THE EFFECT OF GENDER ON THE FORMATION OF SEMANTIC NETWORKS OF OBJECTIVE WORDS IN ADULTS

INVESTIGAR O EFEITO DO GÊNERO NA FORMAÇÃO DE REDES SEMÂNTICAS DE PALAVRAS OBJETIVAS EM ADULTOS

INVESTIGAR EL EFECTO DEL GÉNERO EN LA FORMACIÓN DE REDES SEMÁNTICAS DE PALABRAS OBJETIVAS EN ADULTOS

Ella V. GORIAN[1]

ABSTRACT: Semantic network theory has provided a way to show the structure of human semantic memory and how it works to understand meanings. This study investigates the role of gender variables in the formation and content of these networks on objective vocabulary. The statistical population of this study is 400 male and female Russian students in different educational levels. They answered ten objective words from other semantic domains. Subjects write the words associated with seeing those words in their minds. After collecting data and performing statistical analysis, it can be concluded that for objective words in both sexes, both men and women. The objective and abstract word is used on an almost equal level. In this research, it can be concluded that the semantic network of objective words in the minds of male and female students evokes the same semantic connections with close concepts.

Key words: Semantic network theory. Objective vocabulary. Semantic domains. Students.

RESUMO: *A teoria da rede semântica forneceu uma maneira de mostrar a estrutura da memória semântica humana e como ela funciona para compreender os significados. Este estudo investiga o papel das variáveis de gênero na formação e conteúdo dessas redes no vocabulário objetivo. A população estatística deste estudo é de 400 estudantes russos do sexo masculino e feminino em diferentes níveis educacionais. Eles responderam dez palavras objetivas de outros domínios semânticos. Os sujeitos escrevem as palavras associadas a ver essas palavras em suas mentes. Após a coleta de dados e realização de análise estatística, pode-se concluir que, para palavras objetivas em ambos os sexos, tanto homens quanto mulheres. A palavra objetiva e abstrata é usada em um nível quase igual. Nesta pesquisa, pode-se concluir que a rede semântica de palavras objetivas na mente de alunos e alunas evoca as mesmas conexões semânticas com conceitos próximos.*

Palavras-chave: *Teoria da rede semântica. Vocabulário objetivo. Domínios semânticos. Alunos.*

RESUMEN: *La teoría de la red semántica ha proporcionado una forma de mostrar la estructura de la memoria semántica humana y cómo funciona para comprender los significados. Este estudio investiga el papel de las variables de género en la formación y contenido de estas redes en el vocabulario objetivo. La población estadística de este estudio es de 400 estudiantes rusos masculinos y femeninos en diferentes niveles educativos. Respondieron diez palabras objetivas de otros dominios semánticos. Los sujetos escriben las palabras asociadas con ver esas palabras en sus mentes. Luego de recolectar datos y realizar*

[1] Vladivostok State University of Economics and Service, Russia. Vladivostok, Ph.D, Associate Professor, School of Law, E-mail: ella.gorian@gmail.com, Gogolya str., 41, Vladivostok, Russia, 690014, ORCID https://orcid.org/0000-0002-5962-3929

análisis estadísticos, se puede concluir que para palabras objetivas en ambos sexos, tanto hombres como mujeres. La palabra objetiva y abstracta se usa en un nivel casi igual. En esta investigación se puede concluir que la red semántica de palabras objetivas en la mente de estudiantes y estudiantes evoca las mismas conexiones semánticas con conceptos cercanos.

Palabras clave: *Teoría de redes semánticas. Vocabulario objetivo. Dominios semánticos. Estudiantes.*

Funding

The reported study was funded by RFBR, project number 20-011-00454 "Ensuring the rights of investors in the banking and financial sectors in the context of the digitalization of the economy in the Russian Federation and the leading financial centers of East Asia: a comparative legal aspect".

Relevance of the topic under research

In recent years, states have been taking active steps to improve national mechanisms of information security: the objects of information infrastructure being most vulnerable and critical to the functioning of society and the state are determined; the pool of authorized subjects with the distribution of powers between them is established; the norms and principles of activities for participants of relations to ensure information security, etc. are also determined. Cybersecurity issues are of interest not only from the perspective of national security of a particular state, but also in other seemingly unrelated spheres: the "trade war" between the U.S. and China, which has been going on for years, affects not only the issues of customs tariffs, and other trade barriers, too. The confrontation between the world's first economies concerns, first of all, access to the market in key technological sectors and reducing barriers to cross-border trade (Webster et al., 2019); it is the digital economy that is the main issue on the agenda of many years of negotiations; and the Chinese side is trying to exclude the issue from the consultation process. But the United States insists on the nonseparability of settling the trade dispute with the harmonization of regulatory requirements in the field of information security and personal data protection, as well as cloud technologies (Wei & Davis, 2019).

