and, in some cases, even a picture. The records on such particular public IP address relating to a particular user then mean in their overall context that such person is relatively easy to identify, not by the use of expensive means but by several relatively simple questions and work with Internet browsers. The better and better possibilities of Internet browsers allow working with similar records very easily and relatively efficiently. In this respect, they enable the development of the personality profile of a particular person who was difficult to identify at the outset by means of an IP address. The result of the several seconds' operation may be the finding of a true name and surname, e-mail, photo, and partial exhibitions of a person on the Internet for the last several years (including, for example, information on the downloaded or shared applications, his behaviour on the Internet, etc.). Moreover, modern browsers are able to work highly efficiently in this context, though only on the basis of a seemingly insignificant fragment of such information (for example, a part of a photo of a person on the street)[30] which can be subsequently matched to a number of other photos and records relating to such person thanks to such means. The information so obtained may then represent other (indirect) proofs of identity of any possible spammer in the given context.

A special proof would then undoubtedly be the type of IP addresses which, under certain circumstances and for various technical and organizational reasons, do not enable user identification. An example of this may be IP addresses assigned to a computer, for example, in an Internet café where the identities of customers (users) do not need to be proven. However, spam often uses the so-called e-mail spoofing lying in the alteration of the identification of an e-mail or the misuse of an e-mail (IP address) of a third party for the purpose of sending out spam under a fake identity. In such cases, the chance of tracing back to the originator of spam is nearly zero.[31]

The last problem essential in terms of the efficiency and the principles of a functioning Internet in the global world is the issue of application of a governing law to spamming.

[30] For an opposite opinion on this matter see OTEVŘEL, R. Soumrak užitečného internetu. (Part I) [online]. *JINÉ PRÁVO*. (vid. 18. 10. 2010). Available at http://jinepravo.blogspot.cz/2010/10/soumrak-uzitecneho-internetu-dil-i.html.

[31] Nevertheless, the condition that a person is identifiable based on or through such information does not need to be fulfilled. It is enough if a person is identifiable through other information (context) where this information provides, as an aggregate, a sufficient picture of a spammer's identity.

An absolute majority of spam comes from abroad, usually even outside the EU; that is, the spammer is located out of the factual (territorial) reach of the Czech or European system of protection of subjective rights, including the real possibility of imposing sanction on these operators through an authoritative decision of the public protection bodies.

The conflict standards (provisions pertaining to the conflict of laws) are missing in the relevant European directives. However, the European Commission and the national personal data protection offices generally consider the territorial applicability of Directive of the European Parliament and the Council 200/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector, as similar to the applicability of the directives on consumer protection, such as the Directive on contracts concluded remotely which is applicable to any commercial relationships with an individual in a Member State of the EU. This opinion stems from Article 3(1) of Directive No. 58 which stipulates that *"this Directive shall apply to the processing of personal data in conjunction with the provision of publicly available electronic communications services in public communication networks within the Community"*. Hence, there is a widespread belief that for the Directive on privacy and electronic communications to apply, the respective publicly available electronic communications service must be provided in the public communication networks in the EU, which, as a consequence, means that any use of networks with physical locations in the EU is subject to this Directive and, therefore, any EU individual using such network is subject to the protection provided by the Directive. In this respect, the European Commission is of the opinion that the Directive concerned also applies to unsolicited commercial e-mails sent from non-EU countries to EU individuals despite the fact that the enforceability of such approach is a theory rather than a real track in many respects in terms of any subsequent administrative procedure.

11. CONCLUSION

The problem of the objective definition of spam is closely associated with the non-triviality of the definition of all its defining elements, which cannot be unambiguously, sufficiently flexibly and normatively clearly defined. Even here the old legal rule applies that every (legal) definition is dangerous only because usually there is no principle to which an exception would not exist, all the more so that spam is a strongly non-heterogeneous element. The searched effect of spam is not the number of sent communications but, in particular, some form of secondary capitalization of this activity and its positive transformation into existing commercial models (for example, an increased number of orders) or crime (obtaining of access rights, etc.). Thus, the economic efficiency significantly differs both in the individual types of spam and in the individual industrial segments.

The existing legal tools, whether the protection of moral rights, unfair competition, or the public protection of personal data and data relying on the framework fixed by the European law, seem to be theoretically usable but, with regard to the nature of spam, are strongly inefficient and principally non-applicable. The legislation does not fulfil here its basic punitive function (that is, does not impose sanctions on the liable entity) or reparatory function (that is, does not eliminate the damage suffered). It is also failing when it comes to the fulfilment of the basic function of any prudent legislation lying in its preventive effect on the awareness and behaviour of the addresses of the legal standards.

Another problem is the absence of a clear and, in particular, functional normative regulation, including a legally unambiguous definition of this phenomenon which would prevent spam from continuing to constitute a popular and attractive tool of an extraordinary market effect. The reasons for such absence are obvious and ensue already from the low-cost essence of most information society services which are used to enable easy communication with almost an unlimited number of addressees. In any case, spam as a tool is very efficient, which is evidenced, alongside its existence alone, by numerous studies confirming the efficiency of spam at both theoretical (empirical) and practical levels, completely regardless of its (major) unlawful nature[32].

Hence, the existing legal framework only creates a state of strong legal uncertainty which, in the future, may jeopardize the functioning of several other, otherwise functioning, titles, including, for example, electronic communication, and disrupt the essence of the information society, the concept of which it undermines by its inefficiency.

With regard to the factors mentioned above, the most efficient measures of protection against spam include, in particular, the suitable technological solutions aimed at preventing spam in the form of the primary protection of an electronic contact from its easy obtaining through special programmes (the so-called harvesters, extractors, spiders or finders, etc.)[33]. These procedures may be relatively effectively prevented through the so-called passive forms of technological protection designed to prevent or, at least, aggravate the collection of these details by any possible spammer. The basic forms of this type include, for example, the replacement of publicly available contact details (or their part) with pictures, a part of an e-mail address with a text. Other relatively effective methods of fighting spam, though not necessarily legally flawless (see below), are also the active forms of protection lying in the established existence of the so-called blacklists, white lists or grey lists lying in the grouping of publicly known spam senders and blocking senders based on their origin (in relation to an IP address). Much more complicated, though not less efficient, are other methods of active protection lying in the filtering of spam contents or based on the Bayesian analysis element, etc.

[32] See, for example, FRIEDER, L., ZITTRAIN, J. *Spam Works: Evidence from Stock Tours and Corresponding Market Activity* (March 14, 2007). Berkman Centre Research Publication number 2006–11; Harvard Public Law Working Paper number 135; Oxford Legal Studies Research Paper, available at http://papers.ssrn.com/sol3/papers.cfm?%20abstract-id=920553.

[33] These programmes belong among the most frequently used tools of obtaining electronic contacts on the part of spammers and their main method of obtaining e-mail addresses is the collection of these addresses from websites or the contents of e-mails or otherwise (for example, by guessing an e-mail with a provider, etc.).