



EUROPEAN
UNIVERSITY
R. M A C E D O N I A

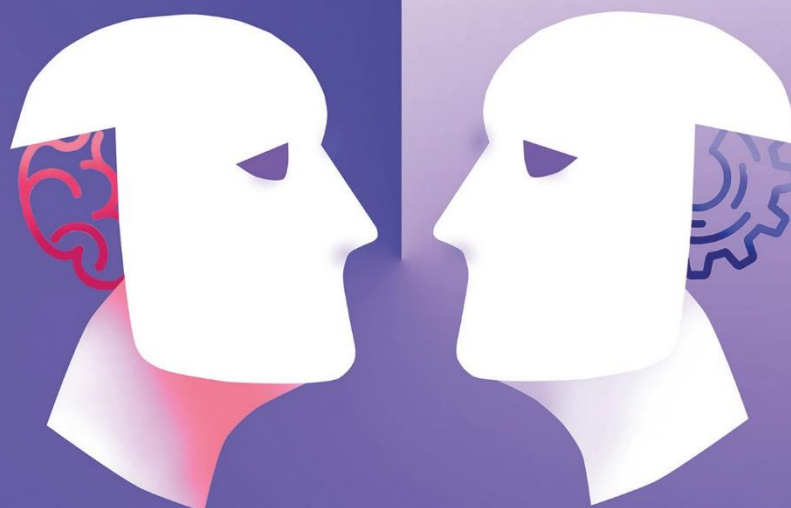
UDC 33

ISSN: 2545-4552 (Print)
ISSN: 2545-4560 (Online)

IDEA

International Journal *of Science and Arts*

ИДЕЈА Меѓународно списание за наука и уметност



IDEA Int. J. Sci. Arts
ИДЕЈА Меѓунар. Спис. Наук. Умет.

VOL.
ГОД. **2**

No.
Број **4**

pp.
стр. **1 - 202**

Skopje
Скопје **2018**

IDEA

**International Journal
of Science and Arts**

ИДЕЈА Меѓународно списание за наука и уметност

IDEA Int. J. Sci. Arts ИДЕЈА Меѓунар. Спис. Наук. Умет.	VOL. Изд. 2	NO. Број. 4	pp. стр. 1-202	Skopje Скопје 2018
--	-------------------------------------	-------------------------------------	--	--

/

International Journal of Science and Arts – IDEA
Меѓународно списание за наука и уметност – ИДЕЈА

Publisher

European University – Republic of Macedonia

About the publisher

Prof. Bojo Andreski, PhD, EURM (Macedonia)

INTERNATIONAL EDITORIAL BOARD

Prof. Stojanka Maneva-Chuposka, PhD, Chancellor, EURM (Macedonia);

Assoc. Prof. Biljana Andreska Bogdanovska, PhD, Faculty of Economics, EURM (Macedonia); Prof. Lidija Naumovska, PhD, Faculty of Economics, EURM (Macedonia); Prof. Savica Dimitrieska, PhD Faculty of Economics, EURM (Macedonia); Prof. Elizabeta Stamevska, PhD Faculty of Economics, EURM (Macedonia); Ognyana Stoichkova, PhD, Faculty of Economics, University of finance, business and entrepreneurship, Sofia (Bulgaria); Assoc. Prof. Yakim Kitanov, PhD, Faculty of Economics, University of finance, business and entrepreneurship, Sofia (Bulgaria); Assist. Prof. Virginiya Zhelyazkova, PhD, Faculty of Economics, University of finance, business and entrepreneurship, Sofia (Bulgaria); Assist. Prof. Dinka Zlateva, PhD South-West University "Neofit Rilski", Faculty of Economics, Blagoevgrad (Bulgaria); Prof. Zdravko Špirić, PhD Green infrastructure Ltd., Zagreb (Croatia); Prof. Mile Matijević, PhD Faculty of Legal Sciences, University of Business Studies, Banja Luka (Bosnia and Hercegovina); Prof. Slobodan Sajnovski, PhD, Faculty of Law, EURM (Macedonia); Prof. Zeljko Bratulovic, PhD, Department of History of Law and State, University of Rijeka (Croatia); Assist. Prof. Zeynep Ece Ünsal, PhD, Başkent University- Ankara (Turkey); Assist. Prof. Abdullah İslamoğlu, PhD, İstanbul University – İstanbul (Turkey); Prof. Atanas Kozarev, PhD, Faculty of Detectives and Criminology, EURM (Macedonia); Assist. Prof. Žarko Čulibrk, PhD, Faculty of Security and Protection, Banja Luka, Republic of Srpska (Bosnia and Hercegovina); Prof. Zdravko Skakavac, PhD, Faculty for Legal and Business Studies dr. Lazar Vrkatić, Novi Sad, Union University, Belgrade (Serbia); Prof. Ljubo Pejanovic, PhD, Faculty of Law and Business Studies dr. Lazar Vrkatić, Novi Sad, University Union, Belgrade (Serbia); Prof. Boris N. Krshev, PhD Faculty for Law and Business Studies Dr. Lazar Vrkatic, Novi Sad (Serbia); Prof. Miroslav Milutinović, PhD, College of Professional Studies of Traffic Management, Niš (Serbia); Eneko Sanz, PhD Band Research, Barselona (Spain); Prof. Gordana Vrencoska, PhD, Faculty of Art and Design, EURM (Macedonia); Prof. Marina Kocareva Ranisavljev, M.Sc. School of Textile Design, Technology, and Management, DTM, Belgrade (Serbia); Prof. Vlado Vankovski, Faculty of dentistry, EURM (Macedonia); Prof. Pietro Zecca, PhD University of Florence, Department of Mathematics and Computer Science "Ulisse Dini" (DIMAI) (Italy); Assist. Prof. Anis Sefidanovski, PhD, Faculty of Informatics, EURM (Macedonia).

Editor-in-Chief

Assist. Prof. Anita Skrcheska, PhD, Faculty of Economics, EURM (Macedonia)

Consultant

Prof. Zivko Andreovski, PhD, Faculty of Law, EURM (Macedonia)

Technical Editor

Stefan Jakimovski, Faculty of Informatics, EURM (Macedonia)

Graphic design Editor

Prof. Gordana Vrencoska, PhD, Faculty of Art and Design, EURM (Macedonia)

Cover Illustration

Milica Mishevska

Proofreader (Macedonian)

Valentina Bacvarovska

Lenka Karadzovska

Proofreader (English)

Marija Dragovic, MA

Elena Prendjova, MA

UDC: "St. Kliment Ohridski" Library – Skopje

Copies: 50

Frequency: 2 Issues Per Year

Address

European University – Republic of Macedonia

Kliment Ohridski Blvd 68

Skopje 1000, Macedonia

Telephone: +389 2 320 2020

Fax: +389 2 320 2030

Email: idea@eurm.edu.mk

www.eurm.edu.mk

Почитувани читатели,

Како современа област во полето на информатиката, вештачката интелигенција опфаќа изградба и развивање *интелигентни машини*. Вештачката интелигенција се заснова на концепцијата дека човечката интелигенција може да биде до тој степен автоматизирана до кој ќе може да биде симулирана од страна на некоја машина. Примената на технологиите кои се засновани на вештачка интелигенција опфаќа интеракција човек – компјутер преку препознавање на лица, говор и допир; анализа на текст и генерација на природен јазик; машински платформи за учење; виртуелни агенти; хардвер оптимизиран со вештачка интелигенција; менаџмент на одлуки; биометрика; како и развој и примена на роботиката.

Овие технологии можат да придонесат кон подобрување на продуктивноста, остварување повисоко ниво на ефикасност и спроведување многу посложени истражувања со кои се внесува креативност и иновации во секојдневниот живот, што го зголемува ентузијазмот за понатамошно унапредување на секој сегмент од општеството. Наспроти ваквите ставови, многубројни истражувања и автори укажуваат дека развојот и примената на вештачката интелигенција може да придонесе кон губење на работни места и целосна замена на луѓето со роботи. Според тоа, може да се каже дека вештачката интелигенција е тема која се дискутира со огромен оптимизам но, истовремено и со определена доза на страв, кој произлегува од неизвесноста за иднината со која може да се соочи човештвото. Како што изјавил Стивен Хокинг: „Развојот на вештачката интелигенција може да биде најдоброто или најлошото нешто што ќе му се случи на човештвото“.

Имајќи ја предвид актуелноста и интригантноста на оваа проблематика, следните два броја на нашето меѓународно списание се посветени токму на истражување на развојот и примената на вештачката интелигенција, како и на проблемите и предизвиците со кои е соочена нејзината практична имплементација. Во презентираните трудови на авторите, предмет на разработка се теми поврзани со: изградба и примена на технологии засновани на вештачката интелигенција; виртуелни агенти и роботи хуманоиди; трансхуманизам и иднината на човештвото; влијанието на вештачката интелигенција врз економијата, маркетингот и човечките ресурси; социо-економски и политички димензии на примената на вештачката интелигенција; етички и правни импликации на вештачката интелигенција; дигитализација и вештачка интелигенција за идната здравствена заштита; примена на вештачката интелигенција во уметноста; ризиците од вештачката интелигенција за безбедноста; вештачка интелигенција и трансформацијата на општеството.

Се надеваме дека презентираните сознанија и заклучоци на авторите, во голема мера ќе ја доближат оваа проблематика до секој од вас, а воедно ќе претставуваат мотив и инспирација за понатамошни истражувања во оваа област.

Главен и одговорен уредник

доц. д-р Анита Скрческа

Dear readers,

Artificial intelligence, a modern field of computer science, refers to the construction and development of intelligent machines. Artificial intelligence is based on the concept that human intelligence can be automated to the extent that it can be simulated by a machine. The application of technologies based on artificial intelligence involves human-computer interaction by recognizing faces, speech and touch; text analysis and natural language generation; mechanical learning platforms; virtual agents; hardware optimized with artificial intelligence; decision-management; biometrics, as well as the development and application of robotics.

These technologies can boost productivity, increase efficiency, and refine research by introducing creativity and innovation in everyday life, and driving enthusiasm for further advancement of every segment of society. In spite of such views, a number of research studies and authors suggest that the development and application of artificial intelligence can contribute to job losses and full replacement of people. Accordingly, one can argue that artificial intelligence is a topic discussed with great optimism, but at the same time with a certain degree of fear, which stems from the uncertainty about the future of the human kind. Stephen Hawking raised this point when he stated that: "The development of artificial intelligence can be the best or worst thing that will happen to mankind."

With the urgency and intrigue of this issue in mind, the following two issues of our international journal will be dedicated precisely to researching the development and application of artificial intelligence, as well as to the problems and challenges that its practical implementation is facing. The presented works discuss topics related to: development and application of technologies based on artificial intelligence; virtual agents and robots humanoids; transhumanism and the future of mankind; the impact of artificial intelligence on the economy, marketing and human resources; socio-economic and political dimensions of the application of artificial intelligence; ethical and legal implications of artificial intelligence; digitization and artificial intelligence for future health care; application of artificial intelligence in art; the risks of artificial intelligence related to security; artificial intelligence and the transformation of society.

We hope that the presented findings and conclusions will stir up important debates and will also serve as a motivation and inspiration for further research in this area.

Assist. Prof. Anita Skrcheska, PhD, Editor-in-Chief

IDEA Int. J. Sci. Arts ИДЕЈА Меѓунар. Спис. Наук. Умет.	VOL. 2 Изд.	NO. 4 Број.	pp. 1-202 стр.	Skopje 2018 Скопје
--	------------------------------	------------------------------	---------------------------------	-------------------------------------

Содржина

ИНФОРМАТИКА

Stefan Jakimovski, Anis Sefidanoski PhD, Tanja Kaurin MSc, Borko Hristov MSc

MACHINE LEARNING FOR AN AUGMENTED ORGANIZATIONAL

AWARENESS.....9

Duc Manh Nguyen, Le Xuan Anh

COMPARISON BETWEEN HYBRID AND NATIVE APP15

Ивана Богоева, проф. д-р Зоран Гацовски, проф. д-р Ристо Христов

МЕТОДИ НА ФОРЕНЗИЧКА ИДЕНТИФИКАЦИЈА ПРЕКУ ПРЕПОЗНАВАЊЕ ОБЛИЦИ –
БИОМЕТРИЈА.....21

Дамјан Мишевски

УПОТРЕБАТА НА МОДЕЛИ НА НЕВРОНСКИ МРЕЖИ ЗА ДЛАБОКО УЧЕЊЕ ВО
АВТОМАТСКОТО ПРЕПОЗНАВАЊЕ НА ГОВОР.....35

ЕКОНОМИЈА

**Проф. д-р Билјана Андреска Богдановска, проф. д-р Митко Ивановски, Проф. д-р Лидија
Наумовска**

БИЗНИС МОДЕЛ -СПОДЕЛУВАЊЕ.....49

Проф. д-р Зоран Јолевски

ЕКОНОМСКИ ИМПЛИКАЦИИ НА AI И ИНДУСТРИЈАТА 4.0 ВРЗ КОМПАРАТИВНАТА
ПРЕДНОСТ НА НАЦИОНАЛНИТЕ

ЕКОНОМИИ.....57

Rositsa Manzurova, PhD candidate; Vesela Serafimova, PhD candidate

ARTIFICIAL INTELLIGENCE AND COMMUNICATION IN A HEALTHCARE INSTITUTION IN
BULGARIA.....65

Sonya Georgieva, PhD; Rositsa Manzurova, PhD candidate

ROBOTIC PROCESS AUTOMATION (RPA) THE EXAMPLE OF COCA-COLA HELLENIC BUSINESS
SERVICE ORGANIZATION.....71

Асс. м-р Верица Најдовска

ВЛИЈАНИЕТО НА ИНТЕРНЕТОТ ВРЗ МЕЃУНАРОДНИТЕ МАРКЕТИНГ
ПРАКТИКИ.....77

M.Sc. Tanja Krsteva

ARTIFICIAL INTELLIGENCE IN MARKETING AND

ADVERTISING.....85

М-р Кирју Николоски

ВЛИЈАНИЕТО НА ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА ВРЗ ЕКОНОМИЈАТА.....	93
--	----

БЕЗБЕДНОСТ**Проф. д-р Атанас Козарев, Д-р Роза Гурмешевиќ**

СОБИРАЊЕ НА ПОДАТОЦИ ЗА ПОЛОЖБАТА НА МАРГИНАЛИЗИРАНИТЕ ГРУПИ КАКО МОЌНА АЛАТКА ВО БОРБАТА ПРОТИВ ДИСКРИМИНАЦИЈАТА И СОЦИЈАЛНАТА ИСКЛУЧЕНОСТ.....	99
--	----

Assistant Professor Aleksandar Nacev, PhD, Professor Marjan Bogdanovski, PhD

THE USE OF ARTIFICIAL INTELLIGENCE IN THE MILITARY DOMAIN	111
---	-----

Доц. д-р Васко Стамевски, Проф. д-р Елизабета Стамевска, д-р Зоран Крстевски

СТРАВОТ ОД ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА.....	115
--	-----

Проф. д-р Ристо Христов, Јордан Ќирковиќ

ПРАВНИ АСПЕКТИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ	123
---	-----

М-р Александар Трајковски

ЕРОЗИЈА НА ПРАВОТО НА ПРИВАТНОСТ НА КОРИСНИЦИТЕ НА КОМПЈУТЕРСКИТЕ СИСТЕМИ, СОЦИЈАЛНИТЕ МРЕЖИ, МОБИЛНИТЕ УРЕДИ И КЛАУД СЕРВИСИТЕ.....	129
--	-----

Јордан Ќирковиќ

ЕТИЧКИТЕ АСПЕКТИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ	139
---	-----

Марија Трајковска

СОВРЕМЕНИ ОБЛИЦИ НА КИБЕРНЕТСКИОТ КРИМИНАЛ.....	145
---	-----

Емилија Дамчевска

САЈБЕР ТЕРОРИЗМОТ КАКО ЗАКАНА ЗА БЕЗБЕДНОСТА НА ДРЖАВАТА.....	155
---	-----

ПРАВО И ПОЛИТИКА**Доц. д-р Марјан Габеров**

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА – ЗАКАНА ИЛИ ГАРАНТ НА БЕЗБЕДНОСТА.....	163
--	-----

Д-р Роза Гурмешевиќ

КОНЦЕПТОТ НА ПОЗИТИВНА ДИСКРИМИНАЦИЈА ВО СОВРЕМЕНОТО ОПШТЕСТВО.....	169
---	-----

АРТ И ДИЗАЈН**Ass. Prof. Blagojche Naumoski, M.A**

HOW ARTIFICIAL INTELLIGENCE CHANGES HUMAN EXPERIENCE IN ART.....	179
--	-----

М-р Самоил Крстевски

ХОЛОГРАФИЈАТА КАКО ТРОДИМЕНЗИОНАЛНО НИВО НА ФОТОГРАФИЈА.....	189
--	-----

Katarzyna Utecht, PhD

TRANSFORMABLE LIVING UNIT – HOMO–CYBER–SAPIENS – IDENTITY OF PLACE AND ARCHITECTURE OF EMOTIONS	195
--	-----

MACHINE LEARNING FOR AN AUGMENTED ORGANIZATIONAL AWARENESS

UDC:004.7/.9: 005.94

*Original scientific paper***Stefan Jakimovski¹, Anis Sefidanoski PhD¹, Tanja Kaurin MSc¹, Borko Hristov MSc²,**¹*European University – Republic of Macedonia, Skopje, Macedonia*³*Euro-Balkan University, Skopje, Macedonia*

Abstract

The rapid digitization and virtualization of the community enables the integration of various communication and collaboration tools and systems, and every initiative of this kind opens up new opportunities for increased productivity and efficiency in many domains of society. Knowledge management based on machine learning (ML) and artificial intelligence (AI) is a tool already applied to many industries, and a medium that is increasingly used by many companies and organizations in order to ensure increased efficiency and productivity in the workplace. The results presented in this paper include the conceptual development of a knowledge management platform, which can be integrated into different departments and domains of collaborative work and thus contribute significantly to development of intellectual capital and increased productivity in various areas and industries.

Adequate integration of other technologies that are in sight of the ICT innovation horizon will enable full automation of the knowledge management process, maximizing the efficiency and results of the same, as well as creating innovative models for learning, training and customer support at a distance.

Keywords: *Organizational Awareness, Knowledge Management, Machine Learning, Artificial Intelligence, Big Data, Digitalization, Virtualization*

Introduction

Employees are using valuable time and information dealing with dispersed data and information silos. Spending more time trying to find information compared to actually using it, decreases productivity and efficiency. Documents, charts, multimedia, project plans, conversations are scattered all over the corporate networks systems, making them hard to access and manage. Employee involvement and user satisfaction quantification is crucial to knowledge management (KM). This paper aims to conceive a platform that will make information tangible, measurable and omnipresent in order to create 360 degree awareness of the organizational knowledge. Ubiquitous capturing, processing and dissemination of knowledge will deliver unified and continuous knowledge management experience and evolve the way organization learns and works. The proposed solution focuses on

increasing consistency of information and standardization of processes, as well as increase efficiency of accessing the specific information workers and/or customers need. Sharing and retaining knowledge as workers retire or leave the company is also one of the research targets.

In order to fulfill its vision and mission, the platform will need to autonomously identify what the employees in the organization don't know but need to know, spot the knowledge leaders, those with inherent curiosity and KM awareness, deliver knowledge via every channel and any format to match each user profile, create motivational interactive knowledge applications for different departments, business units, groups, users, and last but not least, avoid “re-inventing the wheel.”

1. Concept and methodology

In order to be able to search both internal and external information (corporate IP and 3rd party databases) with a single query, the ML platform will consolidate the organization's information assets into a single repository. Through the enhanced search and discovery options which make it easy for users to find information no matter where it originates, the right information will arrive to those who need it at the place and right time. The platform will continuously train models to proactively publish top-down qualified information, while capturing, managing and sharing knowledge from every unique issue related to the core business processes. It can use skills and experience inherited in the employees and customers for the benefit of everyone in order to apply derived knowledge at any step of the customer experience.

Encouraging users to “act on knowledge” and adding value to it by rating, editing, tagging, viewing, sharing, commenting or auditing, our proposed solution will recognize the value of employee's knowledge awareness, monitor them, audit and reward [1]. Having multiple private spaces for each team/sector/department in your organization, as well as multi-layer accessibility according to privacy and privileges policies, the platform will streamline and improve internal communications and alliances [2].

1.1 Objectives and benefits

Following is the list of some core benefits the proposed ML solution aims to deliver:

- Increase cost savings through reduction in redundancies
- Simplify tasks and improve the business process efficiencies
- Increase globalization/standardization of business practices

- Improve the ways the knowledge is shared
- Foster innovation by encouraging the free flow of ideas
- Improve customer service by streamlining response time
- Boost revenues by getting products and services to market faster
- Streamline operations and reduce costs by eliminating redundant or unnecessary processes
- Knowledge updates can be added to certain users/groups with shared interest
- Getting employees to take full advantage of resources
- Optimization of business process across entire company
- Maximization of content re-use
- Common unified interface (universal UI/GUI)
- Aggregate data from multiple sources
- Consistent communication across entire company

Access entire knowledge from the corporate contact centers and online customer self-support services

Encourage users to “act on knowledge” adding value by rating, editing, tagging, viewing, sharing, commenting or auditing

Recognize the value of employees knowledge awareness, monitor, audit and reward

Streamline and improve internal communications and alliances

Keep all users active and motivated with live actions, notifications and mobile access to the knowledge

Automated editing and processing of data

Access the entire knowledge from anywhere, whenever you need it

2. Tacit vs. implicit knowledge

This family of technologies which stand at the basis of the platform belongs to groupware and communication tools for collaboration at a distance, which enable people to be more productive and efficient by

creating virtual work environments and direct communication channels between individuals or groups [3]. The communications can be synchronous (instant messaging, chat, phone, video conferencing, etc.) and/or asynchronous (e-mail, forums, blogs, etc.). Multichanneling is another important ingredient in this set of functionalities (i.e. able to exploit several communication channels such as telematic networks, telephone networks, etc.) alongside with multimodality (access by different devices such as computers, mobile phones, smart wearable technologies, etc.) [4]. These tools are able to "channel" tacit knowledge by recreating the entire context typical of direct interactions and communication between people. Multimedia content such as textual, audio and video communications, can be captured, rendered explicit and automatically structured and classified by the artificial intelligence (AI) module as a metadata in a centralized database, using in the same time advanced machine learning algorithms for data modeling and encryption.

3. Technologies

For knowledge management to be effective, before all, we must be able to capture and incorporate in appropriate forms all preexisting and future data. Knowledge acquisition applications are intended for classifying and explicating tacit and implicit knowledge by people working in an organization where structured representation of knowledge is represented in document sets dispersed throughout the corporate network [5]. Knowledge acquisition can be defined as the set of methods and techniques used by "knowledge engineers" to extract knowledge from experts, texts, technical manuals, correspondence, to the end of transferring it to a centralized knowledge base that is comprehensible and accessible both by users and software systems.

These technologies are one of the focal points in building knowledge management platforms and systems, representing the bottleneck of all knowledge management applications [6]. That is because traditionally the process of acquiring knowledge has always been a manual process, expensive both in terms of time and human resources, as well as subject to individual interpretations. The solution should oriented towards achieving semi-automatic tools that can produce minimization of the cost for knowledge acquisition activities and increasing the objectivity in representation of knowledge across different domain (i.e. tools that automatically translate text using voice recognition, generating narrative stories and offers on expert's level, brain storming sessions for the purpose of decision making, etc.).

The proposed platform implements knowledge acquisition systems that allow you to speed up the process of knowledge modeling, classifying corporate knowledge and making semi-automatic the acquisition of new knowledge (whether it is a new instance of an already known concept or an entirely new concept) [7]. Knowledge, once acquired, can be converted into various forms which can be handled by different software applications either by users or directly from other systems within or outside the corporate network.

3.1. Document and content management

Knowledge management contained in textual documents is one of the most popular issues in many organizations. In the proposed solution this problem is addressed through the family of the technologies identified by the name of document and content management. Different tools for document and content management provide storage, retention, classification, publishing and distribution of documents and content based on algorithmic and information retrieval techniques, ontology-based retrieval, adaptive user profiling, natural language processing and multimedia mining. The structural component of intellectual capital depends heavily on semi-structured and unstructured knowledge: the ability to access in a smart way those knowledge sources of strategic value for the organization [8].

Conclusion

Thanks to the latest technological developments in information and communication technologies, today we have the opportunity to realize sophisticated knowledge management platforms in order to maximize the productivity and benefits of collaborative work and decision making. The synergy of the major representatives of the state of the art emerging technologies, i.e. artificial intelligence, big data, machine learning, natural language processing and predictive analytics, combined with the power of the new communication paradigms and interaction styles, represent the foundation of the development platform that is the subject of scientific and practical research of this project.

Bibliography

1. Etzioni, Amitai; Etzioni, Oren (2016). "AI Assisted Ethics". Ethics and Information Technology
2. Rotolo, D., Hicks, D., Martin, B. R. (2015) What is an emerging technology? Research Policy
3. Beyerlein, M; Freedman, S.; McGee, G.; Moran, L. (2002). Beyond Teams: Building the Collaborative Organization. The Collaborative Work Systems series, Wiley
4. Marcus, Aaron (2015). Design, User Experience, and Usability: Design Discourse
5. Aparicio, M and Costa, C. (2012) Collaborative systems: characteristics and features. In Proceedings of the 30th ACM international conference on Design of communication (SIGDOC '12). ACM, New York, NY, USA
6. Atamturktur, S., Hemez, F., Williams, B., Tome, C., and Unal, C., (2011), "A Forecasting Metric for Predictive Modeling," Computers and Structures (Elsevier)
7. E. Winsberg, Science in the Age of Computer Simulation. Chicago: University of Chicago Press, 2010
8. Courts, B., & Tucker, J. (2012). Using Technology To Create A Dynamic Classroom Experience. Journal of College Teaching & Learning

COMPARISON BETWEEN HYBRID AND NATIVE APP

UDC: 004.438'22:004.439'23

Original scientific paper

Duc Manh Nguyen, Le Xuan Anh

UIST "St. Paul the Apostle" Ohrid, Macedonia

Abstract

This research paper aims to compare native and hybrid application development. The comparative study is based on the advantages and disadvantages between Native and Hybrid Apps. In order to determine which one is the best way of producing an app, this paper introduces the hybrid app paradigm, and analyzes the pros and cons of both paradigms in theory and experiment.

Keywords: *Native apps, hybrid apps, mobile app development, cross-platform web app.*

Introduction

Features and options offered by smartphones through mobile applications are immense. Nowadays, application development for smart devices is an evolving field with great economic and scientific interest. According to Gartner [1] the total number of mobile app store downloads worldwide will increase to 81 billion in 2013, paid downloads will surpass 8 billion and free download 73 billion. The count of mobile apps that are being developed and released into the market increases exponentially by the day [2].

Mobile applications were created for information purposes and productivity, such as electronic mail, calendar and similar, but their diversity and number have increased enormously in the past couple of years [3]. There are three categories of mobile applications: native, web, and hybrid. The choice of the appropriate one depends on the requirements that need to be met [4].

The ultimate goal of cross-platform mobile app development is to achieve native app performance and run on as many platforms as possible. This paper aims at investigating those issues.

Back in the early days of mobile, there was only one way to give users the performance and features they expected. One had to use a native SDK.

Meanwhile, demand for mobile experiences has grown exponentially. By 2022, 70% of all enterprise software interactions are expected to occur on mobile device [5].

1. Native App

These apps are developed exclusively for a platform, and take full advantage of the operating system features and other software that are typically installed on the platform [6]- they can use the cameras , the GPS, the accelerometers, the compass, the list of contacts, battery icon and so on.

Considering the fact that in application development on different platforms one must use different programming languages, expenses of developing it are often higher. However, despite the aforementioned disadvantages, native application offers by far the best usability, features and overall user experience [7].

Development of native mobile applications can be tedious, in the sense that the entire codebase has to be re-written to target a different platform and users, despite having the same business use-case and logic [8].

2. Hybrid app

These apps are developed using multi-platform web technologies, such as HTML5, CSS3 and JavaScript. They are partly native apps that run on the device, inside a native container and device's browser engine to render the HTML and process the JavaScript locally [9]

Hybrid apps are essentially native apps. They are downloaded from a platform's app store or marketplace, and access the same native feature and hardware-based performance acceleration as any app built with a native SDK [5].

Hybrid apps try to combine the advantages of web and native apps. Hybrid apps are primarily built using HTML5 and JavaScript, and a detailed knowledge of the target platform is not required.

Hybrid apps run in a full-screen browser, called a web view that is invisible to the user. The key difference is that hybrid apps are built using open web technologies like JavaScript, HTML, and CSS, rather than the proprietary or specialized languages used by iOS, Android, and other.

The code implementation of the hybrid apps can be done using various technologies and development platforms but in order to achieve a native look and feel it is necessary to use specific development libraries, such as JQuery [10][11].

3. Comparing Hybrid vs. Native

Table1. An explanation of How Native and Hybrid Apps presumably address key Characteristics of Apps Usage and Development [12]

	Native App	Hybrid App
Skills/tools that needed for cross-platform apps development	• Objective –C • C++ • Java • VB.net • C#	• HTML • JavaScript • CSS • Web programming languages • Mobile development frameworks
Apps needed to reach all major smartphone platform	4	1
Installed on device?	Yes	Yes
Distribution	App Store/Market	App Store/Market
Mobile Device integration	Full integration: for example (camera, microphone, GPS, file upload, contact list)	Full integration: for example (camera, microphone, GPS, file upload, contact list)
Best used for	• Highly graphical apps • Apps that need to reach the large consumer audience	• Cross-platform apps that need to full devices access. • Business apps that need to app store distributions

There are pros and cons for both Native and Hybrid apps [13]

A. Why Native development

1. Performance

Build using main device's native language, and installed on the devices itself, native apps offer the best graphics and animations. Native code is still faster than JavaScript and HTML. If a business needs highly graphical applications, such as a game, native apps are their best option.

2. App store distribution

Using native SDKs allow the developer to access the latest features specifically designed for those platform, without the complexity of dealing with native plugins.

3. No third-party dependencies (Device integration)

Native apps are providing full access to the device's hardware, such as its GPS sensor, contact list, camera and so on.

B. Disadvantages of Native Development**1. Platform instability**

The mobile platforms landscape is notoriously unstable.

2. High development cost and time-consuming

The cost rises exponentially over when developing cross-platform native applications. If we try to building native apps for more than one platform, the time requirements rise depending on the number of developers needed and applications complexity. Development time requires more for native apps.

3. Limited control, Native talent difficult to find.**C. Why Hybrid Development****1. One for all**

With a hybrid framework like Ionic, you can run your app on any platform or device, all from a single codebase. Like a native apps, hybrid apps are also installed on the device and launched like a typical application. That mean the users get a great experience across platforms and devices. The code implementation of the hybrid apps can be done using various technologies and development platforms but in order to achieve a native look and feel it is necessary to use specific development libraries, such as JQuery [11][14].

2. Limited developers

According to the 2017 Stack Overflow Survey, only 6, 5% of all developers cited Swift and Objective-C as familiar languages. In contrast, web developers made up 72, 6% of respondents, and JavaScript appeared as the most commonly used programing languages in the survey [15].

3. Device integration, Inexpensive cross-platform development

Hybrid apps offer full device access, including the "native-only" features on mobile apps, like camera, microphone, and address book. Building a cross-platform hybrid app is considerably cheaper than building a cross-platform native app.

4. Future apps

Future applications will be run on growing number and diversity of platforms oriented around the web: wearables, IoT devices, asset tracking systems.

D. Disadvantages of Hybrid Development**1. Limited graphics, Systems overhead**

Hybrid apps offer the same graphical abilities as mobile web apps.

The use of the web view may introduce a degree of overhead compared to native.

2. Requires familiarity with mobile framework

While still simpler than the native apps development, the hybrid approach adds a level of complexity to the mobile web apps development process, as the developers must familiarize themselves with a hybrid frameworks.

4. Artificial Intelligence and Interactive Entertainment

Artificial Intelligence is a relatively new area of computer science involving the development of computer systems that perform and respond like human beings. Some of the activities for which computers with AI are encompassing are: speech recognition, learning, planning and problem-solving. It also can imitate human voice and recognize it, translate from one language to another, make decisions, perceive and recognize objects or remember information.

Nowadays, AI in mobile applications is becoming more and more popular. It's a part of the mainstream, with its innovations include in almost every modern device. AI and machine learning both are causing an extraordinary change in the way that engineers, organizations, and clients consider modeling algorithms and intelligent communications with applications.

The idea of AI portrays computer systems performing tasks or jobs that would normally require a human to finish. One of the major advantages of AI for mobile application development organizations is their capacity to perform and finish tedious jobs that would have generally been excessively exhausting for people. A great majority of energies invested in this process are concentrated on enhancing user experience. More intelligent applications are being developed with the help of AI algorithms thanks to technologies like natural language processing, and speech recognition. With this idea focused on mobile app technology, user interface elements of any mobile app must be immersive, interactive and intuitive. AI achieves this purpose, all so intelligently.

5. Artificial Intelligence in mobile apps

Artificial Intelligence is a relatively new area of computer science involving the development of computer systems that perform and respond like human beings. Some of the activities for which computers with AI are encompassing: speech recognition, learning, planning and problem-solving. It also can imitating human voice and recognizing it, translating from one language to another, making decisions, perceiving and recognizing objects or remembering information.

More and more businesses want their mobile apps to be developed with the use of this technology as they improved user-friendliness, are more interactive and thus more interesting for customers. AI machines are particularly imperative in fields that require a high level of exactness and accuracy. AI helps to complete monotonous work quickly: when such tasks are performed using artificial intelligence, mobile app Development Company can actually concentrate on the more significant tasks, pour some innovative input into the app and solve some real-time app development difficulties.

AI is also applied in apps with automated reasoning. This gives mobile applications the ability to solve very complicated problems. AI's learning algorithms are a way more effective marketing tool than for example manual e-mail sending to potential customers.

Conclusion

Thus, each application has its own advantages and disadvantages. We should choose the right kind of application to build our application. With the worldwide programming trend, mobile applications are becoming more powerful than ever.

This article helps you distinguish each type of application with the advantages and disadvantages that are used best. Hope you can distinguish between the Web app, Native app and Hybrid app. From there, you can choose the technology that meets the specification requirements to develop your application quickly and save time.

Bibliography

- [1] Gartner. Gartner Says Free Apps Will Account for Nearly 90 Percent of Total Mobile App Store Downloads in 2012, (2012). Available online at: <http://www.gartner.com/newsroom/id/2153215>, (last access on February 26, 2013).
- [2] Pavel Smutny, "Mobile development tools and cross – platform solutions", Carpathian Control Conference (ICCC), 2012
- [3] V. N Inukollu, D. D Keshamoni, T. Kang and M. Inukollu, "Factors influencing quality of mobile apps: role of mobile app development life cycle," International Journal of Software Engineering
- [4] N. Litayem, B. Dhupia and S. Ruhab, "Review of cross-platforms for mobile learning application development," International Journal of Advanced Computer Science and Application, vol. 6, pp. 31-39, 2015.
- [5] Ionic_HybridNative_eBook_Jan_2018_v8.pdf
- [6] Pooja Jardosh, Lipi Kothari, "A Comprehensive Survey: Techniques for Mobile Development Cross Platform", IJEDR, Vol. 5 Issue 2, 2017
- [7] Z. Ćović, D. Babić, "Development and implementation of location based native mobile application," International journal of electrical and computer engineering systems, vol. 5, pp. 27-31, 2014.
- [8] <http://blog.techmagic.co/native-vs-hybrid-apps/> Native vs Hybrid Apps. What to choose in 2017?
- [9] Pooja Jardosh, Lipi Kothari, "A Comprehensive Survey: Techniques for Mobile Development Cross
- [10] Mansfield-Devine, S. 2010. Divide and conquer: the threats posed by hybrid apps and HTML 5. Network Security, 2010(3), 4-6
- [11] jQuery Foundation. jQuery write less, do more. Available online at: <http://jquery.com/>, (last access on March 23, 2013).
- [12] Native vs Hybrid Apps K. More, M. Chandran "International Journal of Current Trends in Engineering & Research (IJCTER)" , 2016
- [13] <https://impekable.com/native-vs-hybrid-mobile-app-development/> Creating Top Apps: The pros and cons of Native vs Hybrid Mobile App Development
- [14] jQuery Foundation. jQuery write less, do more. Available online at: <http://jquery.com/>, (last access on March 23, 2013).
- [14] Mansfield-Devine, S. 2010. Divide and conquer: the threats posed by hybrid apps and HTML 5. Network Security, 2010(3),
- [15] Ionic Blog – July 2017 "In-House Teams and Talent Rising to the Challenge"

МЕТОДИ НА ФОРЕНЗИЧКА ИДЕНТИФИКАЦИЈА ПРЕКУ ПРЕПОЗНАВАЊЕ ОБЛИЦИ – БИОМЕТРИЈА

UDC: 004.7/9.056:57.081.1

Стручен Труд

Ивана Богоева, проф. д-р Зоран Гацовски, проф. д-р Ристо Христов*Европски Универзитет Република Македонија - Скопје*

Апстракт

Биометријата е дисциплина која со развојот на науката, а пред сè на дигитално-информациските технологии, добива значајно место во различните области на општествениот живот, човековата работа и интересите. Па така, биометријата сè повеќе наоѓа примена во областите на медицинската дијагностика (пред сè испитување татковство, роднински врски), приватна заштита, контрола на движењето на одредени јавни простори (автентикација), идентификација на лица, како што се изборна контрола, идентификација при преминување од една држава во друга, контрола на аеродроми итн. Биометријата, распознавањето засновано на различните црти на личноста има сè поголеми шанси да стане незаменлив дел на секој систем за идентификација.

Овој труд ги презентира можностите за користење на биометријата за криминални истражувања. Односно, нагласено е дека постојат три аспекти на биометријата - криминолошките достигнувања во криминологијата. Првиот е областа на биометриска идентификација, вториот е област на патолошка идентификација, а третиот е област кога биометриските карактеристики се користат со помалку диференцијални вредности во откривањето - когнитивниот дел од кривичната истрага.

Информациските системи и биометријата се тесно поврзани. Безбедноста на информациите е исклучително важна за зачувување на анонимноста на податоците, а се состои од пет области: физичко обезбедување; безбедност на податоците; деловна соработка; безбедносна проверка; и сигурност на информативниот систем.

Заклучните размислувања во овој труд се и перцепциите на корисниците за биометриските технологии, односно како некои од спроведените истражувања покажуваат колку корисници денес имаат доверба во модерната технологија на биометриската технологија за препознавање.

Клучни зборови: *биометрија, биометриска идентификација, приватност, безбедност*

METHOD OF FORENSIC IDENTIFICATION THROUGH PATTERN RECOGNITION – BIOMETRICS

Abstract

The biometry is a discipline which in fact of the science development, especially of digital-informatics technologies, receiving significant part of various social live areas, human work and interests. In fact of this biometry is increasingly applied in medicine diagnostics (especially parent examination, family relationships), private protection, motion control in public areas (authentication), person identification, like election control, state border crossing identification, airport control etc.

The biometry, the recognition based of different traits of personality, have chance to become an irreplaceable part for every identification system.

This science work has presented the possibility of biometrics use in favor of criminal investigations. Therefore like it is enched in this science work there are tree aspects of biometrics - criminological research of criminology. The first one is the area of biometrics identification, the second one is the area of pathological identification and the third one is area where the biometrics characteristics have been used with less differential values in the detection.

The informatics systems and biometry are closely related. The security of the information is especially important for preserving the anonymity of the data, and it is consist of five areas: physical security, data security, business cooperation, security check and information system security.

The conclusions of this science work are the perceptions of the clients for biometrics technologies, is some of investigations indicate the fact that the costumers have confidence in the modern technology.

Keywords:*biometrics, biometric, identification, privacy, security*

1. Вовед

Биометријата претставува фантастично научно и инженерско подрачје, кое користи знаења од различни подрачја како математичка статистика, форензика, психологија, безбедност, криминалистика и сл.

Биометријата е млада наука иако има дамнешни почетоци. Посериозни биометриски истражувања се започнати да се вршат во 60-тите години на минатиот век. Од средината на 90-тите години на минатиот век биометријата значително се применува во пракса.

Биометрија (грч. *bios* - живот, *metrikos* - мерка) претставува збир на автоматски методи за единствено препознавање на луѓе врз основа на една или повеќе од нивните физички карактеристики и однесувања.

Во информатичката технологија, биометриската автентикација се однесува на технологиите кои ги мерат и анализираат физичките (отпечатоци од прсти, очна рожница, препознавање на лице, итн.) и

карактеристики на однесувањето (ракопис, пишување, одење, итн.) на човекот. Иако биометријата првенствено се користи за проверка на автентичност, истото се применува и во други области, како што се препознавање на говорот на корисникот за цел побрзо пишување.