The Law on Cybersecurity being in force in the People's Republic of China (hereinafter referred to as the Law) (Cybersecurity Law of the People's Republic of China) since 2017 establishes general principles and directions for the development of national regulation in the field of information security of the state; however, special rules concerning certain issues (CII, personal data) are under development and coordination. The Chinese legislator is faced with

the difficult task of building a balanced regulatory mechanism for ensuring the security of the CII, since it is necessary to take into account the interests of national security and maintain the attractiveness of the Chinese market for investment.

Statement of the research problem

In Russia, the processes for the formation of a national cybersecurity mechanism are at the stage of implementing the federal legislation provisions on the "autonomous Internet" (On amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"). As we noted in our previous studies (Ella Gorian, 2020), Russia, like China, implements the model of the so-called “digital nationalism”, which is characterized by the increased responsibility of the states for ensuring the security of information and information systems (including critical information infrastructure, hereinafter referred to as CII), which is embodied in the introduction of special legal regimes for the circulation and protection of data, including personal data. Therefore, the study of China's experience in regulating these processes is of particular interest; this will help to ensure that the Russian mechanism meets modern challenges and efficiency requirements. All of the above determines the relevance of the study.

Methods

In order to obtain the most reliable scientific results, a number of general scientific (system-structural, formal-logical and hermeneutic methods) and special legal methods of cognition (comparative legal and formal legal methods) will be used.

Research results

Russia. Information security in Russia has always been and remains an important part of national security, which is manifested in a prompt response to challenges in this area. In 2018, for the first time at the legislative level, the importance of CII for state security was recognized and a legal mechanism to ensure security in Russia was determined in the Federal Law of the Russian Federation dated 26 July, 2017, No. 187-FZ "On the security of the critical information infrastructure of the Russian Federation" (hereinafter - FZ-187). The criminal legislation was supplemented by a rule establishing liability for unlawful influence on the CII (Article 274.1 of the Criminal Code of the Russian Federation).

FZ-187 defines the concepts of “critical information infrastructure” (Article 2 (6)) as “objects of critical information infrastructure” (clause 7) and “subjects of critical information infrastructure” (Article 2 (8)). Moreover, the law establishes the criteria for classifying objects as CII: these are social, political, economic, environmental significance, as well as significance for "ensuring the country's defence, state security and law and order" (Article 7 (2)). Thus, CII is defined in such sectors as health care, science, transport, communications, energy, banking and other areas of the financial market, the fuel and energy complex, nuclear energy, defence, rocket and space, mining, metallurgical and chemical industries.

A number of by-laws were adopted as part of the implementation of FZ-187, that regulate the procedure for exercising state control, categorizing CII objects, and countering computer attacks, in particular (Critical information infrastructure):

1) Order of the Federal Service for Technical and Export Control of the Russian Federation dated 28 May, 2020, No. 75 "On Approval of the Procedure for the Subject of Critical Information Infrastructure of the Russian Federation to Agree with the Federal Service for Technical and Export Control to Connect a Significant Object of Critical Information Infrastructure of the Russian Federation to a Public Telecommunications Network".

2) Decree of the Government of the Russian Federation dated 8 February, 2018 No. 127 "On approval of the Rules for categorization of critical information infrastructure facilities of the Russian Federation, as well as a list of indicators for the criteria of significance of critical information infrastructure facilities in the Russian Federation and their values".

3) Order of the Federal Service for Technical and Export Control of the Russian Federation dated 25 December, 2017, No. 239 "On Approval of the Requirements for Ensuring the Security of Significant Objects of Critical Information Infrastructure of the Russian Federation".

4) Order of the Federal Service for Technical and Export Control of the Russian Federation dated 21 December, 2017. No. 235 "On Approval of the Requirements to Creating Security Systems for Significant Objects of Critical Information Infrastructure of the Russian Federation and Ensuring Their Functioning".

5) Order of the Federal Service for Technical and Export Control of the Russian Federation dated December 6, 2017. N 227 "On Approval of the Procedure for Maintaining the Register of Significant Objects of Critical Information Infrastructure of the Russian Federation".

