

# Notion and Types of Information Offenses in Social Networks

Oksana Safonchyk, Kateryna Hlyniana, Bekhruz Khashmatulla  
National University «Odesa Law Academy», Odessa, Ukraine

## Article Info

Volume 83

Page Number: 6880 - 6887

Publication Issue:

March - April 2020

## Abstract:

The research paper deals with the problems of determining the nature of information offenses in social networks. Besides, the authors provide definitions of information offenses, outline the types of such offenses, and also propose a vision of ways to improve legislation in the relevant field. Among information offenses there outlined dissemination of illegal collection and use of information, unauthorized access to information resources and social networks, illegal copying of information in electronic systems, theft of information from libraries, archives, banks and databases, breach of information processing technologies, launch of virus programs, Trojans, phishing programs, destruction and modification of data in information systems, interception of information in technical channels of its leakage, manipulation of public and individual consciousness, etc. The article identifies the decisive role of the state in providing protection against information offenses. Thus, he state forms an official information policy, organizes the work of relevant bodies, supports the activities of public organizations, controls the development and production of information security means, as well as conducts practical activities to protect the internal market from penetration of low-quality information products..

## Article History

Article Received: 24 July 2019

Revised: 12 September 2019

Accepted: 15 February 2020

Publication: 05 April 2020

**Keywords:** civil information torts, information crimes, information offenses, information sphere, information technologies, legal mechanism, social networks.

## I. INTRODUCTION

The intensity of the development and introduction of information technologies and communication tools in society has intensified the attention of scientists to various information problems. The particularly relevant area of scientific intelligence is the disclosure of certain aspects of information offenses (in social networks).

At the same time, at present, there is no unified vision of the conceptual and terminological apparatus in this field at the scientific and legislative levels. Along with the notion of "information offenses", as the synonymous of this term, other notions can be used. For example, "computer offenses", "IT-offenses", "information crimes", "computer crimes", "information torts" etc. The researchers do not fully define the notion, nature, content, characteristics of information offenses. There is also no unity in the scientific community regarding the definition of types of information offenses, approaches to the classification of certain offenses to information.

At present, there is serious concern about the spread of illegal data collection and use, unauthorized access to information resources and social networks, illegal

copying of information into electronic systems, theft of information from libraries, archives, banks and databases, breaches of information processing technologies, the launch of virus programs, trojans, phishing programs, destruction and modification of data in information systems, interception of information in the technical channels of its origin, manipulation of public and individual consciousness, etc.

Violations of the human and citizen's right to information, such as failure to provide information by public authorities, untimely or incomplete provision of information, provision of false information, etc., are destructive.

For a long time, information offenses were examined through the prism of threats to information security of Ukraine, which were enshrined in the Law of Ukraine "On the basics of Ukraine's national security" (2003).

## II. METHODOLOGY

The authors use various methods of scientific research (methods of analysis and synthesis, comparative-legal, formal-legal, and other methods of scientific knowledge). Thus, the method of analysis allowed to thoroughly

investigate the peculiarities of information offenses that distinguish this type of offenses from others. Moreover, the synthesis method provided for the formation of scientifically valid conclusions of this study, which can be used in practical activities. Comparative legal and formal legal methods have allowed us to analyze the experience of settling public relations regarding information offenses in foreign countries.

The following legal acts became the legal basis for the study:

- The Constitution of Ukraine (1996);
- On the basics of national security of Ukraine: Law of Ukraine (2003);
- On access to public information: Law of Ukraine (2011);
- On protection of personal data: Law of Ukraine (2010);
- On Information Protection in Information and Telecommunication Systems: Law of Ukraine (1994);
- On Approval of the Procedure for Connection to Global Data Networks: Resolution of the Cabinet of Ministers of Ukraine of April 12, 2002 (2002);
- Criminal Code of Ukraine: Law of Ukraine (2001);
- Code of Administrative Offenses: Law of Ukraine (1984);
- Civil Code of Ukraine: Law of Ukraine (2003).