Биометријата комбинира употреба на специјални уреди кои следат одредени физички или однесувачки карактеристики при што ги анализираат добиените информации. Ова се составните елементи на биометријата - земање мостри (конвертирање на аналогни сигнали во дигитални), како и вештачка интелигенција.

Добиените информации се обработуваат во компјутерот, се креира вештачка интелигенција, компјутерот ги препознава примероците и ги споредува. Целта е да се користи компјутерски систем како агент за земање примероци, додека пак софтверскиот пакет ја донесува одлуката што да прави со дигитализираните примероци. Ова го вклучува целокупниот процес на дигитализација, препознавање примерок, вештачка интелигенција. Со други зборови се користат биометриски сензори и различни алгоритми за управување со биометриските податоци прочитани преку сензорот на компјутерскиот систем. Сите биометриски технологии имаат нешто заедничко, а тоа е процесот влез на податоци, обработка на податоците и излез на податоците.

Биометриските методи за идентификација стануваат сè попопуларни. Има голем број начини за пробивање на лозинка, но обидот да се лажира нешто што лицето го презентира е многу поголем предизвик и токму тоа е причината за популарноста на биометриските методи.

2. Биометрија

Биометријата е иновативна технологија која станува сè повеќе и повеќе присутна во сферите на човечкиот живот. Современите времиња ги отворија вратите за овој тип на технологија и нејзиниот развој и важност растат насекаде секој ден. Луѓето се соочуваат со зголемени закани како што се тероризам, напад, закани, кражба и кражба на идентитет. Затоа, потребата за социјална и лична безбедност се зголемува. Луѓето сакаат да ги заштитат своите имот, предмети, финансии, податоци и својата сигурност. Неопходно е да се заштитат личните компјутери, лаптопи, паметни телефони и активности на интернет. Исто така, луѓето сакаат да ги заштитат своите возила, машини и други вредни предмети од неовластен пристап или употреба. Во областа на финансии има за цел да спречи кражба и фалсификување, а во областите на зголемена безбедност, целта е да се направи дозвола на пристап до работни места исклучиво на овластени лица (на пр. воени подрачја). За успешно обезбедување на социјална и лична заштита потребна е потврда на идентитетот на личноста преку документи, како што се возачки дозволи, лични карти и картички за здравствено осигурување.

Исто така, потребно е да се одржи контролата на летање. Биометриските технологии покажаа извонредна висока ефикасност и сигурност во одржувањето на безбедноста во овие области и сфери на човечкиот живот.

Традиционалните технологии базирани на знаења и материјални поседи не можат да бидат функционални како биометриските технологии.

Биометријата првенствено е наменета за подобрување на безбедноста, но природата на таквите податоци може да открие повеќе информации отколку што е потребно. Иако бројните истражувања во оваа област на биометријата донесоа предлози за заштита на приватноста, сè уште има јаз што се однесува на приватноста во оваа релативно млада област. Основните принципи за заштита на квалитетот на податоците се решаваат на начин податоците да се минимизираат, дека податоците се точни и целосни, дека постои консензус, транспарентност, доверливост и безбедност. Барањата за приватност и безбедност секако се вклучени во рана фаза на дизајнирање на биометриските системи.

Терминот биометрија¹ потекнува од грчкиот збор *bios* што значи живот и *metrikos* (грч. збор) што значи мерка.

Биометријата е наука за препознавање на поединецот која се базира на идентификување на однесувањето и биолошките карактеристики на лицето како што се отпечатоци од прсти, глас, одење, лице, ирис и слично. Можеме да кажеме дека биометријата ги користи физичките и биолошките карактеристики на лицето заради идентификација на лицата. Се разбира, важно е да се истакне дека станува збор за мерење на карактеристиките на луѓето.

Биометриска карактеристика може да биде секое човечко однесување и физички и психолошки особини сè додека тие ги задоволуваат барањата на уникатност, универзалност, трајност и можности за собирање.

Единственоста значи дека две лица во светот треба да бидат различни во однос на овие карактеристики.

Универзалноста значи дека оваа карактеристика мора да биде присутна кај сите лица.

Карактеристиките на стабилност значат дека тие не треба да се менуваат со текот на времето.

И, се разбира, **способноста за собирање** значи дека овие карактеристики се квантитативно мерливи.

Биометријата целосно се потпира на тоа која е личноста и што е, и што таа личност прави, а не на она што личноста го знае, на пример лозинка, или она што го поседува како лична карта. Нејзината предност е што може да ја дополни или целосно замени постоечката технологија, а дури и во моментот во некои технологии таа е единствениот одржлив пристап за лична идентификација.

Кога станува збор за биометриски и биометриски методи за идентификација постојат две противречни групи на автори кои претставуваат различни точки на гледање. Едната група мисли дека сите методи се биометриски идентификатори, а овие се сите класични методи применети во дигиталната средина, додека другата група смета дека современите технолошки можности ја олеснуваат примената на класични методи за идентификација, но и развој на нови.

Биометријата е далеку посигурна од традиционалната технологија за препознавање.

Традиционалните технологии за препознавање се базираат на корисничко знаење (ПИН, лозинка) или на она што корисникот физички го поседува (клуч, картичка). Ако се користат лозинки, се

¹ Usp. Uddin, Jasmin. Matrix of Biometrics // Biometrics, 2016, str. 1. URL: https://www.researchgate.net/publication/301542522_Matrix_of_Biometrics (2016-06-25)

препорачува тие често да се менуваат и да се користат различни лозинки за различни области кои повеќето луѓе не ги практикуваат.

Биометријата (Biometrics) претставува автоматска идентификација на лица врз основа на нивните физиолошки, биолошки карактеристики или карактеристики на нивните однесувања.

Биометриска карактеристика (Biometric)² е мерлива физиолошка, биолошка карактеристика или карактеристика на однесување која се користи за препознавање на лица. Биометриски карактеристики: секое лице треба да биде доволно различно во различни луѓе, да остане постојано односно да поседува постојани карактеристики во одредено време, мора да бидат мерливи квантитативно не само описно.

Биометриски систем (eng. biometric system) е комплетен систем за автентикација на лица. Се состои од интегриран хардвер и софтвер кој се користи за биометриско земање примероци, биометриска верификација, идентификација и враќање на резултати³.

Биометрискиот модалитет (eng. modality) е тип на биометриска карактеристика. На пример, три се вообичаени биометриски модалитети: лице, отпечаток од прсти, глас.

Мултибиометрија претставува автоматска идентификација на лица врз основа на две или повеќе биометриски карактеристики. Овие карактеристики можат да бидат карактеристики кои припаѓаат на исти биометриски модалитети како, на пример, два отпечатока на прсти или комбинација од повеќе модалитети, како отпечаток од прст и биометрика на лице.

Мултибиометријата има две главни предности во однос на поединечната биометрија. Прво, може да се примени на лица со посебни потреби кои немаат специфична карактеристика, второ да се намалат грешките при верификација и идентификација.

Примерок (eng. sample)⁴ е примерок, инстанца, мостра на кориснички биометриски карактеристики, собрани со помош на сензор.

Примероците се непреработени дигитални податоци. Примерокот може да се конвертира во (биометриски) или може да се поврзе со дефинирање за верификација или идентификација.

Шаблон (eng. template) е конвертиран и компактен биометриски модел, складиран во дигитална форма, и е креиран за време на процесот на земање на биометриските примероци.

Резултат од споредбата (eng. match score) е нумеричка вредност која го претставува степенот на сличност на два биометриски примероци (т.е. тековен примерок и образецот, шаблонот). Врз основа на резултатот на споредба и стандардни прагови (eng. threshold) се донесува одлука (eng. match decision) за прифаќање или неодобрување. На пр. ако е резултатот од споредбата 50 а прагот е 40, одлуката за прифаќање на примерокот важи како валидна (прифатено е дека тоа е лицето кое го дало моделот). При прифаќање или отфрлање, можни се две грешки: отфрлете го вистинското лице или прифатете го погрешното. Право е да го прифатиме вистинското лице и да го отфрлиме погрешното.

² Dunstone, T. i Yager N. (2009): Biometric System and Data Analysis, Springer, New York

³ Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. str. 1
URL: <https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf> (2016-06-25)

⁴ Dunstone, T. i Yager N. (2009): Biometric System and Data Analysis, Springer, New York

Идеалниот биометриски систем секогаш ќе работи без грешки. Но, не постои идеален биометриски систем, биометриските системи секогаш работат на двете споменати грешки.

Листа на кандидати (eng. candidate list) е листа која може да се добие со биометриски идентификатори (не за верификација), и е збир на шаблони чија споредба со тековниот модел дава резултати поголеми од прагот, или (алтернативно) збир на шаблони кои се подобро рангирани во споредба со тековниот примерок (пр. првите пет), без оглед дали го поминале прагот.

3. Автентикација

Секое лице поседува особини кои се единствени и препознатливи само за него и истиве овие особини му помагаат да се идентификува. Во компјутерскиот свет идентитетот е дефиниран како „единствен назив на личноста, уредот или двата препознаен од системот“. Често единствен назив за идентификацијата и верификацијата е автентикацијата.

Ситуацијата во светот денес ја чини безбедноста како се побитна ставка во нашите животи, па со самото тоа и секојдневната автентикација има далеку поголемо значење денес отколку во раните периоди.

Кога системот или личноста проверува идентитет на друго лице или систем, се врши автентикација што значи дека секој кој е автентизиран може да потврди дека тој е оној кој треба и да биде. Важно е да се спомене дека автентикацијата само го потврдува идентитетот и ништо повеќе не прави со него, ниту ги дефинира неговите права на пристап.

Постојат два типа на автентикација:

- Верификација - се врши потврдување на идентитетот на некое лице во смисла на споредување на добиените податоци со точно одреден примерок во базата. Овој облик на автентикација претставува 1:1 систем.
- Идентификација⁵ - се проверува поклопувањето на добиените примероци со сите сочувани примероци во базата на податоци со цел добивање на податоци за идентитетот на некое лице. Овој систем претставува 1:N или еден наспрема повеќе систем на автентикација.

Двата типа на автентикација се користат кај биометриските автентикациони системи, а кој ќе биде употребен зависи само од апликацијата. Покрај овие два основни типови, постои и уште еден кој се нарекува негативна идентификација каде корисникот треба да потврди дека неговиот идентитет не одговара со бараниот идентитет. И тука се врши пребарување 1:N, позитивен одговор се добива само ако поклопувањето со поголемиот дел од примероците се совпаѓа со внесениот примерок, во спротивно се прифаќа тврдењето дека лицето не е она кое се бара. Системот често се користи на аеродромите каде патниците се проверуваат дали, евентуално, се на црна листа, односно накратко речено системите за негативна идентификација одговараат на прашањето „Дали си ти оној кој кажуваш дека не си“. За разлика

⁵ Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008)

од верификацијата која може да се врши со пин или лозинка негативната идентификација може да се обезбеди исклучиво преку биометриска проверка.

4. Основни принципи на работа на биометриските техники

Во овој дел се опишани некои од основните елементи на кои се темелат биометриските техники. Во прв ред тоа е дигитализацијата, т.е. претворањето на аналогниот сигнал во дигитален, а потоа и вештачката интелигенција на која е потребно да се темелат одредените облици на биометриските техники.

Најважниот момент во процесот на препознавање примерок е дигитализацијата. Имено, за компјутерски цели податоците добиени со скенирање итн., треба да се преведат во дигитален формат со кој компјутерот може да работи. Ова е процес во кој аналоген сигнал се конвертира во дигитален и ја препознава програмската опрема. Колку е поголем квалитетот на опремата, толку е поголема веројатноста за препознавање на примерокот. Се прима аналоген сигнал, се претвора во дигитален со користење на дигитален аудиовидео конвертор (DAC). Самиот процес во суштина се состои од серија на Фуријеви трансформации, квантизации и други концепти кои се користат за математички што попрецизно да се опише влезниот сигнал. Сите ДАК не се еднакви и квалитетни. DAC се наоѓа во сензорот за препознавање на примерокот и колку сензорот е подобар (и затоа поскап), се добива подобра мостра примерок.

Брза Фуријева трансформација или FFT (eng. Fast Fourier Transformation) е една од најлесните и најбрзите најчесто користени техники за опишување и обработка на сигналот. Работи со релативно мала резолуција, а описоти обработката на сигналот се изведува во процесорот за дигитален сигнал (DSP Digital Signal Processor) користејќи ги Фуриевите трансформации. Тие ја опишуваат кривата на примерокот и неговите хармоници преведени во неколку синусоидални функции. Техниката е именувана по Јозеф Фурие.

Биометријата може да се дефинира како модел на идентификација на лица, базирана на физичките карактеристики или карактеристиките на однесувањата, а се однесува на нешто што таа личност единствено го поседува. Некој автори даваат уште поописна дефиниција дека биометријата се бави со идентификација на поединци, темелејќи се на нивните биолошки карактеристики или карактеристики на однесувања, односно дека претставува своевидна методологија за решавање на идентификација според наведените критериуми.

На самиот почеток на изведбата и користењето на биометриските системи, предноста се давала на физичките карактеристики во однос на карактеристиките на однесувањето. Се верувало во тоа дека физичките карактеристики се посигурни од однесувањето, бидејќи имаат тенденција да имаат мали разлики внатре во групата.

Главните биометриски методи се наведени подолу кои се темелат на физичките карактеристики и однесувањето.

5. Физичка биометрија

Физичката биометрија е дел од биометријата која вклучува земање мостри од физиономијата на човечкото тело и нејзините уникатни карактеристики. Основата на физичката биометрија е човечката физичка единственост што им овозможува на луѓето да бидат препознаени врз основа на истите и со користење на соодветни описи на примероци за нив признавање. Признати модели, шаблони може да се користат во комбинација со други класични записи кои се единствени за едно лице.

Читање ДНК-записи

Читањето на единствената ДНК - деоксирибонуклеинска киселина (ДНК) е релативно нова гранка на биометријата која се занимава со препознавање на ДНК на личноста. Со претпоставка дека секое лице содржи ДНК својствена за себе, почнаа да се изградуваат читачи за ДНК-записи.

Бидејќи ДНК на поединецот е очигледна, истата се споредува со складираниот запис во базата на податоци и тоа е начин за автентикација на корисникот при пристап до систем. Во комбинација со други биометриски техники, може да се обезбеди многу висок степен на заштита и признавање дали навистина е лицето на кое му е доделен одреден авторитет. Оваа техника може да се користи и за воени и за цивилни цели, и постои голема веродостојност за податоците.

ДНК-анализа се користи денес во голем број сфери како што се докажување на татковство или сродни врски или во судството во кое се идентификувани многу криминалци.

Отпечатоци на прстите

Примероците на порите и браздите на отпечатоците од прсти се единствени за секое лице. Отпечатоците од прсти се уникатни за секој прст, вклучувајќи и близнаци. Ова е една од комерцијално најмногу достапните биометриски технологии.

Слика 1: Пример за идентификација fingerprint



Извор: <https://www.livemint.com/Industry/2R8ReDWjLRKTMnPp8gkcSO/Meeting-biometric-authentication-deadline-a-big-challenge-fo.html>

Уреди за препознавање на отпечатоци почнаа да користат и десктоп машините и лаптопите, дури и мобилни во последните години, и сега се широко достапни по многу пониски цени. Со тоа корисниците повеќе не треба да внесуваат лозинки - наместо тоа само со допир обезбедува моментален пристап до компјутерот или мобилниот.

Отпечатоците од прст може да се користат и во идентификационен режим. Неколку држави во САД проверуваат отпечатоци при пријавување за социјални бенефиции за да се осигури дека не се регистрирани и да добиваат привилегии под фалсификувани имиња тоа се прави преку методот препознавање лица.

Слика 2: Отклучување на телефон преку отпечаток од прсти

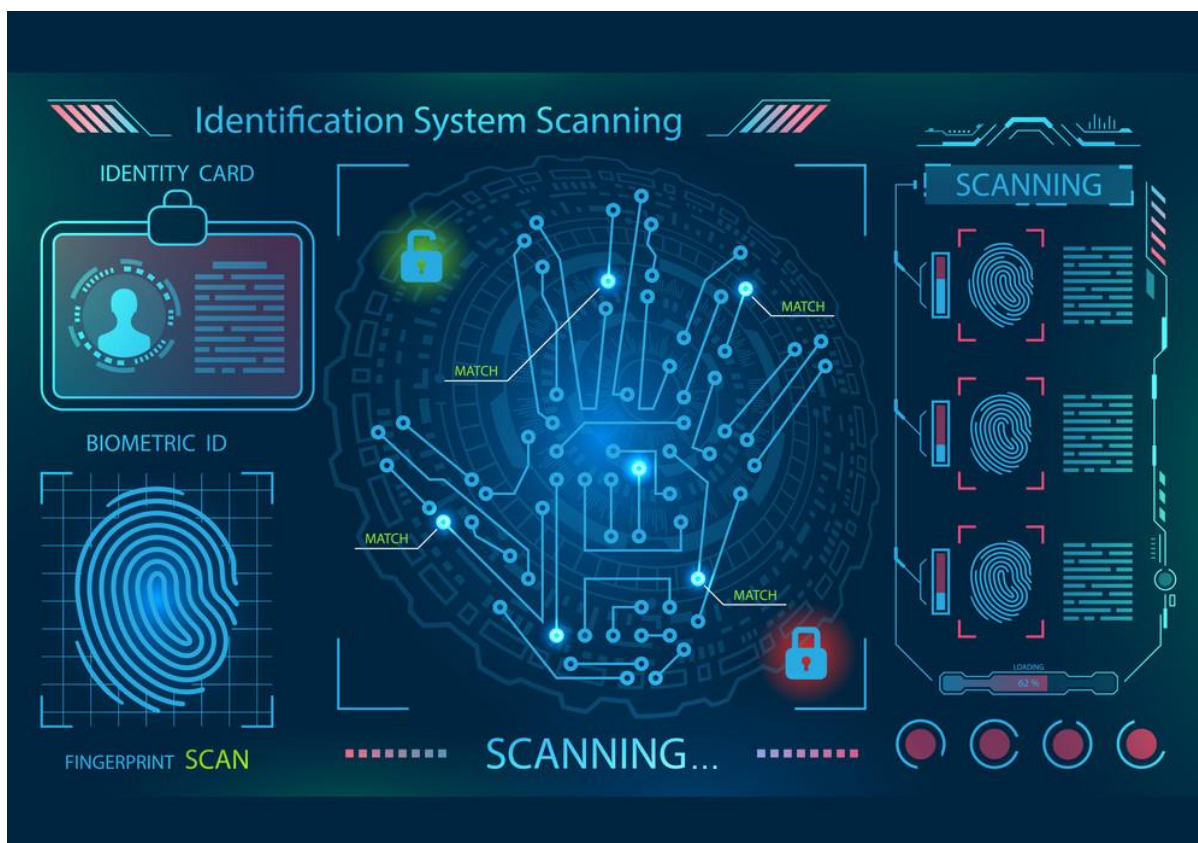


Извор: <https://www.makeuseof.com/tag/protect-phone-fingerprint-pin/>

Геометрија на дланка

Идентификацијата врз основа на препознавање на карактеристиките на дланките на рацете е достапна повеќе од дваесет години. Со цел да се постигне автентикација, системот може да ги мери физичките карактеристики на дланката или прстите и тоа вклучува должина, ширина, дебелина и површина на раката. Една корисна карактеристика е тоа што некои системи бараат мал биометриски модел (неколку октети). Геометријата на раката е постигната подобност во опсегот на апликации и често може да се види во контролирањето на физичкиот пристап во комерцијални и резиденцијални апликации, во временски и сервер системи, и воопшто во апликации за лична проверка.

Слика 3: Геометрија на дланка за идентификација



Извор: <https://www.vectorstock.com/royalty-free-vector/hand-scan-handprint-imprint-finger-print-in-vector-20386264>

Скенирање рожница

Скенирањето на рожницата е технологија која најмногу се користи кога се контролира влезот на лица во одреден простор, спроведување статистика за посетителите и слични варијанти, исто така се користат и при скенирање кориснички сметки и документи. Земањето на примерокот се врши со помош на камера која снима со запис за корисникот, а претпоставувајќи дека секој е единствен, може да се користи во смисла на недвосмислено означување.

Добиената слика на рожницата е опишана со помош на посебни програми со помош на точките и дава поголема можност за недвосмислен опис на примерокот. Користејќи описна технологија на рожницата, можно е таа да се опише со 242 уникатни точки, додека на пример во технологијата за препознавање на отпечатоци на прсти, шаблонот може да се опише со 7 до 22 поени.

Слика 4: Скенирање на рожница



Извор: <https://www.google.com/imgres?imgurl=https%3A%2F%2Fbetanews.com%2Fwp-content%2Fuploads%2F2016%2F08%2Fbiometrics-600x338.jpg&imgrefurl=https%3A%2F%2Fbetanews.com%2F2017%2F07%2F12%2Fchanging-authentication-landscape%2F&docid=bzxAZPp1d-WjyM&tbnid=O77q2nUFDDipWM%3A&vet=10ahUKEwiVu4rcyKTeAhWIEywKHxU3AWEQMwg8KAAwAA..i&w=600&h=338&bih=657&biw=1366&q=verification%20loading%20eye&ved=0ahUKEwiVu4rcyKTeAhWIEywKHxU3AWEQMwg8KAAwAA&iact=mrc&uact=8>

Следнава илустрација покажува пример за користење на методот на скенирање на рожницата за потребите за проверка на девојче во Авганистан што првпат беше забележана во нејзината младост во 1984 година. Таа има стекната популарност во светот поради своите зелени очи и од воената ситуација во Авганистан, во која девојката го занемари со нејзиниот израз на лицето. Сите обиди да се пронајде таа девојка биле неуспешни сè до 2001 кога со методот на скенирање на рожница девојката е пронајдена како веќе возрасна жена, во своето родно село.

Слика 5: Авганистанка - некогаш и денес, препознаена по рожницата



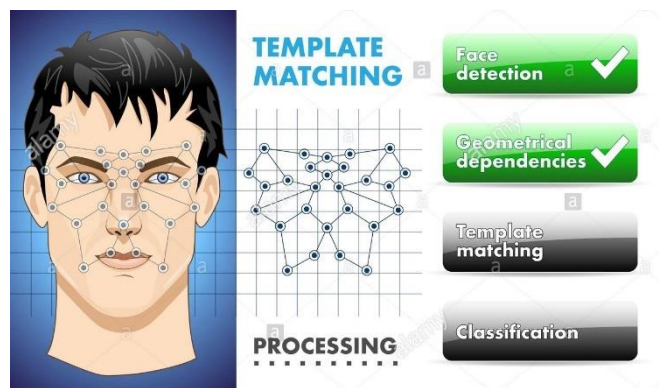
Извор: <https://www.google.com/imgres?imgurl=https%3A%2F%2Fex-magazin.com%2Fwp-content%2Fuploads%2F2018%2F02%2Fw873-1-3.jpg&imgrefurl=https%3A%2F%2Fex-magazin.com%2Fwp-content%2Fuploads%2F2018%2F02%2Fw873-1-3.jpg&imgrefurl=https%3A%2F%2Fex-magazin.com%2Fwp-content%2Fuploads%2F2018%2F02%2Fw873-1-3.jpg&imgrefurl=https%3A%2F%2Fex-magazin.com%2Fwp-content%2Fuploads%2F2018%2F02%2Fw873-1-3.jpg>

magazin.com%2F2018%2F02%2F08%2Fnajljepse-oci-svijeta-kriju-pricu-koje-zastaje-dah%2F&docid=llOZEpmScsuVdM&tbnid=xCqhryF6Jg1j8M%3A&vet=10ahUKEwjXwb3IxaTeAhVMFywKHVlHCawQMwhCKAUwBQ..i&w=640&h=470&bih=657&biw=1366&q=Djevojka%20iz%20Afganistana%201985&ved=0ahUKEwjXwb3IxaTeAhVMFywKHVlHCawQMwhCKAUwBQ&iact=mrc&uact=8

Препознавање на лица

Оваа биометриска технологија е една од релативно поевтините методи, бидејќи не бара посебна сет опрема. Таа бара само компјутер и видеокамера. Во пракса тоа е доволно за една личност да помине пред камерата за да се сними примерок, додека препознавањето на лицето се врши со препознавање на обликот со анализа на примерокот со одвојување на клучните индикатори, карактеристичен одраз.

Слика 6: Биометрија - препознавање на лице



Извор: https://www.google.com/imgres?imgurl=https%3A%2F%2Fcomps.gograph.com%2Faccess-biometric-face-recognition_gg80852010.jpg&imgrefurl=https%3A%2F%2Fwww.gograph.com%2Fclipart%2Faccess-biometric-face-recognition-gg80852010.html&docid=LFr2qoAwYoI5QM&tbnid=NVIYDRjRsQXFqM%3A&vet=10ahUKEwi509WHyKTeAhXBWSwKHW6iAhAQMwhxKCcwJw..i&w=450&h=282&bih=657&biw=1366&q=face%20recognition%20biometric%20security%20system&ved=0ahUKEwi509WHyKTeAhXBWSwKHW6iAhAQMwhxKCcwJw&iact=mrc&uact=8

Почетната фаза го опфаќа скенирањето на одразот на лицето во различни размери, а потоа го оценува клучот за да се утврди со одредена веројатност дали лицето е тоа. Втората фаза ја одредува позицијата на главата која мора да предизвика одредени корекции во тоа време и бара корекции на x, y и z оските. Со цел да се препознае лицето толку лесно колку што е можно, пожелно е да поседува снимена мостра од голем број агли.

Проверка на вени

Биометрискиот опис на вената се користи како дополнителен дел во описот на една личност. Вените се големи, непроменливи и претежно скриени шаблони. Во комбинација со геометријата на раката или технологијата за отпечатоци од прсти постигнува многу високо ниво на препознавање на лица. Оваа технологијата исто така може да се користи во физичката контрола при минување на интелигентни врати, брави и слично, физички бариери во кои корисниците доаѓаат во контакт со своите раце. На пример,

банките во Јапонија ја користат оваа технологија која е решена со закон. Вообичаено се користат камерите за препознавање на шаблоните на вените преку користење и на инфрацрвен сензор кој ги препознава оние детали кои човечкото око не е во можност да ги регистрира.

Заклучок

Биометријата секојдневно станува сè почеста во разни сфери на животот, па така и користењето на автоматски систем за препознавање на идентитетот со следење на физичките карактеристики или однесување, веќе долго време е дел од реалноста. Големата предност на биометријата е што ги реши проблемите со лозинките. Лозинките можат да бидат изгубени, заборавени или обелоденети од малициозни корисници или напаѓачи. Затоа, каде што физички е можно, тие имплементираат биометриски методи за пристап до локалната мрежа. Веќе е споменато дека дури и за отклучување на мобилни се користи отклучување преку отпечаток од прсти, или finger face отклучување на телефонот со поглед, односно детекција на лице, ваквото користење на fingerprint веќе одамна наоѓаше примена за стартување, односно отклучување на лаптопи и компјутерски системи. Во блиска иднина се очекува ваква примена да се најде и во автомобилската индустрија за стартување и отклучување на автомобилите и слично.

Сепак, основната цел на биометријата е да контролира влегување или излегување од одредени физички локации. Како би било тоа постигнато, во моментот се применуваат различни форми на биометриски техники, но најкомплетно решение може да се постигне со комбинирање на различни методи - мултимодална биометрија.

Биометријата, исто така, ја наоѓа својата предност при апликација за контрола на работното време. Користењето на картичка или лозинки остава можност за заемна солидарност меѓу вработените, каде што еден вработен ја потврдува автентичноста на друг вработен, но со користење пример за влегување и излегување со пријава преку отпечаток на прст, ваквата злоупотреба би била избегната. Исто така, се очекува дека биометријата ќе има значајна улога во банкарскиот систем.

Иако биометријата има значителни предности, првенствено за зголемување нивото на безбедност во смисла на автентикација на корисници, истите сè уште имаат свои недостатоци. Имено, неопходно е да се примени биометријата преку специјализирана опрема која ќе врши извлекување и обработка на различни примени податоци. Овие специјализирани уреди може да бидат скапи или незгодни поради нивната физичка околина.

Исто така, еден од недостатоците на одредени биометриски техники е можноста за лажна автентикација. Поточно, корисникот може да постави снимка од различен глас, печатење, па дури и потпис кога се автентичира.

Оттука, не е неопходно процесот на проверка на автентичност да се базира само на еден метод, стабилизираат работата на мозокот, а кои овде нема да бидат наведени.

Литература

- ❖ http://www.cs.cmu.edu/~epxing/Class/10701-06f/project-reports/jiang_xu.pdf
- ❖ <https://www.dhs.gov/biometrics>
- ❖ <https://www.bayometric.com/cyber-crime-biometrics-solution/>
- ❖ <https://www.tportal.hr/tehnolo/clanak/smartfon-mozete-otkljucati-i-listom-papira-20160311>
- ❖ <https://www.cnbc.com/2016/04/05/biometrics-future-of-digital-cyber-security.html>
- ❖ http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf
- ❖ Jain, A. K., Ross, A., Pankanti, S. (1999.). A Prototype Hand Geometry-based Verification System. 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C
- ❖ Fotak, T. (2008). Razvoj biometrijskih tehnika. Završni rad na preddiplomskom studiju. Fakultet organizacije i informatike, Varaždin
- ❖ DeCoursey, W.J. (2003): Statistics and Probability for Engineering Applications, Newnes, Woburn Massachusetts
- ❖ De Marsico, M. i ostali (2009): Fractal Indexing in Multimodal Biometric Contexts
- ❖ Dunstone, T. i Yager N. (2009): Biometric System and Data Analysis, Springer, New York
- ❖ Garnett, W.P. (1997): Chaos Theory Tamed, Joseph Henry Press, Washington
- ❖ A.K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information security, IEEE Trans. Inf. Forensics Secur.
- ❖ Dunstone, T. i Yager N. (2009): Biometric System and Data Analysis, Springer, New York
- ❖ Usp. Angeliki-Toli, Christina; Preneel, Bart. Biometric Solutions as Privacy Enhancing Technologies, 2015. str. 1
- ❖ URL: <https://securewww.esat.kuleuven.be/cosic/publications/article-2531.pdf> (2016-06-25)
- ❖ Radmilović, Želimir. Biometrijska identifikacija. // Polic. sigur 17, 3-4(2008)
- ❖ Usp. Uddin, Jasmin. Matrix of Biometrics // Biometrics, 2016, str. 1. URL: https://www.researchgate.net/publication/301542522_Matrix_of_Biometrics (2016-06-25)

УПОТРЕБАТА НА МОДЕЛИ НА НЕВРОНСКИ МРЕЖИ ЗА ДЛАБОКО УЧЕЊЕ ВО АВТОМАТСКОТО ПРЕПОЗНАВАЊЕ НА ГОВОР

UDC: 004.85.032.26:004.934

Прегледен труд

Дамјан Мишевски

Европски Универзитет Република Македонија - Скопје

Апстракт

Автоматското препознавање говор е процес на преведување на изговорените зборови во текст. Денес таа е една од главните предизвикувачки задачи, пред сè поради високата одржливост на говорните сигнали. Невронската мрежа е техника на градење на компјутерска програма која учи од податоците. Таа во основа се базира на нашата претстава за тоа како човечкиот мозок функционира.

Главната цел на овај стручен труд е да понуди основни знаења за сите оние кои сакаат да применат типични алгоритми за длабоко учење за автоматско континуирано препознавање на говор. Намерата е заинтересираните програмери да се запознаат со целиот процес на препознавање на говор, да разберат како функционираат алгоритмите за длабоко учење и како можат да ги користат во апликациите за препознавање на говор.

Длабокото учење (Deep Learning), е прилично нова област на машинското учење која станува водечка технологија за препознавање на говор. Длабокото учење понекогаш уште се нарекува репрезентативно учење (Representational Learning) или учење без надзор (Unsupervised Learning). Тоа стана доминантен модел за препознавање на говор и сè повеќе преовладува во имплементацијата во многу индустрии и апликации.

Мрежата е претставена како колекција на софтверски "неврони" кои се поврзани меѓу себе и имаат можност да испраќаат пораки еден на друг. Таа е програмирана да реши одреден проблем така што ја повторува постапката одново и одново, на начин со кој секојпат ги зајакнува врските што доведуваат до успех и го намалува влијанието на врските што доведоа до неуспех.

Автоматското препознавање говор денес е една од главните предизвикувачки задачи во компјутерската технологија. Моделите базирани на примената на длабоки неврронски мрежи станува доминантен модел во имплементацијата во многу индустрии и апликации.

Клучни зборови: *невронска, мрежа, длабоко, учење, препознавање, говор*

USAGE OF DEEP NEURAL NETWORK MODELS IN APPLICATION OF AUTOMATIC SPEECH RECOGNITION

Abstract

Automatic speech recognition, is a process of translating of spoken words into text. Today it is one of the major challenging task due to the high variability in speech signals. Neural Network is a technique for building a computer program that learns from data. It is based very loosely on how we think the human brain works.

Aim and main target of this article is to give a basic knowledge to those who wants to apply typical deep learning algorithms for automatic continuous speech recognition. An intention is to make interested developers familiar with general speech recognition process, to give understanding on how deep learning algorithms works and how to use them in speech recognition applications.

Deep learning, is fairly a new area of machine learning which is becoming a mainstream technology for speech recognition. Deep learning is sometimes referred as representation learning or unsupervised feature learning. It has become a dominant models for speech recognition and prevails in implementations in many industries and applications at an increasingly larger scale.

The network is a collection of software "neurons" that are created and connected, allowing them to send messages to each other. It is instructed to solve a problem, which it attempts to do over and over, each time strengthening the connections that lead to success and diminishing those connections that lead to failure.

Automatic speech recognition today it is one of the major challenging task in computer technology. Usage of deep neural network models in application of automatic speech recognition become a dominant model which prevails in implementations in many industries and applications.

Keywords: *neural, network, deep, learning, speech, recognition*

Вовед

Длабокото учење е метода на машинско учење која ги учи компјутерите преку примери, што е природен начин на учење кај луѓето.

Во длабокото учење, компјутерскиот модел учи да прави класификација директно од слики, текст или звук. Моделите на длабоко учење постигнуваат точност во препознавањето кои често ги надминува човечките способности [1,3,4].

Моделите се обучуваат со големи множества на означени податоци и користат архитектури на невронски мрежи кои имаат многу леери. Поради тоа и се нарекуваат невронски мрежи за длабоко учење.

Терминот длабоко обично се однесува на бројот на скриени леери на невронската мрежа. Традиционално невронската мрежа користи 2-3 скриени леери додека длабоката невронска мрежа може да има и 150 леери.

Моделите за длабоко учење ги учат својствата директно од податоците.

Автоматско препознавање на говор

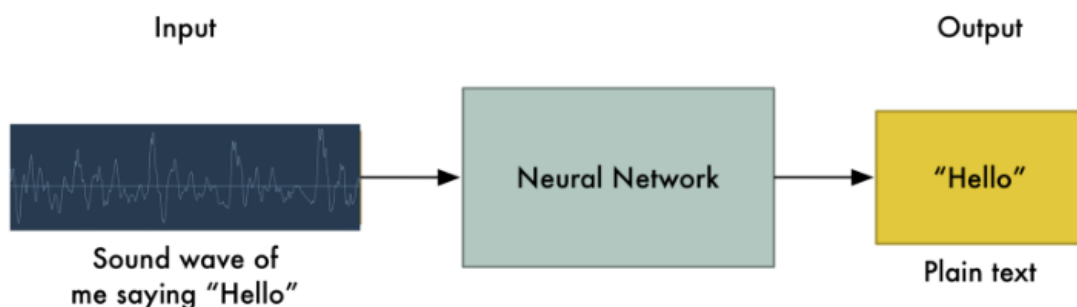
Автоматското препознавање на говор, преведување на изговорените зборови во текст, сè уште е предизвикувачка задача поради високата сложеност и нестабилност на говорните сигнали. **Длабоко учење (Deep learning)**, кое понекогаш се нарекува **representation learning** или **unsupervised learning**, е нова област на машинско учење кое станува водечка технологија за препознавање на говор. Главната цел на оваа технологија е да се применат типични алгоритми за длабоко учење, вклучувајќи длабоки невронски мрежи (DNN) за автоматско континуирано препознавање на говор. Автоматското препознавање на говор, сè уште претставува предизвикувачка задача поради високата варијабилност во говорните сигнали. На пример, лицата кои зборуваат може да имаат различни акценти, дијалекти или изговори и да зборуваат во различни стилови, со различен интензитет и во различни емоционални состојби. Присуството на бучава во животната средина, реверберацијата, различни микрофони и уреди за снимање резултираат со дополнителна варијабилност.

Препознавањето на говор е присутно со децении, па се прашаеме зошто токму сега станува толку актуелно? Причината е дека алгоритмите на длабокото учење конечно го направија препознавањето на говорот доволно точно за да биде користено надвор од контролирани средини - лаборатории, студија итн.. Познато е дека досега точноста во препознавање на говорот се движеше од 95% до 99% точност. Благодарение на длабокото учење, овој 4% јаз во точноста значително е намален.

Да видиме како длабокото учење е искористено за препознавање на говор.

Да претпоставиме дека можеме да ги пренесеме звучните сигнали во невронска мрежа и дека мрежата можеме да ја обучиме за да произведе текст:

Слика 1. Шематски приказ на системот за препознавање на зборови



Adam Geitgey, "Machine Learning series of articles", 2016

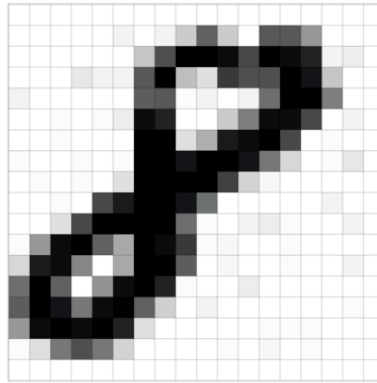
Тоа е клучот на препознавање говор со длабоко учење, но сè уште не е сè. Голем проблем е што говорот варира во брзина. Едно лице може да каже "Hello" многу брзо, а друго да каже "heeeellllllllllloooooo!" многу бавно, произведувајќи многу подолг звучен фајл со многу повеќе податоци. Двете звучни датотеки треба да се препознаат како точно ист текст - "Hello". Автоматското израмнување на аудио-датотеки од различни должини во парче текст со фиксна должина се покажува како прилично тешко. За да се надмине овој проблем, покрај користење на длабоката нервна мрежа, треба да користиме специјални техники и дополнителна прецизност [6,7].

Претворање на звуци во битови

Првиот чекор во препознавањето на говор е очигледен - ние треба да ги пресликаме звучните бранови во компјутерот.

Да се послужи со пример на слика која треба да се внесе во невронската мрежа за препознавање на слика. Сликата можеме да ја мапираме во низа од броеви кои претставуваат интензитет на сиво на секој пиксел од сликата, како што е дадено подолу. Како пример да го земеме бројот 8 напишан со рака:

Слика 2. Бројот "8" напишан со рака



Adam Geitgey, "Machine Learning series of articles", 2016

За да ја внесеме сликата во нашата невронска мрежа едноставно ја трансформираме сликата од 18x18 пиксели во низа од 324 бројки.

Слика 3. Мапирање на сликата "8" во низа од броеви

```

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 12 0 11 39 137 37 0 152 147 84 0 0 0
0 0 1 0 0 0 41 160 250 255 235 162 255 238 206 11 13 0
0 0 0 16 9 9 150 251 45 21 184 159 154 255 233 40 0 0
10 0 0 0 0 0 145 146 3 10 0 11 124 253 255 107 0 0
0 0 3 0 4 15 236 216 0 0 38 109 247 240 169 0 11 0
1 0 2 0 0 0 253 253 23 62 224 241 255 164 0 5 0 0
6 0 0 4 0 3 252 250 228 255 255 234 112 28 0 2 17 0
0 2 1 4 0 21 255 253 251 255 172 31 8 0 1 0 0 0
0 0 4 0 163 225 251 255 229 120 0 0 0 0 0 11 0 0
0 0 21 162 255 255 254 255 126 6 0 10 14 6 0 0 9 0
3 79 242 255 141 66 255 245 189 7 8 0 0 5 0 0 0 0
26 221 237 98 0 67 251 255 144 0 8 0 0 7 0 0 11 0
125 255 141 0 87 244 255 208 3 0 0 13 0 1 0 1 0 0
145 248 228 116 235 255 141 34 0 11 0 1 0 0 0 1 3 0
85 237 253 246 255 210 21 1 0 1 0 0 6 2 4 0 0 0
6 23 112 157 114 32 0 0 0 0 2 0 8 0 7 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

```

Adam Geitgey, "Machine Learning series of articles", 2016

По аналогија, звучниот бран можеме исто така да го претвориме во низа од броеви.