6) Order of the Federal Service for Technical and Export Control of the Russian Federation dated March 14, 2014 N 31 "On Approval of the Requirements to Ensuring

Information Protection in Automated Control Systems for Production and Technological Processes at Critically Important Facilities, Potentially Hazardous Facilities, and Facilities of Increased Risk to Human Life and Health and the Environment".

China. Since 2014, the issues of defining and protecting CII have been raised in every speech of the head of the PRC at government meetings and national conferences dedicated to cybersecurity. In his 2016 speech on cyber strategy, he stressed the importance of protecting CII sectors such as finance, energy, telecommunications and transportation, and urged the government to accelerate work on building a national CII security mechanism. The law on cybersecurity of the PRC was adopted in 2016, and the protection of CII is linked to building the capacity of the national cyber industry, consolidation and centralization of platforms for collecting information on cybersecurity (Lu, 2018).

The law is divided into seven sections: (1) general provisions; (2) ensuring and promoting cybersecurity; (3) security of the network, including two sections: general provisions and security of operations at critical information infrastructure facilities; (4) security of information on the network; (5) monitoring, prevention and response to cyberattacks; (6) legal liability; (7) additional provisions.

The legal protection regime is established by section 2 of the Law, and the CII sectors are represented by information and communication services, energy, transport, water management, finance, government services, and government e-mail services. The State Council of the People's Republic of China is entrusted with the responsibility of determining the CII facilities and security measures for their protection, and the CII operators are responsible for the safety of the CII. All personal data used by CII operators must be stored in China and is subject to national security checks if they are transferred abroad. The Cyberspace Administration of China has been designated as the body responsible for planning and coordinating measures to protect CII.

It should be noted that a specific feature of the Chinese legal system is the existence of an array of by-laws that supplement and clarify the regulatory requirements of legislative acts. To date, active work is underway to form a similar block of regulations and orders in the field of CII protection: the Guidelines for the National Cybersecurity Inspection 2016 were approved with the regulation of the CII identification procedure (National Cyber Security Inspection Operation Guide); compared with the Law on Cybersecurity, the list of CII objects (health care, education, social security and environmental protection, research and production (defence industry, mechanical engineering, petrochemical and food and pharmaceutical industries), media (radio stations, television stations and news services), radio and television networks and

the Internet, service providers that provide cloud computing, big data and other large publicly available information and network services); in 2020, the departmental regulation "Measures for Cybersecurity Inspection" (Cyber Security Review Measures), which imposes the obligation on CII operators to pass security inspection of applied network products and services, may affect the national security of China.

Let us move on to a direct characterization of institutional mechanisms.

Russian Federation

The Law FZ-187 establishes a balanced and coordinated institutional mechanism for CII security: in addition to state authorities implementing general measures for CII security (Article 6), it provides for a special state system for detection, prevention and elimination of consequences of computer attacks on information resources (Article 5). The President of the Russian Federation, the Government of the Russian Federation, the Federal Service for Technical and Export Control, the Federal Security Service and the Ministry of Digital Development, Communications and Mass Communications are included among the former.

The President of the Russian Federation determines the main directions of state policy and the bodies of special competence responsible for ensuring the security of CII (part 1 of Article 6).

The Government of the Russian Federation determines the mechanism for categorization of CII objects, peculiarities of state control in this area, and procedure for preparation and use of resources included in the unified state telecommunications network to ensure operation of significant CII objects (part 2 of Article 6).

In accordance with the Presidential Decree No. 569 dated November 25, 2017, the Federal Service for Technical and Export Control (hereinafter - FSTEC) was appointed as a federal executive body authorized in the field of CII security, and acting on the basis of the relevant regulation (Issues of the Federal Service for Technical and Export Control). With regard to CII security, FSTEC is vested with the following powers: 1) making proposals on improvement of normative-legal regulation; 2) approval of the procedure and maintenance of the register of significant CII objects; 3) approval of the form of sending information on the results of categorization of CII objects; 4) establishment of requirements to ensure security of significant CII objects and to create security systems for such objects; 5) implementation of state control in the sphere in question (part 3 of Article 6).

The Federal Security Service (hereinafter - FSB) was appointed as a federal executive

body authorized to ensure the functioning of the state system of detection, prevention and elimination of consequences of computer attacks on information resources of the Russian Federation (On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation). Its powers include: 1) making proposals to improve normative legal regulation; 2) legal regulation of the National Computer Incident Coordination Centre and coordination of CII subjects (CII security assessment, provision and exchange of information on computer incidents, use of means designed to detect, prevent and eliminate consequences of computer attacks and response to computer incidents) (part 4 of Article 6).