### III. ANALYSIS OF RECENT RESEARCH

Some issues of legal liability for information offenses were investigated through the prism of administrative, civil and criminal law. Such an approach is presented in the works of Turuta (2012), Lipkan&Maksimenko(2011, 2013), Maksimenko(2004, 2010), Kormich (2001, 2002, 2003), Polushkin(2009), Tarasenko(2010). Most scientific studies address certain types of offenses: criminal law, civil law, administrative law, etc.

Information offenses on social networks are characterized by all the characteristics that are inherent in other types of offenses: public danger (harm), wrongfulness, guilt, and punishment (Polushkin, 2009). The problem of the information security were studied by Kormich(2001, 2002, 2003). In addition to the common features, information offenses in social networks have a number of specific ones, those that are unique to them.

Moreover, the issue of copyright protection on the Internet is being raised in most countries around the world. Unfortunately, in Ukraine, it is given little

attention, so it is necessary to find the best ways to solve this problem, based on international experience. Besides, there may be some gaps in the implementation of the national copyright program on the Internet, due to the lack of regulations that would deal exclusively with this issue. On the contrary, in the post-Soviet state studies literature on various aspects of the theory and practice of protecting the right to privacy, the problem of social networks is still out of focus, although the number of Internet users from the former Soviet republics is increasing with geometric progression. The issue of information delictology were studied by Yu.Y. Maksimenko, V.A. Lipkan (2011, 2013).

### IV. RESULTS AND DISCUSSION

#### 4.1. The Notion and Essence of the Information Offenses

Information social relations are inevitably accompanied by tortious relations arising from the offense in the information sphere. The basis for the occurrence of a tortious information legal relationship is the fact of committing an offense in the information sphere. Based on the general concept of an offense, an information offense is defined as a guilty, socially dangerous, unlawful act of a tortious person, which infringes on the information interests of the owner or manager of the information or another participant of information relations, for whose act comes legal responsibility.

The level of public danger of information offenses is determined by the social values that they violate. Considering this criterion, information offenses should be classified as information torts and information crimes. An information tort has general and special characteristics that allow them to be divided into a separate group.

The general signs of an information offense are the public danger, wrongfulness, guilt, and tort of the person who committed it. The peculiarity and degree of public danger of information tort are determined by the social values that the offender is encroaching on. These values include some information rights, which are enshrined in the Constitution of Ukraine and other legal acts. This may be the right of free access to information and the freedom to disseminate it in any manner not prohibited by law, restrictions on access to certain types of information, protection and protection of intellectual property, interference with privacy and collection, storage, use and dissemination of confidential information about a person without his or her consent, etc.

Special features of an information offense that distinguishes it from others are committing torts in the information sphere of public relations, the use of information technologies and means of committing offenses. Information offenses have a complex structural nature, which is explained by the unity of social-conflict, information, and legal elements. Such offenses are committed in the sphere of information activity of a person, society and state in the creation, collection, receipt, use, dissemination, and protection of information, etc. A special feature of information offenses is the fact that different types of technological systems, techniques, and methods of influencing the information environment in the form of computer equipment and the Internet, electronic communications, etc. are used in their commission. This feature points to the widespread content of information offenses, which covers notions such as cybercrime, cybercrime, and other information-related harm.

The essence of an information offense is manifested in the close combination of the system of permits, prohibitions, restrictions, and incentives that shape the legal regime in the information sphere with the rules that establish legal responsibility for their commission. This interconnection plays a significant role in shaping the composition of information offenses and in addressing issues of counteraction to such violations.

The complexity of the nature of information offenses determines the variety of methods and means of preventing and terminating information offenses based on the rules of civil, administrative and criminal law. The illegality of tort in the information field is expressed in violation of the legal rules governing information relations. Legal structures of information torts are fixed by the laws of Ukraine and normative legal acts of different state authorities and local self-government bodies and their officials. A necessary feature of information torts is guilt in the form of intent or negligence, and the punishment for their perpetration is the application to the offenders of specific legal sanctions stipulated by the rules of administrative, criminal and civil law.