Брановиот облик при изговарање на зборот "Hello" е следниот:

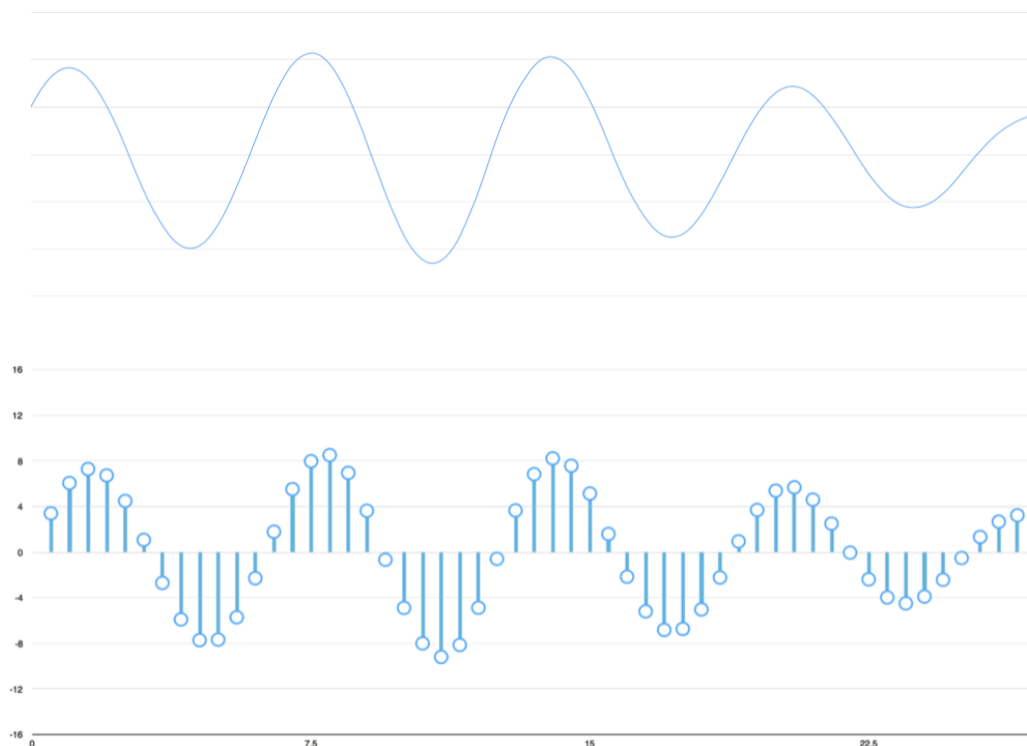
Слика 4. Бранов облик при изговарање на зборот "Hello"



Adam Geitgey, "Machine Learning series of articles", 2016

Звучните бранови се еднодимензионални. Во секој момент, тие имаат единствена вредност врз основа на висината на бранот. Да зумираме еден мал дел од звучниот бран и да погледнеме. За да го претвораме овој звучен бран во броеви, ние само ја снимивме висината на бранот во подеднакво одделени точки:

Слика 5. Семплирање на звучниот бран



Adam Geitgey, "Machine Learning series of articles", 2016

Ова се нарекува семплирање. Читаме илјадници пати во секунда и снимаме број кој ја претставува висината на звучниот бран во тој момент во времето. Тоа е во основа сите некомпресирани .wav аудио-датотеки.

Аудио "CD квалитет" се зема на примерок од 44,1kHz (44,100 читања во секунда). Но, за препознавање говор, стапката на земање примероци од 16kHz (16.000 примероци во секунда) е доволна за да се покрие фреквентниот опсег на човечкиот говор. Да го испитаме нашиот "Hello" звучен бран 16.000 пати во секунда. Еве ги првите 100 примероци:

Слика 6. Секој број ја претставува амплитудата на звучниот бран од 1 / 16000. секунди интервал

```
[-1274, -1252, -1160, -986, -792, -692, -614, -429, -286, -134, -57, -41, -169, -456, -450, -541, -761, -1067, -1231, -1047, -952, -645, -489, -448,
-397, -212, 193, 114, -17, -110, 128, 261, 198, 390, 461, 772, 948, 1451, 1974, 2624, 3793, 4968, 5939, 6057, 6581, 7302, 7640, 7223, 6119, 5461,
4820, 4353, 3611, 2740, 2004, 1349, 1178, 1085, 901, 301, -262, -499, -488, -707, -1406, -1997, -2377, -2494, -2605, -2675, -2627, -2500, -2148, -
1648, -970, -364, 13, 260, 494, 788, 1011, 938, 717, 507, 323, 324, 325, 350, 103, -113, 64, 176, 93, -249, -461, -606, -909, -1159, -1307, -1544]
```

Adam Geitgey, "Machine Learning series of articles", 2016

Може да се помисли дека дигиталниот примерок создава само грубо приближување до оригиналниот звучен бран, бидејќи тоа е само земање на повремени состојби. Бидејќи имаме празнини меѓу поединечните отчитувања, се поставува прашање, дали се губи дел од информацијата? Дали дигиталните примероци совршено го пресоздаваат оригиналниот аналоген звук? Што е со тие празнини? Благодарение на теоремата на Nyquist, знаеме дека можеме да ја користиме математиката за совршено да го реконструираме оригиналниот звучен бран сè додека земањето примерок е најмалку два пати побрзо од највисоката фреквенција што сакаме да ја снимиме. Ова го споменуваме само затоа што речиси сите го разбираат ова погрешно и претпоставуваат дека користењето на повисоки стапки на земање примероци секогаш води до подобар аудио квалитет. Тоа не е секојпат така.

Преработка на семплираните податоци

Сега имаме низа броеви со секој број кој ја претставува амплитудата на звучниот бран на 1 / 16.000-тиот дел од вториот интервал. Ние би можеле да ги нахраниме овие броеви директно во невронската мрежа. Но, обидот да се препознаат обрасците на говорот со обработка на овие примероци директно е тешко. Наместо тоа, можеме да го направиме проблемот полесен со изведување на некоја претходна обработка на аудио-податоците. Ајде да почнеме со групирање на нашиот избрани аудио во 20-милисекунди долги парчиња. Еве ги првите 20 милисекунди аудио (т.е. нашите први 320 примероци):

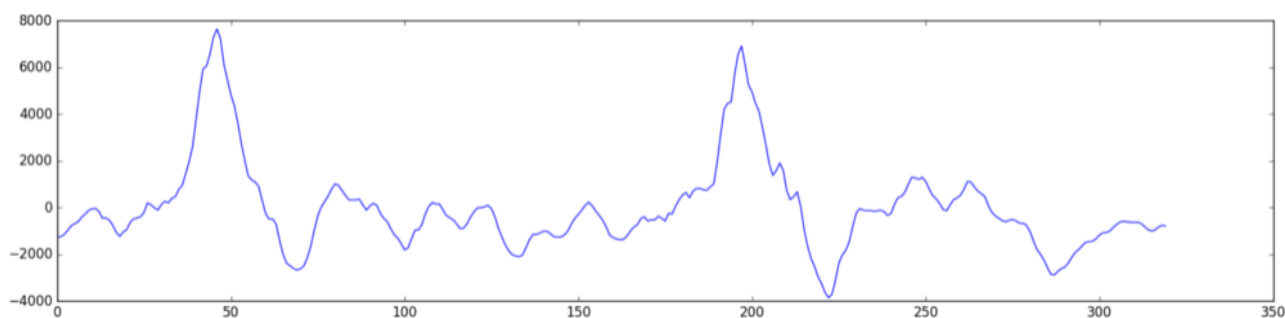
Слика 7. Броевите во листата претставува колку енергија има во еден фреквентен опсег од 50hz

```
[-1274, -1160, -986, -792, -692, -614, -429, -286, -134, -57, -41, -169, -456, -450, -541, -761, -1067, -1231, -1047, -952, -645, -489, -448,
-397, -212, 193, 114, -17, -110, 128, 261, 198, 390, 461, 772, 948, 1451, 1974, 2624, 3793, 4968, 5939, 6057, 6581, 7302, 7640, 7223, 6119, 5461,
4820, 4353, 3611, 2740, 2004, 1349, 1178, 1085, 901, 301, -262, -499, -488, -707, -1406, -1997, -2377, -2494, -2605, -2675, -2627, -2500, -2148, -
1648, -970, -364, 13, 260, 494, 788, 1011, 938, 717, 507, 323, 324, 325, 350, 103, -113, 64, 176, 93, -249, -461, -606, -909, -1159, -1307, -1544,
-1815, -1725, -1341, -971, -959, -723, -261, 51, 210, 142, 152, -92, -345, -439, -529, -710, -907, -887, -693, -403, -180, -14, -12, 29, 89, -47, -
398, -896, -1262, -1610, -1862, -2021, -2077, -2105, -2023, -1697, -1360, -1150, -1148, -1091, -1013, -1018, -1126, -1255, -1270, -1266, -1174, -10
03, -707, -468, -300, -116, 92, 224, 72, -150, -336, -541, -820, -1178, -1289, -1345, -1385, -1365, -1223, -1004, -839, -734, -481, -396, -580, -52
7, -531, -376, -458, -581, -254, -277, 50, 331, 531, 641, 416, 697, 810, 812, 759, 739, 888, 1008, 1977, 3145, 4219, 4454, 4521, 5691, 6563, 6909,
6117, 5244, 4951, 4462, 4124, 3435, 2671, 1847, 1370, 1591, 1586, 713, 341, 462, 673, 60, -938, -1664, -2185, -2527, -2967, -3253, -3636, -38
59, -3723, -3134, -2380, -2032, -1831, -1457, -804, -241, -51, -113, -136, -122, -158, -147, -114, -181, -338, -266, 131, 418, 471, 651, 994, 1295,
1267, 1197, 1291, 1110, 793, 514, 370, 174, -90, -139, 104, 334, 407, 524, 771, 1106, 1087, 878, 703, 591, 471, 91, -199, -357, -454, -561, -605,
-552, -512, -575, -669, -672, -763, -1022, -1435, -1791, -1999, -2242, -2563, -2853, -2893, -2740, -2625, -2556, -2385, -2138, -1936, -1803, -1649,
-1495, -1460, -1446, -1345, -1177, -1088, -1072, -1003, -856, -719, -621, -585, -613, -634, -638, -636, -683, -819, -946, -1012, -964, -836, -762,
-788]
```

Adam Geitgey, "Machine Learning series of articles", 2016

Завршувањето на тие броеви како едноставен линиски график ни дава груба приближна вредност на оригиналниот звучен бран за тој 20-милисекунден временски период:

Слика 8. Линиски граф на семплираниот звучниот сегмент



Adam Geitgey, "Machine Learning series of articles", 2016

Оваа снимка е само 1/50 од секундата. Но, дури и оваа кратка снимка е комплексна минијатурна каша со различни фреквенции на звукот. Има некои ниски звуци, звуци од среден опсег, па дури и некои звуци од висок опсег. Кога ќе се земат сите заедно, овие различни фреквенции се мешаат и заедно го сочинуваат сложениот звук на човечкиот говор.

За да ја олесниме обработката на овие податоци за невронските мрежи, ќе го разделиме овој комплексен звучен сигнал на составни делови. Делењето го правиме така што почнуваме од најниските фреквенциски опсези и редоследно одиме кон повисоките фреквенции. Потоа додаваме податок колку енергија има во секој од овие фреквенциски опсези (од ниско до високо) и така создаваме отпечатоци за целиот аудио фрагмент.

Замислете дека сте имале снимање на некој кој свирел С мајор на пијано. Тој звук е комбинација од три музички ноти - С, Е и Г - сите измешани заедно во еден сложен звук. Ние треба да го разложиме тој сложен звук во поединечните записи за да кажеме дека тие се С, Е и Г. Ова го правиме користејќи математичка операција наречена Fourier-ова трансформација. Го разложуваме сложениот звучен бран на едноставни звучни бранови што го сочинуваат. Откако ќе ги имаме тие поединечни звучни бранови, додаваме колку енергија е содржана во секој од нив.

Крајниот резултат е показател на тоа колку е важен секој фреквентен опсег, од ниски тонови (на пр. бас тонови) до високи тонови. Секој број подолу претставува колку енергија има во секој 50hz опсег на нашите 20 ms аудио-клипови:

Слика 9. Листа на вредности на енергија во конкретниот фреквентен опсег од 50hz

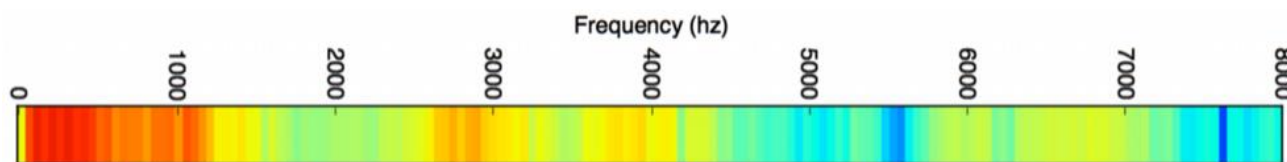
```
[110.97481594791122, 166.61537247955155, 180.43561044211469, 175.09309469913353, 180.01686918959216, 176.00619877472167, 179.79737781786582, 173.53825213548219, 176.87177119846058, 170.42684732853121, 159.26023828556598, 163.24469810981628, 149.1552733931867, 154.34196586290136, 151.46179061113971, 152.99674239973979, 143.98878156117371, 156.6033727693738, 155.78237530428544, 157.1793094101783, 146.2863297599679, 164.37233032929228, 158.1282656446088, 147.23166451005145, 133.26597973863801, 116.5170100028831, 116.85501120577126, 115.40519005123537, 120.85619013711489, 112.4840612316109, 111.80244759457571, 92.590676871856431, 105.75863927434719, 95.673146446282971, 90.391748128054208, 79.355818055314899, 86.080143147713926, 84.748200268709567, 83.050509583779005, 86.207180362242, 758.90.252031938154876, 89.361567351948437, 90.917307309643206, 90.746777849123049, 86.726552726337033, 85.709412745006928, 95.938480816664865, 99.89254375917069, 96.632437741434885, 103.2396123166, 6669, 105.80328302591124, 109.53029281234707, 116.4648827060996, 129.20890691592615, 130.43460361780441, 138.15581799444712, 128.25056761852832, 138.14492240466387, 140.8352714810314, 128.151381394, 29752, 123.93018478493934, 121.19289035588113, 119.03159255422509, 114.23827889344033, 119.1717342154997, 101.02568719093093, 110.91192243698025, 106.04872005953503, 100.8697927980990, 92.123301579, 000341, 94.376766266598295, 97.850702698634489, 113.37126364077845, 110.24526597732718, 113.72249347908021, 120.63960942628063, 122.06482533759932, 117.96716716036715, 120.87682744817975, 125.060973, 81947157, 111.57319012901624, 115.54483708595507, 116.99830750130265, 114.40659619324526, 79.869543980883975, 104.8311191845597, 104.66218607004588, 104.91691734587642, 97.143620527536072, 78.43459, 781117835, 82.214144782667248, 67.246072805959614, 66.578937262360313, 74.100307226086798, 64.861423011415653, 59.167561212002269, 62.479712687304911, 63.568362396107467, 55.906096471453267, 42.7908, 82009362830, 55.693023524361097, 50.77636487715011, 41.196111220671208, 51.062413666348945, 58.493563858289065, 53.081835042022769, 73.0606631128159547, 68.21625202122361, 66.7701034934517, 59.76625, 124915202, 35.413635503802389, 22.705615809958832, 16.458048045346381, 44.910670465379937, 59.282513769840705, 69.241933677323856, 81.778634874076346, 88.409923803546008, 94.688033733251245, 96.6408, 67526244051, 91.806226496828543, 94.570526932206619, 99.250924315589074, 97.899164767741183, 75.176507616277235, 88.947474423758905, 71.859103451990862, 93.863684037461738, 96.757146539348298, 96.52, 8614354976241, 99.366456533638413, 102.18717608176904, 102.06596663023235, 101.7849313991082, 103.78833582899547, 99.915220403870748, 107.43478470929935, 104.46449552620618, 105.70789868105298, 101, 10596541338749, 100.75737831526195, 91.742897073196886, 88.307278943060993, 90.936627732905402, 71.134275744339803, 72.504304977841457, 76.233185506299705, 63.281284410272761, 45.380164336858961, 43, 018963766250437, 49.133789791276826, 53.50751009532953, 48.586423556688746, -4.4730776113028883, 50.833000650183408, 51.003802143009629, 39.577356593427531, 47.096919248906332, 55.442197175664383, 56.967128095484341, 49.383247263177985]
```

Adam Geitgey, "Machine Learning series of articles", 2016

Секој број во листата претставува колку енергија има во тој фреквентен опсег од 50hz

Ова е многу полесно да се види ако го нацртате како график.

Слика 10. Графичко претставување на енергијата на семплираниот звучен сегмент

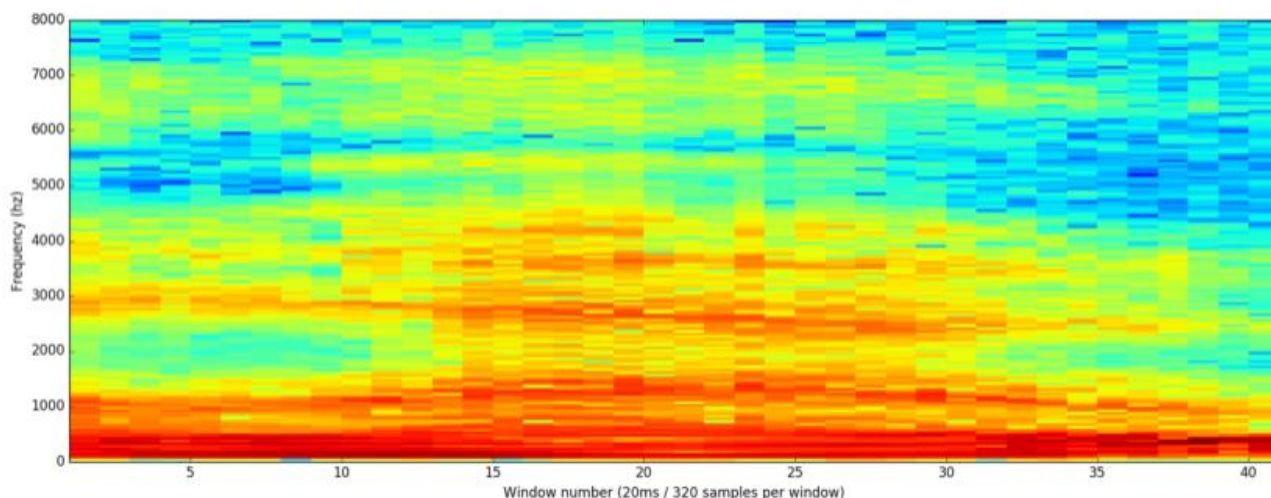


Adam Geitgey, "Machine Learning series of articles", 2016

Може да се види дека нашиот 20 ms звучен фрагмент има многу ниска фреквентна енергија и не многу енергија во повисоките фреквенции. Тоа е типично за "машки" гласови.

Ако го повториме овој процес на секои 20 ms од аудио сигналот, ќе добиеме целосен спектрограм (секоја колона од лево кон десно е еден 20ms дел):

Слика 11. Целосен спектрограм на звучниот клип "Hello"



Adam Geitgey, "Machine Learning series of articles", 2016

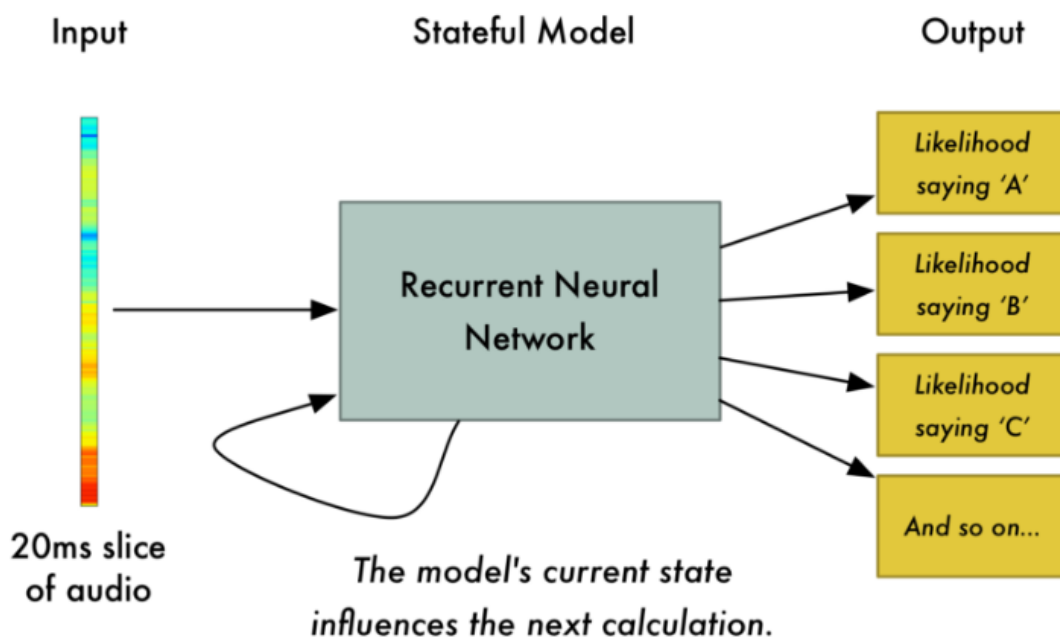
Ова е целосниот спектрограм на звучниот клип "Hello"

Спектраграмот е интересен, бидејќи всушност можете да ги видите нотите и другите музички шаблони во аудио податоците. Невронската мрежа може полесно да открие шаблони во ваков вид на податоци отколку во природни звучни бранови. Следно е оваа презентација на податоците да ја внесуваме во нашата невронска мрежа.

Алгоритам за препознавање

Сега кога имаме аудио во формат кој е лесен за обработка, ќе го внесеме во невронската мрежа. Влезот во невронската мрежа ќе бидат 20 милисекунди аудио сегменти. За секој аудио сегмент, мрежата ќе се обиде да ја разбере буквата што одговара на звукот кој се изговара.

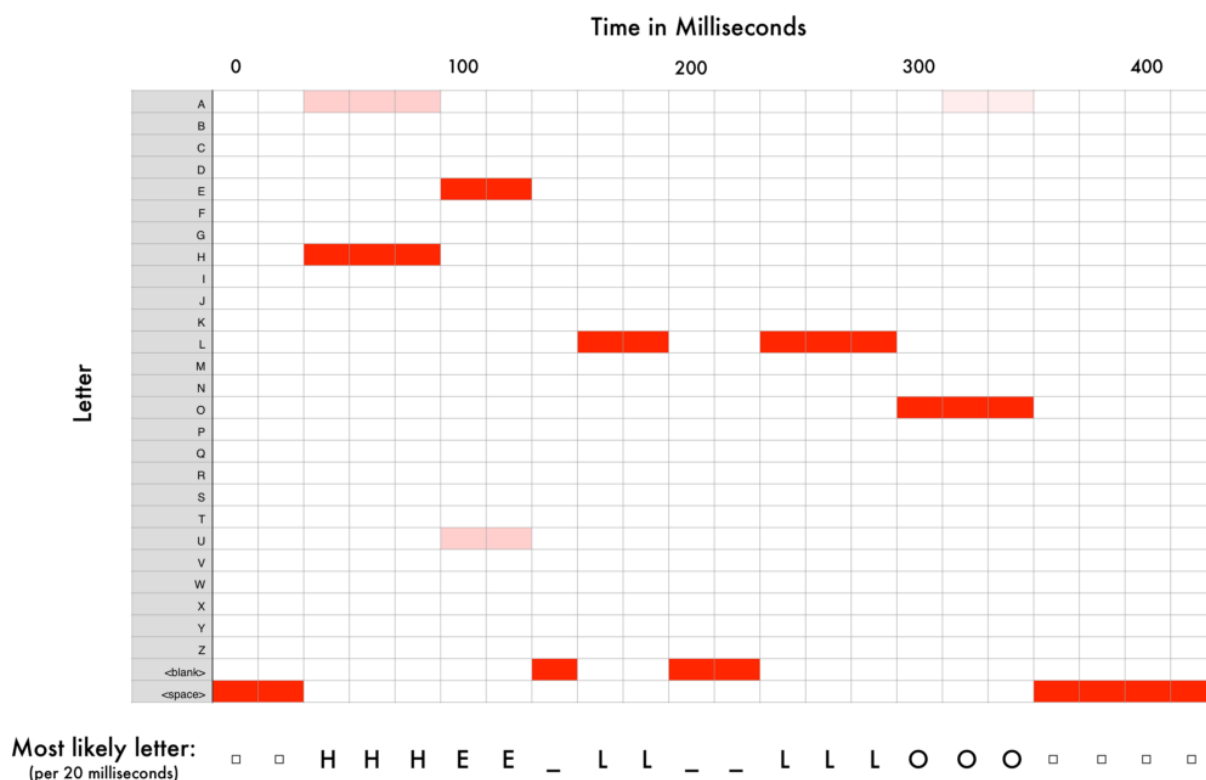
Слика 12. Рекурентна невронска мрежа



Adam Geitgey, "Machine Learning series of articles", 2016

Ќе користиме рекурентна невронска мрежа - т.е. невронска мрежа која има меморија која влијае на идните предвидувања. Тоа е затоа што секоја буква што ја предвидува треба да влијае на веројатноста на предвидување на следната буква. На пример, ако сме рекле "HEL", многу е веројатно дека ќе кажеме "LO" до завршувањето на зборот "Hello". Многу е помалку веројатно дека следно ќе речеме нешто како "XYZ". Значи имајќи ги во меморија претходните предвидувања им помага на невронските мрежи да направат попрецизни предвидувања за она што следува. Откако ќе го поминеме целиот аудио клип низ нервната мрежа (сегмент по сегмент), ќе завршиме со мапирање на секој аудио сегмент во букви што најверојатно се изговорени за време на тој дел. Еве како изгледа тоа мапирање за зборот "Hello":

Слика 13. Манирање за зборот "Hello"



Adam Geitgey, "Machine Learning series of articles", 2016

Имаме неколку чекори што ги следиме за да го исчистиме овој излез. Прво, ние ќе ги замениме сите повторени знаци со еден карактер:

- HHHEE_LL_LLLOOO станува HE_L_LO
- HHUU_LL_LLLOOO станува HU_L_LO
- AAUU_LL_LLLOOO станува AU_L_LO

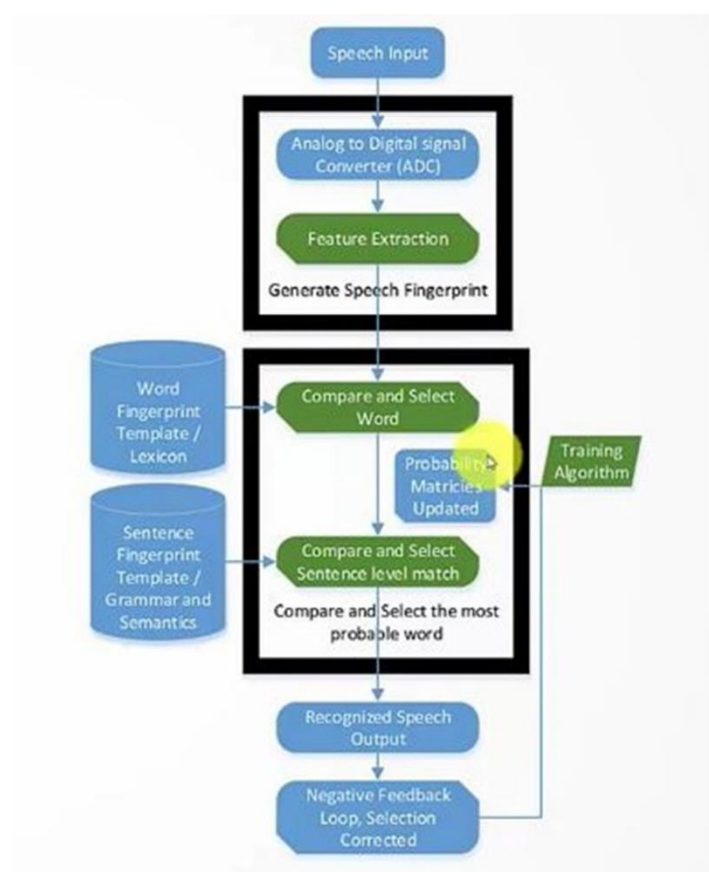
Потоа ќе ги отстраниме сите празнини:

- HE_L_LO станува HELLO
- HU_L_LO станува HULLO
- AU_L_LO станува AULLO

Тоа ни остава три можни транскрипции - "Hello", "Hullo" и "Aullo". Ако ги кажете гласно, сите овие звуци се слични на "Hello". Бидејќи таа предвидува еден карактер во единица време, невронската мрежа ќе ги даде овие транскрипции. На пример, ако кажете "He would not go", тоа би можело да даде една можна транскрипција како "He wud not go". Трикот е да се комбинираат овие предвидувања базирани на изговорот со оценки за веројатност врз основа на голема база на податоци од пишан текст (книги, статии од весници и сл.). Се исфрлаат транскрипциите што изгледаат најмалку веројатни да бидат вистински и се задржат транскрипциите што се чини дека е најреална. Од нашите можни транскрипции "Hello", "Hullo" и "Aullo", очигледно "Hello" ќе се појави почесто во текстуалната база на податоци (а секако и во нашите оригинални аудио-базирани податоци за обука) и на тој начин веројатно е точна. Затоа ќе го избереме

"Hello" како наша конечна транскрипција наместо другите. Можеби размислувате "Но, што ако некој навистина рече" Hullo "? Тоа е валиден збор. Можеби "Hello" е погрешна транскрипција! ". Се разбира дека е можно некој да каже "Hullo" наместо "Hello". Но, системот за препознавање говор како овој (обучен на американски англиски) во основа никогаш нема да го произведе "Hullo" како транскрипција. Тоа е толку неверојатно нешто што корисникот може да го каже во споредба со "Hello" така што алгоритмот секогаш ќе мисли дека велите "Hello", без разлика колку го нагласувате звукот "U". Ако вашиот телефон е поставен на американски англиски, обидете се да го добиете дигиталниот асистент на вашиот телефон за да го препознаете зборот "Hullo". Не можете! Секогаш ќе го разбере како "Hello". Неприфакот на "Hullo" е разумно однесување, но понекогаш ќе најдете случаи каде што вашиот телефон само одбива да разбере нешто валидно што го кажувате. Затоа овие модели за препознавање говор секогаш се обучуваат со повеќе податоци со цел да ги опфатат овие гранични случаи. Сумирано, ова се компонентите кои ги има еден стандарден алгоритам за препознавање на говор[5,6,7].

Слика 14. Шематски приказ на стандарден алгоритам за препознавање на говор



Casey Petersen, A Guide to Speech Recognition Algorithms, 2015

Заклучок

Автоматското препознавање говор како процес на преведување на изговорени зборови денес е една од главните предизвикувачки задачи во компјутерската технологија. Моделите базирани на примената на длабоки невронски мрежи станува доминантен модел за препознавање на говор и се повеќе преовладува во имплементацијата во многу индустрии и апликации.

Длабокото учење (Deep Learning) како нова област во машинското учење со можностите кои ги нуди и едноставноста во имплементацијата би можело во иднина да претставува основа за решавање и на други проблеми од вештачката интелигенција (AI).

Користена литература

1. Ристо Христов, PhD, "Препознавање на облици, предавања", EURM, 2015
2. Adam Geitgey, "Machine Learning series of articles", 2016
3. Yan Zhang, "Speech Recognition Using Deep Learning Algorithms", 2016
4. Judith Hurwitz and Daniel Kirsch, "Machine Learning", John Wiley & Sons, Inc., 2018
5. V.T.UmrilaShrawanker, "Techniques for feature Extraction in Speech Recognition systems: a Comparative study", 2015
6. C.L. Shanthi Therese, Review of Feature Extraction Techniques in Automatic Speech Recognition, International Journal of Scientific Engineering and Technology, Vol 1, No 6, pp 19-24, 2013
7. Casey Petersen, A Guide to Speech Recognition Algorithms, 2015

БИЗНИС МОДЕЛ - СПОДЕЛУВАЊЕ

UDC: 005.591.4:629]:004.822

Прегледен труд

005.591.4:661]:004.822

Проф. д-р Билјана Андреска Богдановска¹, проф. д-р Митко Ивановски², Проф. д-р Лидија Наумовска¹

¹Европски Универзитет Република Македонија – Скопје

²Аџибадем Систина

Апстракт

Компаниите сè повеќе ги сфаќаат придобивките од процесот на споделување, гледајќи го енормниот економски раст на компаниите кои први го примениле овој процес на споделување ресурси и затоа скандалозно брзо го менуваат принципот на работа, со години негуван. Инвестициите за истражување и развој во раните фази во фармацевтската и автомобилската индустрија, често преку конзорциум на партнери, со назначување на клучни луѓе, создаваат заеднички проекти, кога лидерите ја гледаат вистинската можност за бизнис. Современите трендови забележуваат позајмување на експерти од други компании преку сеопфатни начини, преку платформи за размена на вработени.

Клучни зборови: *вештачка интелигенција, софтверска платформа, бизнис модел, споделување*

BUSINESS MODEL – SHARING

Abstract

Companies are increasingly grasping the benefits of the sharing process, looking at the enormous economic growth of companies that first realized this process of sharing resources and therefore scandalously quickly change the principle of work, with years of care. Research and development investments in the early stages of the pharmaceutical and automotive industry, often through a consortium of partners, with the appointment of key people, create joint projects when leaders see the right business opportunity. Modern trends note the lending of experts from other companies through comprehensive ways through employee exchange platforms..

Key words: *artificial intelligence, softver platform, business model, sharing*

Вовед

Компаниите сè повеќе ги сфаќаат придобивките од процесот на споделување, гледајќи го енормниот економски раст на компаниите кои први го сфатиле овој процес на споделување ресурси и затоа

скандалозно брзо го менуваат принципот на работа, со години негуван. Инвестициите за истражување и развој во раните фази во фармацевтската и автомобилската индустрија, често преку конзорциум на партнери, со назначување на клучни луѓе, создаваат заеднички проекти, кога лидерите ја гледаат вистинската можност за бизнис. Современите трендови забележуваат позајмување на експерти од други компании преку сеопфатни начини, преку платформи за размена на вработени. Еден он-лајн пазар за персонал со кој раководи Elance и oDesk, разменува сајтови за хонорарни работни места, и заработува 750 милиони долари годишно. Таквите платформи им овозможуваат на фирмите да регрутираат флексибилна работна сила, ориентирана кон задачата, без да се грижат за тоа како да ги задржат, за време на криза.

Во современиот свет, ниедна економија не може да се замисли без бизнис моделот – **споделување**, односно, популарното „**sharing**“. Тоа има силно влијание во животот на граѓаните на општеството, бидејќи штеди пари и човечки ресурси. Карактеристичен пример е превозот преку Uber, или сместувањето преку booking, Airbnb, слушањето музика преку Spotfy, или споделување информации на блогот Reddit¹.

Сите овие деловни модели не би можеле да функционираат, без гуруто на вештачката интелигенција, Danny Lange, данскиот компјутерски научник, кој застана позади Amazon, Uber, и Unity. Тој му ја даде на светот платформата за машинско учење на овие три технолошки гиганти. Ланге исто така ја направил платформата за создавање на видеоигри, Unity, со цел да се развиваат работи, подоцна во секоја сфера на животот и работата.

Споделување

Трендот на споделување претставува исто така поголема можност за потрошувачите. Тоа е отворена размена на ресурси помеѓу бизнисите: меѓусебна размена. За само неколку години на активност, стана јасно дека неограничената размена на инаку неискористени големи средства, вклучувајќи го физичкиот простор, човечките ресурси и индустриската опрема, им овозможува на компаниите за споделување да работат поефикасно од своите не-споделувачки ривали. Компаниите кои сесрдно го прифаќаат споделувањето на материјални средства, може да имаат корист од различен вид на промени, во кои е вклучена културата, која гради нови видови врски и сочувство кон светот. Со кинење на сидовите - без разлика дали се „недоволно искористени таленти“ или „имаме одлично знаење, но не сме сигурни како да го претворите во нешто што луѓето сакаат да го купат“ - овие компании можат и да ги подобрат своите сопственички удели, во крајна линија и да придонесат за колективното добро.

Веројатно, најраспространетата пракса за споделување на компаниите вклучува неискористени недвижности, што е сè поголем товар за профитабилноста. Ако го читате ова во типична канцеларија,

¹www.fastcompany.com *By Sean Captain*

половина од клупите околу вас можеби се слободни за размена. Но, бизнисите сега можат да најдат дигитални платформи, кои создаваат глобални врски меѓу сопствениците и закупувачите кои ќе им помогнат, поефикасно да ги користат овие средства.

На пример, Sharemyoffice.co.uk, нуди услуга, издавање резервен деловен простор, со која ги поврзува краткорочните станари со бизниси.

Слично на тоа, синцирот на хотели „Мариот“ ги претвори празните конференциски сали во изнајмувачки работни простори преку он-лајн платформата LiquidSpace².

Сето ова може веднаш да се сподели на Твитер, LinkedIn, Facebook, Google.

Вистинската моќ на размена може да се најде во B2B трансакции. Може да се изнајми (сподели), произведен капацитет или опрема. Ова е важно бидејќи денешните фабрики работат со ангажираност од околу 20 проценти, помалку од капацитетот. Во 2011 година, Med-Immune (единица за биологија на фармацевтската компанија AstraZeneca), се согласи да ги сподели своите производствени капацитети со колегите од фармацевтскиот гигант Мерк.

Како што се појавуваат он-лајн платформи кои се ориентирани кон индустриски компании, сè повеќе ќе биде изводливо да се споделат вишокот сировини, дистрибутивна инфраструктура и други капитални трошоци. На пример, FLOW2, холандски старт ап, го олеснува споделувањето на опрема, производството на средства и времето на вработените, правејќи ги транспарентни и разменливи на својата он-лајн размена. Компанијата, исто така, развива сопственички технолошки платформи, кои им овозможуваат на компаниите да градат споделување на нивните продукти. Заедничките извори на платформи, исто така, би можеле да ги подобрат напорите за одржливост, што ќе им олесни на компаниите да ја здружат набавката на материјали, со мало влијание врз животната средина.

Пазарот за споделување на нематеријални средства - мозокот, знаењето и интелектуалниот капитал на компанијата - покажува исто толку ветувања. Во многу компании, на пример, техничката експертиза е сериозно недоволно искористена, едноставно поради тоа што работата на персоналот не се совпаѓа со актуелните стратешки приоритети на компанијата. Но, наместо да ги отуѓи своите капацитети, компанијата може да го дели својот персонал со други компании.

Во извесна смисла, компаниите го менуваат својот мозок на овој начин со години. Инвестициите за истражување и развој во раните фази во фармацевтската и автомобилската индустрија, често се случуваат преку конзорциум на партнери, со назначување на клучните луѓе, што се случува кога лидерите ја гледаат вистинската можност за бизнис. Но, сега експертите можат да се позајмат на други компании на многу потешки, сеопфатни начини, преку платформи за размена на вработени. Еден он-лајн пазар за персонал со кој раководи Elance и oDesk, разменуваат сајтови за хонорарни работни места и заработуваат 750 милиони долари за таа работа годинава. Таквите платформи им овозможуваат на фирмите да регрутираат флексибилна работна сила, ориентирана кон задачата, без да се грижат за тоа како да ги задржат за време на криза. Тие, исто така, веројатно ќе привлечат повеќе талентирани луѓе, кои сега можат да стекнат вакви

²Rachel Botsman noted in the September 2014 issue of [Harvard Business Review](#)

креативни можности кај повеќе компании, кои обично се достапни само кај еден работодавач. Овој пристап на најдоброто од двата света може да се смета за најзавиден начин за работа.

Интелектуалниот капитал е друго нематеријално средство со потенцијал за споделување. Техноинтензивните компании натрупуваат големи залихи на патенти. Во првите пет американски патентни досиеја - IBM, Samsung, Canon, Sony и Microsoft - заедно поднеле повеќе од 21.000 во 2013 година. Но, само мал дел од сите поднесени патенти се ставаат на продуктивна употреба, поради инвестицијата вклучена во носењето производи на пазар.