The Ministry of Digital Development, Communications and Mass Media in coordination with the Federal Security Service approves the procedure and technical conditions for installation and operation of means designed to search for signs of computer attacks in telecommunications networks used to organize interaction of CII objects (Part 5, Article 6).

The special state system of detection, prevention and liquidation of consequences of computer attacks on information resources plays a special role in the security mechanism. It includes units and officials of the Federal Security Service, representatives of CII subjects, which take part in detection, prevention and elimination of consequences of computer attacks and in response to computer incidents, as well as the National Coordination Centre for Computer Incidents (hereinafter NCCI), created by the Federal Security Service of Russia, acting on the basis of the relevant regulation (On the National Coordination Centre for Computer Incidents). Its main task is to coordinate the activities of CII subjects in this area (clause 3). For this purpose, the NCCI collects, accumulates, systematizes and analyses information from CII and FSTEC subjects, and organizes and exchanges this information both between Russian CII subjects and between CII subjects and authorized bodies of foreign states, international and international non-governmental organizations and foreign organizations (clause 4.2).

China. The Law on Cybersecurity in the PRC does not contain norms that determine the structure of the institutional mechanism for ensuring the security of the CII, as is the case in the Russian Federation. Analysis of the regulatory framework for ensuring information security makes it possible to single out the bodies of general and special competence endowed with appropriate powers in the area under consideration. The former include the State Council, the Ministry of Public Security (represented by the Office of Cybersecurity), and the Ministry of Industry and Information Technology.

Specifically, the Ministry of Public Security enforces a regime called the Multi-Level

Protection System (MLPS) for information and telecommunications technologies and systems in accordance with their degree of vulnerability and potential threat to national security in the event of a breach or damage. In addition, the Ministry sets specific cybersecurity standards for networks that are critical to the government and military sectors (Level 4 and 5) (Creemers et al., 2020). In fact, before the cybersecurity law came into force, it was the ministry that ensured the security of the CII.

But the MLPS regime and the Critical Information Infrastructure (CII) regime introduced by the 2017 law are two different legal regimes, and the Cyberspace Administration of China has the power to enforce the latter and oversees the activities of regulators in such key sectors of economy like finance, transport and energy. In this regard, there was a certain ambiguity in the delineation of powers between the Ministry of Public Security and the Cyberspace Administration of China, since the adoption of an official act on this was not followed. Researchers have noted the fact of lengthy bureaucratic disputes between the authorities in question over the leading role in setting cybersecurity standards and conducting reviews of network products and services, as it is required by the Cybersecurity Act (Webster et al., 2019).

However, with the adoption of the Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System (Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System), this problem was resolved: the provision of MLPS and CII modes was assigned to the Ministry of Public Security, which allows us to speak about the strengthening of its position in the institutional mechanism for ensuring the security of CII: its area of responsibility covers measures to protect CII, as well as standards for verification and certification of network products and services used in CII networks.

The Cyberspace Administration of China is mandated to regulate security reviews of information and communications technology products and services in the supply chain. In addition, the Cyberspace Administration of China leads a high-level interagency cybersecurity review body composed of eleven ministries and agencies: the National Development and Reform Commission; the Ministry of Industry and Information Technology; the Ministry of Public Security; the Ministry of National Security; the Ministry of Commerce, and the Ministry of Industry and Information Technology; the Ministry of Security; the Ministry of Commerce; and the Ministry of Industry and Information Technology (the State Cryptography Administration).

These Guiding Opinions clarify the authority of the Ministry of Public Security to form and implement the CII security protection system. Specifically, Section III empowers public safety authorities to direct and oversee the security work of CII by organizing the designation of CII processes.

The so-called defence departments are the departments of government regulators responsible for cybersecurity in important sectors and areas (public telecommunications and information services, energy, transport, plumbing, finance, public services, e-government); they should formulate rules for determining the CII for their sectors and areas and report on them to the Ministry of Public Security for registration purposes. Defence departments are responsible for organizing the designation of CII within their sector or area and are required to promptly notify the relevant CII operators of the identification results and report them to the Ministry of Public Security. In the event of any changes in the structure and quality of CII facilities, the operators are obliged to inform the protection departments of the relevant regulators, who will notify the Ministry of Public Security.