An information tort is a socially dangerous encroachment on the values protected by the information right by causing or threatening to harm them. In content, it is the guilty act of the subject of the offense, which infringes on information relations. In the form of a tort, it is an unlawful act or omission, for which the act provides

for legal liability. That is, an information tort is a legal fact that gives rise to the right of a person authorized by the State to prosecute the perpetrator.

Power legal relations of legal responsibility arise between the authorized body or its official and the offender, based on the mechanism of state legal coercion against the guilty person. The attribution of the offense to one or another type depends on the degree of public danger, the amount of harm caused, the person of the offender, other qualifying features that affect the level of responsibility.

Thus, an information offense recognizes the unlawful, socially dangerous, guilty encroachment of a tortious subject on the information interests of a person, society and state, protected by the law for which legal responsibility is established. In recent years, social networking sites have become very popular. These are sites that allow users to upload information to a public profile, create an online list of friends, and view other users' profiles. Social network is a social structure formed by individuals or organizations. It displays relationships between them through a variety of social relationships, starting with casual dating and ending with close family ties.

It should be noted that the Internet quickly became the main tool for exercising the right to express opinions, ideas, and views on the exercise of the right to free speech. However, due to the variety of content and ease of use, online information has become controversial and controversial and may be used for various purposes. On the one hand, for example, it provides information about current events in countries where other media are subject to severe censorship; on the other, the Internet can be used to promote an offense and even a crime.

First of all, it should be noted that the Internet (Turuta, 2012) was primarily created as a network for free dissemination and obtaining useful data for the society, taking into account the rules of law and moral and ethical principles that ensure social justice and the movement towards freedom. However, unfortunately, today the Internet has become a daily means of sending out any information that is not always reliable, which often leads to human rights violations.

The widespread use of the Internet raises significant legal problems relating to, in particular, such important issues as information security, information rights and freedoms, access to information, information resources, information products and information services, e-

commerce (trade), taxation of online business, contracting electronically, use of computer software, use of domain names, online misconduct and (cybersquatting, hacking), security and protection of intellectual property rights (copyrights, patents, rights to means of individualization, etc.).

Human rights violations on social networks should be analyzed. On the one hand, the Constitution of Ukraine (1996) guarantees the possibility of free expression of the Internet users. Art. 34 of the Constitution of Ukraine (1996) is guaranteed the right to freedom of thought and expression, the free expression of their views and beliefs. The question is how to protect their honor, dignity, and goodwill in the event of their breach on the World Wide Web, and who will be responsible for such breach.

#### 4.2. The Composition of Information Crimes

Information crimes are classified into disciplinary, administrative, civil and criminal offenses, depending on the degree of public danger. The criteria for such classification of information offenses are the level of public danger of unlawful acts in the information sphere, the statutory form and the degree of legal responsibility of the subject of the information offense, etc. For the proper qualification of any offense, including the information offense on social networks, it is important to establish its composition, elements of which are always the object and the objective side, the subject and the subjective side (Criminal Code of Ukraine: Law of Ukraine, 2001).

The object of an information offense on a social network is regulated by the rules of law, public relations formed on social internet networks. Objects may include relations in the fields of information security, activities of the media, copyright, library and archives, relations in the legal regime of dissemination of information with restricted access, the privacy of the person, etc. They are the subject matter of material, spiritual and other social goods, as well as the phenomena and processes, actions and actions of subjects to create such benefits. The object of the information offense and its subject matter are the main element by which it is distinguished from other types of offenses.

Moreover, the objective side of an information offense on social networks is the act or omission of the subject of the offense. Actions may be in the form of a violation of the established rules or procedure for collecting or disseminating information, providing false information,

unspoken ways of obtaining information, etc. Inaction is manifested, in particular, in refusing to answer an information request, withholding information. Optional features of the objective side are the time, place, method, nature of the offense, its harmful effects. On the whole, the objective side of an informal offense with a formal composition is characterized by a violation of the rule of law governing information relations, and with material damage – the infliction of property damage on the information interests of a person, society or state and the existence of a causal link between the act and the harm caused.