Иновации во светските компании

Компаниите Quirky и General Electric планираа да донесат неколку производи на пазарот, вклучувајќи го и паметниот контролиран климатик; мерач на резервоарот на пропан кој покажува кога горивото е ниско; и домашен монитор кој потрошувачите можат да го постават за да ги следат движењето, звукот, светлината или температурата според нивната дискреција. (Во септември 2014 година, Quirky го изгуби пристапот до патентите на апаратот на GE, кога Електролюкс го купи бизнисот на GE, чија понуда на Quirky не победи.)

Потенцијалот тука не е само да се соберат идеи од надворешни пронаоѓачи, преку отворени иновации. Ниту, пак, тоа е начин да се отвори платформа за трети лица, програмери да се воведат за помошни производи и софтвер, како компјутерски компании кои го прават тоа со децении. Вистинскиот потенцијал е да се развијат нови платформи кои нудат еден сегмент од базата на интелектуална сопственост на компанијата, така што другите можат да сторат нешто со тоа, а сопственикот на патентот може да профитира. Во сегашната форма на овој однос, двете страни соработуваат во пронаоѓање иновации на пазарот.

Кинеската компанија за апарати Haier, на пример, ги повикува пронаоѓачите, надвор од компанијата, да предлагаат иновации што би можеле да ги произведат заедно.³ Но, соработката можеби не е секогаш неопходна. Компанијата со патент за нов тип технологија на батерии, на пример, може да избере да не ја развива, но со ставање на технологијата на батеријата на размена, компанијата може да направи врска со друга компанија со комплементарна технологија, која инаку никогаш нема да ја направи. Во некои технолошко интензивни индустрии, повеќе ликвиден пазар во интелектуалната сопственост гледа конкурентите да станат соработници. Епл објави широк спектар договори за лиценцирање на патент со НТС во 2012 година. Google и Samsung се согласија да ги споделат сите нови патенти поднесени во текот на следната деценија. Постои можност за такви договори да помогнат во спречувањето на скапи патентни војни, ослободувајќи ги ресурсите со кои компаниите можат да се фокусираат на иновациите.

³Art Kleiner, The Thought Leader Interview: Zhang Ruimin.

Искусството со напорите за споделување на потрошувачите како Airbnb сугерира дека учесниците стануваат поколегијални и сочувствителни, бидејќи нивното искуство не е само трансакциско. Нешто слично може да се случи во бизнисот, бидејќи раководителите и вработените ги споделуваат своите ресурси, нивната интелектуална сопственост, нивното време и работен простор. Тоа би можело да биде најголема корист за сите, што ќе резултира со поголема ефикасност, појестока работна сила и нови производи и услуги кои ќе ги задоволат потребите на потрошувачите.

Можностите се ограничени само од имагинацијата на носителите на одлуки.

Бидејќи тие создаваат размени кои овозможуваат повеќе B2B врски и ги користат тие размени ефикасно и креативно, тие ќе најдат повеќе и различни начини да профитираат од нивните напори како споделување на компании.

Во овој бизнис има повеќе заработка, отколку заработка по акција. Капиталните трошоци се занемарливост за помагање на компаниите кои ги зголемуваат готовинските текови - и на крајот тоа му се враќа на акционерот.

Деловните медиуми, финансиските аналитичари и многу менаџерски тимови, се интензивно фокусирани на корпоративните приходи. Бизнис коментаторите се опседнати со профитот на компанијата по акција (ЕПС), со споредување со минатогодишниот квартал и она што се очекува да биде во следниот квартал. Тимовите за управување често ги рационализираат структурите на трошоците за да можат да водат побрз пораст на заработката. Како и да е, сè уште Кеш е крал, а вредноста на компанијата во крајна линија е поттикната од пазарните очекувања за идните парични текови. На врвот на управување со приходи, управувањето со готовинските текови значи искористување на капиталните инвестиции кои се направени за генерирање на тие заработки, како што се купување на опрема, финансирање истражувања и развојни трошоци и плаќање на набавки. Иако компаниите направија големи чекори во оптимизирањето на приходите, многумина се борат со капиталните трошоци.

Подобрувањето на распределбата на капиталот е особено важно во капитално-интензивните индустрии. Да наведеме еден пример: По воведување на стандардизирана рамка за вредности, фокусирана на клучните двигатели на вредност и водење на портфолиото преку оптимизиран модел, една голема енергетска компанија ги намалила капиталните трошоци за 50 отсто, а генерирала ист принос.

Нивоата на капитални трошоци значително варираат во индустријата. Во индустриите како што се комуналии, енергија, транспорт, телекомуникациски услуги и автомобили и компоненти, компаниите реинвестираат повеќе од 50 проценти од оперативните парични текови во бизнисот секоја година, во вид на капитални расходи. Инвестициите што ги прави компанијата, нивниот раст и времето на бенефиции ја одредуваат идната вредност на компанијата.

Штедењето, по пат на изнајмување, односно со моделот на споделување е вистинска причина за намалување на капиталните трошоци.

Тимовите за менаџирање честопати се борат да постигнат конзистентни, позитивни резултати, бидејќи анализата и оптимизирањето на капиталните трошоци е сложена задача. Тоа бара менаџментот да ги процени во некои случаи стотици инвестиции и да им даде приоритет врз основа на голем број финансиски и нефинансиски ограничувања за да одлучи кои проекти ќе ги финансираат, и според кој редослед. Процесот на распределба бара три елементи: робусна методологија за вреднување, софистицирани алатки за оптимизација и сеопфатен процес на управување.

Вреднување

Компаниите треба да започнат со стандардизирана, робусна методологија за вреднување на индивидуално ниво на проектот, која го опфаќа целиот спектар на придобивки, како и релевантниот профил на ризик и дистрибуција на потенцијалните резултати. Ова е слично со анализите што многу компании ги прават од постојните деловни портфолија и се вкоренети во логиката на вредно инвестирање, пример од Ворен Бафет и неговиот поранешен ментор, инвестициски научник Бенџамин Греам.⁴

Но, разбирањето на лидерите за финансиска вредност е само почеток. Компаниите мора да го сфатат и квантифицираат придонесот на секој проект, заедно со клучните нефинансиски стратешки вредносни двигатели, како што се регулаторните ефекти и влијанието на перцепциите и застапеноста на засегнатите страни, безбедноста, животната средина и здравјето и безбедноста. Иако овие компоненти може потешко да се квантифицираат, тие можат да бидат значајни фактори за долгорочната вредност на компанијата.

Споделување на автомобили, Airbnb, најголем синџир на хотели

Споделување на автомобили (AU, CA и US) е модел на рент-а-кар, каде што луѓето изнајмуваат автомобили за куси временски периоди, честопати по час. Тие се атрактивни за купувачите кои само повремено користат возило. Организацијата што ги изнајмува автомобилите може да биде комерцијален бизнис или корисниците можат да бидат организирани како компанија, јавна агенција, кооперативна или ad hoc групација. Споделувањето на автомобили е дел од поголем тренд на споделена мобилност. Споделената мобилност ги вклучува сите начини на патување кои нудат краткорочен пристап до превоз по потребна основа, или за личен транспорт или испорака на стоки.⁵ Услугите се достапни во повеќе од 1.000 градови во неколку земји. Заклучно со декември 2012 година, имаше околу 1.7 милиони членови за споделување на автомобилите во 27 земји, вклучувајќи ги т.н. peer-to-peer услуги, според Центарот за истражување на одржливост на транспорт на U.C. Беркли⁶. Од нив, 800.000 беа членови на споделување

⁴Aaron Gilcreast and Larry Jones The Real Value of Your Company, October 2, 2017

⁵ www.pwc.co.uk

⁶ www.pwc.co.uk

на автомобилите во САД. Во 2017 година, се формираше car2go, која денес е најголемата компанија за автомобили во светот со 2.500.000 регистрирани членови и флота од скоро 14.000 возила на 26 локации во Северна Америка, Европа и Азија, по што следи Zipcar со 767.000 членови и 11.000 возила. Според Навигант Консалтинг, приходите од услуги за глобални автомобили достигнуа една милијарда долари во 2013 година и ќе растат до 6,2 милијарди американски долари до 2020 година, со над 12 милиони членови низ целиот свет. Главните фактори кои го поттикнуваат растот на автомобилите се зголемувањето на застојот со кои се соочуваат градските жители; менувањето на генерациските мисли за сопственоста на автомобилите; зголемување на трошоците за сопственост на лични возила; и конвергенција на бизнис модели. Carsharing придонесува за одржлив транспорт, бидејќи тоа е помалку автоинтензивно средство за урбан транспорт, а според „Економист“, овој вид транспорт може да ја намали сопственоста на автомобилите со проценета стапка на еден автомобил за замена, кој ќе ги замени 15 возила во сопственост⁷.

Друштвото за споделување peer-to-peer е мирна B2B револуција

Од средината на 2000-тите, таканаречената економија за споделување се зголеми од речиси ништо, во базенот на глобални бизниси вреднувани во милијарди долари. Концептот - луѓето што ја користат технологијата за да пронајдат и купат дополнителни ресурси од еден на друг - претставува триумф на доверба. Финансиските фирми од типот „кредити“, транспортните услуги како што се Uber и сместувањето на туристи, како Airbnb, брзо ги симнаа, користејќи интернет-платформи за директно поврзување на луѓето без високоплатените посредници. Не е ни чудо што инвеститорите се толку заинтеригирани, а остатокот од нас се малку загрижени од таа возбуда⁸.

Една од жешките теми досега оваа година е она што ќе стане со услугите на P2P и економијата за споделување. Минатата година Airbnb стана најголем синцир на хотели во светот, Убер се прошири во странство со големи протести од актуелните во такси индустријата, а лекувањето клуб на P2P-давателот на кредити доби на котација на Вол Стрит. Во исто време, ПВК ја проценува економијата за споделување со цел да генерира приходи до 335 милијарди американски долари до 2025 година, а само Убер ќе биде проценета на 41 милијарда долари. Милениумската генерација, исто така, изрази недостаток на доверба кај операторите и желбата за алтернатива, а претпочиташе да им верува на врсниците над брендовите. Со предвидувањата на економијата за споделување кои влијаат речиси на сите индустрии, вложувачите на капитал вложуваат инвестиции во она што, се надевам, е следниот Убер.

⁷Robert Vaughan, is an economist with PwC's economics and policy team, and is based in London, www.Strategy Business.com
Reprint No. 0028

⁸www.strategy-business.com

Заклучок

Со оглед на тоа што економијата за размена станува распространета, исто така, се јавуваат критики од функционерите, вниманието од регулаторите и барањата од учесниците. Заеднички именител на овие реакции е како што беше наведено од страна на Harvard Business Review, дека економијата за споделување не е за споделување воопшто. Она што се гледа од новите услуги за споделување, се всушност комерцијални платформи кои ја пренесуваат дистрибуцијата од традиционална дистрибуција до дигитални екосистеми. Можностите се огромни, а можат да бидат ограничени само од имагинацијата на носителите на одлуки.

Литература

1. www.fastcompany.com *By Sean Captain*
2. Rachel Botsman noted in the September 2014 issue of Harvard Business Review
3. Art Kleiner, The Thought Leader Interview: Zhang Ruimin,
4. Aaron Gilcreast and Larry Jones The Real Value of Your Company, October 2, 2017
5. www.pwc.co.uk
6. www.pwc.co.uk
7. Robert Vaughan, is an economist with PwC's economics and policy team, and is based in London, www.Strategy Business.com Reprint No. 0028
8. www.strategy-business.com

ЕКОНОМСКИ ИМПЛИКАЦИИ НА AI И ИНДУСТРИЈАТА 4.0 ВРЗ КОМПАРАТИВНАТА ПРЕДНОСТ НА НАЦИОНАЛНИТЕ ЕКОНОМИИ

UDC: 334.72:338.45]: 004.896

*Прегледен труд***Проф. д-р Зоран Јолевски***Европски Универзитет Република Македонија – Скопје*

Апстракт

Индустрија 4.0. се состои од "паметни фабрики" во кои процесот на производство е управуван од автоматизирани системи, роботи и вештачка интелигенција која ги интегрира неопходните информации за автоматските одлуки за производство на "паметни производи". Новиот модел на индустрија се базира на интегрирање на машини со компјутери, а вештачката индустрија кој управува со производните процеси.

Вештачката интелигенција придонесува за промени во организациската структура на компаниите, ефикасноста, продуктивноста и спецификите на компаниите, видот на средствата потребни за нивното функционирање и влијае врз пазарот на работна сила. Владите не треба да се мешаат во бизнисот, но неопходно дадат поддршка на компаниите за истражување и развој и да посветат посебно внимание на создавање на човечки ресурси со вештини потребни кои ги бара Индустријата 4.0. и вештачката интелигенција.

Оваа индустриска револуција се движи експоненцијално и веќе почна сериозно да го промени типот на потребните средства на компанијата и оттаму конкурентноста на компаниите. Земјите чии компании ги користат придобивките од AI и влегуваат во производствениот процес Индустрија 4.0 ќе бидат поконкурентни на меѓународните пазари. Од друга страна, националните економии чии компании нема брзо да го ангажираат и усвојат концептот Индустрија 4.0, каде што AI има доминантна улога, ќе заостанува во развојот.

Развиените индустриски земји треба да вложат напори да создадат услови за најмалку развиените и економиите во развој да имаат корист од Индустријата 4.0, во спротивно, јазот меѓу развиените земји и земјите во развој ќе се зголеми.

Клучни зборови: *Индустрија 4.0, вештачка интелигенција, компаративна предност, продуктивност*

THE ECONOMIC IMPLICATIONS OF AI AND THE 4.0 INDUSTRY ON THE COMPARATIVE ADVANTAGE ON NATIONAL ECONOMICS

Abstract

Industry 4.0 is consisted of "smart factories" in which the production process is managed by automated systems, robotics and artificial intelligence (AI) that integrates the necessary information for making the automated decisions for the production of "smart goods". The new model of industry is based on integrating machines with computers, and AI manages production processes.

AI contributes to changes in the organizational structure of companies, the efficiency, productivity and the specificity of the companies, type of assets required for their operation, affects the job markets etc. The governments should not interfere in the business, but it is necessary to support the research and development of the companies and pay special attention to the creation of human resources with skills needed to meet the requirements of the Industry 4.0. and AI.

This industrial revolution is moving exponentially and has already begun to seriously change the type of company assets needed and hence the competitiveness of companies. Countries whose companies are using the AI benefits and are entering in Industry 4.0 production process will be more competitive on international markets. On the other hand, national economies whose companies will not quickly engage and adopt the Industry 4.0 concept, where AI has a dominant role will lag behind in development.

Developed industrial countries should make efforts to create conditions for the least developed and developing economies to benefit from Industry 4.0 otherwise, the gap between developed and developing countries will increase.

Key words: *Industry 4.0; Artificial Intelligence; comparative advantage, productivity*

Вовед

Вештачката интелигенција (Artificial Intelligence – AI) е основа за развој на Индустијата 4.0, која ја сочинуваат „паметни фабрики“ во кои производствениот процес е управуван од автоматизирани системи, роботика и преку вештачка интелигенција ги интегрира по потребните информации за носење на автоматизирани одлуки за производствена „паметна стока“. Новиот модел на индустрија се базира на интегрирање на машините со компјутерите, а вештачката интелигенција ги управува производствените процеси.

Индустијата 4.0 придонесува за зголемување на продуктивноста на капиталот и работната сила и со тоа и на конкурентноста. Од навременото вклучување на државите во оваа индустриска револуција зависи позиционирањето на националната економија во светската, односно и ќе биде одлучувачки за компаративната предност на секоја национална економија. Затоа неопходно е компаниите, но и државите

да донесат соодветни бизнис стратегии, односно национални стратегии за искористување на предностите што ги носи Индустриската револуција 4.0 и вештачката интелигенција. Големите корпорации имаат капацитет и ресурси самостојно да вложуваат во иновациите, развојот на нови методи на производство со кои се зголемува продуктивноста. Исто така, општествата, односно државите каде што иновативноста се стимулира, каде се поттикнуваат луѓето кои имаат идеи за подобрување на постојните производствени процеси или стоки, или пак за нови производни постапки или нови производи и услуги, имаат поголеми шанси за успех и обезбедување подобра позиција во светската економија. Значи за успешно вклучување на националните економии во тековите на современата светска економија треба нов посебен микс на политики, како на државно ниво, така и на корпоративно ниво, но и промени во општеството.

Факторите за производство како што се капитал, работна сила, природни богатства не се гаранција за успех во економијата која брзо и драматично се менува. Дури и технологијата, доколку перманентно не се инвестира во нејзин развој, не е веќе гаранција. Националната економија и општеството во една држава треба да се определат дали се стремат да бидат лидери во Индустриската револуција 4.0, дали ќе бидат имплементатори, или пак ќе останат во класичната економија? Првата опција прилично захтевна и само одреден број на национални економии ќе можат да бидат лидери. Последната опција, продолжување на функционирање на економијата и општеството со традиционалниот и класичен модел е рецепт за заостанување во компаративните предности. Еден сериозен дел од националните економии ќе се најдат во категорија на имплементатори на Индустриската револуција 4.0 и вештачката интелигенција. Но за да можат добро да се позиционираат во рамките на оваа група неопходно е да создадат соодветно опкружување во:

- правниот систем (каде клучно место ќе има заштитата на интелектуалната сопственост, ефикасен судски систем за заштита на интересите на корпорациите, предвидливост на правната легислатива поврзана со економскиот систем, правна регулатива која обезбедува флексибилни работни односи)
- образовниот систем, вклучувајќи го тука и системот на животно учење, кој ќе продуцира работна сила со вештини потребни за новата Индустрија 4.0.
- создавање на општество во кое ќе почитуваат и охрабруваат лицата и компаниите кои се стремат кон нови работи, институции и индивидуи кои прифаќаат промени, организации во кои се знае како се менаџираат промените и сл.

Вештачката интелигенција (Artificial Intelligence –AI) предизвикува за сериозни промени во организационата поставеност на компаниите, влијае врз продуктивноста и конкурентноста на компаниите, но и врз потребните квалификации на работната сила. Државата не смее да се меша во бизнисот, но неопходно е ги поддржи истражувачките и развојните активности на компаниите, а посебно внимание да посвети на создавање на кадровски ресурси подготвени да одговорат на барањата на Индустријата 4.0. и AI.

„Извештајот за работните места во иднина“, подготвен од Светскиот економски форум¹, укажува дека во следните 5 години ќе дојде до значајни промени во соодносот меѓу задачите што ќе ги извршуваат луѓето и машините. Така во 2018 година во 12-те индустрии кои се анализирани во овој Извештај, 71% од потребното време за производство се врши од страна човек, додека 29% се врши од машини и алгоритми. Според Извештајот, во 2022 година човечкиот ангажман изразен во време поминато за производство на одреден производ ќе се намали на 58%, дека пак 42% ќе биде извршено од машини и алгоритми.

Ова не значи дека потребата од човечкиот труд ќе се намали во целина, туку ќе се променат квалификациите што е потребно да ги има работната сила за новиот вид индустриски и услужни компании. Ова укажува на потребата за брза промена на образовниот систем, но и премин кон т.н. доживотно учење. Промените во економијата што ќе настанат следните 25 години ќе бидат многу поголеми од тие што настанале последните два века. Неопходноста за постојано доусовршување, па и преквалификување на работната сила, ќе стане императив за секоја национална економија. Голем број професии се во фаза на изумирање и ќе бидат преземени од автоматизирани системи. Потребата за шалтерски работници во банките, туристичките агенции и некои други бизниси полаку изумира. Транспортот кој моментално е една од стопанските гранки кои вработува голем број лица, со појавата на камиони, автобуси и такси возила кои ќе бидат управувани со AI солүции драстично ќе ја намали потребата за возачи. Но паралелно со ова ќе се зголеми потребата за одржување на овие системи, нивно сервисирање и сл. Според McKinsey Global Institute AI, роботиката и автоматизацијата со 2030 година ќе елиминираат околу 73 милиони работни места само во САД. Но истовремено, Извештајот укажува Индустриската револуција и Вештачката интелигенција не само што ќе ја зголеми продуктивноста, туку ќе креира и многу нови работни места. Така според истиот Извештај до 2022 година ќе се креираат нови 135 милиони работни места. Значи новата економија ќе создава нови работни места, но за да тие бидат пополнети неопходно е работната сила да има соодветни квалификации, кои се разликуваат од денешните. За да се постигне успех во оваа трансформација неопходно е индивидуите, кооперациите, државата, но и општеството во целина, да бидат определени да ги искористат потенцијалите и можностите кои се пред нив. Индивидуите треба да се свесни и целосно посветени на изучување на новите вештини кои ќе бидат потребни во новата економија. Секоја индивидуа треба да го прифати и целосно да се посвети на концептот на животно учење, односно постојано надградување со вештини кои се потребни на пазарот на трудот. Корпорациите, исто така, треба бидат подготвени поинтензивно да инвестираат во обуки и доквалификации на нивните вработени. Државата треба да го трансформира образовниот процес, со цел да се произведат кадар со знаења и вештини потребни за новата Индустрија 4.0 базирана врз вештачката интелигенција.

Пол Ромер, еден од двата добитници на нобеловци за економија за 2018 година, ја доби наградата за неговиот придонес за природата и значењето на иновациите во економскиот раст. Според него

¹ World Economic Forum - Centre for the New Economy and Society: The Future of Jobs Report 2018, Женева 2018 г.

децентрализираните пазари не можеле самите да обезбедат поддршка за развојот на нови идеи и технолошки иновации. Новите идеи се јавно добро и од новите технологии има корист целата економија, односно општество. Но можна е ситуација во која тие кои ги создале иновациите да не се соодветно наградени. Ова може да резултира во опкружување во кое иноваторите нема да бидат стимулирани за иновации. Недостатокот на иновации, според Ромер, треба да се реши преку креирање политики со кои вистински ќе се стимулираат иновациите, односно иноваторство. Ова не е нова идеја, но Ромер е првиот економист што го претстави во траен модел за економски раст. Во неговите анализи и препораки за политиките што треба обезбедат економски развој се инвестициите во човечки капитал, поддршката на истражувањето и развојот, и носење и спроведување на легислатива за заштита на правата што произлегуваат од интелектуалната сопственост.

Според Првиот Индекс на човечки капитал², кој го објави Светска банка во октомври 2018 дете родено денеска во Македонија ќе достигне 53% од својот потенцијален човечки капитал кога ќе стане полнолетно, во споредба со она што би можело да го достигне доколку има квалитетно образование и биде потполно здраво. Ако се има предвид дека природните ресурси, расположливиот капитал и нивото на технолошки развој на Македонија се релативно скромни, тогаш човечкиот капитал е најважен за нејзиниот економски развој. Анализата на Светска банка покажува дека Македонија треба да направи сериозни напори да го подобри образовниот процес со цел да биде конкурентна на светскиот пазар. Воедно неопходни се реформи во високото образование, но и во неформалното образование.

Постепено ќе се менува и изгледот на работното место. Веќе се гледаат промени во консултантските компании, каде што повеќе од нивните вработени работат од дома. Големите управни згради се трансформираат во т.н. хотел канцеларии и сали за состаноци. Вработените повеќето задачи ги извршуваат дома користејќи ги персоналните компјутери, а само кога треба да одржат состанок се појавуваат во некоја од претходно резервираните канцеларии. Така една од петте најголеми консултантски компании во САД, Буз Ален Хамилтон, задржа само една од трите згради во нивната централа во МекКлејн во близината на Вашингтон и покрај тоа што бројот на вработени остана ист. Ова овозможува поголема флексибилност како кај вработените така и кај менаџментот. Но истовремено бара вложувања во поставување на матрици за задачи кои треба да бидат исполнети и следење на реализираните проекти, односно постигнатите цели.

Понатаму, во иднина ќе се зголемува бројот на работни места кои ќе бидат аутсорсирани. Се помал дел од вработените ќе бидат постојано ангажирани со полно работно. Се повеќе ќе се ангажираат работници, експерти, инженери и сл. на определено време, односно само кога ќе има потреба. Флексибилноста на работната сила е особено значајна. Државите треба да ги променат регулативите што се однесуваат на трудот, да овозможат поголема флексибилност, како за компаниите така и за вработените. Воедно треба да се промени општеството, да ја прифати реалноста дека ќе има се помалку

²Дефиниција на Светска банка за Индексот на човечки капитал: Индексот е дизајниран со цел определи обемот на човечки капитал што ќе го има дете родено денеска кога ќе наполни 18 години

постојано вработени, а ќе се зголеми бројот на вработени лица кои ќе имаат временски ограничени договори. Ова можеби ќе претставува културолошки шок за сегашните генерации, но за идните генерации ќе стане нормала.

Оваа индустриска револуција се движи со експоненцијална брзина и веќе почна сериозно да ја менува формата на средствата на компаниите, а со тоа и конкуретноста на компаниите. Така Џонатан Хаскел и Стиан Вестлејк во својата книга Капитализам без капитал³ укажуваат зголемената улога на невидливите средства, односно на инвестициите во невидливи средства во економијата, која е посебно изразена во последната деценија. Ако во XIX и XX век инвестициите беа главно во средства кои можеа да видат и допрат, како што се машини, згради, компјутери и слично, последнава деценија се повеќе се вложува во истражување, развој, дизајн, софтвер, создавање на брендови отколку во видливи материјални инвестиции. Како пример се наведува Uber која е најголема такси компанија во светот, има присуство во огромен број на држави, но не сопствени на нема ниту едно такси возило, нема ниту еден вработен возач на такси. Вредноста на оваа компанија не се пресметува преку видливите, материјалните средства што ги располага, туку преку системот што има развиено за користење на такси услугите.

Државите чии компании побрзо ќе почнат да се вклучуваат Индустриската револуција 4.0, во чија основа е вештачката интелигенција ќе бидат поконкурентни во меѓународната трговија и подобро ќе се позиционираат во светската економија. Од друга страна националните економии, чии компании кои нема брзо да се вклучат во тековите на Индустијата 4.0 ќе заостанат во развојот. Шведскиот главен информатичар, д-р Åsa Zetterberg истакнува: „AI е многу моќна алатка и технологија која отвора можности за нови вештини, методи за работа, бизнис идеи и услуги, што ја прави клучен катализатор за иновации и развој. Ова може да ја зајакне конкурентноста и благосостојбата на Шведска“⁴. За Владата на Финската AI е „новата струја“, односно смета дека AI ќе донесе промени како што донесе откривањето на струјата. Министерот за економија на Финска Mika Lintilä јасно кажува „Вештачката интелигенција е клучен фактор за успехот и на Финска и на ЕУ“⁵.

Во САД приватниот сектор инвестираат големи суми во AI, а и администрацијата донесе план во 2016, во кој се вклучени долгорочни истражувачки инвестиции во AI⁶. Канадската влада, исто така, во 2016 година одвои значителни средства за инвестирање AI⁷. In 2017, Кина го донесе Развоен план за AI, со цел да обезбеди надмоќ на AI до 2030 година⁸. Европа со мало задоцнување почна да презема чекори за интензивирање на активностите за јакнење на AI. За таа цел повеќе од 120 научници подготвија

³ Jonathan Haskel и Stian Westlake, „*Capitalism without Capital: The Rise of the Intangible Economy*“, 2017

⁴ <https://www.government.se/articles/2018/03/artificial-intelligence-will-strengthen-swedens-welfare-and-competitiveness/>

⁵ The AI Forum 2018 кој се организира на Aalto University in Espoo на 8–9 Октомври 2018.

⁶ „*Preparing for the Future of Artificial Intelligence*“, Executive Office Of The President, National Science and Technology Council, Committee on Technology, the Office of Science and Technology Policy, 12.10.2016, Вашингтон

⁷ „*Canada funds \$125 million Pan-Canadian Artificial Intelligence Strategy*“, Canadian Institute for Advanced Research, 22.03.2017, <https://www.newswire.ca/news-releases/canada-funds-125-million-pan-canadian-artificial-intelligencestrategy-616876434.html>

⁸ „*New Generation Artificial Intelligence Development Plan*“, State Council of China 2017. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm, преведено во <https://www.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf>

документ Европска визија AI (A European Vision for AI)⁹ со кој укажуваат дека Европската Унија треба да донесе стратегија за развој на AI.

Во Извештајот на MIT „Вештачката интелигенција во бизнисот станува стварност“ се истакнува дека 88% од компаниите кои биле пионери во развојот на Вештачката интелигенција во инвестирале повеќе тековната година во споредба со претходната. Понатаму повеќето од овие компании се насочени кон решенија кои ќе им овозможат да генерираат поголеми приходи, отколку кон намалување на трошоците од работењето. Во овој Извештај исто така се истакнува дека и кинеските компании агресивно инвестираат во вештачката интелигенција.

Развиените индустриски земји треба да направат напори за создавање услови најмалку развиените економии да можат да ги искористат бенефитите од Индустријата 4.0 и AI. Во спротивно разликата меѓу развиените и земјите во развој ќе се зголеми.

Заклучок

Индустријата 4.0 придонесува за зголемување на продуктивноста на капиталот и работната сила и со тоа и на конкурентноста на компаниите и со тоа на компаративната предност на националната економија.

За да можат националните економии добро се позиционираат Индустриската револуција 4.0 и вештачката интелигенција неопходно е да создадат соодветно опкружување во:

- правниот систем, каде клучно место ќе има заштитата на интелектуалната сопственост, ефикасен судски систем за заштита на интересите на корпорациите, предвидливост на правната легислатива поврзана со економскиот систем, правна регулатива која обезбедува флексибилни работни односи
- образовниот систем, вклучувајќи го тука и системот на животно учење, кој ќе продуцира работна сила со вештини потребни за новата Индустрија 4.0.
- создавање на општество во кое ќе почитуваат и охрабруваат лицата и компаниите кои се стремат кон нови работи, институции и индивидуи кои прифаќаат промени, организации во кои се знае како се менаџираат промените

Развиените индустриски земји треба да направат напори за создавање услови најмалку развиените економии да можат да ги искористат бенефитите од Индустријата 4.0 и AI.

Литература

World Economic Forum - Centre for the New Economy and Society: The Future of Jobs Report 2018, Женева 2018 г.

⁹Holger Hoos (Universiteit Leiden, The Netherlands), Morten Irgens (Oslo Metropolitan University, Norway), and Philipp Slusallek (German Research Center for Artificial Intelligence, Germany): A European Vision for AI, 03.09.2018 г. <https://claire-ai.org/>

Дефиниција на Светска банка за Индексот на човечки капитал: Индексот е дизајниран со цел определи обемот на човечки капитал што ќе го има дете родено денеска кога ќе наполни 18 години
Jonathan Haskel и Stian Westlake, "*Capitalism without Capital: The Rise of the Intangible Economy*", 2017
<https://www.government.se/articles/2018/03/artificial-intelligence-will-strengthen-swedens-welfare-and-competitiveness/>

The AI Forum 2018 кој се организира на Aalto University in Espoo на 8–9 Октомври 2018.

"*Preparing for the Future of Artificial Intelligence*", Executive Office Of The President, National Science and Technology Council, Committee on Technology, the Office of Science and Technology Policy, 12.10.2016, Вашингтон

"*Canada funds \$125 million Pan-Canadian Artificial Intelligence Strategy*", Canadian Institute for Advanced Research, 22.03.2017, <https://www.newswire.ca/news-releases/canada-funds-125-million-pan-canadian-artificial-intelligencestrategy-616876434.html>

"*New Generation Artificial Intelligence Development Plan*", State Council of China
2017. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm, преведено во
<https://www.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf>

Holger Hoos (Universiteit Leiden, The Netherlands), Morten Irgens (Oslo Metropolitan University, Norway), and Philipp Slusallek (German Research Center for Artificial Intelligence, Germany): A European Vision for AI, 03.09.2018 г. <https://claire-ai.org/>

ARTIFICIAL INTELLIGENCE AND COMMUNICATION IN A HEALTHCARE INSTITUTION IN BULGARIA

UDC: 614.2:004.7/8(797.2)

Reviews

Rositsa Manzurova, PhD candidate; Vesela Serafimova, PhD candidate*South-West University "Neofit Rilski" Blagoevgrad, Bulgaria*

Abstract

Technology development has resulted in the use of artificial intelligence in various spheres of public life. It is increasingly implemented mainly to facilitate work and save resources to achieve higher results and productivity, especially in the field of healthcare, where many platforms and programmes based on artificial intelligence can be observed. The use of modern digital marketing platforms and of artificial intelligence (AI) in healthcare institutions has a significant impact on improving day-to-day communication with patients. An example of a successful Bulgarian healthcare institution that uses an effective platform based on artificial intelligence (Darvin.ai) is *Dr. Shterev Hospital*, Sofia. In future, more and more medical centers will rely on such platforms that have a positive impact on increasing the patient flow and facilitating the process of making an appointment with a doctor at any time of the day.

Key words: *Artificial intelligence, automation, chatbot, mobile applications, communication channels, patients, healthcare*

Introduction

The term "Artificial Intelligence" appeared in the 1950s, but was first used in the 1960s at the First International Conference on Artificial Intelligence in Washington. Since then, scientists from all corners of the world have given many definitions of this concept, but, generally, the research work in this area is distributed in the following directions: evolutionary, informational and biophysical.

Winston defined artificial intelligence as a science of the concepts that allows computers to perform activities that seem reasonable to the people. Bulgarian authors Nisheva and Shishkov define artificial intellect "as a science of the views (principles, concepts), methods and tools for the creation of intelligent (sensible) computer programming systems and for the investigation of the natural intellect through computer systems"¹. One of the first articles on artificial intelligence is Alan Turing's seminal paper 'Computing Machinery and Intelligence' (1950), which mainly analyzes the question "Can the Machine Think?"². Potanov uses the term

¹ Nisheva, M., Shishkov, D. Нишева, М., Д. Шишков, *Изкуствен интелект*, изд. Интеграл, Добри, 1995, P. 16

² Turing A. *Computing machinery and intelligence*// Mind: Oxford: Oxford University Press, 1950. No. 59. P. 433

“artificial intelligence” to denote “a large field of scientific and applied research”³, i.e., the term is associated with intelligent robots or thinking computers.

Artificial intelligence elaboration continues increasingly; it is implemented in all spheres of public life – politics, economics, health, education, science, etc. Very often, business organizations deploy artificial intelligence systems that are designed to facilitate the production or management which has a positive impact on the business efficiency improvement.

It is a well-known fact that the robots can perform many tasks the ordinary person does, but it is also a fact that without people this cannot take place. Artificial intelligence can be used as a management assisting tool to facilitate different processes and reduce costs.

This article presents an example of a successful Bulgarian healthcare institution (*Dr. Shterev Hospital*, Sofia) that uses an effectively implemented platform based on artificial intelligence (Darvin.ai).

The hospital is one of the healthcare institutions in Bulgaria that offers quality services, good interpersonal communication and appropriate facilities. The hospital has highly qualified specialists in the field of reproductive medicine, obstetrics and gynecology. The corporate image of the healthcare facility is impeccable due to the marketing and communication policy provided by the management. All this results in the increase of the number of patients trying to make an appointment in the hospital, which, at one point, makes it difficult for receptionist to answer all the calls. In order to solve this problem and avoid the negative consequences of missing a number of potential patients, the management undertook innovation trusting a firm that develops computer software based on AI. Together with the world-renowned IT company Progress, in April 2017, a tool for chatbots was developed and implemented through which one can make an appointment in the hospital through “artificial intelligence”. The name of the tool is Darvin.ai and its goal is to increase the productivity of the hospital by at least 30%. As a matter of fact, artificial intelligence chatbots favor the automation of business processes within various organizations.

By using AI and modern digital marketing platforms the day-to-day communication with patients is improved which is particularly important for the efficiency of the healthcare institution.

According to Ivan Todorov, the marketing director of *Dr. Shterev Hospital*, the reasons for establishing the contact center are due to the fact that, in 2016, the number of the average daily calls increased (about 250–300 calls per day); “depending on intensity, about 30% to 60% of the calls were missed”⁴; with the increase of the volume of the online communications with patients, a need for a well-trained team that would interact with patients on a daily basis emerged.

One year after the introduction of the Darvin.ai instrument, the results show a positive contribution in terms of an increased number of appointments and, respectively, of patients examined. According to the hospital data⁵, the average number of the daily phone calls increased almost double – about 300 to 500, e-mail requests – from

³ Potanov, A. S. Потанов, А.С. Технологии искусственного интеллекта, Учебное пособие, Национальный исследовательский университет Санкт-Петербург, 2010

⁴ Todorov, I. High Quality and Digitized E-healthcare in Bulgaria, 13th E-Healthcare Conference, Inter Expo Center, 28 February 2018

⁵ Ibid.

20 to 40, and social networking comments – about 15 to 30, i.e. phone calls for making an appointment have increased by approximately 50-60%.

In order to establish the number of *Dr. Shterev Hospital* patients who use the services of the chatbot based on AI and what its advantages are, a survey was conducted among 100 persons attending the clinic. The survey was conducted in June 2018: a questionnaire was distributed using the free application Google Forms.

The results of the survey are as follows: 58% of the surveyed made an appointment through Facebook, Messenger, Viber, or the Chatbot; 22% of the persons made a phone call; 20% made it face to face going to the clinic, i.e. more than half of the patients who took part in the survey used the chatbot.

Regarding the advantages of using the platform, 38% of the respondents pointed out the fact that the chatbot allows connection at any time of the day and, in the busiest hours, patients can freely communicate and make an appointment; 44% of the patients are happy with the fact that the chatbot saves time and costs.

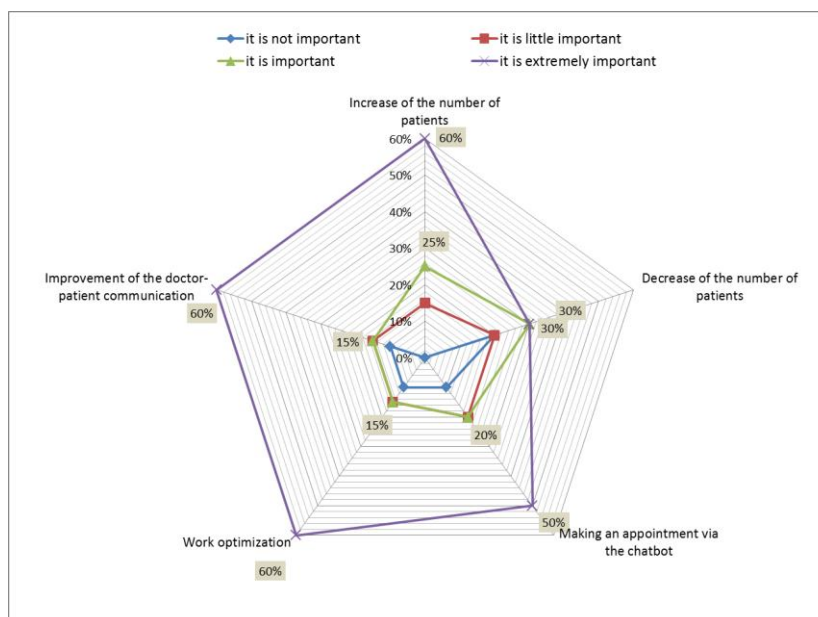
However, some drawbacks of using the platform based on AI were listed: 26% of the surveyed persons noted that the chatbot presupposes specific and accurate formulation of the question; 32% suggested that the chatbot could block at any time (system crash); a small percentage of the respondents indicated as a disadvantage that they were talking with a robot and that there was no emotional connection and sympathy.

What must be highlighted is that when choosing a hospital, many people (46%) prefer easy communication and contact with the medical establishment, doctors and staff. Some of the respondents (18%) would not choose the services of a hospital that does not provide good communication, or if they have to wait for too long. More than half of the respondents (56%) had to look for another channel of communication to make an appointment because the telephone lines were busy.

The chatbot based on the Darwin.ai platform has helped to increase the number of appointments with healthcare professionals. Online appointments are made via Facebook, Messenger, Viber, or the chatbot at *shterevhospital.com*. The abilities of chatbots with AI are related to the possibility that intelligent chatbots can be trained as people, with available goals and concrete steps based on the example of existing systems (such as Cognitive Flow technology of Progress). The advantages of AI chatbots include: they understand natural language and skip steps, unlike traditional chatbots that follow a script; quick menus are available to help the user choose.

Considering the analysis above, some significant data from the results may be presented in Graph 1:

Fig. 1 Influence of the artificial intelligence on the efficiency of the hospital (Source: authors' investigation)



The graph presents the results achieved over a period of one year after the implementation of the platform. Individual achievements have been ranked as important. It is obvious that the increase in the number of patients in the healthcare institution is of utmost importance, as well as improving doctor-patient communication and work optimization. Less important are: the decrease of the number of phone calls and making an appointment via the chatbot. In fact, by optimizing the work and improving the communication channels, the main goal has been achieved, namely 100% workflow and maximum patient intake.

The platform is integrated with the Joystick Hospital system which greatly facilitates the work of the healthcare receptionists. The access to the specialists in the assisted reproduction, obstetrics and gynecology at the medical center is easy and fast. Viber VoIP technology facilitates making the appointments, checking the schedules and, when a more specific conversation is needed, patients are redirected to other communication channels.