The Ministry of Public Security is responsible for developing and planning CII security measures at the highest, national level. Defence departments are responsible for organizing CII protection efforts in their sectors and areas of activity, based on the requirements of national cybersecurity laws and regulations, as well as relevant standards and regulations: formulate and implement overall CII security plans, protection policies for their sectors or areas and also fulfil responsibilities for the leadership and oversight of cybersecurity in their sectors or areas. CII operators are responsible for setting up dedicated security controls, organizing and conducting the work to protect the CII security, and the main responsible person has overall responsibility for protecting the CII security in the relevant work unit.

Conclusions

Summing up the results of our research, we consider it important to note the following. Ensuring the security for the critical information infrastructure in the Russian Federation and in the People's Republic of China is determined by a special normative act of the highest order, i.e. the relevant laws. The Russian law directly establishes the list of CII sectors, while the list of CII sectors in the Chinese law is expanded by the inclusion of new sectors by the relevant by-laws, which indicates the growing role of standards adopted by the responsible authorities, in particular, the Cyberspace Administration of the PRC, the Ministry of Industry and Information Technology of the PRC, and the Ministry of Public Security of the PRC. A similar

situation is observed with respect to authorized government bodies: the Russian law contains such a list with the distribution of powers between them in the field of security of the CII, while there are no such norms in the Chinese law.

Despite the multitude of existing and emerging sources of legal regulation of critical information infrastructure, the regulatory mechanism for ensuring its security is interconnected and reflects the general nature of China's digital policy regime. The PRC's Cybersecurity Law establishes general norms, its by-laws, in turn, establish special norms, and standards contain high-tech methodological recommendations that can clarify the possible ambiguity of general and specific norms. The institutional mechanism is represented by state bodies of general and special competence, but there is a problem of partial duplication of powers.

In the PRC, the establishment of a mechanism for ensuring the security of critical information infrastructure has not yet been completed and is complicated by the need to simultaneously achieve goals in the spheres of national security and economy, in particular, when confronting the negotiations with the United States, promoting the policy of economic expansion in the Chinese market, using tariff and non-tariff measures. This approach to the formation of a national mechanism must be borrowed by Russia as well, since economic factors radically affect the national security of the state.

References

Creemers, R., Triolo, P., Lu, X., Webster, G. (2020). Chinese Government Clarifies Cybersecurity Authorities [translation]. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-government-clarifies-cybersecurity-authorities-translation/

Critical Information Infrastructure Security Protection Regulations (opinion-seeking draft) [translation]. Retrieved from https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/

Critical information infrastructure. Federal Service for Technical and Export Control. Retrieved from https://fstec.ru/normotvorcheskaya/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury (retrieved on 19.04.2021)

Cyber Security Review Measures (网络安全审查办法). Retrieved from http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

Cybersecurity Law of the People's Republic of China: Order №53 of the President, 11/07/2016

Ella Gorian (2020). Genesis of Russian cyber security legal mechanism: an authentic or a trend alike model?. In Denis B. Solovev (ed.): Smart Technologies and Innovations in Design for Control of Technological Processes and Objects: Proceeding of the International Science and Technology Conference "FarEastCon-2019". Cham: Springer, pp. 937-949

Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System (贯彻落实网络安全等级保护

制度和关键信息基础设施安全保护制度的指导意见). Retrieved from https://www.mps.gov.cn/n6557558/c7369310/content.html.
Issues of the Federal Service for Technical and Export Control: Decree of the President of the Russian Federation dated 16 August, 2004 No. 1085.
Lu, X. (2018). Scoping Critical Information Infrastructure in China: CII is a major policy challenge in implementing Xi Jinping's cybersecurity strategy. Retrieved from https://thediplomat.com/2018/05/scoping-critical-information-infrastructure-in-china/
National Cyber Security Inspection Operation Guide (国家网络安全检查操作指南). Retrieved from https://wlzx.hebtu.edu.cn/resources/43/20161027101045853.doc
On amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection": Federal Law dated 01.05.2019 No. 90-FZ
On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation: Decree of the President of the Russian Federation dated 22 December, 2017 No. 620.
On the National Coordination Centre for Computer Incidents (together with the Regulations on the National Coordination Centre for Computer Incidents): order of the FSB of Russia dated 24 July, 2018 No. 366.
Webster, G., Sacks, S., & Triolo, P. (2019). Three Chinese Digital Economy Policies at Stake in the U.S.–China Talks. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/
Wei, L., & Davis, B. (2019). U.S. Trade Negotiators Take Aim at China's Cybersecurity Law. Retrieved from https://www.wsj.com/articles/u-s-trade-negotiators-take-aim-at-chinas-cybersecurity-law-11553867916