Subjects of information offenses on social networks can be individuals and legal entities, depending on the type of offense and the degree of legal responsibility. Legal entities can only be subject to administrative or civil liability. The common subject of information offenses is convicted individuals aged 16 and over. Special subjects may be officials authorized to carry out organizational, administrative and administrative-economic functions in state authorities and local self-government bodies in the information sphere. A special subject may be servicemen and other persons who are subject to disciplinary statutes or special provisions on service in cases of offenses related to the observance and keeping of state secrets.

The subjective side of the information offense in the social network reflects the mental attitude of the person to their actions and represents guilt in the form of intent or negligence. The form of guilt affects the qualification of the act and the individualization of punishment. The peculiarity of the fault of the legal person is to establish the possibility of observing the rules and rules for the violation of which provides for legal liability. At the same time, the prosecution of the legal entity does not release the responsible individual.

Thus, an information crime is a socially dangerous, guilty, unlawful act of a convicted person committed in the information sphere, for which criminal responsibility is provided. Deliberate actions aimed at stealing or destroying information in information systems and networks that come from selfish or hooliganism. The peculiarity of information crimes is manifested in a special subject, such as state secrets and other secret or confidential information, computer information, etc.

#### 4.3. Administrative Information Tort

Administrative information tort is a socially



dangerous, guilty, unlawful act that encroaches on the established order of public administration in the information sphere and violation of the information rights of the person, which entails administrative responsibility. The objective side of an information administrative offense is manifested in acts or omissions prohibited by the information right and the harmful consequences of this act. Public harmfulness of an information administrative offense means that it causes damage to information relations protected by information legal norms (the rights and freedoms of a person and a citizen, as well as the established order of management of the information sphere). Subjects of administrative offenses are citizens or officials. Officials are subject to administrative responsibility for offenses related to non-compliance with the established rules in the field of information management and violations of other rules of information activity, the performance of which is included in their official duties. This means that officials are responsible not only for violating certain rules by their actions but also for improperly ensuring that they are enforced by other persons, first and foremost subordinates. They are subject to disciplinary action if the offense was committed in the course of their official duties. The subjective side of an information administrative offense covers the guilt, motive, and purpose of the offender's behavior and can be committed both intentionally and negligently.

Disciplinary information offense is a socially dangerous, guilty, unlawful act, which is manifested in the employee's failure to perform or improperly perform the duties assigned to him by the information legislation in the position of holding a position to create, collect, retain the use of protection and information protection and protection. disciplinary responsibility. It follows that disciplinary misconduct is manifested in violation of labor, service or military discipline in the field of information relations. The subject of disciplinary misconduct is always a person who is in an employment relationship with the owner or his authorized body and who is empowered with relevant powers in the information field. The subjective side of disciplinary information misconduct is characterized by wines in the form of intent or negligence. The objective side of disciplinary misconduct reflects the unlawful behavior of the subject, which consists in the violation of work responsibilities assigned to a particular employee. The object of a disciplinary offense is work responsibilities in

the information field that are not performed or performed improperly.

#### 4.4. Civil Information Tort

Civil information torts are socially dangerous, guilty, unlawful acts that encroach on the property and personal non-property benefits in the information sphere, for which civil liability is provided. Civil-law misconduct in the information field by the rules of civil law and entail remedial measures (failure to fulfill obligations under a civil-law contract). A peculiarity of a civil offense is the causal link between the unlawful behavior of the subject and the actual damage suffered by the injured party.

#### 4.5. State Legal Mechanism for Preventing Information Offenses

At the same time, the norms of the Code of Administrative Offenses (1984), the Criminal Code of Ukraine (2001), the Civil Code of Ukraine (2003), and other normative acts not only establish a measure of responsibility for information offenses but also perform a preventive and restorative function.

Authorized state and other bodies for the protection of information, information systems and networks against unlawful encroachment, ensuring information security developments and use special elements of the mechanism of legal regulation. Components of this mechanism are legal means and ways of influencing participants of information relations and other persons, which should contribute to the development of legitimate behavior, an appropriate level of legal consciousness and legal information culture in them. The means of such influence are information and legal norms, which not only establish rules for the circulation of information but also the order of behavior of participants in information relations and other persons. Such norms are contained in the Constitution of Ukraine, the Law of Ukraine "On Information", and other normative acts regulating information relations and they have a law enforcement content.