The results from the implementation of the chatbot with artificial intelligence for a period of one year show that the number of patients who communicated via Facebook, Messenger, Viber and the chatbot on the site was over 3500 patients. About 15500 messages were exchanged between the patients and the chatbot, with about 2000 appointments made.

The benefits of *Dr. Shterev Hospital* from the introduction of the AI chatbot are the following⁶:

- the patient flow is increased by about 20% over a period of a year;
- the number of telephone calls for making an appointment or another type of consultation after the implementation of the service is reduced by about 30%;
- about half of the appointments or other types of consultation are made through the automated system – online.

⁶ Todorov, I. High Quality and Digitized E-healthcare in Bulgaria, 13th E-Healthcare Conference, Inter Expo Center, 28 February 2018
68

The AI based chatbot tool can be successfully implemented in other areas of public life, especially in organizations where the communication policy is not at a good level. The priority of any health organization that insists on being up-to-date with the global trends must be the implementation and use of such innovations.

Bibliography

1. Potanov, A. S. Потанов, А.С. Технологии искусственного интеллекта, Учебное пособие, Национальный исследовательский университет Санкт-Петербург, 2010
2. Todorov, I. High Quality and Digitized E-healthcare in Bulgaria, 13th E-Healthcare Conference, Inter Expo Center, 28 February 2018
3. Turing A. Computing machinery and intelligence (англ.) // Mind : Journal. — Oxford: Oxford University Press, 1950. — No. 59. — P. 433 - 460.
4. Winston, P., Artificial intelligence, 1992, p. 11
5. <http://shterevhospital.com/>

ROBOTIC PROCESS AUTOMATION (RPA) THE EXAMPLE OF COCA-COLA HELLENIC BUSINESS SERVICE ORGANIZATION

UDC: 004.896:[334.72:663.86(497.2)]

Reviews

Sonya Georgieva, PhD; Rositsa Manzurova, PhD candidate*South-West University "Neofit Rilski" Blagoevgrad, Bulgaria*

Abstract

In any business context, Robot Process Automation (RPA) is an automated computer process, using smart technology to perform a specific transactional task. The use of RPA helps to reduce the time spent on transactional, repetitive, rule-based tasks-the "clicking" type of activities. RPA has seven key "Robot skills": Gather and Collate information; Validate; Record data; Calculate; Produce; Orchestrate; Transport and Connect; and Report. RPA allows automation of repetitive straightforward activities and gives an opportunity for humans to focus on value-adding, analytical and customer-centric activities. The example of Coca-Cola Hellenic Business Service Organization is a case that has been presented and analyzed in this paper. The data have been provided by the company.

Key words: *Robotic Process Automation (RPA), Technology, Business, Coca-Cola Hellenic Business Service Organization (CCHBSO)*

1. Introduction

Coca-Cola Hellenic Business Services Organization (CCHBSO) is a Shared Services Center that provides financial services and data processing for Coca-Cola Hellenic Group companies – a producer of soft drinks. The main services presented at the center in Bulgaria are the financial and the human resources. The company was established in 2011. It operates not only for the Bulgarian market but also for all other countries in which the group operates. It is a total of 28 countries, mainly European, but Russia and Nigeria, too. Business Services Organization (BSO) always explores new ways to make its business more agile by making daily processes faster and more efficient. Recently, it pushed the boundaries of innovation by piloting the use of robots for handling parts of 5 processes in finance and HR (human resources).

A pilot of this new RPA technology was conducted by BSO in July, in collaboration with Business Systems and Solutions (BSS) and UiPath – a leading RPA technology provider.

2. What is RPA (Robot Process Automation)?

Generally speaking, RPA is delivered through software that can be configured to perform rule-based tasks. Inherently, RPA is computer-coded software. It is also a program that assists humans when performing repetitive rules-based tasks and cross-functional and cross-application macros. On the other hand, RPA is not a walking, talking auto-bots, physically existing machines, processing paper or voice recognition and reply software. RPA has seven key “robotics skills” which explain what RPA actually does; namely: Gather and Collate information; Validate; Record data; Calculate, Produce; Orchestrate; Transport and Connect; and Report.

The RPA has three main applications – Unattended mode, Attended mode and Hybrid mode. A “software robot” interacts with these applications and systems like a human employee would do.

- An unattended mode is traditional Robotic Process Automation. It executes repetitive, rules-based tasks 24/7 which are common in back office and Shared Services use. The robot runs on virtual desktop without human involvement.
- An attended mode is desktop automation. It is used broadly across different functions. The robot runs on employee desktop and assists actively in the work. It works alongside the human worker providing process guidance and ensuring compliance.
- In a hybrid mode, the robot runs in unattended and attended mode. It fits well for contact centers. The work in this mode enables the passing of work between employees and robots, letting each do what they do best. The robot does some pieces of work automatically and helps employees to do others.

Fig. 1: The most suitable processes for RPA



Source: Coca-Cola Hellenic Bottling Company

How does RPA help CCHBSO? RPA offers more benefits than merely cost reduction. The most important benefits are the following:

- 24/7 Operations. It suggests non-stop performance without queues at the busiest time.
- Valuable work. The Employees do not waste any capacity for routine tasks.

- Speed increase.
- Quality. Increase quality by avoiding human errors and focusing on exceptions.
- Cost reduction.
- Scalability. The Capacity can be increased without long build-up phase.
- Internal Control. Avoiding human fraud, easily performed Control & Compliance checks.

The approach that enables CCHBSO to identify the most suitable processes to be robotized follows four basic steps:

Step 1 – Understand. Understand the key selection criteria for robotization and understand how the RPA process suitability assessment framework and model works.

Step 2 – Process walkthroughs. Detailed process walkthroughs to access the process steps, exceptions, and systems involved and document manual activities and key process characteristics (volumes, FTEs, etc.), demonstrated by CCHBSO process experts.

Step 3 – Summarize & confirm findings. It is necessary to summarize and confirm the followings: the process flow documents, the process characteristics both from a "value" and "complexity" perspective, and the findings.

Step 4 – Rank and prioritize. This step is connected with identification of the most suitable process for robotization by ranking and prioritizing based on "value" and "complexity" criteria.

In RPA strategy, each major organizational area (organization, governance, processes, technology, and people) has its roles and responsibilities. As far as the organization is concerned, they are related to the organizational setup based on the increased use of RPA solutions (e.g. potential introduction of RPA CoE within Coca-Cola Hellenic Bottling Company (CCHBC) organization). The role of the governance concerns the impact and the definition of governance bodies, management of external technology partners (including the license management) and governance concept for ongoing process changes due to RPA. The processes responsibilities refer to the definition of workflows, such as RPA demand processes and compliance-related workflow impacts, including audit procedures and additional management review controls. The technology is related to the long-term RPA technology strategy, the embedding RPA within existing CCHBC's IT architecture, the lifecycle management of RPA solutions, and the RPA security concept. One of the most important roles and responsibilities belong to people. The RPA strategy needs long-term HR/people strategy based on RPA and, therefore, changing skill requirements, which includes adjusted training and development structures and changing the workforce structure.

Based on the experience of CCHBSO, they can teach their insights and lessons learned. The most important and valuable ten lessons are as follows:

- Selection of the right processes. One must ensure that the process is well defined and the Robotic Process Automation can be implemented.
- No automatization of broken processes. The processes should be amended and made as efficient as possible before or during the implementation of Process Robotics Automation in order to minimize the robots roll-out effort and tool license cost.

- Agreement on up-front approach to measuring and tracking the benefits. Clear purposes should be defined and agreed upon prior to implementation.
- Having a checklist in place regarding infrastructure and compliance requirements. One must ensure that the correct infrastructure is in place and compliance requirements have been met early on in the project.
- Investment in comprehensive stakeholder management. Stakeholders need to be engaged from the program's outset to ensure effective buy-in, collaboration and adoption of change.
- Assurance vendor and business vision alignment. The chosen IT vendor should meet the long-term process automation requirements of the business.
- Considering wider strategic technology initiatives. Selected automation of a process should align with broader technological investment in the client's overall IT strategy.
- Providing adequate education and user adoption approach. It is crucial that the robots are adapted to the business. To ensure proper user adaption, the organization should be educated on the needs and workings of the Robotic Process Automation.
- Conduction robust testing. Business process testing is required to ensure that any issues which the robot may have when determining the next step can be identified, before large scale implementation.
- Monitoring the quality of the outputs and invest heavily in exceptions management. The quality of the output from the robots must be continuously monitored to ensure that they are trustworthy. It is important for quality purposes to invest heavily in exceptions management.

Conclusion

RPA has achieved good compliance with procedures and policies, as well as with the ability to find compliance with laws and regulations. Further on, its additional value derives from activities taken from error-prone humans to automation platforms that do specifically what they are configured to do. Benefits, such as diminishing the risks from enhanced compliance, are difficult to quantify, but the use of automation as tools for eliminating errors and proving compliance is steadily increasing.

Similar to the compliance, the positive impact of robotic automation on risk and control is measured mainly through the reduced numbers of violations or risk exposures experienced by the business. These can be related to reputation or to fines and penalties. In a nutshell, automation is real; its value is real; its benefits are measurable.

Bibliography

1. Global Intelligent Automation Market Report, *Managing Disruptive Change: A New Operational Model Enabled and Built by Intelligent Automation*, Vol.1, 2017
2. Global Intelligent Automation Market Report, *COE Models-Pro and Con; Governance and Automation Anxiety*, Vol.2, 2017
3. Global Intelligent Automation Market Report, *Howto design for Enterprise Scale and Total Program Yield – if You are Just Embarking on Intelligent Automation*, Vol.1, 2018
4. Winston, P., *Artificial intelligence*, Addison-Wesley Publishing Company, 1992, pp. 13
5. <https://coca-colahellenic.com/>
6. <https://www.ssonetowork.com/>
7. <https://www.automationanywhere.com/>

ВЛИЈАНИЕТО НА ИНТЕРНЕТОТ ВРЗ МЕЃУНАРОДНИТЕ МАРКЕТИНГ ПРАКТИКИ

UDC: 004.738.5:[339.138:339.9]

*Прегледен труд***Асс. м-р Верица Најдовска***Европски универзитет- Република Македонија - Скопје*

Абстракт

Во услови на експанзија на светската трговија, а со цел компаниите да постигнат одржлив раст на пазарите кои стануваат глобални или, пак, само за да преживеат на домашните пазари, кои се сè повеќе „нападнати“ од меѓународните компании, од особена важност е менаџерите да ја разберат комплексноста на меѓународниот маркетинг како и да развиваат вештини, способности и знаења неопходни за ефикасно да се натпреваруваат на меѓународните глобални пазари. Токму појавата на отворена светска економија, глобализација на вкусовите на потрошувачите и пристапот на интернет овозможува зголемена меѓузависноста на националната економија со економиите од целиот свет. Целта на овој труд е да се утврди влијанието и користа од интернет експанзијата врз меѓународните маркетинг практики преку ситуациона анализа и студија на случај.

Светскиот пазар не е повеќе збир на голем број независни пазари туку сè повеќе е мултилатерален, економско, културно и технички зависен глобален пазар. Под дејство на големиот обем на информации кои се за петпати зголемени во споредба пред 30 години, се трансформираат очекувањата и потребите на купувачите, а со тоа во континуитет се менува глобалниот пазар и потребата од иновациски маркетинг стратегии. Успешните брендови се водени од јасна цел која е фокусирана на создавање значајно позитивно влијание во светот.

Клучни зборови: меѓународен, маркетинг, глобални пазари, интернет, меѓународни пазари, вештачка интелигенција

THE INFLUENCE OF THE INTERNET OVER THE INTERNATIONAL MARKETING PRACTICES

Abstract

In today's expansion of the world commerce, for the companies to stay in the run on the home markets, while being "attacked" by international companies, the management must understand the complexity of the

international markets and develop skills and knowledge that are necessary to enable the small companies to efficiently compete on the global international markets. The goal of this article is to prove that the influence and the benefit of the internet expansion on the international marketing practices through a situational analysis and case study.

The world market is not a gathering of a big number of independent markets, but, it is a multilateral, economically, culturally and technically dependend global market. Under the influence of the vast information that are up to 5 times bigger than 30 years ago, the demand of the buyers is easily and frequently transformed.

The most successful brands are driven by a very clear goal which is focused on creating positive influence over the buyers and the world.

Keywords: *international marketing, global market, internet, AI*

Вовед

Благодарение на интернетот, глобалниот дострел веќе не е резервиран само за големите и успешни брендови

Во согласност со анализите на Светската трговска организација (World Trade Organization), извозот на стоки во 2017 година се зголемил на 17,73 американски долари, споредено со 16,03 американски долари во 2016, додека светскиот извоз на услуги се зголемил за 8% во 2017 година, достигнувајќи 5,28 трилиони американски долари. Како резултат на зголемената побарувачка на стоки и услуги низ целиот свет светската трговија се зголемила за 4,7% во 2017 година.¹

Глобалниот пазар денес (2018) се состои од 7,7 милијарди население и според последните предвидувања од страна на Обединетите нации се очекува да достигне 10 милијарди до 2050 година. Повеќе од 30% од светската популација се тинејџери кои го сочинуваат најголемиот светски пазарен сегмент на млади купувачи, односно младата тинејџерска популација креира глобална младинска култура "global youth culture".² Токму компаниите Nike, Coke, Gap, Sony Walkman, Sega, Nintendo, Sony Playstation, кои ја таргетираа младата тинејџерска популација, бележат значителен пораст во пазарните удели и профити во изминатиов период.

Токму младата популација како пазарен таргет, интернетот и пристапот на World Wide Web поттикна револуција во меѓународните маркетинг практики. Компаниите независно дали се мали, средни или големи сè повеќе согледуваат дека потенцијалот на глобалните пазари е во е-трговијата, во таа насока сè повеќе компании регистрираат виртуелни продавници и ги продаваат своите услуги и стоки online. Н&М од година во година го зголемува пазарното учество за 10-15% годишно. Еден од факторите кои

¹ World Trade Statistical Review 2018, Достапно на: https://www.wto.org/english/res_e/statis_e/wts2018_e/wts2018chapter03_e.pdf

² Cara Heaven And Matthew Tubridy, Global Youth Culture And Youth Identity,p. Достапно на: http://www.ccivs.org/New-SiteCCSVI/institutions/jpc-youth/youth-open-forum/Section_for_Youth/Resources_and_tools/Other_documents_on_youth/OXFAM_INTERNATIONAL_YOUTH_PARLIAMENT/Chapter6_Global_Youth_Culture_and_Identity.pdf, стр.149

поттикнуваат стратегија за глобална експанзија е преку оптимизирање на онлајн трговија. Со онлајн продавница достапна на 21 пазар, вклучувајќи ги и САД, Н&М прави сè што е во нејзина моќ за да создаде лесно за навигација, мобилно онлајн шопинг искуство, а со тоа да освои нови пазари.

Според Internet World Stats 4,2 билиони луѓе, односно 55% од вкупното светско население имаат пристап на интернет. Очекуван е податокот дека Азискиот регион е во предност со 55% од популацијата, но изненадува фактот дека Африканскиот регион е пред Европа со 16,9% наспроти 10,8 % од вкупната популација во тие региони.

Табела бр1. Корисници на интернет во светски рамки

World Internet Users and 2018 Population Stats

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2018 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 30 June 2018	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	464,923,169	36.1 %	10,199 %	11.0 %
Asia	4,207,588,157	55.1 %	2,062,197,366	49.0 %	1,704 %	49.0 %
Europe	827,650,849	10.8 %	705,064,923	85.2 %	570 %	16.8 %
Latin America / Caribbean	652,047,996	8.5 %	438,248,446	67.2 %	2,325 %	10.4 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,894 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.2 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,208,571,287	55.1 %	1,066 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics estimates in June 30, 2018. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the [United Nations Population Division](#). (4) Internet usage information comes from data published by [Nielsen Online](#), by the [International Telecommunications Union](#), by [GfK](#), by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the [Website Surfing Guide](#). (6) The information from this website may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2018. Miniwatts Marketing Group. All rights reserved

Извор: Internet World Stat, Достапно на: <https://www.internetworldstats.com/stats.htm>

Виртуелната реалност на фирми со пониски капитални ресурси им овозможува значително да ги намалат трошоците за освојување на меѓународни пазари, да ги намалат трошоците за меѓународно рекламирање им овозможува да станат глобални продавачи, во некои случаи преку ноќ.

Благодарение на интернетот, глобалниот дострел веќе не е резервиран само за големите и успешни брендови, туку всушност, глобалното присуство е можно за секој бизнис со креативна стратегија и разбирање на светските пазари. Компанијата Airbnb, чија мисија е огласување и закуп на сместување низ светот е основана во Сан Франциско, Калифорнија во 2008 година, а денес брои над 1,5 милиони огласи во повеќе од 34.000 градови. Експлозивниот глобален раст на оваа компанија е резултат успешна глобална маркетинг стратегија и брилијанта промоција преку социјалните медиуми. Имено, во јануари 2015 година Airbnb лансираше кампања како online „глобален социјален експеримент“ со цел да се поттикне гостопримство за непознати лица, а сликата или видеото од делото да го објават на социјалните медиуми со хаштаг #OneLessStranger. Само три недели по започнувањето на кампањата, над 3 милиони луѓе низ светот активно учествувале во креирањето на содржини или ја споделиле кампањата.³

Интернетот создава фундаментално различно опкружување за меѓународен маркетинг и бара радикално поинаков стратегиски пристап кој влијае врз сите аспекти на маркетиншкиот процес.⁴

³ [Hannah Fleishman](#), 13 Businesses With Brilliant Global Marketing Strategies, Достапно на: <https://blog.hubspot.com/marketing/global-marketing-and-international-business>

⁴ Isobel Doole, Robin Lowe, International Marketing Strategy, Analysis, Development And Implementation, 5th Edition, ISBN: 978-1-84480-763-5, British Library Cataloguing-In-Publication Data, Uk, 2008, p.44

Меѓународен маркетинг микс на компанијата амазон

Amazon е основана е во 1995 година, а денес ги надмина своите конкуренти и стана лидер на пазарот, има околу 240 милиони кориснички сметки низ светот и глобален нето-приход од 100.764 милијарди американски долари.⁵ Според Интербренд компанијата, Amazon која токму искористувајќи го интернет пристапот, просторот и неговата достапност до популацијата преку имплементирање на иновациски меѓународни стратегии во 2018 година, успева да оствари најголем раст кој е за 56% поголем во споредба со изминатата година (2017)⁶ и станува најбрзорастечки бренд во светот. Денес личното богатство на извршниот директор на Amazon, Џеф Безос, се проценува на околу 166 милијарди долари, односно просечно во денот заработува околу 260 милиони дневно⁷ и работи со над 500.000 талентирани вработени кои делат заедничка визија за компанијата.

„Амазон“ е меѓународна компанија за електронска трговија, која има изградено огромна база на производи и продава речиси сè, вклучувајќи, книги, дивиди, мобилни телефони / таблети, игри, облека за мажи/ жени и деца, накит, градинарска опрема итн.⁸

„Амазон“ првично почна со продажба само на книги и до денес е најголем продавач на книги во светот. Следејќи ги потребите на купувачите и наметнувајќи трендови, Amazon го лансираше Kindle читачот на е-книги со што доживеа голема експанзија на својот бизнис. Тековно продолжува да го проширува својот асортиман, истовремено нудејќи конкурентни цени на клиентите и побрзи испораки, користејќи компании за испорака.

Водени од желбата да се реорганизираат и да станат компанија која се грижи за своите клиенти, Amazon креираат маркетинг алатки со кои не само што полесно и побрзо ќе ги продадат своите производи туку ќе го олеснат купувањето и ќе бидат во функција и ќе им „служат“ на потрошувачите со цел да изградат силни заемни релации со нивните клиенти.⁹

Во почетокот на 2000 година - пред речиси 20 години - извршниот директор на Amazon, Џеф Безос, истакнал дека: „Ние сакаме Amazon да биде најголема 'customer-centric', компанија која е ориентирана кон основните четири групи на клиентите: потрошувачи, продавачи, претпријатија и креатори на содржини. Безос на своите состаноци поставувал празни столови велејќи им на вработените дека секој стол претставува клиент, кој е „најважната личност во салата за состаноци“.

Следејќи ги желбите, вкусовите и потребите на клиентите, компанијата Amazon во континуитет го приспособува и подобрува своето портфолио на производи и услуги. Токму, како резултат на иновациски решенија во изминатиов период, Amazon овозможи прегледност на своите производи за

⁵ Ranking best global brands, достапно на: <https://www.interbrand.com/best-brands/best-global-brands/2018/ranking/>

⁶ Ranking best global brands, достапно на: <https://www.interbrand.com/best-brands/best-global-brands/2018/ranking/>

⁷ Brad Tuttle, Amazon Just Became the Second Company to Reach \$1 Trillion. Here's How Much Jeff Bezos Is Worth Now, Достапно на: <http://time.com/money/5386380/amazon-1-trillion-jeff-bezos-net-worth/>, Sep.2018

⁸ Dave Chaffey, Amazon.com case study – 2018 update, Достапно на: <https://www.smartinsights.com/digital-marketing-strategy/online-business-revenue-models/amazon-case-study/>

⁹ Charles Trevail, Best Global Brands 2018, стр.4

360 степени, Fire Phone го заменува со Amazon Echo smart speaker, Amazon MP3 станува Amazon Music Unlimited, а според Морган Стенли, моден бизнис на Amazon сега е втор по обем продавач на облека во САД.¹⁰ Широкото портфолио на производи овозможува лесно да се приспособи за секој пазар одделно.

Најголемата светска онлајн продавница Amazon, при сегментирање на пазарите користи демографска и психографска сегментација, сегментацијата се базира на фактичкото купувачко однесување, не она што купувачите пројавиле интерес туку што всушност прават. Сегментацијата на микро ниво на Amazon е насочена кон секој клиент поединечно, дозволувајќи ѝ на компанијата да ги претвори посетителите во долгорочни клиенти со висока вредност. Најчести купувачи се тинејџери, или пак адолесценти од средната и висока класа кои имаат искуство во основната технологија, но немаат време или не сакаат да купуваат од физички продавници.¹¹

Дури и големите брендови учат од глобалниот ефикасен стратегиски пристап на Amazon кон дигиталниот маркетинг во насока на користење на RACE (Reach, Act, Convert, Engage) рамката за маркетинг планирање.¹²

Целите на стратегијата за маркетинг комуникации во компанијата Amazon се во насока на зголемување на „сообраќајот“ на клиентите на нивните веб-страници, кои во 2018 изнесува 76 милиони купувачи и 1,3 милиони понудувачи на производи, зголемена свест за нивните производи и услуги, унапредување на повторни купувања, развивање на стратегии за постепено зголемување на приходите како и зајакнување и проширување на брендот Amazon.com.

Интегрираниот план за маркетинг комуникации на Амазон вклучува употреба на традиционалните и нетрадиционалните медиуми. Секоја форма на медиуми што ја користи Амазон е избрана заради нејзината уникатна предности. Традиционалните форми на медиуми кои се користат се: весници, списанија, радио и ТВ. Нетрадиционалните медиуми вклучуваат online прикажување, социјални медиуми, е-мејл маркетинг.¹³ Трошоците за рекламирањето и другите промотивни активности во Amazon изнесуваат 3,8 милијарди долари (2015), 5,0 милијарди долари (2016) и 6,3 милијарди американски долари за 2017 година.¹⁴ Амазон, верува дека нивниот најефикасен метод на маркетинг комуникации е препораката “word-of-mouth” од нивните клиенти и за таа цел компанијата вложува напори за континуирано подобрување на искуството на своите клиентите. Ваквиот пристап сметаат дека најефективно ќе придонесе во стекнување на нови клиенти и исто така може да ги поттикне повторните посети на клиентите.

10 Morgan Stanley raises its Amazon price target to the highest on Wall Street, predicts \$1.2 trillion valuation, Достапно на: <https://www.cnbc.com/2018/08/29/morgan-stanley-raises-amazon-target-to-street-high-sees-1point2-trillion-valuation.html>, 2018

¹¹ **Hitesh Bhasin**, Marketing mix of Amazon, Достапно на: <https://www.marketing91.com/marketing-mix-amazon/>, Dec.2017

¹² **Dave Chaffey**, Amazon.com case study – 2018 update, Достапно на: <https://www.smartinsights.com/digital-marketing-strategy/online-business-revenue-models/amazon-case-study/>

¹³ **Michael Angelo Quiroz**, Amazon.com's Integrated Marketing Communications, Достапно на: https://medium.com/@michaelangelo_q/amazon-coms-integrated-marketing-communications-901a6a2a77ef

¹⁴ Amazon annual report 2018, Достапен на: <https://ir.aboutamazon.com/static-files/917130c5-e6bf-4790-a7bc-cc43ac7fb30a>

PEST анализа за освојување на нови пазари

Од компанијата Amazon истакнуваат дека меѓународните деловни активности се значајни за остварување на поголеми профити и секако нивната меѓународна маркетинг стратегија во иднина ќе биде насочена кон освојување на нови меѓународни сегменти. Стратегијата прв на неосвоените пазари носи високи трошоци како и ризик од непрофитабилност. PEST анализата, која е направена од страна на маркетинг менаџерите во Amazon, укажува на следниве ризици со кои би се соочиле на новите меѓународни пазари:¹⁵

- локални економски и политички услови;
- владина регулација на е-трговија, електронски уреди и конкуренција, и рестриктивни владини мерки (како што се мерките за трговска заштита, вклучувајќи извозни давачки и квоти и царински давачки и тарифи), национализам и ограничувања на странската сопственост;
- несоодветни правни системи, локални закони, недостаток на законски регулативи и практики во однос на физичката и дигиталната дистрибуција на медиумски производи и спроведување на правата на интелектуална сопственост;
- закони и прописи за заштита на потрошувачите и податоците, приватност, мрежна безбедност, енкрипција, рестрикции на цените или попустите;
- барања за деловни лиценци или сертификати, како на пример за увоз, извоз, веб-услуги и електронски уреди;
- несоодветна технолошка инфраструктура;
- пониски нивоа на користење на интернет;
- пониски нивоа на потрошувачка и помалку можности за раст во споредба со САД;
- пониски нивоа на користење на кредитни картички и зголемен ризик за плаќање;
- тешкотии во кадровско екипирање, развивање и управување со странските операции како резултат на далечина, јазик и културните разлики;
- различни односи помеѓу вработени/работодавачи и постоење на работни совети и синдикати;
- усогласеност со Законот за странски коруптивни практики на САД
- закони и политики на САД и други јурисдикции кои влијаат врз трговијата, странските инвестиции, заеми и даноците; и
- геополитички настани, вклучително и војна и тероризам.

Како резултат на растот на меѓународната е-трговија и другите онлајн и веб-услуги, компанијата Amazon очекува дека конкуренцијата ќе се интензивира, во таа насока локалните компании можат да имаат значителна конкурентска предност како резултат на нивното поголемо етаблирање и препознавање од страна на локалните клиенти.

¹⁵ Amazon annual report 2017, Достапно на: <https://ir.aboutamazon.com/static-files/917130c5-e6bf-4790-a7bc-cc43ac7fb30a>

Кооперативна маркетинг стратегија со цел постигнување на конкурентска предност

Компанијата Amazon со својата одлука да се ориентираат на меѓународниот пазар создава таква меѓународна маркетинг стратегија која им овозможува рационален пристап на поодделните сегменти на меѓународниот пазар. Кооперативната рамка на маркетинг стратегијата се покажала како клучно стратегиско решение во остварување на конкурентска предност на пазарот.¹⁶ Успешното дејствување на меѓународниот пазар е резултат на партнерства и остварување на заедничка соработка со голем број компании во различни сектори, како на пример: Drugstore.com (аптека), Living.com (мебел), Pets.com (миленичиња), Wineshopper.com (вина), HomeGrocer.com (намирници), Sothebys.com (аукции), Kozmo.com (урбана испорака дома), Waterstones, Toys R' итн. Амазон успева да ја консолидира својата сила во различни сектори преку своите партнерски аранжмани и преку користење на технологија за олеснување на промоција и дистрибуција на производи преку овие партнерства, корист имаат и двата деловни субјекти.

На пример, во Велика Британија, Waterstones (www.waterstones.co.uk) една од најголемите традиционални книжарници се соочила со големи трошоци за продажба на своите книги online, но со партнерските договори со „Амазон“ ја користат трговската платформа на „Амазон“ во замена за спроведување на маркетинг активности и овластување при online продажба. Сличен договор имаат и со компанијата Toys R'.¹⁷ Ваквите партнерства им помагаат на „Амазон“ да ги прошират своите асортимани во широчина и во длабочина и, се разбира, на корисниците кои купуваат во една категорија, како што се книги, им се овозможуваат да купуваат и производи како што се: облека, електроника итн. На овој начин „Амазон“ ја напушта концепцијата на изолација и ја зајакнува својата позиција на глобалниот пазар преку соработка и поврзување.

Заклучок

Светскиот пазар не е повеќе збир на голем број независни пазари туку сè повеќе е мултилатерален, економско, културно и технички зависен глобален пазар, а пристапот до информации во меѓународниот маркетинг е моќ. Повеќе од 30% од светската популација се тинејџери кои го сочинуваат најголемиот светски пазарен сегмент на млади купувачи.

¹⁶ Amazon annual report 2017, Достапно на: <https://ir.aboutamazon.com/static-files/917130c5-e6bf-4790-a7bc-cc43ac7fb30a>

¹⁷ Dave Chaffey, Amazon.com case study – 2018 update, Достапно на: <https://www.smartinsights.com/digital-marketing-strategy/online-business-revenue-models/amazon-case-study/>

Токму младата популација како пазарен таргет, интернетот и пристапот на World Wide Web поттикна револуција во меѓународните маркетинг практики. Според Internet World Stats 4,2 билиони луѓе, односно 55% од вкупното светско население имаат пристап на интернет и претставуваат потенцијални online купувачи. Благодарение на интернетот, глобалниот дострел веќе не е резервиран само за големите и успешни брендови, туку всушност, глобалното присуство е можно за секој бизнис со креативна стратегија и разбирање на светските пазари. Интернетот создава фундаментално различно опкружување за меѓународен маркетинг и бара радикално поинаков стратегиски пристап кој влијае врз сите аспекти на маркетиншкиот процес.

Користејќи го интернет пристапот, просторот и неговата достапност до популацијата преку имплементирање на иновациски меѓународни стратегии, во 2018 година, компанијата „Амазон“ успева да оствари најголем раст во 2018 година, кој е за 56% поголем во споредба со изминатата година (2017) и станува најбрзорастечки бренд во светот.

Литература

1. Amazon annual report 2018, Достапен на: <https://ir.aboutamazon.com/static-files/917130c5-e6bf-4790-a7bc-cc43ac7fb30a>
2. Brad Tuttle, Amazon Just Became the Second Company to Reach \$1 Trillion. Here's How Much Jeff Bezos Is Worth Now, Достапно на: <http://time.com/money/5386380/amazon-1-trillion-jeff-bezos-net-worth/>, Sep.2018
3. Cara Heaven And Matthew Tubridy, Global Youth Culture And Youth Identity,p. Достапно на: [http://www.ccivs.org/New-SiteCCSVI/institutions/jpc-youth/youth-open-forum/Section for Youth/Resources and tools/Other documents on youth/OXFAM INTERNATIONAL YOUTH PARLIAMENT/Chapter6 Global Youth Culture and Identity.pdf](http://www.ccivs.org/New-SiteCCSVI/institutions/jpc-youth/youth-open-forum/Section%20for%20Youth/Resources%20and%20tools/Other%20documents%20on%20youth/OXFAM%20INTERNATIONAL%20YOUTH%20PARLIAMENT/Chapter6%20Global%20Youth%20Culture%20and%20Identity.pdf)
4. Charles Tremain, Best Global Brands 2018, Достапно на: <https://www.interbrand.com/best-brands/best-global-brands/2018/>
5. Dave Chaffey, Amazon.com case study – 2018 update, Достапно на: <https://www.smartinsights.com/digital-marketing-strategy/online-business-revenue-models/amazon-case-study/>
6. Hannah Fleishman, 13 Businesses With Brilliant Global Marketing Strategies, Достапна на:<https://blog.hubspot.com/marketing/global-marketing-and-international-business>
7. Hitesh Bhasin , Marketing mix of Amazon, Достапно на: <https://www.marketing91.com/marketing-mix-amazon/>, Dec.2017
8. Isobel Doole, Robin Lowe , International Marketing Strategy, Analysis, Development And Implementation, 5th Edition, ISBN: 978-1-84480-763-5, British Library Cataloguing-In-Publication Data, Uk, 2008
9. Michael Angelo Quiroz, Amazon.com's Integrated Marketing Communications, Достапно на: https://medium.com/@michaelangelo_q/amazon-coms-integrated-marketing-communications

ARTIFICIAL INTELLIGENCE IN MARKETING AND ADVERTISING

UDC: 004.8:339.13/16

Reviews

M.Sc. Tanja Krsteva*European University – Republic of Macedonia - Skopje*

Abstract

Throughout history, when a new technology promises amazing progress in work efficiency, personal safety and happiness, the public often greets the development with trepidation. If a machine can perform a task better than humans can, the thinking goes, do we still need humans on the job?

New uses and applications of artificial intelligence (AI) are developed every day, bringing us closer to an unparalleled future – a future that we could have never imagined.

Keywords: *Artificial Intelligence, digital marketing, internet, e-commerce.*

1. Search

How will artificial intelligence (AI) affect digital marketing in 2018?

In 2005, if you “searched” an e-commerce store to find a product, you had been unlikely to find the result you had in mind unless you knew its name or title in full. Today’s “search” is much smarter, and its improved capacity not only helps you find information on *Google*, but it helps you find the right products on *Amazon* or *Target.com*, the right movies on *Netflix*, etc.

Ten years ago, typing “men’s flip flops” at *Nike.com* may not have yielded the results looked for. Today, it very much does.

Search improvement for e-commerce and marketing has improved due to the same underlying factors that have improved “search” at large, including:

- Technologies like *Elasticsearch* are now relatively mainstream, allowing any small e-commerce stores to have search that goes beyond simply matching keywords;
- Data-as-a-Service companies (like *Indix*, among others) make it easier than ever to draw from search data from other larger sources, informing your own online product search without having to train your own search models from scratch;
- Other misc improvements, such as: Software to detect common misspellings is now more commonplace, and can calibrate for misspellings by context (IE: “Season cikets” can be understood to mean “season tickets”, while “cikets” alone might be more difficult to discern without context).

Google has done good work in simplifying and explaining some of their own search improvements and developments in their “*Inside Search*” writings.

In the future, consumers can expect even more e-commerce sites to follow the footsteps of *Google* and others in implementing autosuggest, suggested corrections, “advanced” search options, and other similar improvements.

2. Self-Driving Cars

Have you ever heard of cars that drive without a driver, that are only guided by artificial intelligence technologies and automatic learning?

Tesla was one of the first automotive brands to launch a self-driving vehicle, and *Audi*, *Cadillac*, and *Volvo* have been already developing their own models. But that’s not all. *Uber* already made the first 50,000-beer delivery with a self-driving truck.

The Japanese carmaker *Toyota* is to invest \$500m (£388m) in the ride-hailing company *Uber* as the two companies expand their partnership on the development of self-driving cars. It deepens the existing relationship in a bid to catch up with rivals in the race to design and produce autonomous vehicles for the mass market. The aim of the partnership is to use technology from both companies in purpose-built *Toyota* cars to be deployed across *Uber*’s ride-sharing network from 2021. *Toyota*’s investment values *Uber* at \$72bn, despite mounting losses that totaled \$4.5bn in 2017.

3. The Fortune Teller That Will Know It Before You

One day, AI may know more about people than you ever imagined.



AI can assertively predict if someone is gay or straight based on the photographs of their face. A Stanford University study discovered an algorithm that can correctly identify which men are gay and which are not with 81% accuracy and with 74% accuracy for lesbian women.

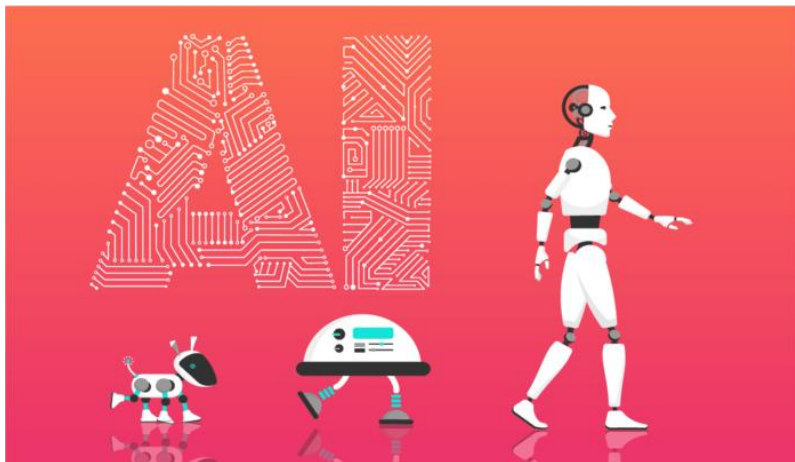
The research found that gay men and lesbian women tended to have “gender-atypical” features, expressions and “grooming styles”, essentially meaning gay men appeared more feminine and vice versa. The

data also identified certain trends, including that gay men had narrower jaws, longer noses and larger foreheads than straight men, and that lesbian women had larger jaws and smaller foreheads compared to straight women.

Yet, that's not all. *Facebook* is using artificial intelligence bots that can save the lives of people at risk of committing suicide. As an article by *Fast Company* explains, the company announced a pilot project in the United States that used AI to proactively identify *Facebook* posts that could indicate suicidal tendencies. *Facebook*'s AI technology identified over 100 cases that required intervention. How is it possible that these kinds of things can be anticipated or predicted with this level of accuracy? Even if you're thinking about quitting your current job, AI may know it before Human Resources does. *IBM* has a solution that uses predictive analytics to identify personnel retention problems. This program can find common factors that cause its staff to quit, creating a quality score for each employee based on the projected probability that they will leave the company soon.

4. The Smartest Investor

In 2009, Ira Sages from *Businessweek* magazine challenged the Director of *Quid AI*, Bob Goodson, to program a computer to choose 50 companies that no one had heard of and turn them into the most successful startups.



Almost 8 years later, the magazine reviewed the list to see how accurate "Goodson and his machine" were. The results surprised even the creator: *Evernote, Spotify, Etsy, Zynga, Palantir, Cloudera, OPOWER*, and the list continuous...

20% of the companies the computer chose were valued at a billion dollars.

5. The Marketing Guru

AI is becoming the "right hand" of marketers and retailers around the world.

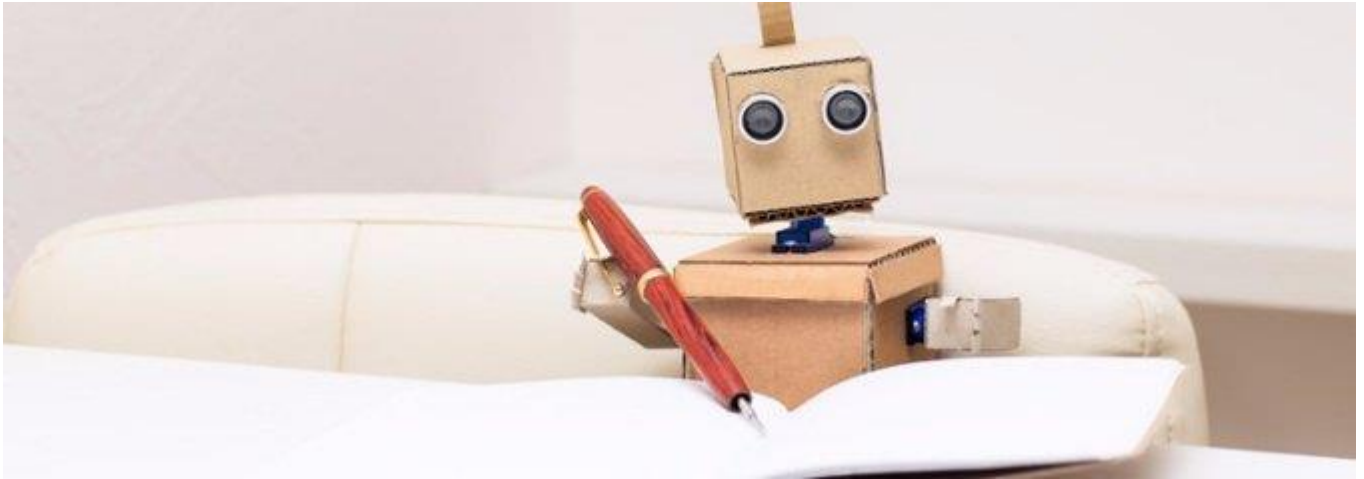
Through AI and machine learning, the most profitable audiences can be found for any advertisement. This means that intelligent algorithms are able to learn, detect, and predict which types of users are more likely to become clients at a lower cost per acquisition.

Adext is software that functions as a service that applies AI to find the most profitable audience for any advertisement. Using machine learning algorithms, it manages, optimizes, and automatically updates the digital campaign budget in over 20 different demographic groups per advertisement and on several platforms. With 480 daily adjustments to every single advertisement, its advanced AI has been able to increase advertisements' conversion performance by an average of 1265%.



With respect to content marketing, more and more intelligent tools are being created that provide, and even perform, the task of creating content. In fact, a few years ago, Gartner predicted that by 2018, 20% of content would be generated by machines. So, now, in 2018, one may have already read posts on social media or articles that were written by artificial intelligence.

Organizations like *BBC*, *CBS*, the *New York Times*, *Forbes*, *Associated Press* and *Reuters* are already using AI on a daily basis to develop and present their news publications to the public.



These kinds of advances are also tangible in email marketing, where AI can personalize emails based on preferences and user behaviors to obtain a better interaction that can turn into a sale. Companies such as *Phrasee* and *Persado* even determine what email subject, text for the email body, calls-to-action, and sending times will help prompt the user to make the desired action.

AI can even design website from scratch, like *Grid* does. The only thing you have to do is provide the text, images, and calls-to-action. The app is in charge of everything else and will make your website look professional and 100% functional.

6. The Sales And Customer Service Genie

We have already seen how AI is revolutionizing marketing, but sales are not far behind. What is the best price for a product or service? With automatic machine learning, price trends can be correlated with sales trends through an algorithm that aligns other factors, such as category management and inventory levels. The establishment of dynamic prices driven by AI will mean higher profit margins for companies.

AI is also becoming a retailer's best friend since there are already AI platforms that monitor the habits of sales representatives, giving them recommendations to improve their performance.



These intelligent CRMs allow them to have a better overview of all the elements involved in the sales process and discover sales opportunities in an unprecedented way. For example, it's been proven that cold emails are 20% more effective on Tuesdays, and that making a follow-up call 10 minutes after an online registration leads to more conversions.

What about customer service?

For many companies that offer a monthly subscription service (such as *Netflix*, *Spotify*, gyms, etc.), attracting clients is only half the process. Keeping them is another story. Predictive analysis can be used to know which clients will unsubscribe, making it possible to contact them ahead of time to offer them incentives and provide them with specialized care to change their minds.

In this same field, **chatbots** have been extremely useful since they make it possible to quickly and efficiently respond to the customers' main worries, questions, or problems. The most advanced chatbots are already able to answer open questions by using the natural language process and automatic learning to respond in a human-like way.

Even brands like *Sephora* and *H&M* use chatbots that serve as sales consultants and, believe it or not, they're extremely useful to the users. *Sephora*, for example, lets its users "try out" their cosmetic products (such as lipstick, eyeshadows, highlighters, etc.) on a photo of themselves that they share with the bot. The bot's artificial intelligence technology can identify the user's facial features and then use augmented reality to apply these makeup tests.



On the other hand, *H&M* helps users who visit its e-commerce platform find exactly what they're looking for by making suggestions on what they might like or look good on them according to their preferences.

Conclusion

In the future, consumers can expect more and more e-commerce sites to follow the footsteps of *Google* and others in implementing autosuggest, suggested corrections, "advanced" search options, and other such improvements.

The advantage of cognitive technology isn't that it can do the work a human can; it is that it can handle vast amounts of structured and unstructured data with a speed and accuracy that a human could never achieve. Watson-powered tools and APIs can help humans work much better and more efficiently. Given all the time in the world, no human could process thousands of resumes enough to find the themes and insights that might turn out the optimal candidate.

Bibliography

1. <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph>
2. <https://www.ibm.com/blogs/collaboration-solutions/2016/12/19/ibm-watson-transforming-human-resources/>
3. <https://blog.adext.com/en/applications-of-artificial-intelligence-in-digital-marketing>

ВЛИЈАНИЕТО НА ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА ВРЗ ЕКОНОМИЈАТА

UDC: 004.8:334.72.012.63/.64

Прегледен труд

М-р Кирју Николоски
Општина Кисела Вода – Скопје

Апстракт

Вештачката интелигенција би можела да овозможи неверојатен развој на економиите на државите особено на водечките светски сили.

Распространетоста на вештачката интелигенција може да доведе до поефикасно користење на ресурсите, но тоа не доаѓа само од себе туку зависи од секоја земја посебно. Истражувањето и развојот, поттикнувањето на компаниите за автоматизација на процесите бараат големи инвестиции.

Вештачката интелигенција и роботиката можат да овозможат не само големите туку и малите и средни претпријатија да ја подобрат оптимизацијата.

Клучни зборови: автоматизација, роботика, истражување и развој, мали и средни претпријатија, оптимизација

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE ECONOMY

Abstract

The artificial intelligence could allow an incredible development of the countries' economies, especially those of the leading world economies.

The prevalence of artificial intelligence can lead to using the resources more effectively, which by all means does not come by itself, but it depends from every country separately. The research, development and encouragement of companies to automatize their processes require massive investments.

Artificial intelligence and robotics can enable not only large companies, but also the small and medium ones to improve their optimization.

Key words: automatization, robotics, research and development, small and medium companies, optimization.

Вовед

Вештачката интелигенција како гранка од компјутерската наука може да се дефинира како проучување и дизајн на систем способен за перципирање на околината и преземање на активности кои му ги максимизираат шансите за успех.

Истражувањето во делот на вештачката интелигенција е од високотехнички и специјализиран карактер, во основа поделен во подобласти. Некои од подобластите се фокусираат на решавање на специфичен проблем, други пак, се фокусирани на еден од можните пристапи или користење на конкретна алатка или пак насочени кон реализирање на соодветна апликација.

Целта на истражувањето во областа на вештачката интелигенција е интеграција од резонирање, знаење, планирање, учење, комуникација, перцепција како и способност за движење и манипулирање со предмети.

Бројот на алатките користени во вештачката интелигенција е голем, вклучувајќи видови пребарувања, математичка оптимизација, логика, методи базирани на веројатност и економика, и многу други.

Комплексните реални проблеми се почесто бараат интелигентни системи кои комбинираат знаење, техники и методологии од различни извори. Интелигентните системи базирани на техниките на вештачката интелигенција може да обавуваат процеси на учење, заклучувања и решавање на разновидни проблеми. Ваквите системи, кои автоматски може да извршуваат задачи зададени од страна на корисниците, се нарекуваат интелигентни агенти.

Самостојно, интелигентните агенти можат многу успешно да изведат некоја пребарувачка работа во име и за потребите на разни корисници.

Поради ефикасното собирање, манипулирање и управување со податоци овие софтвери можат да бидат многу интересни од аспект на интелигентна анализа на податоци во многу области. Анализата на податоците собрани од страна на интелигентниот агент (софтверски робот) може да биде корисна за многу работи како, на пример, на полето на криминалот, а особено сајбер криминалот, безбедноста на сообраќајот, вонредни ситуации и др.

Од друга страна треба да се искористат методите на вештачката интелигенција кои овозможуваат пронаоѓање на податоци при интелигентна анализа на податоци (data mining) која наоѓа широка примена во областите на работењето на претпријатијата, економијата, механиката, генетиката, сообраќајот и сл.

Интелигенцијата – разумот на хомосапиенсот како круцијалната карактеристика на луѓето, може да биде прецизно обработена, до тој степен, да може да биде симулирана од страна на некоја машина. Ова ги покренува филозофските прашања во врска со природата на умот, како и одделот на етиката, во смисла на креирање на вештачко суштество, прашање кое датира од времето на митовите, античката филозофија и фантастика. Денес таа стана неизоставен дел од технолошката индустрија и најкомплицираниот проблем во компјутерската наука.

Вештачката интелигенција главен фактор во светот на бизнисот во иднина

Стручњациите веќе подолго време опоменуваат дека роботите ќе ја земат работата на луѓето, па се поставува прашањето што луѓето ќе работат и од што ќе живеат.

Иако бројни стручњаци со години опоменуваат што не чека во иднина кога роботите и вештачката интелигенција ќе ни ја земат работата (тоа се случува и денес), во моментот нема некое конкретно решение како да се постапи во дадената ситуација. Исто така се поставува прашањето од што луѓето ќе живеат ако не работат.

За овој проблем зборуваа и John Sculley поранешен претставник на Pepsi кој кажа дека “вештачката интелигенција ќе биде основа за се што ќе се случува во светот на бизнисот во иднина”¹ и дека концепцијата на работата во иднина ќе изгледа сосема различно во однос на денешниот начин на работа.

Вештачката интелигенција би можела да има големо влијание на целокупната работна сила. Се претпоставува дека за 10 до 15 години роботите би можеле да пишуваат подобри софтверски кодови од најдобрите програмери. Некои моментални предвидувања зборуваат за тоа како во САД до 2030 год. скоро 40% од роботите би можеле да ги обавуваат работи и дека за 120 год. роботите ќе ги обавуваат скоро сите работи на светот.

Како едно од решенијата за луѓето кои нема да има што да работат и од што да живеат се споменуваат т.н. универзални основни приходи т.е. пари кои државата ќе ги дава на луѓето како би имале барем некој извор на приходи за преживување. Сепак примената на едно такво решение би била неверојатно комплексна, па би требало потполно да се промени начинот на кој компаниите ја концептуализираат работата, па така компаниите и државата се пред големи предизвици и прашање е како ќе ги решат.

Исто така, се претпоставува дека мнозинството од луѓето не би биле задоволни со таквиот начин на живот затоа што ништо нема да работат и нема да се чувствуваат корисни туку само би добивале пари за преживување.

Вештачката интелигенција поттикнувач на развојот на Бруто домашниот производ

Глобалниот Бруто домашен производ (БДП) се претпоставува дека до 2030 година ќе порасне за 14% благодарение на вештачката интелигенција. Пресметано во пари тоа значи “зголемување за 15,7 билиони американски долари што ја прави вештачката интелигенција најголема бизнис прилика во

денешната брзо променлива економија”² според истражувањето на компанијата “PricewaterhouseCoopers”.

Ваквото зголемување кое се наведува во соопштението, а е резултат на вештачката интелигенција, е поголемо од сегашното обединето производство на Кина и Индија заедно.

Се очекува зголемена економска добивка од вештачката интелигенција и тоа преку зголемување на продуктивноста на работата и зголемена побарувачка на потрошувачите која произлегува од подобрувањето на квалитетот на производите.

Како вештачката интелигенција може да биде од конкретна корист за компаниите

По повеќедецениски ветувања и горки разочарувања вештачката интелигенција конечно почнува да им носи конкретна корист на компаниите кои меѓу првите почнаа да се бават и инвестираат во оваа област. Таа денес на машините им дава различни способности за кои долго време се сметаше дека му припаѓаат исклучиво на човечкиот род.

Дигитално иновативните компании кои се бават со малопродажба имаат работи кои работат во нивните магацини, па дури и автоматски нарачуваат стоки кога ќе се намалат количините на лагер до критичните граници.

Комуналните претпријатија ја користат вештачката интелигенција за да ја проектираат побарувачката за струја, вода, комунален смет и сл., а произведувачите на автомобили ја употребуваат во автомобили без возач.

Збир на различни фактори поттикна нов бран на развој на вештачката интелигенција. Компјутерите се сè помоќни, алгоритмите и моделите стануваат се посоефицирани и што е можеби најважно се генерираат некогаш незамисливи количини на податоци. Најголемиот дел од инвестициите од областа на вештачката интелигенција се состојат од интерни трошоци за истражување и развој. Тоа се компании на кои не му недостасуваат пари и кои своето работење го базираат на дигиталното опкружување.

Наспроти сите тие инвестиции голем дел на почеток на примената на вештачката интелигенција надвор од технолошкиот сектор е се уште во рана, експериментална фаза. Во студијата што ја објави Глобалниот институт McKinsey, “Вештачка интелигенција следна дигитална граница”³, а која опфаќа анализа на повеќе од 3.000 компании кои се запознаени со вештачката интелигенција во целиот свет утврдено е дека компаниите кои меѓу првите почнаа со примена на вештачката интелигенција обично се поблиску до дигиталната граница, дека се меѓу водечките фирми во своите гранки, ја применуваат ВИ во сите технолошки групи, а исто така да ги зголемат приходите и намалат трошоците.

²<http://ekonomski.net/pwc-vestacka-inteligencija-ce-podstaci-rast-bdp-a.html>

³<http://bif.rs/2017/10/kako-vestacka-inteligencija-moze-da-bude-od-konkretne-koristi-kompanijama/>

Компаниите кои сè уште не ја имаат воведено ВИ во поголем обем или во најважниот сегмент од нивното работење не се убедени дека постои аргументација во прилог на ВИ ниту се уверени во тоа какви приноси би можеле да очекуваат од инвестициите во ВИ, покажале резултатите од истражувањето.

Високоразвиените економии, како на пример Германија, со висок БДП по глава на жител и предизвици како, на пример, популација која брзо старее, исто така ќе мора повеќе да се насочува на автоматизација на база на вештачка интелигенција како би можела да ги постигне целите во поглед на БДП. Околу една третина од проектираниот БДП на Германија за 2030 год. зависи од зголемувањето на продуктивноста, а еден од најважните извори на продуктивноста е автоматизацијата на база на вештачка интелигенција. Работите кои се обавуваат на база на вештачка интелигенција би можеле да ја зголемат продуктивноста на Германија за 0,8 до 1,4% годишно.

Со тоа што е меѓу првите земји која ја вовеле во употреба вештачката интелигенција, Германија би можела дури и да ја промаши својата цел во поглед на БДП во 2030 год. и тоа за 4%. Меѓутоа доколку земјата побавно ја вовеле во употреба вештачката интелигенција, а продуктивноста не се зголеми по некој друг пат, планираниот БДП за 2030 год би можел да потфрли за една третина.

Исто така према извештајот кој го побарала Владата на Велика Британија нејзината економија со примена на ВИ ќе забележи пораст од 837 милијарди долари во следните 20 години. Користењето на ВИ ќе доведе до поефикасно користење на ресурсите.

Се разбира тоа не доаѓа само од себе туку зависи од секоја земја посебно. Исто така константното истражување и развој и поттикнување на компаниите на автоматизација бараат огромни инвестиции. Велика Британија во моментот се наоѓа меѓу водечките светски земји во поглед на вештачката интелигенција и во овој момент е во тек брза трка во развојот на технологиите така што луѓето можат да ги користат нејзините предности на се поголем број начини.

Заклучок

Може да се заклучи дека аргументацијата во врска со примената и развојот на вештачката интелигенција и тоа како постои, т.е. истата може да биде од конкретна корист на компаниите кои се спремни да ја употребат во различни аспекти на работењето. Спрема истражувањата, компаниите кои меѓу првите почнаа да ја применуваат вештачката интелигенција и кои покрај значајните дигитални капацитети имаат и активни стратегии можат да се пофалат со поголеми профитни маргини.

Секторите кои се на врвот на ранг-листата по Индексот на дигитализација на дејноста на Глобалниот институт McKinsey, како на пример високотехнолошките и телекомуникациските компании, како и оние кои се бават со давање на финансиски услуги исто така се и меѓу водечките компании кои ја примениле ВИ и имаат најамбициозни инвестициски планови.

Така, на пример, производителите на автомобили ја користат ВИ за да го унапредат производството и да развијат возила без возач додека компаниите кои даваат финансиски услуги ја

користат ВИ во функциите кои се однесуваат на искуствата со клиентите. Фирмите кои се повеќе ја користат ВИ и собираат повеќе податоци ќе бидат во голема предност во однос на оние кои во примената на ВИ доцнат.

Иднината на ВИ ќе биде иновативна. САД и Кина усвоија национални стратешки планови со значаен нагласок на ВИ во некои случаи со поддршка на иницијативи за финансирање на ВИ вредни повеќе милијарди долари. Слични такви стратешки планови усвоија и Јужна Кореја и Велика Британија.

Значајната корист е на дофат на раката. За многу компании, тоа подразбира забрзување на активности на полето на дигиталната трансформација. Вештачката интелигенција нема да дозволи на компаниите да ја прескокнат фазата на воспоставување на дигитални основи на прав начин туку ќе мораат да прибават соодветни дигитални средства и вештини како би можеле да ја применуваат оваа технологија.

Државите исто така мораат да држат чекор со овие промени преку усвојување закони и идентификација на работите за кои постои најголема веројатност да бидат автоматизирани, а исто така и обезбедување на програми за преквалификација за луѓето чија работа е под ризик од автоматизацијата поради примена на ВИ. На вработените треба да им се овозможи да стекнат соодветни вештини за да не се тркаат туку да работат со машините.

Литература

1. Piter Norvig „Veštačka inteligencija“, 2011
2. Кенет К.Лаудон, „Менаџмент информациски системи“, 2009.
3. S. Russell, P. Norvig, Artificial Intelligence – A Modern Approach. the 3rd Edition. Prentice Hall, Englewood Cliffs, New Jersey, 2009.
4. Стјуарт Расел, Питер Норвиг, Вештачка интелигенција – Современ приод, Превод на македонски јазик – проект* на Владата на РМ, 2010.
5. <https://imagazin.rs/>
6. <https://naslovi.net>
7. <https://www.danas.rs>
8. <https://www.blic.rs>
9. <https://ebooks.iien.bg.ac.rs/>
10. <https://bif.rs/>
11. <https://ekonomski.net/>

СОБИРАЊЕ НА ПОДАТОЦИ ЗА ПОЛОЖБАТА НА МАРГИНАЛИЗИРАНИТЕ ГРУПИ КАКО МОЌНА АЛАТКА ВО БОРБАТА ПРОТИВ ДИСКРИМИНАЦИЈАТА И СОЦИЈАЛНАТА ИСКЛУЧЕНОСТ

UDC: 316.647.82-058.5:004.62

Прегледен труд

364.624.4-058.5:004.62

Проф. д-р Атанас Козарев, Д-р Роза Гурмешевиќ*Европски Универзитет Република Македонија*

Апстракт

Систематското собирање и анализирање на сеопфатни податоци за еднаквоста и регистрирање на сите форми на дискриминација претставува моќна алатка во борбата против дискриминацијата и исклученоста, како и во расветлувањето на состојбата во која се наоѓаат групите кои се изложени на ризик од дискриминација. Податоците за положбата на маргинализираните групи во сите области на општествениот живот, како што се вработувањето, социјалната заштита, здравството, образованието, домувањето и правосудството, претставуваат неопходен предуслов за обликување и спроведување на мерките за промоција на еднаквоста на сите граѓани, без оглед на расата, етничкото потекло, полот, возраста, сексуалната ориентација, инвалидноста или некој друг статус. Недостатокот на овие податоци влијае на мерењето на степенот на дискриминацијата и нееднаквоста, како и на проектирањето на ефикасни закони и политики за борба против дискриминацијата. Во многу случаи во земјите ширум Европа, недостатокот на соодветни податоци за положбата на осетливите групи претставува еден од главните показатели за неефикасност на политиките на рамноправност и недискриминација во сите области на општествениот живот.

Клучни зборови: *осетливи групи, осетливи податоци, политики на еднаквост, дискриминација, социјална исклученост*

DATA COLLECTION ON THE SITUATION OF MARGINALIZED GROUPS AS A POWERFUL TOOL IN THE FIGHT AGAINST DISCRIMINATION AND SOCIAL EXCLUSION

Abstract

Systematic data collection and analysis of comprehensive data on equality and registration of all forms of discrimination is a powerful tool in the fight against discrimination and exclusion, as well as in clarifying the situation of groups at risk of discrimination. Data collection on the situation of marginalized groups in all areas of social life, such as employment, social protection, health, education, housing and justice is an essential prerequisite for the adoption and implementation of measures for promotion of equality of all citizens, regardless of race, ethnic origin, gender, age, sexual orientation, disability or any other status. Lack of data collection affects the measurement of the degree of discrimination and inequality, as well as the adoption of effective laws and policies to combat discrimination. In many cases, in countries across Europe, the lack of adequate data on the situation of vulnerable groups is one of the main indicators of the inefficiency of policies of equality and non-discrimination in all aspects of social life.

Keywords: *Sensitive groups, sensitive data, policies of equality, discrimination, social exclusion.*

1. Прашањето на легитимноста на собирање на податоци за еднаквоста и злоупотребата на таквите податоци

Дискриминацијата и нееднаквоста кои се присутни во сите области на општествениот живот се резултат на мноштво фактори кои делуваат заедно. Тие предизвикуваат негативни последици и штета на припадниците на одредена група во однос на останатите припадници на населението, кои можат да се утврдат по пат на квантитативни и квалитативни студии. Таквите студии најчесто ги откриваат показателите како што се: разликите во платите на припадниците на одредена група во однос на останатите слично квалификувани припадници на населението, разликите во квалитетот на домување, различните нивоа на здравје, нивото на образование кое е пониско од просечното итн. Утврдувањето на ситуациите на нееднаквост, кое само по себе не докажува дека нееднаквостите се резултат на дискриминација, има посебна важност бидејќи на тој начин им се пружа помош на креаторите на политиките да утврдат мерки на поддршка на групите кои се наоѓаат во неповолна положба, со цел да ја надминат истата.¹

¹ GLAUDE, M.: Eurostat /Directorate F, Director Social statistics and information society, 2007, p. 3.

Без мерење на степенот на дискриминација и нееднаквоста во општеството не можеме да осигураме ефикасни решенија на проблемите со кои најчесто се соочуваат припадниците на маргинализираните и дискриминираните групи. Доколку немаме податоци колку ромски деца се запишани и посетуваат настава во училиште не можеме ефикасно да се бориме против сегрегацијата на Ромите во образованието. Во областа на вработувањето без постоење на податоци за етничката или верската припадност на вработените работодавците не би можеле да креираат и спроведуваат ефикасни политики на различност на работната сила. Исто така не е доволно само креирање и усвојување на добри антидискриминациони политики и мерки за борба против дискриминацијата и исклученоста, без нивна ефикасна примена. За да дознаеме дали навистина таквите политики и мерки се спроведуваат во праксата, потребни ни се податоци за социо-економската состојба на групите кои се често жртви на дискриминација.

Во бројни извештаи на европските институции, вклучувајќи ги и извештаите на Европската комисија и Агенцијата на Европската унија за основни права, детално се утврдени причините поради кои собирањето на ваквите податоци може да ги унапреди антидискриминационите агенди на државите. Во тој контекст актерите за заштита и промоција на еднаквоста во општеството нагласуваат дека податоците за еднаквоста и регистрирање на сите форми на дискриминација посебно помагаат во: а) обезбедувањето на докази на судовите во случаите кога се работи за систематска дискриминација; б) информирањето и креирањето на ефикасни јавни политики; в) проценката на политиките на еднаквост и интеграција; г) зголемувањето на индикаторите за следење на политичкиот напредок итн. Меѓутоа, за жал, во повеќето европски држави, вклучително и кај нас, таквите податоци се повеќе недостасуваат и на тој начин го доведуваат во прашање исходот на борбата против дискриминацијата во судовите, невладините организации и телата за промоција на еднаквост, како и ефикасноста на јавните политики за борба против дискриминација и промоција на принципот на еднаков третман.²

Една од главните препреки за имплементација на стандардите за собирање на сеопфатни податоци за потребите на следење на еднаквоста и мерење на степенот на дискриминација е широко распространетото сфаќање меѓу државните актери и организациите на цивилното општество дека националните закони за заштита на податоците забрануваат собирање на „осетливи“ податоци кои го откриваат расното или етничкото потекло, политичкото мислење, верските или филозофските уверувања, членството во синдикатите, генетските и биометриските податоци, како и податоци во врска со здравјето на луѓето и сексуалниот живот. Меѓутоа правото на ЕУ (вклучително и националните закони на државите членки на ЕУ), сепак дозволува собирање на „осетливи“ податоци, под одредени услови првенствено пропишани со одредбите на Директивата на Европскиот парламент и Советот 95/46/EЗ од 24 октомври 1995 година за заштита на граѓаните во врска со обработката на личните податоци и слободното движење на таквите податоци (Директива за заштита на личните податоци), а подоцна со одредбите на Општата регулатива за заштита на личните податоци на Европскиот парламент и Советот 2016/679 (усвоена на 27

²Abdikeeva, A: Measure, Plan, Act: How data collection can support racial equality, ENAR 2014, p. 5.

април 2016 година, а стапила во сила на 25 мај 2018 година) со која е заменета Директивата за заштита на личните податоци. Во членовите 2а и 7 на Директивата за заштита на личните податоци било утврдено дека „обработката на личните податоци, односно информациите во врска со физичкото лице кое е утврдено или може да се утврди (лице кое е предмет на обработката на податоците) директно или индиректно е легитимна под строги услови, вклучително и под услов лицето кое е предмет на обработка на податоците да даде своја изречна согласност.“³

До стапувањето во сила на Општата регулатива за заштита на личните податоци Директивата за заштита на личните податоци 95/46/EЗ била централен законодавен инструмент за заштита на личните податоци во ЕУ. Меѓутоа, со оглед на фактот дека таа не успеала да го обезбеди потребниот степен на хармонизација на законодавството на државите членки од областа на заштитата на личните податоци со законодавството на ЕУ, ниту пак успеала да оствари ефикасна заштита на личните податоци во условите на дигитализација и развој на ИТ индустријата, ЕУ пристапила кон реформа на правната рамка за заштита на личните податоци со усвојување на Општата регулатива за заштита на личните податоци и Директивата на Европскиот парламент и Советот 2016/680 од 27 април 2016 година за заштита на поединците во врска со обработката на личните податоци од страна на надлежните органи за целите на спречување, истрага, откривање или гонење на кривичните дела или извршување на кривичните санкции и за слободно движење на таквите податоци.

Во согласност со член 9, став 1 на Општата регулатива за заштита на личните податоци забранета е обработката на „осетливи“ податоци односно „обработката на личните податоци кои го откриваат расното или етничкото потекло, политичкото определување, верските или филозофските убедувања или членството во синдикатот, као и обработката на генетските податоци, биометриските податоци со цел единствена идентификација на физичкото лице, податоците за здравствената состојба или податоците за сексуалниот живот или сексуалната ориентација на физичкото лице.“ Меѓутоа, член 9, став 2 на Општата регулатива за заштита на личните податоци прави исклучок од правилото на став 1, дозволувајќи

³Кога е во прашање обработката на „осетливи“ податоци до стапувањето во сила на Општата регулатива за заштита на личните податоци државите членки на ЕУ најчесто се повикувале на член 8, став 1 на Директивата за заштита на личните податоци кој *prima facie* го забранува собирањето на „осетливи“ податоци кои го откриваат расното или етничкото потекло, политичкото мислење, верските или филозофските уверувања, членството во синдикатите и обработка на податоците во врска со здравјето и сексуалниот живот. Меѓутоа, член 8, став 2 на Директивата прави исклучок од правилото на став 1, дозволувајќи обработка на „осетливи“ податоци под одредени услови. Тоа значи дека обработката на „осетливи“ податоци може да биде законита под услов: а) лицето чии податоци се обработуваат да даде своја изречна согласност за обработка на тие податоци, освен кога со законодавството на државите членки е предвидено дека забраната од став 1 не може да се укине на начин лицето чии податоци се обработуваат да даде своја согласност; б) обработката да е потребна со цел извршување на обврските и посебните права на надзорникот во областа на законодавството за вработување во онаа мера во која е тоа дозволено со националното законодавство кое пружа соодветна заштита; в) обработката да е потребна поради заштита на виталните интереси на лицето чии податоци се обработуваат или друго лице кога лицето чии податоци се обработуваат не е физички или правно способно да даде своја согласност; г) обработката да е спроведена во рамките на своите законити активности со соодветна заштита на установите, здруженијата или некое друго непрофитно тело со политичка, филозофска, верска или синдикална цел, и под услов обработката единствено да се однесува на членовите на телата или на лицата кои се во редовен контакт со него во поглед на нивните цели, и податоците да не се откриваат на трета страна без согласност на лицето чии податоци се обработуваат; д) обработката да е поврзана со податоците кои ги објавило лицето чии податоци се обработуваат или е потребна поради воспоставување, спроведување или одбрана на правните барања. Вид. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 (Article 8, paragraph 2).

обработка на „осетливите“ податоци под одредени услови.⁴ Тоа значи дека држави членки на ЕУ овозможуваат собирање на податоци за еднаквоста, се додека таквите податоци се дадени доброволно и во согласност со стандардите за заштита на податоците. За разлика од Директивата 95/46/ЕЗ, Општата регулатива за заштита на личните податоци е правно обврзувачка и директно применлива во државите членки, што значи дека не треба да се транспонира во нивните национални законодавства. Значајна новина во однос на Директивата е фактот дека Општата регулатива го става поединецот во прв план и наметнува цел список на обврски за обезбедување на соодветна правна рамка и правила на однесување на сите правни субјекти кои се занимаваат со личните податоци на граѓаните на ЕУ, независно од тоа каде им се наоѓа седиштето.

Покрај Директивата за заштита на личните податоци, односно Општата регулатива за заштита на личните податоци, директивите на ЕУ за еднаков третман (како што се Директивата на Советот 2000/43/ЕЗ од 29 јуни 2000 година за примена на принципот на еднаков третман на поединците независно од расното или етничкото потекло – Директива за расна еднаквост; Директивата на Советот 2000/78/ЕЗ од 27 ноември 2000 година за воспоставување на општа рамка за еднаков третман при вработувањето и во професијата – Директива за еднаквост при вработувањето; Директивата на Советот 2004/113/ЕЗ од 13 декември 2004 година за примена на принципот на еднаков третман на жените и мажите во поглед на достапноста и испораката на добра и услуги; и Директивата на Европскиот парламент и Советот

⁴ Обработката на посебни категории на лични податоци е законита ако е исполнет еден од следните услови: (а) лицето на кое се однесуваат податоците дало изречна согласност за обработка на тие лични податоци за една или повеќе конкретни цели, освен кога правото на Унијата или правото на државите членки пропишува дека лицето на кое се однесуваат податоците не може да отстапи од забраната од став 1; (б) обработката е потребна поради извршување на должноста и посебните права на раководителот или лицето на кое се однесуваат податоците во областа на правото на вработување и правото на социјално осигурување и социјална заштита, ако тоа го дозволува правото на Унијата или државите членки или колективниот договор во согласност со правото на државите членки кое пропишува соодветни заштитни мерки за основните права и интереси на лицето на кое се однесуваат податоците; (в) обработката е потребна поради заштита на животните интереси на лицето на кое се однесуваат податоците или друго лице кога лицето на се однесуваат податоците физички или правно не е способно да даде согласност; (г) обработката во рамките на своите легитимни интереси, со соодветни гаранции, ја врши фондација, здружение или било кое друго непрофитно тело со политичка, филозофска, верска или синдикална цел, и тоа под услов обработката да се однесува исклучиво на членовите на тоа тело или на лица кои имаат редовни контакти со него во врска со неговата цел и личните податоци да не се откриваат надвор од тоа тело без согласност на лицето на кое се однесуваат податоците; (д) обработката се однесува на лични податоци за кои е очигледно дека ги објавило лицето на кое се однесуваат податоците; (е) обработката е неопходна за воспоставување, остварување или одбрана на правните барања или кога судовите постапуваат во правосудно својство; (ж) обработката е неопходна за потребите на значајниот јавен интерес, на основа на правото на Унијата или правото на државите членки кое е сразмерно со саканата цел и со кое се почитува суштината на правото на заштита на податоците и се обезбедуваат примерени и посебни мерки за заштита на основните права и интереси на лицето на кое се однесуваат податоците; (з) обработката е неопходна за потребите на превентивната медицина или медицината на трудот поради проценка на работната способност на вработените, медицинската дијагноза, пружање на здравствена или социјална заштита или лечење или управување со системите и услугите на здравствена или социјална заштита на основа на правото на Унијата или правото на државите членки или во согласност со договорот со здравствениот работник и следствено со условите и мерките на заштита од став 3; (з) обработката е неопходна од причина на јавниот интерес во областа на јавното здравје, како што е заштита од сериозни прекугранични закани за здравјето или обезбедување на високи стандарди на квалитет и безбедност на здравствената заштита и лековите и медицинските средства, на основа на правото на Унијата или правото на државите членки со кое се пропишуваат соодветни и посебни мерки за заштита на правата и слободите на лицето на кое се однесуваат податоците, а посебно чување на професионалната тајна; (с) обработката е неопходна за потребите на архивирање во јавен интерес, потребите на научно или историско истражување или статистички потреби во согласност со член 89, став 1 на основа на правото на Унијата или правото на државите членки кое е сразмерно со саканата цел со кое се почитува суштината на правото на заштита на податоците и обезбедуваат примерени и посебни мерки за заштита на основните права и интереси на лицето на кое се однесуваат податоците.

2006/54/EЗ од 5 јули 2006 година за примена на принципот на еднакви можности и еднаков третман на мажите и жените во прашањата на вработување и професијата – Директива за родова рамноправност) исто така содржат референци за собирање на статистички податоци. На пример, параграф 37 на преамбулата на Директивата на Советот 2006/54/EЗ пропишува дека „за подобро разбирање на различното постапување спрема мажите и жените во прашањата на вработување и работа, би требало и понатаму да се изработуваат, анализираат и да се стават на располагање на соодветни нивоа споредливи статистики расчленети спрема полот.“

Во теоријата постојат гледишта дека собирањето на податоци за еднаквоста не подразбира воведување на нови структури, што би значело изложување на државата на дополнителни трошоци, туку ревизија на категориите кои при секој настан поминуваат низ процесот на ревизија, на пример за секој попис или процес на собирање на податоци (административни регистри, истражувања на домаќинствата, вработеноста и сл.) Така на пример истражувањето на ЕУ за работната сила кое обезбедува податоци во врска со вработувањето од сите држави членки на ЕУ истовремено ги расчленува податоците по возраст и пол. Во овој случај за целите на политиките на еднаквоста можат да се додадат и категориите како што се етничка или верска припадност со цел да се утврдат и измерат подрачјата на прогрес, без при тоа да се додаваат нови индикатори или прашања.⁵ Меѓутоа, од праксата на земјите кои имаат развиено добар систем на собирање на податоци (на пример Финска) произлегува дека собирањето на податоци за еднаквоста сепак бара одреден износ на ресурси како што се персоналот, стручноста и финансиските ресурси, вклучително и знаењето, кои често недостасуваат.⁶

Иако систематското собирање на податоци за еднаквоста помага во утврдувањето на различните облици на дискриминација, докажувањето на дискриминацијата во судовите и креирањето на антидискриминационите политики и агенди, често се случува да дојде до злоупотреба на ваквите податоци и тоа на штета на дискриминираните групи. Таквите дискриминирачки практики, како што се расното профилирање и неправилната употреба на личните осетливи податоци од страна на полицијата, кои се вообичаени во Европа, допринесуваат кон зголемување на недовербата на малцинствата во собирањето на податоците. Расното профилирање е дискриминирачка пракса која води кон нееднаквост како резултат на стигматизација на цела група на луѓе. Европската комисија против расизам и нетолеранција (ЕКРИ) под поимот расно профилирање подразбира ситуации во кои „полицијата при вршењето на својата должност, без никакво објективно или разумно оправдување, ја користи раса, бојата на кожата, јазикот, вероисповеста, националноста, односно националното или етничкото потекло како основа за спроведување на контролни, надзорни или истражувачки активности.“⁷

Една од главните разлики помеѓу собирањето на податоци за еднаквоста и останатите практики во кои често доаѓа до злоупотреба на податоците е почитување на основните принципи на кои се заснова собирањето на податоците, а посебно принципот на самоидентификација и приватност на поединците.

⁵ ENAR, EQUALITY DATA COLLECTION: FACTS AND PRINCIPLES, Open Society Foundations, 2015.

⁶ Mayrhofer, M.: DOBRE PRAKSE U PRIKUPLJANJU PODATAKA O (NE)JEDNAKOSTI, Zagreb, 2017, str. 33.

⁷ ECRI General Policy Recommendation N°11: Combating racism and racial discrimination in policing, 2007, para. 1.

Во случаите во кои доаѓа до злоупотреба на податоците, како што е случај со расното профилирање, не се почитува принципот на самоидентификација, ниту пак се дава гаранција на еднаквоста. Во тој контекст, важно е да се напомене моделот на собирање на податоци кој го предлага Европската мрежа против расизам (ЕНАР) кој се заснова на шест клучни принципи:

1) *Самоидентификација* – идентификацијата треба да биде заснована на поединечно мислење на субјектот на податоците во врска со нејзиното/неговото етничко или расно потекло или некоја друга заштитена карактеристика;

2) *Доброволно учество* – секој поединец има право да бира во собирањето на податоци (нема потреба да се постигне консензус меѓу сите заедници/поединци), и никој не може да биде присилен да обезбеди осетливи податоци. Поединците да бидат известени дека неучествувањето во процесот на собирање на податоци нема да предизвика никакви негативни последици;

3) *Тајност на личните податоци* - осетливите податоци секогаш треба да се третираат доверливо. Тоа подразбира анонимизација на сите информации во врска со осетливите податоци;

4) *Информирана согласност* – секој поединец да добие јасни, транспарентни информации во врска со целта на собирањето на податоците и за бенефициите и ризиците од нивното учество. Потоа треба да бидат прашани дали се спремни да дадат своја согласност или не;

5) *Учество на заедницата* – групите кои се изложени на ризик од дискриминација треба активно да учествуваат во текот на целиот процес, директно или со посредство на репрезентативни организации, посебно во поглед на дефинирањето на категориите, анализите и евалуацијата на собраните податоци, како и ширењето на податоците;

6) *Повеќекратни основи/идентитети* – субјектите на податоците треба да имаат право да бираат повеќекратни и интерсекционални идентитети и треба да се овозможи комбинација на основите при анализа на податоците.⁸

Иако повеќето експерти сметаат дека собирањето на податоци за еднаквоста не дава точна слика за дискриминацијата со оглед на фактот дека најчесто е засновано на *ad hoc* основи на дискриминација и многу земји во светот немаат усвоено политики на собирање на податоци, важно е да се напомене дека добивањето на веродостојни и објективни податоци за различните аспекти на дискриминацијата е далеку од лесна задача. Ако се земат во предвид различните облици на дискриминација (директна и индиректна, вознемирување, упатства за дискриминација и сл.), како и фактот дека дискриминацијата се одвива во различни сфери на општествениот живот (вработување, здравство, образование, домување, пружање на услуги и сл.), сосема е јасно дека повеќето модели на собирање на податоци не се применливи во однос на сите основи на дискриминација (како што се, на пример, инвалидноста, возраста или сексуалната ориентација). Затоа постои потреба од превземање на сериозни напори за ревидирање на собирањето на податоци.⁹

⁸ENAR, COMBATING INEQUALITY AND DISCRIMINATION IN EMPLOYMENT: Data collection as a necessary step to plan action, Open Society Foundations, 2015, http://www.enar-eu.org/IMG/pdf/edc-business_factsheet_final.pdf.

⁹ Study on Data Collection to measure the extent and impact of discrimination in Europe Final Report 7.12.2004, p. 4, <http://edz.bib.uni-mannheim.de/daten/edz-ath/gdem/04/collection%20data.pdf> ;

Во праксата најчесто се застапени следните модели на собирање на податоци: социјални и економски статистики, статистики на националниот правен систем (како што се статистиките на полициските извештаи за криминал), истражувања за жртвите на дискриминација и другите таргет групи, истражувања на ставовите, тестирање на дискриминацијата, квалитативни истражувања (како што се студиите на случај), лабораториски експерименти и внатрешна евиденција од страна на омбудсманите, специјализираните тела, специјализираните невладини организации и јавните и приватните организации и компании. Сите овие модели имаат свои предности и ограничувања. На пример, социјалните и економските статистики можат да обезбедат важни информации за евентуално неповолната положба на членовите на одредена група, но директно не мерат до кој степен неповолната положба е резултат на дискриминација. Сите модели на собирање на податоци се сметаат за корисни. Меѓутоа, експертите нагласуваат дека употребата на таргет истражувања, како што се анкетите и тестирањето на дискриминацијата, обезбедува најдобри индикатори за мерење на дискриминацијата.¹⁰

2. Собирање на податоци за еднаквоста во европските држави

Од правната рамка на ЕУ произлегува дека директивите на ЕУ повеќе дозволуваат, отколку што бараат од државите членки да собираат податоци за еднаквоста. Од друга страна тие ја охрабруваат употребата на статистички докази, посебно кога е во прашање докажувањето на индиректната дискриминација. Обврската за собирање на податоци за еднаквоста или дискриминацијата не е директно забележана ни во другите меѓународни инструменти за човекови права. Меѓутоа, во извештајот на Специјалниот известувач на ОН за современите форми на расизам, расна дискриминација, ксенофобија и слична нетолеранција, се вели дека „[...] етничките податоци може да се сметаат како една компонента на право на недискриминација. [...] Државата има обврска да обезбеди еднаквост и би било во ред тоа да се толкува на начин кој ја вклучува должноста за собирање и анализа на податоци во врска со етничката припадност, со цел да се идентификуваат нееднаквостите и да се следи ефикасноста на мерките за отстранување на нееднаквостите (Генерално собрание на ОН 2015, параграф 18).¹¹

Во согласност со обврската на државите членки на ЕУ да го усогласат своето законодавство со европското (сите држави членки на ЕУ ја транспонирале во своето национално законодавство Директивата за заштита на личните податоци), сите држави членки на ЕУ собираат податоци за еднаквоста, вклучително и податоци кои го откриваат расното или етничкото потекло, со користење на алтернативни категории како што се државјанството, државата на раѓање, државата на раѓање на родителите, јазикот кој се зборува во семејството, мигрантското потекло и името. Од друга страна податоците кои се собираат по пат на јавните статистики или специфичните прашалници ретко се користат за потребите на еднаквоста и недискриминацијата, посебно во пристапот на економските и

¹⁰ *Ibid.*, p. 4-5.