In the framework of preventive measures, the state forms a state information policy, organizes the work of relevant bodies, supports the activities of public organizations, controls the development and production of information security means, conducts practical activities to protect the internal market from penetration of low-quality information products. The activities of the state to prevent information offenses cover the main

directions and ways of implementing the state information policy, which is based on ensuring information security of the person, society, and the state.

Information relations are part of public relations and are under the protection and protection of the state. One of the law enforcement measures in the information field is the prevention of offenses using a special state mechanism of legal regulation. The basis of such a mechanism is, first of all, an aggregate of state bodies and non-governmental organizations authorized to perform the functions of the state in law enforcement and law enforcement activities.

It should be noted that the legislation of Ukraine distinguishes two ways of protection: general and special, which are applied in court and extrajudicial order.

Named and other bodies who are involved in the protection of objects of information relations, through legal norms, influence the public information relations and behavior of the subjects of these relations, which is generally a method of legal regulation. The methodological support for the legal regulation of information relations is based on the systematic complex application of the methods of constitutional, civil, administrative, labor and criminal law, that is, a combination of imperative and dispositive methods using common law and special methods. Elements of common law influence are permits, obligations and prohibitions, the use of which is accompanied by compliance with the principles of legality, democracy, humanism, and the protection of judicial protection. The use of industry-specific ways of regulating the information sphere depends on the subject of the legal protection, which may be access to information, privacy, restricted information, intellectual property objects and more.

The mechanism of the legal protection of objects of information relations involves practically all state bodies at the central and local levels. A special place in this mechanism is played by law enforcement agencies, among which are prosecutors, security services, and internal affairs bodies, which are vested with special powers for the prevention, disclosure, and investigation of crimes and other offenses. The courts of Ukraine perform a human rights function in the process of considering specific civil, administrative or criminal cases, and their activities are aimed at establishing the truth of the case and, if necessary, restoring the violated rights to the injured party of information relations.

The role of government bodies in the mechanism of

legal regulation depends on the status of the body and its powers. The Verkhovna Rada of Ukraine adopts laws aimed at regulating information relations, determines the directions of state information policy and information security, etc. (On the basics of national security of Ukraine: Law of Ukraine, 2003; On access to public information: Law of Ukraine, 2011; On protection of personal data: Law of Ukraine, 2010; On Information Protection in Information and Telecommunication Systems: Law of Ukraine, 1994). The President of Ukraine, the Cabinet of Ministers of Ukraine (On Approval of the Procedure for Connection to Global Data Networks: Resolution of the Cabinet of Ministers of Ukraine of April 12, 2002 No. 522, 2002), the central executive authorities in order to comply with the laws of Ukraine issue the necessary by-laws to specify a certain sphere of information relations, that is, organize the implementation of legislative provisions aimed, in particular, at protecting the objects of information relations from unlawful encroachments.

To prevent and eliminate the threat of such specific objects, special rules of information legislation, informatization of the legal sphere, use of organizational and technical means, public control over the activity of public authorities are used. In general, legal methods of preventing information offenses are the filling of information legislation with the norms aimed at enhancing information security of a person, society, state, harmonization of domestic legislation with the relevant norms of international law, etc. Organizational and technical methods of prevention of offenses include improvement of technical means of protection of information and development of system of counteraction to unauthorized penetration into the information environment. The organizing component of the mechanism for preventing information offenses involves determining the competence of public authorities, non-governmental organizations in the field of information security, their activities and tasks, balancing the interests of the individual, society and the state in the information sphere.

## V. CONCLUSIONS

1. Therefore, in the case of posting on the Internet information that violates the honor, dignity, and goodwill of the person whose rights have been violated, he or she can directly appeal to the person who committed the violation, with a request to refute such information, or to

court.

2. Among the many risks to social networking, there are at least three: full awareness of the person; communication of information to criminals; lack of real control over the validity of information about oneself.