¹¹ Mayrhofer, M., *op.cit.*, str. 6-7.

социјалните права.¹² Се до стапувањето во сила на Општата регулатива за заштита на личните податоци во мај 2018 година, националните закони за заштита на личните податоци на државите членки на ЕУ не биле во потполност усогласени со правото на ЕУ. Меѓу нив постои одреден степен на варијација што се должи на различното толкување на одредбите на Директивата за заштита на личните податоци. Поединечните истражувањата на националните закони за заштита на личните податоци на државите членки покажуваат дека повеќето држави членки на ЕУ не ја исклучуваат можноста за обработка на осетливите податоци на основа на давање на согласност на субјектот на податоците. Но сепак, некои држави членки ја ограничуваат употребата на таквото правило, на пример со додавање на дополнителни критериуми.¹³

Во ревидираната верзија на Европскиот прирачник за податоците за еднаквоста од 2016 година Макконен (*Makkonen*) вели дека „иако сите европски држави превземале некои иницијативи за собирање и употреба на податоци за еднаквост, се уште има проблеми во неколку аспекти: собирањето на податоците не е систематски планирано или изведено; се покажува тенденција за периодично собирање на податоци кое не е постојано; податоците се ограничени само на некои основи на дискриминација; индиректните показатели укажуваат на фактот дека резултатите не се репрезентативни за целната група; податоците се фокусирани на одредени области на животот и овозможуваат само ограничен увид.“ Од тие причини во повеќето европски држави и понатаму недостасува систематско, точно и сеопфатно собирање на податоци за (не)еднаквоста.¹⁴

3. Собирање на податоци за еднаквоста во Република Македонија

Република Македонија во 2010 година донела Закон за спречување и заштита од дискриминација, што претставува значаен чекор на земјата за развој на законодавната и институционалната рамка за борба против дискриминација. Во согласност со Стратегијата за еднаквост и недискриминација 2016-2020 и извештаите на Европската комисија, државата во 2016 година пристапила кон измена на Законот за спречување и заштита од дискриминација и подготовка на нов предлог закон кој треба да биде усогласен со меѓународните стандарди и да обезбеди поефикасна заштита од дискриминација. Со цел потполно усогласување на законодавството на државата од областа на заштитата на личните податоци со законодавството на ЕУ, државата пристапила кон изработка на нов текст на Законот за заштита на личните податоци („Службен весник на Република Македонија“ бр.7/05, 103/08, 124/10, 135/11, 43/14, 153/15 и 99/16) и усвоила и други документи за заштита на човековите права и справување со дискриминацијата. Меѓутоа, следењето на резултатите на таквите документи, мерки и политики, односно нивната имплементација не е едноставна задача и бара сериозни напори. И покрај бројните препораки на

¹² Abdikeeva, A., *op.cit.*, pp. 9-10.

¹³ Makkonen., T.: *Measuring Discrimination: Data Collection and EU Equality Law*, 2006, p.8.

¹⁴ Mayrhofer, M., *op.cit.*, str. 16.

европските институции за важноста на собирање на податоци за еднаквоста, истражувањата покажуваат дека собирањето на таквите податоци не е задоволително во Република Македонија.

Во извештајот на ЕКРИ за Република Македонија од 7 јуни 2016 година повторно е нагласено дека во земјата „не постојат официјални статистички податоци за употребата на расистичкиот говор на омраза во медиумите или во другите облици на јавниот дискурс, иако во различните извештаи на меѓународните и невладините организации се укажува дека во последните години постои ескалација на говорот на омраза.“¹⁵ Исто така, не постои ниту официјален механизам за мониторинг на хомофобичниот/трансфобичниот говор на омраза и властите не собираат статистички податоци за овие инциденти¹⁶, ниту за расното или хомофобично/трансфобично насилство во земјата, и не се доставени никакви податоци за годишниот извештај за криминалот од омраза на ОБСЕ/ОДИХР.¹⁷ Во извештајот се утврдени и недостатоците на законската и институционална рамка за унапредување и заштита на правата на припадниците кои се помалку од 20% од населението, посебно во областа на вработувањето, со цел да се подготви нова законска рамка која ќе го насочи процесот на вработување на сите етнички заедници и ќе воспостави систем за собирање на податоци со кој ќе се следи дистрибуцијата на вработувањата по етничка основа во јавниот сектор. Недостаток на релевантни статистички податоци постои и за бројот на ромски деца кои се на возраст која одговара на основното образование, што произлегува од проблемите со евидентирање во матичните книги на родените.¹⁸ Државата не располага ниту со статистички податоци за големината на ЛГБТ заедницата и има многу мал број на официјални податоци за прашањата поврзани со ЛГБТ заедницата, бидејќи не постојат официјални мерки за собирање и анализирање на податоци за дискриминација по основ на сексуална ориентација или родов идентитет. Тоа е резултат на непостоење, на пример, на официјални податоци или истражувања за дискриминацијата на припадниците на ЛГБТ заедницата во областа на вработувањето, домувањето и здравствената заштита. Во Препораката CM/Rec(2010)5 на Комитетот на министри на Советот на Европа за мерките за борба против дискриминацијата по основ на сексуална ориентација или родов идентитет се укажува дека може да се собираат лични податоци кои се однесуваат на сексуалната ориентација или родовиот идентитет на лицето доколку тоа е неопходно за определена, законска и легитимна цел. Без такви податоци не може да се има солидна основа за градење и спроведување на политики со кои ќе се адресира нетрпеливоста и дискриминацијата на припадниците на ЛГБТ заедницата.¹⁹

Недостатоцие во врска со собирањето на податоци и квалитетот на податоците се потврдени и во годишниот извештај на Европската комисија за Република Македонија објавен 2018 година, што ја отежнува политика на подготовка и донесување на квалитетни закони. Со ратификацијата на Истанбулската конвенција на Советот на Европа во декември 2017 година постигнат е одреден напредок

¹⁵ ECRI, Fifth report on “the Former Yugoslav Republic of Macedonia” (fifth monitoring cycle), Strasbourg, 2016, p. 13.

¹⁶ *Ibid*, p.14.

¹⁷ Во 2013 година Хелсиншкиот комитет за човекови права на Република Македонија, со поддршка од Мисијата на ОБСЕ во Скопје, започнал да собира податоци и да ги следи и мапира актите на насилство со цел да ја пополни празнината од непостоење на официјални податоци. Вид. *Ibid*, p. 19.

¹⁸ *Ibid*, p. 26.

¹⁹ *Ibid*, pp. 32-33.

во областа на еднаквоста помеѓу жените и мажите и постоечките закони за родова еднаквост во голема мера се усогласени со законодавството на ЕУ, но и понатаму остануваат предизвици кога станува збор за нивно спроведување. Собирањето на податоците по основ на полот е систематско во одредени сектори, како што се социјалната политика, вработувањето, образованието или статистички податоци за населението во однос на раѓање и смрт. Меѓутоа не постои унифицирано собирање на податоци и мониторинг на повеќето аспекти кои се однесуваат на состојбата на децата. Од тие причини потребно е земјата да воспостави систем на собирање на податоци кој ќе осигура точност на податоците, доверливост, достапност и навременост, како и координацијата на активностите за собирање на податоци со соседните земји.²⁰

Заклучок

Собирањето на податоци за еднаквоста претставува процес кој во голема мера е поврзан со имплементацијата на националните и меѓународните акти за човекови права. Во таа смисла посебна важност има толкувањето на одредбите на меѓународните инструменти кои не предвидуваат обврска за државите членки да собираат податоци за еднаквоста. Но, и покрај тоа, истражувањата покажуваат дека сите држави членки на ЕУ превземаат мерки за собирање на податоци за еднаквоста во поглед на основите како што се етничкото потекло, вероисповеста, возраста, инвалидноста, сексуалната ориентација и/или родовиот идентитет. Сепак, само неколку европски држави имаат развиено систематска и институционална рамка за собирање на таквите податоци (Финска, Велика Британија и др.) Во Република Македонија постои недостаток од собирање на податоци за еднаквоста во скоро сите категории. Со цел да се надмине таквиот недостаток Европската комисија во 2016 година утврдила неколку прашања на кои државите членки, како и оние кои се на патот кон ЕУ, треба да обрнат посебно внимание: недоволна споредливост на податоците не само надвор од границите на ЕУ, туку и меѓу државите членки; недостаток од кохерентен, систематски и долгорочен пристап на собирање на податоци за еднаквоста; податоците често се собираат на основа на ирелевантни или застарени категории и дефиниции; оние кои се обично спремни и компетентни да собираат податоци за еднаквоста, како што се телата за промоција на еднаквост и истражувачките институции, често немаат потребни ресурси; неразбирањето на законодавството за заштита на податоците води кон собирање на помалку податоци отколку што е вообичаено; податоците кои се на располагање, обично не се користат во својот полн потенцијал и сл.²¹ Поради сето ова собирањето на податоци за еднаквоста заслужува посебно внимание во повеќето европски држави и кај нас. Тоа пред се бара навремено и потполно усогласување на националното законодавство со европското, зголемување на свеста за потребата од податоци за ранливите и маргинализираните групи, посебна стручност, искуство и знаење кои можат да се превземат од земјите

²⁰ European Commission, The Former Yugoslav Republic of Macedonia 2018 Report.

²¹ Makkonen, T.: European handbook on equality data, Brussels, 2016, p.13

или заедниците кои веќе се стекнале со различно и долгогодишно искуство во оваа област. Учењето од таквите практики и размена на искуство, не само што го подобрува знаењето, туку помага и во избегнувањето на грешки и на тој начин штеди време и финансиски ресурси.²²

Литература

- Alpha Abdikeeva: Measure, Plan, Act: How data collection can support racial equality, ENAR 2014;
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995).
- ENAR, COMBATING INEQUALITY AND DISCRIMINATION IN EMPLOYMENT: Data collection as a necessary step to plan action, Open Society Foundations, 2015. http://www.enar-eu.org/IMG/pdf/edc-business_factsheet_final.pdf
- ENAR, EQUALITY DATA COLLECTION: FACTS AND PRINCIPLES, Open Society Foundations, 2015.
- ECRI, Fifth report on "the Former Yugoslav Republic of Macedonia" (fifth monitoring cycle), Strasbourg, 2016;
- ECRI General Policy Recommendation N°11: Combating racism and racial discrimination in policing, 2007;
- European Commission, The Former Yugoslav Republic of Macedonia 2018 Report.
- Michel GLAUDE: Eurostat /Directorate F, Director Social statistics and information society, 2007;
- Monika Mayrhofer: DOBRE PRAKSE U PRIKUPLJANJU PODATAKA O (NE)JEDNAKOSTI, Zagreb, 2017;
- Study on Data Collection to measure the extent and impact of discrimination in Europe Final Report 7.12.2004, <http://edz.bib.uni-mannheim.de/daten/edz-ath/gdem/04/collection%20data.pdf>
- Timo Makkonen, European handbook on equality data, Brussels, 2016.
- Timo Makkonen: Measuring Discrimination: Data Collection and EU Equality Law, 2006;

²² Mayrhofer, M., *op.cit.*, str. 10-11.

THE USE OF ARTIFICIAL INTELLIGENCE IN THE MILITARY DOMAIN

UDC: 004.8:355.1

Reviews

Assistant Professor Aleksandar Nacev, PhD, Professor Marjan Bogdanovski, PhD

European University Republic of Macedonia – Skopje

Abstract

Artificial intelligence (AI) is having a moment in the national security and defense domain. What does this really mean, especially when you move beyond the rhetoric of revolutionary change and think about the real world consequences of potential applications of artificial intelligence to militaries? Artificial intelligence is not a weapon. Instead, artificial intelligence, from a military perspective, is an enabler, much like electricity and the combustion engine. Thus, the effect of artificial intelligence on military power and international conflict will depend on particular applications of AI for militaries and policymakers. The potential promise of AI, including its ability to improve the speed and accuracy of everything from logistics to battlefield planning and to help improve human decision making, is driving militaries around the world to accelerate their research into and development of AI applications.

Keywords: *Artificial intelligence, military, battlefield, warfare, cyber.*

Introduction

Artificial intelligence (AI) also known as **machine intelligence (MI)** is **intellect** displayed by computer system (or machine), in contrast with the **natural intelligence (NI)** displayed by humans and other animals. Given the complexity involved in application of AI in both military and civilian spheres, a working definition of AI is required. There is no one commonly decided definition, even among computer scientists and engineers, but a general definition of AI is **the capability of a machine to perform tasks that normally require human intellect, such as visual perception, speech recognition and decision-making.**¹ Advances in artificial intelligence (AI) are enabling new military capabilities that will have a disruptive impact on military strategies. The effects of these capabilities will be felt across the spectrum of military requirements - from intelligence, surveillance, and reconnaissance to offense/defense balances and even on to nuclear weapons systems themselves. What does this really mean, especially when you move beyond the rhetoric of revolutionary change and think about the real world consequences of potential applications of artificial intelligence to militaries?

¹ Gupta Kumar Deepak (2018). "Military Applications of Artificial Intelligence". Centre for Land Warfare Studies (CLAWS)

Artificial intelligence is not a weapon. Instead, artificial intelligence, from a military perspective, is an enabler, much like electricity and the combustion engine. Thus, the effect of artificial intelligence on military power and international conflict will depend on particular applications of AI for militaries and policymakers. The potential promise of AI, including its ability to improve the speed and accuracy of everything from logistics to battlefield planning and to help improve human decision making, is driving militaries around the world to accelerate their research into and development of AI applications.²

Top Applications of Artificial Intelligence in Military

The advent of AI could fundamentally change the character of warfare, resulting in a transformation from today's "informatized" ways of warfare to future "intelligentized" warfare, in which AI will be critical to military power. AI provides disproportionate advantage to otherwise technologically disadvantaged enemy as a disruptive technique.³ It is also evident that AI can be gainfully utilized to integrate Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities and works towards deeper fusion of systems and sensors across all domains of warfare. Adopting AI tools in defense enhances the processing and utilization of data which in turn improves the speed of decision-making on the battlefield. AI can be gainfully employed to enhance future capabilities in the following areas:

- Computational military reasoning;
- Intelligent and autonomous unmanned systems;
- AI-enabled data analysis, information processing and intelligence analysis;
- Cyber Defense and Cyber warfare;
- Electronic warfare.

Computational Military Reasoning

Computational military reasoning solves military problems that humans face and focuses on making the right battlefield decisions. It analyzes the area of conflict and acts on the data it received from the set of orders (known as Course of Action or COA). Computational military reasoning is a computer solving human-level military problem and concentrates on tactical artificial intelligence or battlefield decisions. Tactical AI analyzes the battlefield and acts on that information by creating a set of coherent orders (commonly known as a Course of Action or COA) that exploit the weaknesses in enemy's position that were found during battlefield analysis. Many international labs have successfully demonstrated the hypothesis that an unsupervised machine learning program could also learn this skill and perform battlefield analysis that was statistically indistinguishable from

² Michael C. Horowitz (2018). The promise and peril of military applications of artificial intelligence. Bulletin of the Atomic Scientists

³ Gupta Kumar Deepak (2018). Military Applications of Artificial Intelligence". Centre for Land Warfare Studies (CLAWS)

analyses performed by Subject Matter Experts (SMEs). The said application of AI can be gainfully utilized for terrain analysis, war gaming and tactical training.⁴

Intelligent and Autonomous Unmanned Weapon Systems

Unmanned vehicles that are used by armed forces, as well as the most sophisticated weapons and robotics, are some of the direct uses of AI. These weapon systems have the requisite intelligence to observe, pursue and destroy enemy targets distinctly. AI can be used in the development of Intelligent and Autonomous Weapons Systems, including **unmanned aerial, surface and underwater vehicles**, as well as military robotics and cruise missiles.

AI-Enabled Information Processing and Intelligence Analysis

AI can be applied for effective processing of sensor data and raw intelligence which incorporates intelligent sensing and automation of multi-sensor data fusion to enhance situational awareness. Deep learning algorithms can be used to effectively process sensor data and raw intelligence that was collected from satellite imagery. All this information can in turn aid in making accurate decisions during an operation.

Cyber Defense and Cyber Warfare

AI can be leveraged to enhance the defense of critical military networks and information systems, to scale the effects of offensive cyber operations, and to inform command decision-making in cyber warfare. Cyber attacks can be detected and curbed through pattern matching, statistical analysis, machine learning and big data analysis. For example, Distributed Denial of Service (DDoS) attacks can be detected and mitigated through pattern matching, statistical analysis, machine learning and big data analysis. In particular, given the speed of cyber operations, AI could serve as a critical enabler of rapid command.⁵ Offensive cyber operations unleash a large scale of destruction in a matter of minutes. Considering the speed at which AI works, it serves as a counter-intuitive force against malicious cyber threats.

⁴ Gupta Kumar Deepak (2018). Military Applications of Artificial Intelligence". Centre for Land Warfare Studies (CLAWS)

⁵ Ibid.

Electronic Warfare (EW)

EW employs the electromagnetic spectrum (that includes radio waves, infrared signals or radar) to sense, protect, and communicate data. It can be also used to block enemies from using signals. As the electromagnetic spectrum becomes ever more complex and contested, the introduction of AI will be critical to achieving an advantage and pursuing offensive capabilities in cognitive electronic warfare through the application of machine learning to learn and rapidly devise countermeasures for adversary systems.⁶

Conclusion

The consequences of AI for the world will likely exceed the consequences for military power and the future of war. Advances in military applications of AI are the reality, and it can be expected that AI will eventually manifest in all warfare dimensions.

It is a good idea for all serious countries to make efforts to evaluate the range of short, medium, and long-term applications of AI in warfare. There is also a need to train and cultivate human resource for military applications of AI. Talented young generation needs to be targeted to transform the same into a potent force and remuneration should be attractive enough to render long term service.⁷

Bibliography

1. Cummings L. M.: *Artificial Intelligence and the Future of Warfare*. The Royal Institute of International Affairs. Chatham House. London.2017
2. Gupta Kumar Deepak: *Military Applications of Artificial Intelligence*. Centre for Land Warfare Studies (CLAWS).2018 <http://www.claws.in/1878/military-applications-of-artificial-intelligence-deepak-kumar-gupta.html>
3. Horowitz C. Michael: *The promise and peril of military applications of artificial intelligence*. Bulletin of the Atomic Scientists.2018 https://thebulletin.org/landing_article/the-promise-and-peril-of-military-applications-of-artificial-intelligence/
4. The Hague Centre for Strategic Studies: *Artificial intelligence and the future of defense: Strategic implications for small and medium-sized force providers*. The Hague Centre for Strategic Studies. Hague.2017

⁶ Gupta Kumar Deepak (2018). *Military Applications of Artificial Intelligence*". Centre for Land Warfare Studies (CLAWS)

⁷ Ibid

СТРАВОТ ОД ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА

UDC: 004.8:159.942

*Прегледен труд***Доц. д-р Васко Стамевски, Проф. д-р Елизабета Стамевска, д-р Зоран Крстевски***Европски Универзитет Република Македонија - Скопје*

Апстракт

Неоспорлив факт е дека вештачката интелигенција е популарна тема внатре и надвор од информатичката индустрија. Мислењата во врска со користењето на вештачката интелигенција се поделени, а стравот е сè поприсутен од последиците при создавање на нешто што би можело да се мери или дури да го надмине човекот.

Стравувањата одат во насока дека вештачката интелигенција, иако засега е на рудиментарно ниво, можно е наскоро да развие свест која ќе ѝ дозволи да ги оптимизира своите цели и да стори сè за да ги оствари. Односно, ако одредена вештачка интелигенција еноормно се развие и реши дека човекот ѝ пречи во реализирањето на своите цели, поставени токму од него, тогаш може да одлучи дека луѓето се непотребни и да почне да дејствува во насока на елиминација на човештвото.

Клучни зборови: *вештачка интелигенција, информатичка индустрија, човештво, интелигентни агенти, компјутерска наука*

THE FEAR OF ARTIFICIAL INTELLIGENCE

Abstract

An indisputable fact is that artificial intelligence is a popular topic inside and outside the information industry. Opinions about the use of artificial intelligence are divided, and fear is more prevalent than the consequences of creating something that could be measured or even surpassed by man.

The fears go in the direction that artificial intelligence, although it is at the rudimentary level for now, it is possible to develop an awareness soon, which will allow it to optimize its goals and make them realize them. That is, if a certain artificial intelligence is enormously developed and resolved that a person bothers in the realization of his goals set by him, he can then decide that people are unnecessary and begin to act in the direction of the elimination of humanity.

Key words: *artificial intelligence, information industry, humanity, intelligent agents, computer science.*

Вовед

Вештачката интелигенција (ВИ) е интелигенција којашто ја демонстрираат машините, за разлика од природната интелигенција, застапена кај луѓето и животните. Во компјутерската наука истражувањето на вештачката интелигенција е дефинирано како проучување на „интелигентни агенти“, односно кој било уред којшто ја перципира околината и презема активности кои ги максимизираат шансите за успешно постигнување на целите.¹

Традиционалните проблеми (или цели) на истражувањата на вештачката интелигенција вклучуваат размислување, презентирање на знаење, планирање, учење, обработка на природниот јазик, перцепција, способност за движење и манипулација со предмети.² Во 21 век, техниките на ВИ повторно оживеаја и станаа суштински дел од технолошката индустрија, помагајќи да се решат многу предизвикувачки проблеми во компјутерската наука, софтверското инженерство и оперативните истражувања.³

Побарувачката за персонализирано корисничко искуство поттикнува поголема употреба на вештачката интелигенција во работата на компаниите. Од една страна се наоѓа утопистичкото општество на иднината, во кое луѓето се ослободуваат од секојдневниот напор и комплексните работни задачи, кои сè повеќе ги работат машините, од друга страна, забележителна е дистописката анксиозност, чувството на хумана инфериорност и страв од ментално завладување. Во контекстот, некои сметаат дека вештачката интелигенција е опасност за човештвото, доколку напредува со несмалено темпо, други, пак, веруваат дека, за разлика од претходните технолошки револуции, ВИ ќе создаде ризик од масовна невработеност.⁴

Последниве години сè почесто во медиумите и јавноста се поставува прашањето - оправдан ли е стравот од вештачката интелигенција? Одговорот, се чини, зависи од тоа до која мера ќе се развие оваа интелигенција што компјутерската наука сака што повеќе да наликува на човечкото однесување. Но, зависи и од фактот, доколку биде постигнато потенцијално опасно ниво на нејзиниот развој, во чии раце би паднала, бидејќи и нуклеарната енергија ветуваше решение на растечките енергетски потреби на човештвото, но, за жал, се искористи и за создавање оружје за масовно уништување. Прашањето за развојот на вештачката интелигенција научната заедница го решава низ два главни концепта: „силна“, односно „целосна“ вештачка интелигенција и „слаба“ или „ограничена“ вештачка интелигенција.

Приврзаниците на идејата за „силна“ вештачка интелигенција веруваат дека е можно создавање на „вистинска“ вештачка интелигенција, што би значело машините во перспектива не само да им парираат туку и да ги надминат луѓето во апстрактното и креативното мислење, па, дури и да чувствуваат, односно да имаат емотивен живот. Но, најголем дел од стручната светска јавност смета дека со

¹ Russell, S., Norvig, P., „Artificial Intelligence: A Modern Approach“ (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13-790395-2, 2003

² Luger, G.; Stubblefield, W., „Artificial Intelligence: Structures and Strategies for Complex Problem Solving“ (5th ed.). Benjamin/Cummings. ISBN 0-8053-4780-1. 2004.

³ Kurzweil, R., „The Singularity is Near“, Penguin Books. ISBN 0-670-03384-7, 2005, p.265.

⁴ Ford, M., Colvin, G., „Will robots create more jobs than they destroy?“. The Guardian. Retrieved 13 January 2018

концептите на кои е базирана денешната кибернетика, развојот на „силна“ вештачка интелигенција е неизведлив.

Научниците што ја поддржуваат теоријата за „слаба“ вештачка интелигенција, сметаат дека врвот на интелигенцијата на машините не би одел подалеку од уверлива симулација на човечкото однесување. Добар пример за „слаба“ ВИ е паметниот личен асистент на Apple, Siri, кој препознава говор и овозможува говорно управување со одредени операции на уредот, каде што е инсталиран. За „слаба“ вештачка интелигенција зборуваме сè дури софтверот е програмиран за одредени намени, колку и фасцинантно нам да ни изгледа неговата изведба.

Како и да гледаме на вештачката интелигенција, сепак, вистината е дека влегуваме во огромен трансформативен циклус во речиси секој бизнис. Додека ВИ во моментот е најприсутна преку големото внимание што го добива од медиумите, како и бизнис секторот, начинот на кој компаниите и потрошувачите комуницираат веќе е подготвен за коренити промени преку користење на вештачката интелигенција како основа на нивните решенија. Со успехите на вештачката интелигенција се зголемува одговорноста да се разгледаат општествените импликации на технолошкиот успех и да се едучираат оние кои ги донесуваат одлуките за јавноста да може да планира на нив.⁵

1. Опасноста од вештачката интелигенција

Современите машински способности, генерално, класифицирани како вештачка интелигенција, вклучуваат успешно разбирање на човечкиот говор,⁶ се натпреваруваат на највисоко ниво во стратешките играчки системи (како шах), автономни оперативни возила и интелигентно рутирање во мрежите за испорака на содржини и воени симулации.

Во последно време сме преплавени со апокалиптични предвидувања за тоа како вештачката интелигенција ќе не пороби ако не го зауздаме нејзиниот развој. Ваквите прогнози не доаѓаат од лица кои слепо веруваат во теории за заговор туку од некои од највлијателните ликови во технолошко-научната заедница на денешницата, како Елон Маск, Бил Гејтс, Стивен Хокинг...

Илон Маск со години предупредува на потенцијално катастрофалните последици од развојот на вештачката интелигенција. Тој пред извесно време укажа дека автоматизацијата на работната сила не е единствениот одговор, а луѓето неправедно се потценуваат. Оваа изјава можеби не е соодветна за човек кој се смета за еден од водечките технолошки и бизнис-лидери и кој неспорно, длабински ги промени финансиската, автомобилската и вселенската индустрија. Но, тој не е единствениот. Бил Гејтс, во неколку настапи, исто така, предупреди на овие проблеми, а во февруари годинава, дваесет и шест научници од „Кембриџ“, „Оксфорд“ и од други важни институции објавија научен труд за опасностите од ВИ.

⁵ Buchanan, Bruce G., „A (Very) Brief History of Artificial Intelligence“ (PDF), AI Magazine, 2005, p.60

⁶ Russell, S., Norvig, P., „Artificial Intelligence: A Modern Approach“ (3rd ed.). Upper Saddle River, New Jersey: Prentice Hall. ISBN 0-13-604259-7, 2009

Генерално, нивните аргументи се дека вештачката интелигенција не мора да биде малициозна за да биде опасна. Маск, на оваа тема истакнува: „Ако на ВИ, на пример, ѝ кажеме дека сакаме планета без загадување, таа може да донесе заклучок дека најбрзиот пат до тоа би бил да ја исчисти планетата од човекот“. Така, напредната вештачка интелигенција би била експоненцијално помоќна од човекката и, едноставно, сите основни задачи би ги извршувала неколку илјади пати побрзо од нас, смета тој.

Маск е на мислење дека вештачката интелигенција е далеку поопасна од нуклеарните бомби. Нашиот фокус мора да биде на безбеден развој на ВИ, затоа што нерегулираниот развој би можел да доведе до катастрофа. Слично мисли и легендарниот основач на „Мајкрософт“, Бил Гејтс, кој смета дека спојот на брзината на мислење и хипервисок коефициент на интелигенција би можел да биде катастрофален доколку не се ограничи навреме.

Покојниот британски научник Стивен Хокинг, иако поклоник на компјутерските и комуникациски технологии, потенцираше дека создавањето совршени мислечки машини би можело да претставува закана за опстанокот на човештвото. Легендарниот физичар и космолог, во однос на понатамошниот напредок на технологијата, која поради неговата прогресивна невромоторичка болест и самиот ја користеше за комуникација, како основен облик на вештачка интелигенција, предупреди дека развојот на целосно вештачка интелигенција би можело да го означи крајот на човекката раса. Таа би се осамостоила и сè позабрзано би се редизајнирала, а луѓето условени од бавната биолошка еволуција, би можеле да се натпреваруваат со неа и би биле надминати.

Во ерата на машинското учење работите се помалку примитивни и помалку буквални. Наместо точно зададени алгоритми за секоја активност и ситуација, компјутерот би можел самиот да измислува нови, непрограмирани начини за решавање на проблемите. Во еден неодамнешен експеримент два компјутери во неколку часа, без наредба, измислиле сопствен јазик кој авторите не можеле да го препознаат. Тоа не го направиле со намера да ја скријат содржината на својата комуникација, туку за да ја забрзаат, но импликациите од таквата одлука се потенцијално проблематични. Токму во тоа е стравувањето - можноста од енормен развој на компјутерската индустрија, којшто во еден момент на невнимание или наивност би можел да произведе исклучително силна интелигенција, што не ќе може да се контролира.

Ако ги слушаме сите овие предупредувања, тогаш треба да сме скептични кон иднината во која коегзистираме со интелигентна и свесна вештачка интелигенција.

2. Дали вештачката интелигенција ја презема улогата на човекот?

Денешните потрошувачи очекуваат високо контекстуализирани, течни интеракции со брендovите, кои традиционалните бизниси не можат да ги доловат. Потребата за персонализација и автентичност стануваат приоритет и нешто без кое не се може. Компаниите како Google, Uber, Netflix често се наведуваат како авангардни и први во обидот да ползуваат вештачка интелигенција, сепак

прашање на време е кога целата индустрија ќе биде преземена од технолошките алатки на вештачката интелигенција.

Промените незапирливо надоаѓаат. Банкарските услуги кои се борат за задоволување на барањата на потрошувачите, веќе се онлајн, со мобилни апликации и интеракција, а во моментот банкарите веруваат дека вештачката интелигенција ќе одигра клучна улога во премостувањето на дигиталниот јаз. Според извештајот на Accenture Banking Technology Vision 2017, кој анкетираше повеќе од 600 банкари, ВИ ќе биде револуцијата во начинот на кој банките ги собираат податоците, како и начинот на комуникација со своите клиенти.

Консултирањето со технолошките индустрии, академци и експерти покажа извештај во кој вештачката интелигенција станува прв и основен начин на кој банките ќе соработуваат со своите корисници во наредните години. Додека главна грижа е дека вештачката интелигенција ќе ги одземе човечките ресурси во банкарството, вистината е дека новите технологии им овозможуваат на банките да ги поедностават релациите со корисниците и да им ги испорачуваат само најрелевантните искуства за нив. Наспроти ова, ВИ на банкарските маркетинг тимови им овозможува оддалечување од секојдневните податоци и кампањи, во замена со квалитетно поминато време на креативни и иновациски процеси.

Во ултра конкурентната и заситена телекомуникациска индустрија, главните оператори постојано си ги „крадат“ претплатниците еден на друг за да си го зајакнат сопствениот раст. Новите платформи на вештачката интелигенција им овозможуваат на мобилните оператори да ги разберат сигналите во однесувањето на клиентите, како и да го предвидат евентуалното преместување на клиентите неколку недели порано. Со ова, можат да направат превентивни активности за да ги усогласат или изменат односите во соработката на корисниците со брендот (намалени цени, нови податоци, поттикнување со новости, примамливи понуди). Поради темпото на индустријата, големиот обем на достапни податоци и позицијата на главен канал за сите мобилни искуства, телекомуникациите имаат изгледи да постигнат најголем поврат на инвестициите од страна на технологијата поврзана со вештачката интелигенција.

Истражувајќи ја иднината на музичката вештачка интелигенција, се открива дека „Гугл“ и „Сони“ користат технологија со чија помош, во иднина, музиката би можела сама да се компонира. Денес, компјутерите пишуваат сè повеќе и повеќе музика, а фирмите вложуваат милиони долари во овој сложен процес.

Интересен е и примерот со вештачката интелигенција на „Гугл“, наречена „Алфа гоу“, создадена за потребите на древната кинеска игра што личи на шах, но е многу покомплицирана и потешка за играње. Иако имаше мислење дека компјутерите не можат да ја совладаат оваа игра барем уште дваесет години, односно дека немаат шанса против професионалните играчи, „Алфа гоу“ буквално ги демолира најдобрите играчи на светот. Притоа, особено загрижува тоа што со неочекувана брзина усвојува нови стратегии, проучувајќи ги потезите на своите противници и приспособувајќи се многу побрзо во споредба со човечкиот мозок. Патем, измислува сосема нови, на прв поглед, лудо ризични тактики кои играчите досега не ги користеле, што експертите го толкуваат како целосен недостиг на емоции.

Сепак, паралелно со овој процес, се очекува да се изродат и нови работни позиции кои ќе бараат човечки инпут. Едно истражување објавено во MIT Sloan Management Review се осврна кон резултатите од глобалната студија на повеќе од 1.000 големи компании кои користат или тестираат ВИ и машинско учење. Според него, неминовна е појавата на нови улоги и категории на работни места кои се уникатно човечки. Тоа сугерира дека когнитивната технологија ќе бара вештини што машините најверојатно нема да ги поседуваат во блиска иднина.

Заклучок

Стравот дека вештачката интелигенција ќе ги окупира сите области и професии кои бараат човечки инпут, сè повеќе ја бранува јавноста. Сепак, меѓу експертите постои без малку консензус дека сме многу далеку од точката на технолошки сингуларитет. Но, и од постојниот развој на вештачка интелигенција не недостасуваат причини за загриженост; на пример, за пазарот на трудот. Истражување на професори од „Оксфорд“ предвидува дека во САД, до 2033 година, половина од работните места на луѓето ќе бидат заменети со интелигентни машини.

Иако владее анксиозност кога ќе се помисли на автоматизацијата на работните места и нивната замена со вештачка интелигенција, некои се на мислење дека тоа остава простор за зголемување на креативноста и иновативноста што можат да ја дадат луѓето. Тие сметаат дека преоптоварените научници ќе имаат повеќе време за посериозни и покомплексни таргетирања. Без оглед на големата загриженост околу спектарот предизвици и стравови поврзани со вештачката интелигенција, очекувањата се зголемената креативност на крајот да резултира со подобро искуство за корисниците, но и со подобро искуство, воопшто, за сите луѓе.

Како позитивен пример е даден „Гугл“, кој започна светска кампања за поттикнување и развивање на вештачка интелигенција, којашто ќе реши некои од светските проблеми, преку „AI Impact Challenge“ натпревар, на кој можат да се пријават сите што имаат идеја како со помош на вештачката интелигенција да се решат проблемите во природната средина, здравството или зачувувањето на природата. Желбата на „Гугл“ е да се фокусираат на развивање на вештачка интелигенција во проекти што ќе му донесат корист на човештвото, која нема да биде пристрасна и нема да има предрасуди кон одредени категории луѓе. Поттикнувањето на оваа иницијатива и предизвиците на глобално ниво се причината за компанијата да се дистанцира од користењето на вештачката интелигенција за производство на оружје. Имено, на почетокот на јуни 2018, од „Гугл“ објавија дека компанијата се повлекува од соработка со американската војска, а за понатамошен развој на вештачката интелигенција ќе ги користи своите етички принципи. Тие вклучуваат одбивање работа за развој на вештачката интелигенција, која намерно ги крши прифатените норми на приватност во проектите за надзор, како и оние проекти што ги кршат меѓународните закони и човековите права.

Сепак, и покрај ваквите хумани интенции на дел од компаниите, при употребата на вештачката интелигенција остануваат отворени прашањата: „Дали треба да се плашине или нестрпливо да очекуваме вештачката интелигенција да го замени човекот речиси во сите сфери на неговиот живот? Колку навистина ни е потребно тоа?“

Не може да се знае со сигурност дали стравовите се оправдани, не може ни да предвидиме како ќе се однесува свесната вештачка интелигенција. Во однос на загубата на работни места, треба да се напомни дека, барем засега, вештачката интелигенција не е многу способна во работи кои бараат креативност, емпатија, критичко размислување, уметничко изразување и низа други особини кои вообичаено ги сметаме за „човечки“, но не знаеме што може да се случи во иднина.

Литература

1. Buchanan, Bruce G., „A (Very) Brief History of Artificial Intelligence“ (PDF), AI Magazine, 2005
2. Kurzweil, R., „The Singularity is Near“, Penguin Books. ISBN 0-670-03384-7, 2005
3. Luger, G., Stubblefield, W., „Artificial Intelligence: Structures and Strategies for Complex Problem Solving“ (5th ed.). Benjamin/Cummings. ISBN 0-8053-4780-1. 2004
4. McCorduck, P., „Machines Who Think“, Twenty-Fifth Anniversary Edition. Natick, MA: A. K. Peters, Ltd, 2004
5. Milosavljević, M., „Veštačka inteligencija“, ISBN: 978-86-7912-590-3, Univerzitet Singidunum, Beograd, 2015
6. Russell, S., Norvig, P., „Artificial Intelligence: A Modern Approach“ (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13-790395-2, 2003
7. Russell, S., Norvig, P., „Artificial Intelligence: A Modern Approach“ (3rd ed.). Upper Saddle River, New Jersey: Prentice Hall. ISBN 0-13-604259-7, 2009

ПРАВНИ АСПЕКТИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

UDC: 343.9:004.056

Прегледен труд

Проф. д-р Ристо Христов, Јордан Ќирковиќ*Европски Универзитет Република Македонија - Скопје*

Апстракт

Со Конвенцијата не е предвидена ни обврската на провајдерот да ги чува податоците за своите корисници, кои подоцна можеби би им требале на надлежните органи и тоа заради повреди на одредени начела. Во 2003г. донесен е додатен протокол со кој се регулира ширењето на омраза, нетолеранција према расните, верските или одредени национални групи и заедници. Ширењето на овие погубни идеологии и ставови, на пример ширењето на неонацизам, тероризмот можат многу брзо да се развиваат и да излезат од контрола.

Клучни зборови: *податоци, протокол, нетолеранција, контрола.*

LEGAL ASPECTS OF CYBER CRIME

Abstract

The Convention does not provide for the obligation of the provider to store data for its users, which may later be required by the competent authorities for violations of certain principles. In 2003, an additional protocol was adopted that regulates the spread of hatred, intolerance against racial religious or certain national groups and communities. The spread of these destructive ideologies and attitudes, for example, the spread of neo-Nazism, terrorism can develop very rapidly and get out of control.

Keywords: *data, protocol, intolerance, control.*

Вовед

Информатичката технологија покрај многу практични предности во производството и животот, донесе и низа промени кои можат да го нарушат истиот. Многу е важно да се разберат ограничувањата на користењето на информатичката технологија, односно да се разберат начините на користењето со што не би се нарушиле одредени дали законски, дали морални или етички норми.

Бидејќи ИТ технологијата овозможува многу дејствија кои се злоупотреби или незаконски дејствија, факт е дека тие дејствија би требало да бидат правно протолкувани и да има законски акти за нивно санкционирање.