3. Finally, it should be noted that the Internet should not be an end in itself for society, but merely a means for the development of the human personality. The human right to development should be a basic criterion for assessing the extent to which all other rights and freedoms, including freedom of expression and access to information, are exercised. After all, what destroys a person cannot be considered freedom for the sake of which the right to free internet is asserted. In general, the Internet is emerging as a rapidly growing and changing field of communication, and the legal regulation of such industries is always delayed.

4. Thus, information offenses in social networks is the newest independent type of offenses, which necessitates the formation and development of information delictology, the purpose of which is to study the content, nature, essence, specificity, and variety of information offenses, as well as the development and implementation of specific ways, directions, their prevention.

## VI. REFERENCES

1. Civil Code of Ukraine: Law of Ukraine. (2003). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <http://zakon4.rada.gov.ua/laws/show/435-15>. 2003.
2. Code of Administrative Offenses: Law of Ukraine. (1984). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/80731-10>
3. Criminal Code of Ukraine: Law of Ukraine. (2001). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/2341-14>
4. Kormich, B. A. (2001). National security as a legal category of analysis of customs activity of the state. Current issues of policy, 10, 56–61.
5. Kormich, B. A. (2002). Information as a category of information law. Current problems of the state and law, 16, 367–374.
6. “Trends and Patterns of Crimes in Dhaka City: An Analysis of Recent Cases”, BEST: International Journal of Humanities, Arts, Medicine and Sciences (BEST: IJHAMS), Vol. 3, Issue 10, pp. 87-96
7. Kormich, B. A. (2003). Legal content of the concept of "national security. Customs: Scientific-analytical journal, 1, 116–123.
8. Lipkan, V., & Maksimenko, Yu.E. (2011). National Security Studies: Problems of Formation of the Categorical-Conceptual Apparatus. Entrepreneurship, Economy, and Law, 8, 7-11.
9. Maksimenko, Yu.E. (2004). Some aspects of defining the concept of national security. Scientific Bulletin of the Law Academy of the Ministry of Internal Affairs, 3, 77-81.
10. “When Virtual World Meets the Real World: Cyber Crime Induced Drug Trafficking”, IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL), Vol. 2, Issue 2, pp. 115-126
11. Maksimenko, Yu.E. (2010). Legal regulation of national security of Ukraine: separate aspects. Imperatives of development of legal and security science: materials of the international scientific-practical Internet conference. Kyiv.
12. Maksimenko, Yu.Y., & Lipkan, V.A. (2013). Bases of development of information delictology. Law of Ukraine, 10, 249-256.
13. “Criminal Justice Delivery System in India: An Exploratory Analytical Overview”, International Journal of Humanities and Social Sciences (IJHSS), Vol. 7, Issue 5, pp. 65-82
14. On access to public information: Law of Ukraine. (2011). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/2939-17/ed20150426>
15. On Approval of the Procedure for Connection to Global Data Networks: Resolution of the Cabinet of Ministers of Ukraine of April 12, 2002 No. 522. (2002). Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/522-2002-%D0%BF>
16. “Security of Information with Biometric

- Applications”, IASET: International Journal of Library & Educational Science (IASSET: IJLES), Vol. 2, Issue 2, pp. 81-88
17. On Information Protection in Information and Telecommunication Systems: Law of Ukraine. (1994).Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
  18. On protection of personal data: Law of Ukraine. (2010).Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17>
  19. On the basics of national security of Ukraine: Law of Ukraine. (2003).Bulletin of the Verkhovna Rada of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/964-15>
  20. “A Comprehensive Study of Various Kinds of Frauds & It’s Impact”, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 6, Issue 3, pp. 47-58
  21. Polushkin, A.V. (2009).Information offense: concept and types. Ekaterinburg.
  22. Tarasenko,R.B. (2010). Information Law. Lugansk.
  23. “Instrument and Technology for Computer Forensic: Research in Ghana”, International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), Vol. 6, Issue 5, pp. 33-40
  24. The Constitution of Ukraine. (1996). Bulletin of the Verkhovna Rada of Ukraine.Retrieved from <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
  25. Turuta,O. (2012). Internet and the Right to Freedom of Speech (Comparative Legal Aspect). Public Law, 4(8) 31–32.