Правни аспекти на компјутерскиот криминал

Во позитивните закони на Република Македонија се наведени следните кривични дела против безбедноста на компјутерските податоци:

1. Во **неовластено користење на компјутерскиот систем и компјутерската мрежа** спаѓаат следните активност: оштетување, прикривање, бришење, измена или некоја друга активност со кои податоците или програмите стануваат неупотребливи.
2. Под **компјутерска саботажа** се класифицираат активностите: уништување, бришење, измена, оштетување прикривање или некоја друга активност со која податоците или програмите стануваат неупотребливи; оштетување на компјутерскиот систем или некој друг електронски уред за обработка и пренос на податоци кој е од важност за државните органи, јавните служби, институциите, претпријатијата или некоја друга организација.
3. **Креирање и внесување на компјутерски вируси или некои други малициозни програми** со или без намера да се предизвикаат штети на туѓиот компјутер, односно на туѓата компјутерска мрежа.
4. **Компјутерска измама** претставува: внесување на неточни податоци, невнесување на важни податоци или друг начин на криење на податоци и влијание на резултатите при електронската обработка на податоците, односно при преносот на податоците со намера себе или на некој друг да се обезбеди незаконска материјална корист, а со тоа на некој друг да му се нанесе материјална или друга штета.
5. **Спречувањето на функционирање на електронската обработка, на пренос на податоци и на компјутерската мрежа** е неовластен пристап до електронската обработка на податоци, до компјутерската мрежа со цел да се предизвика застој и пореметување на функционирањето на електронската обработка и преносот на податоци или на функционирањето на мрежата.
6. **Неовластен пристап до заштитен компјутер, односно компјутерска мрежа** е секој пристап со кој не се почитуваат или кршат физичките и/или електронските мерки за нивна заштита.
7. **Спречување и ограничување на пристапот до јавна компјутерска мрежа** е секое неовластено спречување или отежнување на пристапот на корисникот до било која јавна компјутерска мрежа од страна на приватно или службено лице или институција.
8. **Одбивање на соработка и недавање на докази** исто така претставува кривично дело.

Најчести типови на напади на компјутерските мрежи од интернет се:

- вирусни напади кои ги уништуваат податоците;
- напади од тип на прекинување на сервисите – DOS – Denial of Services;
- повторување на испратени пораки;

- **погодување на лозинката;**
- **напади од типот на тројански коњ – дистрибуција на злонамерни програми на работната страница кои при одредени услови се активираат;**
- **лажно претставување – неавторизиран пристап до податоците или креирање на неавторизирани податоци;**
- **прислушување;**
- **криптоанализа – откривање на тајни клучеви, односно пристап до отворени податоци врз основа на откриените клучеви.**

Со текот на времето оваа поделба станала застарена и нефункционална, бидејќи постоеле и многу внатрешни поделби и нови разграничувања, како поделбата на многу видови вируси или пак тројанци како оние кои делуваат на компјутерите од далечина (Remote administration Trojan). Нападот на компјутерскиот систем од далечина е посовршен и потежок за детекција и форензичка анализа, но како напредуваат системите на напади, така се усовршуваат и форензичките техники. Со помош на овие програми, оддалечен корисник има можност да преземе целосна контрола врз заразениот компјутер, а без знаење на неговиот сопственик. На овој начин создадено е ново поглавје во анализите на компјутерскиот криминал, кога веќе не е само прашање на докажување дека нападот е извршен од некој компјутер, туку и дали сопственикот на компјутерот бил свесен, односно дали знаел за тоа.

Биохакирањето сè повеќе се спомнува и претставува голема опасност. FDA ги предупредува производителите на медицинска опрема и болниците да посветат повеќе внимание особено на пејсмејкерите, дефибрилаторите и другата опрема. “Притоа мора да се напомене дека најголемиот стручњак за ИТ сигурност од биохакирање Барнаби Џек (Barnaby Jack) тврдеше дека на оддалеченост од 15 метри може да хакира лице со пејсмејкер и сериозно да му наштети.”

“Иронично е што и Barnaby почина после една недела од таа своја презентација за хакирање на лице со пејсмејкер на Black Hat Conference во Лас Вегас и тоа од срцев удар.”

¹ Инфо тренд 25 194/01/2014

¹ Инфо тренд 25 194 /01/2014

Многу корисници се свесни дека со помош на тројанци може да се изведе напад со нивниот компјутер, додека тие работат на истиот и тоа да не го забележуваат. Праксата покажала дека осомничените за компјутерски криминал токму тоа знаеле да го искористат во својата одбрана, дека нивниот компјутер бил преземен од друг корисник. Имало повеќе такви случаи во Велика Британија и во САД. Главна цел на форензиката е да се детектира криминалот и да се обезбедат цврсти и валидни докази кои ќе го разоткријат делото.

Основни елементи на кривичното дело компјутерски криминал го сочинуваат:

- **случајот - што се случило во дадениот момент;**
- **како се случило тоа;**
- **профил на можниот извршител на кривичното дело.**

Како главни категории за поделба на компјутерскиот криминал можат да се земат неколку фактори како:

- дали компјутерот бил цел на напад;
- дали компјутерот бил средство за напад (измами со кредитни картички);
- дали компјутерот бил врска за обичен криминал (трговија со луѓе, дрога, детска порнографија);
- репозиториум (магацин на докази на компјутерски криминал).

Првично и најчесто користена поделба на дигиталната форензичка истрага е следната на:

- официјална - јавна; и
- корпоративна - приватна.

Официјалната дигитална форензичка истрага вклучува повеќе органи, пред сè полициските истражни органи, специјалното обвинителство, како и специјалното судство за борба против компјутерскиот криминал. Нивната истрага, неопходно, мора да биде во склад со:

- Законот за кривична постапка;
- Законот за борба против високотехнолошки криминал;
- Законот за електронски попис;
- Законот за електронска трговија.

При официјалните истраги за компјутерски криминал, истражните органи мора да почитуваат строго определени стандарди за оперативни процедури како:

- истрага;
- привремено одземање и испитување на компјутерските системи и други мрежни уреди;
- аквизиција;
- дигитални податоци кои можат да бидат доказ.

Антивирусните компании McAfee Sumantec во своите годишни извештаи за 2008г., објавиле дека во текот на таа година се појавиле повеќе од милион малициозни програми, а само бројот на тројанците бил проценет на повеќе од 120.000 видови, што значи дека сега после пет години веројатно станува збор за уште поголема бројка и за посериозни програми со кои сè потешко се соочуваат.

Корпоративната форензичка истрага е модел на истрага на компјутерски криминал кој е интересен и не е од јавен карактер, бидејќи се однесува за истраги во круг на организација. Современите мобилни телефони, Bluetooth уредите, мемориските чипови, разните PDA-уреди, можат да ги вршат сите задачи на еден компјутер, некои од нив имаат и поголеми перформанси од послабите компјутери, вклучуваат и оддалечен пристап на компјутерска мрежа без знаење на организацијата. Ова претставува само дел од системот на новата технологија која бара заштита на ИТ системот на организацијата, но истовремено е и предизвик за примена на техника и алати на корпоративната дигитална форензика за реконструкција на компјутерскиот инцидент.

Заклучок

Информатичката технологија стана дел не само од професионалниот живот туку и од приватниот. За жал, користењето на техниката може и да уништи многу животи, кариери, да ги уништи сите морални вредности на некој бидејќи се појавуваат лажни информации и лажни слики, но и вистински реални и информации кои требале да бидат приватни, а станале јавни. Се поставува прашањето каде почнува, но и каде завршува моралноста на луѓето, дали за нечиј успех или пак за одмазда треба да се згазат сите морални човечки вредности и дали се заборавени сите морални вредности и етиката, а како главен и примарен фактор според кој човекот си го наоѓа местото во општеството станаа парите, богатството, колата и моќта. Никогаш не треба да се заборави дека атомската бомба е чудо на техниката, голем дострел на човечкиот ум да ја искористи фузијата и да создаде огромна енергија, но каде е етичкиот момент таа да се искористи за воени цели, да се употреби за бомби, за уништување многу човечки жртви во Хирошима и Нагасаки. Последиците од тие бомби се уште се чувствуваат зашто болестите кои се појавени од радијацијата и денес се видливи, а да не заборавиме тоа не се жртви на некои природни непогоди кои човекот не можел да ги спречи човекот е создател, творец. Слична е состојбата и во фармацијата како се создадени толку бојни отрови, толку вируси и лабораториски болести, не за барање лек, туку за создавање на болести кои ќе сеат смрт, науката и технологијата во секој од тие случаи без оглед од исходот дали со злоупотреба на информатичката технологија ќе се доведе до психичка болка, до траума или пак со други научни пронајдоци се доведе до фактичка смрт, одговорноста е иста, човекот треба да биде човек, да ги користи подобностите, но не по секоја цена и не по цена на туѓи несреќи.

Литература

1. Законот за кривична постапка
2. Законот за борба против високотехнолошки криминал
3. Законот за електронски попис
4. Законот за електронска трговија
5. C.Reed, Internet Law: Text and Materials, butterworths, 2004
6. H.Tavani, Ethics and Tehnology, ontroversies, Questions, and Strategies for Ethicalm Computing, John Willey and Sons, 2011

ЕРОЗИЈА НА ПРАВОТО НА ПРИВАТНОСТ НА КОРИСНИЦИТЕ НА КОМПЈУТЕРСКИТЕ СИСТЕМИ, СОЦИЈАЛНИТЕ МРЕЖИ, МОБИЛНИТЕ УРЕДИ И КЛАУД СЕРВИСИТЕ

UDC: 342.738:004.77

*Прегледен труд***М-р Александар Трајковски**

Апстракт

Целта на истражување во овој труд е да се прецизираат причините кои предизвикаа сериозна порозност на правото на приватност на корисниците на компјутерските системи, социјалните мрежи, мобилните уреди и клауд сервисите. Едновременно со тоа ќе се направи проценка на безбедносните текови во виртуелниот простор и однесувањето на техничко-технолошките гиганти на светската сцена, вклучително и нивните заемни (условени) соработки со националните безбедносни, одбранбени, разузнавачки и контраразузнавачки служби на современите земји. Исто така, ќе се направи и обид за поединечно профилирање на категориите на корисници на производите и услугите кои ги нудат гигантите, а истовремено и анализираат нивните реакции при злоупотреба на нивните лични податоци. Покрај тоа, ќе се направи проценка на степенот на доверливост, но исто така и на ризиците од злоупотреба на личните податоци на корисниците. Во меѓувреме, додека во фокусот се ставени горенаведените клучни точки, ќе се направат и обиди за хронолошки преглед на начините на кои техничко-технолошките гиганти (преку своите производи и услуги кои тие ги нудат на пазарот) ги пречекорија овластувањата за прибирање секаков тип на лични податоци од корисниците и како тие ги користат за свои потреби, вклучително и за потребите на националните служби на современите земји. Акцентот, исто така, ќе биде ставен и на некои држави и меѓународни организации кои преземаат конкретни чекори за ревоспоставување на потребното ниво на безбедност на личните податоци на корисниците, воедно и отпочнување конкретни судски постапки за утврдување на вина и санкционирање поради допуштените безбедносни пропусти од масовни размери на сметка на корисниците.

Клучни зборови: право на приватност, ранливост на корисниците, злоупотреба на лични податоци, безбедносни пропусти.

THE EROSION OF THE PRIVACY RIGHT TO USERS OF COMPUTER SYSTEMS, SOCIAL NETWORKS, MOBILE DEVICES AND CLOUD SERVICES

Abstract

The purpose of the research in this paper is to specify the reasons that caused the porosity of the right to privacy of users of computer systems, social networks, mobile devices and cloud services. At the same time, will be made an assessment of the security flows in the virtual space and the behavior of technical and technological giants on the world stage, including their mutual (conditional) cooperation with national security, defense, intelligence and counterintelligence services of modern countries. An attempt will also be made to individually profile the categories of users of the products and services offered by the giants, while at the same time analyzing their reactions when misusing their personal data. In addition, will be made an assessment of the degree of confidentiality, but also the risks of misuse of personal data of users. In the meantime, while focusing on the above mentioned key points, attempts will be made for a chronological review of the ways in which the technical-technological giants (through their products and services that they offer on the market) exceeded the authority to collect any type of personal user data and how they use it for their own needs, including for the needs of the national services of modern countries. Emphasis will also be placed on some countries and international organizations that take specific steps to restore the necessary level of security of personal data to users, as well as launch specific court procedures for convictions and sanctions due to the admissible security vulnerabilities from mass scale on users account.

Keywords: *right to privacy, vulnerability of users, abuse of personal data, security vulnerabilities.*

Вовед

Загрозувањето на правото на приватност на луѓето не е нешто ново, туку само доби нова димензија во современиот дигитализиран свет. Па така, со почетокот на втората деценија од 21 век, почнаа да се забележуваат тектонски поместувања (на глобално рамниште) во областите на техниката и технологијата, а предизвикани од заднинските несопирливи глобализациски процеси. Со други зборови, вината за појавата на ерозија на правото на приватност може да ја лоцираме во самите себе, бидејќи (не)свесно станавме заробеници на своите техничко-технолошки достигнувања кои секојдневно се насекаде околу нас и влијаат на нас. Тоа го постигнавме на два начини. Прво, со аспирациите за развој и доаѓање до нови откритија во техниката и технологија. Второ, дозволувајќи таквите техничко-технолошки пронајдоци да бидат дел од нашето секојдневие и да влијаат на нас, така што практично дозволивме нашата приватност да биде ставена под лупа (мониторирана), вклучително и дозволивме право на пристап скоро на секој до истата, а притоа не исклучувајќи ја можноста од изложување на сè во

јавност. Како последица на тоа, неоспорно се наметна потребата за потрага по изнаоѓање нови стратегии за поголема приватност во виртуелниот простор.

1. Ерозија на правото на приватност на корисниците на компјутерски системи

Денес е невозможно животот на човекот да се замисли без компјутер. Практично, тој овозможи голем број на поволности и значително го олесна функционирањето во секојдневието без притоа да се вложи преголем напор, а едновременно и за релативно кратко време да се постигнат бројни конкретни резултати. Но, затоа, пак, од друга страна драстично се изместија концептите за виртуелна и индивидуална безбедност и правото на приватност на личните податоци на корисниците. Како главен причинител за ваквите предизвикани појави и состојби е технолошкиот гигант Microsoft. Неговата вина може да се лоцира во неговиот софтверски производ – оперативниот систем Windows 10. Во него беа вложувани големи надежи, иако на почетокот беа воочени голем број на недоследности, грешки и пропусти кои подоцна со секое безбедносно ажурирање се елиминираа, односно надминуваа. Но на крај прерасна во класична (мега)разузнавачка ИТ-алатка која слободно и без поголем проблем презема лични податоци од корисниците. Тоа е така, затоа што Microsoft со овој, а и со преостанатиот асортиман на производи, веќе со децении доминира на светскиот пазар, а со ваквата зацементирана позиција тој, практично, ги истиснува (од пазарот) на останатите (алтернативни) софтверски (и друг вид) производи на конкурентските компании, како на пример, Linux, Unix, Ubuntu, macOS, SteamOS, Chrome OS, Haiku, Fedora, FreeBSD, FreeDOS, ReactOS, Remix OS, Phoenix OS, Android-x86 и други. Меѓу кои, дури и сопствените застарени Windows платформи како, на пример, Windows XP, Windows Vista, Windows 7 и Windows 8 (заедно со надградбата Windows 8.1). Во контекст на ова, се наметнуваат следните клучни прашања:

1. Зошто Microsoft прибира лични податоци од корисниците?
2. Каков вид на лични податоци прибира?
3. Колкаво количество и за колкава временска рамка прибира лични податоци?
4. На кој начин се прибираат лични податоци од корисниците?
5. Како реагираат корисниците кога ќе дознаат дека нивните лични податоци се компромитирани?

Ова се низа прашања за кои ќе се направат обиди да се дадат одговори подолу во овој труд. Имено, иако Microsoft, во не толку далечното минато, започна да прибира лични податоци од корисниците со претходните верзии на оперативни системи, сепак со Windows 10 го забрза, т.е. револуционерира, овој процес создавајќи нови можности за проширување на дијапазонот на дејствување во ова насока. Поедноставно кажано, почна да манифестира поагресивен пристап. Тоа почна да го прави под изговорот дека сака да ги „предвиди потребите“ на корисниците за да може навреме да одговори на нивните барања на пазарот на понудата и побарувачката. Меѓутоа, другата скриена вистина е дека старите верзии на оперативни системи не испорачуваа доволно количество на лични податоци од корисниците за потребите

на Microsoft. Па, според тоа, Microsoft излезе со образложение во јавноста дека неговите софтверски инженери немаат повеќе време и сили за истовремено изготвување на безбедносни закрпи за сите оперативни системи. А, секако, всушност поентата беше присилно да мигрираат корисниците на новиот оперативен систем за да може повеќе да се „копа по нивната приватност“ со крајна цел да се воспостави апсолутна контрола над нив преку профилирање на нивните потреби и мониторирање на нивните активности со цел правење на детални пресметки и проектирање на стратегии и планови за изработка на следните нови генерации на техники и технологии. Меѓутоа, за жал, Microsoft забележа дека корисниците се уште пружаат отпор кон мигрирањето на новата оперативна платформа – главно заради сè уште популарниот Windows 7, но исто така и заради протекувањето во јавност на информации за неовластено прибирање лични податоци на Microsoft. За да ги совлада овие препреки, Microsoft почна да вметнува програмски кодови во новите генерации на процесори (Kaby Lake и Coffee Lake) кои всушност оневозможуваат поддршка за сите застарени оперативни системи, а со исклучок на Windows 10. Тоа го примени и кај застарените генерации на процесори (Celeron, Pentium, Core 2 Duo, Core 2 Quad, Core 2 Extreme, Core i3, Core i5, Core i7; едновременно постигнувајќи двоен ефект – зголемена продажба на нови процесори, вклучително и новиот оперативен систем) без знаење и побарана дозвола од корисниците, така што повремено значително им ја успорува работата на нивните компјутерски системи, но воедно и со покажување на периодични известувања преку „информативни прозорчиња“ со цел да се информираат дека постојат некакви системски грешки при обработката и процесирањето на податоците и информациите.

Компјутерските корисници (особено оние кои се приклучени и активни на Интернет) станаа претерано ранлива категорија на лица, бидејќи станаа честа мета на напади од страна на Microsoft. Најчеста категорија на лични податоци кои се предмет на неовластено прибирање се: име и презиме, пол, возраст, брачен статус, образование, работа и висина на месечни примања, адреса на живеалиште/престојувалиште, мајчиниот јазик на кој се пишува и говори (вклучително и други странски јазици, доколку се користат), моментална локација на компјутерскиот корисник, податоци за социјален живот, телефонски броеви и контакти, електронска пошта, заведени податоци од календарот на активности на оперативниот систем, банкарски сметки и историја на реализирани банкарски трансакции, сопственост на движен и недвижен имот, кориснички имиња и лозинки и профили на социјални мрежи, фотозаписи, видеозаписи и гласовни записи од социјалните мрежи и/или тврдите дискови; податоци од и-мејли кои се поврзани (синхронизирани) со Windows 10, политичка определеност, податоци за конфигурација на компјутерските системи, најчесто користени инсталирани апликации на компјутерските системи, историја на пребарувања преку веб-пребарувачи и сервисите за веб-пребарување, податоци за преземени содржини преку Интернет, податоци за преземени и/или игнорирани безбедносни софтверски надградби, гласовни и видео податоци преку вградените или инсталираните звучници и микрофони и (веб)камери на/од компјутерските системи, податоци за дијагностика на потенцијални грешки во оперативниот систем, податоци за сè што се пишува преку тастатура, собирање поединечни настани од компјутерските системи на корисниците итн.

Во однос, пак, на количеството на преземени податоци и временската рамка во која се изведува тоа, според спроведените анализи на извесен CheesusCrust, член на Voat, и покрај сите преземени безбедносни мерки од страна на корисниците на Microsoft оваа активност продолжува без поголеми проблеми и во континуитет да ја спроведува. Љубопитен да го дознае степенот на шпионажа на Windows 10, CheesusCrust го поставил неговиот Linux лаптоп со Windows 10 Enterprise виртуелна машина, како и со DD-WRT рутер кој бил користен за следење на сообраќајот.¹ CheesusCrust, исто така, ги оневозможил сите карактеристики за следење и предностите на телеметријата во оперативниот систем.² Тој потоа ја оставил машината да работи со Windows 10 преку ноќ, во обид да ги следи врските што оперативниот систем се обидува да ги направи.³ Осум часа подоцна, тој открил дека Windows 10 се обидел да воспостави над 5.500 врски со 93 различни IP-адреси, од кои речиси 4.000 биле воспоставени со 51 различни IP-адреси кои припаѓаат на Microsoft.⁴ По оставањето на машината за 30 часа, Windows 10 таа врска ја проширил со 113 не-приватни IP-адреси, потенцијално дозволувајќи им на хакерите да ги пресретнат овие податоци.⁵

Постојат бројни начини преку кои Microsoft обезбедува „рударење со личните податоци“ на компјутерските корисници. Во прв ред, може да се спомене пребарувачот Cortana кој функционира на база на облак-сервисите, а презема лични податоци преку сè што корисниците ќе впишат во полето за пребарување преку тастатурата или, пак, преку активирање на микрофонот и давање на гласовни инструкции на истиот за пронаоѓање на одреден вид на резултати. А, исто така, ја споделува и историјата на пребарувања. Подеднакво значајна е и улогата на ребрендираниот веб-пребарувач Internet Explorer, т.е. Microsoft Edge кој е составен дел од Windows 10, вклучително и сервисот за веб-пребарување Bing. Инвазијата на Microsoft врз приватноста на компјутерските корисници успешно ја остварува и преку алатките на Windows 10 кои се активираат со експресно наредување при инсталација на оперативниот систем, а кои активно и незабележително работат во заднина. Во широка лепеза на производи на овој технолошки гигант влегува и социјалната апликација Skype. Оваа апликација, во буквална смисла, овозможува споделување на (комбинација од) пишувани и гласовни податоци, вклучително и фотозаписи и видеозаписи на корисниците. Во оваа конотација вреди да се спомене и клауд сервисот Microsoft OneDrive кој, всушност, не само што нуди услуги за складирање и чување на секаков тип на податоци, како и можност за споделување и пристап до истите од било кој уред (без оглед на временската и просторната димензија), има, исто така, и капацитети за злоупотреба на истите во корелација со Microsoft серверите. Дополнително на ова, и Microsoft Office 365 пакетот (кој е достапен во он-лајн издание и ДВД-диск) дополнително влијае на ранливоста на приватноста на корисниците. Поентата е во тоа што и овој пакет може креираните и складираните содржини на корисниците да ги споделува со Microsoft преку телеметријата на Windows 10 (доколку е инсталиран) или преку OneDrive клауд сервисот (доколку

¹“Windows 10 Sends Your Data 5500 Times Every Day Even After Tweaking Privacy Settings.” *The Hacker News*. Swati Khnadelwal. 10th February 2016. Web. 20th July 2018. <<https://thehackernews.com/2016/02/microsoft-windows10-privacy.html>>.

²*Ibid.*

³*Ibid.*

⁴*Ibid.*

⁵*Ibid.*

станува збор за пристап до и работа преку Интернет). Понатаму, заканата по безбедноста на личните податоци може да извира и од Microsoft Outlook. Овој персонален информациски менаџер, кој игра улога на повеќенаменски сервис, собира и споделува лични податоци на различни начини како, на пример, при креирање на профил за електронска пошта (најчесто генералии на корисниците, телефонски броеви за верификација, или, пак, алтернативни и-мејл адреси како потврда и поддршка, матична држава, временска зона и сл.), преку Android и iOS-апликациите на Outlook итн.

Поради ваквите наметнати појави и состојби од страна на Microsoft, а кои (ин)директно разорно се рефлектираат врз правото на приватност, компјутерските корисници почнаа да манифестираат различни реакции. Па така, може да се забележи како едни реагираат панично и избезумено. Додека други реагираат револтирано (и се откажуваат од некои производи и услуги кои ги нуди Microsoft и/или мигрираат на производите и услугите кои ги нудат конкурентите). Трети, пак, реагираат скептично (со верување дека ефектот за скандалот во медиумите е поголем отколку штетите кои може да бидат предизвикани со споделувањето на личните податоци со Microsoft). Но, исто така, има и некои кои реагираат превентивно (со преземање на конкретни алтернативни безбедносни чекори).

Посебно кога станува збор за последнава категорија на компјутерски корисници (посебно оние кои се подлабоко упатени во компјутерското програмирање), почнаа да преземаат промислени чекори како, на пример, селективна перманентна деактивација, блокирање и/или бришење на телеметријата и преостанатите сервиси и регистри кои се специјализирани за „рудање со лични податоци“ во Windows 10 оперативниот систем. Додека, пак, некои други (помалку упатени во оваа проблематика) се насочија кон користење на готови софтверски решенија (кои некои од нив се бесплатни за преземање, а додека за други е потребен одреден паричен надоместок). Меѓу сите нив, најупотребувани се: StopWinUpdates, DisableWinTracking, Spybot Anti-Beacon, Ultimate Windows Tweaker 4 и др. А има и такви кои применуваат комбиниран пристап, т.е. комбинација и од првиот и од вториот начин. Некои, пак, од нив започнаа да внимаваат дури и со безбедносните надградби на оперативните системи, така што се насочија кон селективен и обмислен пристап кој подразбира избегнување на некои безбедносни закрпи кои всушност во себе не вклучуваат исклучиво ажурирање на системите, туку и реактивација, одблокирање, реинсталација и надградба на постоечките телеметрии и другите истородни сервиси и регистри, вклучително и инсталација на исти такви потполно нови. Впрочем причината за избегнување на ваквите закрпи не е единствено заради тоа, туку и заради надградба на самата програма за општи нагодувања, како и програмата специјализирана за нагодувања на приватноста на компјутерските корисници.

2. Ерозија на правото на приватност на корисниците на социјални мрежи

Социјалните мрежи, исто така, подеднакво ја еродираат безбедноста на личните податоци на корисниците. Речиси не постои социјална мрежа која (на било кој начин) не ја злоупотребила или продолжува во континуитет да ја злоупотребува дадената доверба на корисниците. Facebook се издвојува

како најеклатантен пример во однос на ова. Овој технолошки гигант, практично, го девалвира својот прогресивен напредок и кредибилитет и довербата која ја имаше стекнато кај корисниците и тоа токму поради соочувањето во јавноста со серија на скандали поврзани со злоупотреба на личните податоци на повеќемилионски корисници ширум светот. А сето тоа кулминираше со спектакуларен пад на акциите на берзата на Wall Street и неизвесните изгледи за финансиско опоравување во иднина, давањето отказ на шефот на безбедност – Алекс Стамос и други позначајни ИТ-кадри од редовите на компанијата, откажувањето од услугите на значителен дел од корисниците и др. Да биде работата уште полоша, во оваа афера активна улога одигра и Cambridge Analytica која обезбедила непречен пристап до базата на податоци на Facebook (со претходна дозвола на компанијата), а сè со цел да се влијае на јавното мнение во врска со одредени клучни настани како, на пример, со претседателската кампања на Доналд Трамп за избор на претседател на САД, со гласачкиот процес за Брежит и сл. Меѓутоа, ваквата афера не завршува тука. Впрочем, уште пред да избијат ваквите скандали во јавноста, Facebook призна пред јавноста дека пред 2011 година (уште пред да реагира американската Federal Trade Commission во врска со злоупотреба на личните податоци) склучила најмалку 60 конспиративни договори со други компании од ИТ-секторот од „калибарот“ како Apple, Samsung, Amazon, BlackBerry, Microsoft и многу други на кои, исто така, им обезбедила слободен пристап до базата со лични податоци на компанијата. Од друга страна, пак, за штетата да биде далеку поголема Facebook почна да изработува и имплементира свои разузнавачки ИТ-алатки над своите корисници од типот на Broadcast content view analysis based on ambient audio recording, myPersonality и др. Експертите на Facebook ја продлабочија ранливоста на корисниците и поради нивниот невнимателен однос при што допуштија да се појави грешка, односно безбедносен пропуст во системот, така што личните податоци на 14 милиони корисници станаа јавно достапни. Грешката која ги погоди овие корисници од 18 мај до 22 мај, се случи, додека Facebook тестираше нова функција.⁶ Грешката била целосно исправена до 27 мај.⁷ Тоа значи дека севкупните активности на корисниците во тој период биле изложени на увид на јавноста, а додека нивните профили кои биле блокирани или невидливи за другите станале целосно отклучени, односно достапни. Како последица на ваквиот след на немили настани, основачот на Facebook беше повикан на разговор за да даде образложение за ваквите безбедносни пропусти пред британските и американските законодавци, вклучително и пред законодавците на ЕУ. Од страна на САД и В. Британија беа иницирани темелни истраги за утврдување на кривична одговорност. А Европската комисија на ЕУ, пак, на Facebook и изрече дури и глоба од неколку милиони евра за повреда на правото на приватност на европските корисници. Воедно, како одговор на сето ова, ЕУ изготви и специјална регулатива за заштита на личните податоци (GDPR) која стапи на сила на 25 мај 2018 година со цел да превенира вакви непосакувани инциденти во иднина. За жал, од ваквата голгота (низ која поминуваат овие корисници) не се поштедени ниту пак корисниците на Instagram, Twitter, Viber, WhatsApp, Snapchat и др. Впрочем, тоа претходно го најави и поранешниот разузнавач на Агенцијата за

⁶“Facebook bug set 14 million users’ sharing settings to public.” *CNN tech*. Heather Kelly. 7th June 2018. Web. 4th August 2018. <<https://money.cnn.com/2018/06/07/technology/facebook-public-post-error/index.html>>.

⁷“Facebook bug made up to 14 million users’ posts public for days.” *Wired*. Louise Matsakis. 7th June 2018. Web. 4th August 2018. <<https://www.wired.com/story/facebook-bug-14-million-users-posts-public/>>.

национална безбедност (NSA), Едвард Сноуден, кој тоа го потврдува со објавувањето во јавност на тајни документи на Агенцијата, а во врска со прибирањето на лични податоци на корисниците од социјалните мрежи. Како резултат на сето тоа, корисниците на сите овие мрежи се ориентираа кон алтернативните решенија кои гарантираат далеку поголема безбедност и приватност како, на пример, Ello, Vero, Signal, Diaspora, Path, Rafter, Nextdoor, Tumblr, EyeEM, Mastodon, Plurk, Vine, Viddy, Medium и др.

3. Ерозија на правото на приватност на корисниците на мобилни уреди

Заканите по безбедноста и приватноста на корисниците се прелеваат дури и во светот на мобилните уреди и мобилните апликации. Поконкретно, опасностите со кои овие корисници се соочуваат доаѓаат токму преку мобилните телефони, таблетите, мобилните оперативни системи, па дури и мобилните апликации. Имено, корисниците на мобилните уреди на доминантните техничко-технолошки гиганти Samsung и Apple почнаа да се соочуваат со масовно прислушување преку вградените камери, микрофони и звучници дури и кога истите се ставени во мирување, односно се исклучени. Тоа значи формирање бази на фотографски, видео и гласовни записи. Неовластеното собирање кориснички податоци го интензивираа Google и Apple преку Android и iOS оперативните системи и сервисите за дигитална дистрибуција на апликации Google Play и App Store. Како дополнение на ова, овие гиганти почнаа дури и меѓусебно да се прислушуваат и следат. Ова кулминираше дури и со одредување глоба од неколку милијарди долари на Google од страна на В. Британија за следење на британските корисници на iPhone мобилните телефони во периодот меѓу 2011 и 2012 година. Google пред јавноста призна дека го следи движењето дури и на своите Android-корисници независно дали опцијата „Location Share“ е исклучена или не е. Исто така, поради серијата скандали со кои се соочи Apple, но и поради судирот со новата построга европска регулатива (GDPR) на ЕУ, одлучи да повлече значителен број на апликации од App Store кои собираат кориснички податоци без претходно известување и побарана дозвола од корисниците. Facebook продолжи да ја демне приватноста на нејзините корисници преку мобилната апликација Facebook Messenger. А, исто така, и преку WhatsApp. Но, тука не заостанува ниту, пак, Viber, кој практично наголемо обезбедува, освен текстуални, и гласовни и видео разговори од корисниците. За жал, пред да воспостави построги безбедносни стандарди ЕУ со новата регулатива, со истото се соочуваат и корисниците на Snapchat. Во јавноста излегоа информации и дека мобилните телефони на Samsung (претежно од серијата Galaxy, но и од други серии) преку апликацијата Samsung Messages споделуваат фотографии без знаење на корисниците. Microsoft продолжи да ја демне приватноста на корисниците и преку Nokia и Microsoft уредите и Windows Phone и Windows 10 Mobile мобилните оперативни системи. Токму поради сето ова, некои корисници ги избегнуваа најпродаваните мобилни брендови и почнуваа да мигрираат на Huawei, Xiaomi, Lenovo, Doogee, Blackview, Vivax, Phonemax, Meizu, Homtom и др., кои ги нарачуваа од азискиот пазар (бидејќи тие се помалку подложни на прислушување и следење). Во однос, пак, на апликациите тие почнаа да ги претпочитаат Signal, Telegram, Line, Dust, KakaoTalk, Threema,

Wickr, Cyphr, CoverMe, Silence, Pryvate Now, SureSpot и др. Овие апликации обезбедуваат end-to-end енкрипциска комуникација. Во контекст на ова, Пентагон покажа огромен интерес за технологиите со кои располага Google (посебно за вештачката интелигенција), така што и двете страни склучија договор за соработка. Меѓутоа, договорените страни се соочија со изразено огромно незадоволство од широката јавност и професионалниот кадар и корисниците на Google. Причината за тоа е стравот од можноста од злоупотреба на производите и услугите од областа на вештачката интелигенција на компанијата од страна на Пентагон за воени цели, па дури и за изработка на оружје. Од страна на професионалниот кадар беше иницирана петиција за поднесување колективен отказ доколку Google продолжи да соработува на ова поле со Пентагон. Google на крајот се огласи со изјавата дека нема да ја продолжи оваа соработка по завршувањето на договорот во 2019 година. Паралелно со ова, и Агенцијата за национална безбедност покажа огромни аспирации да се инволвира во сферата на телекомуникациите. Ова го потврдуваат и тајните документи кои беа објавени во јавност, во кои биле содржани разработени планови и стратегии како да се собираат апсолутно секаков тип на лични податоци од граѓаните од сите можни извори. Како поткрепа на овој факт е и фактот дека продолжената рака на Агенцијата, AT&T, која е специјализирана мултинационална телекомуникациска компанија, споделува ама апсолутно секакви лични податоци од нејзините корисници со Агенцијата. NSA смета дека AT&T е еден од нејзините најдоверливи партнери и ја пофали „екстремната подготвеност за помош“ на компанијата.⁸ Тоа е соработка која датира со децении наназад.⁹ Атланта, Чикаго, Далас, Лос Анџелес, Њујорк, Сан Франциско, Сиетл и Вашингтон.¹⁰ Во секој од овие градови, The Intercept имаше идентификувано објект на AT&T кој содржи мрежна опрема која пренесува огромно количество на интернет сообраќај низ САД и светот.¹¹ Сето ова укажува на тоа дека Агенцијата преку овие центри спроведува апсолутна контрола и надзор како во домашни, така и во меѓународни рамки. А тоа значи нејзино дејствување без ограничувања.

4. Ерозија на правото на приватност на корисниците на клауд сервис

Технологиите кои се базираат на виртуелен облак се новата генерација на мемориски уреди во виртуелниот простор. Меѓу најпознатите и најкористените можат да се издвојат: OneDrive, Google Drive, Dropbox, Box, Mega, iCloud, NextCloud, SpiderOak, IDrive, pCloud, SugarSync, CertainSafe и др. Некои од нив се бесплатни, а за некои е потребен одреден паричен надоместок за користење на нивните услуги и дополнителни привилегии. Предноста на овие технологии е тоа што гарантираат приватност и безбедност, можност за складирање и споделување на секаков тип на содржини, на располагање нудат ограничен или неограничен капацитет на меморија, нудат можност за пристап до нив од било каде и во

⁸“The NSA’s Hidden Spy Hubs in Eight U.S. Cities.” *The Intercept*. Ryan Gallagher, Henrik Moltke. 25th June 2018. Web. 05th August 2018. <<https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/>>.

⁹*Ibid.*

¹⁰*Ibid.*

¹¹*Ibid.*

било кое време, некои од нив се бесплатни за користење, а за некои е потребен паричен надоместок; а единствен услов е уредите од кој се пристапува до нив да се приклучени на Интернет. За жал, постојат и примери во практиката каде што некои од овие облак-сервиси се покажале како недоволно безбедни за корисниците. Најеклатантен пример од практиката е случајот со славната звезда Парис Хилтон, која беше жртва на хакерски напад од извесна хакерка Пејтсар Бкхчадијан (Paytsar Bkhchadzhyan) која противправно и одзела 130.000 долари од нејзините кредитни картички и лични фотографии од нејзината корисничка сметка на облак-сервисот iCloud. Овој случај потврдува дека дури и овие виртуелни сервиси го немаат и/или не можат да го одржат потребното ниво на безбедност и приватност.

Заклучок

Безбедноста и правото на приватност на корисниците станаа неизвесни, а нивната доверба во техничко-технолошките гиганти и нивните производи и услуги почна нагло да се губи. Microsoft почна опсесивно-компулсивно да собира лични податоци од своите корисници. Но, ова стана редовна пракса и кај останатите компании од ИТ-секторот. Освен за свои потреби, тие почнаа личните податоци да ги споделуваат и со некои национални служби на современите земји. Најочигледни примери за тоа се соработките меѓу Google и Пентагон, и меѓу Агенцијата за национална безбедност и АТ&Т. Ваквите (конспиративни) потези на компаниите им се удрија од глава, така што резултираа со пад на вредноста на акциите на берзите, намалување на приходите и зголемување на расходите, губење на значителен дел од постоечките корисници и неможност за привлекување на нови, нарушен кредибилитет и влошен квалитет во комбинација со намалена побарувачка на производи и услуги, зголемен број на нови конкурентни ИТ-компаниии и производи и услуги на глобалниот пазар.

Литература

1. "Facebook bug set 14 million users' sharing settings to public." *CNN tech*. Heather Kelly. 7th June 2018. Web. 4th August 2018. <<https://money.cnn.com/2018/06/07/technology/facebook-public-post-error/index.html>>.
2. "Facebook bug made up to 14 million users' posts public for days." *Wired*. Louise Matsakis. 7th June 2018. Web. 4th August 2018. <<https://www.wired.com/story/facebook-bug-14-million-users-posts-public/>>.
3. "The NSA's Hidden Spy Hubs in Eight U.S. Cities." *The Intercept*. Ryan Gallagher, Henrik Moltke. 25th June 2018. Web. 05th August 2018. <<https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/>>.
4. "Windows 10 Sends Your Data 5500 Times Every Day Even After Tweaking Privacy Settings." *The Hacker News*. Swati Khnadelwal. 10th February 2016. Web. 20th July 2018. <<https://thehackernews.com/2016/02/microsoft-windows10-privacy.html>>.

ЕТИЧКИ АСПЕКТИ НА КОМПЈУТЕРСКИОТ КРИМИНАЛ

UDC: 343.9:004

Прегледен труд

Јордан Ќирковиќ*Европски Универзитет Република Македонија – Скопје*

Апстракт

Етиката е науката на животот, на правилата кои го одредуваат доброто и лошото во сите сфери на животот, не подучува на нештата кои би требале да ни се мото “не го прави она што не сакаш да ти го прават.” Но многу пати се сретнуваме со неетичко однесување и каде се границите и сферите каде етиката допира.

Клучни зборови - етика, живот, добро, лошо, подучува.

ETHICAL ASPECTS OF COMPUTER CRIME

Abstract

Ethics is the science of life, the rules that determine good and bad in all spheres of life, it does not teach things that should be our motive, does not do what you do not want to do to you,, But many patches we encounter unethical behavior and where are the boundaries and spheres where ethics touches.

Keywords - ethics, life, good, bad, teaching.

Вовед

Етички дилеми и недоумици

Етиката како наука ги проучува моралните вредности, принципи и верувања за нештата дали се добри, исправни и позитивни, но и нормите до кои луѓето треба да се придржуваат за да се остварат нивните идеи и намери во морална сфера. Таа има за цел да ги оспособи луѓето во секојдневниот живот да постапуваат исправно и да носат праведни одлуки. Вработените во јавниот сектор често се сретнуваат со етички дилеми кога ситуацијата од нив бара да се определуваат за алтернативни решенија или одлуки кои се во полза за едни, но не за сите групи. „Интернетот е основна глобална комуникациска компјутерска мрежа. Неговиот развој довел до големи промени во начинот на живеење и работење во современото општество. Овозможил едноставна и брза комуникација и пренос на многу информации на големи

далечини,¹ „Проблемот кој постои на Интернет, а многу е погоден за вршење на недозволените дејствија е проблемот со идентитетот.² Во такви случаи донесувањето на одлуки воопшто не е лесно, но моралниот субјект кој ја познава етиката и, секако, законските решенија ќе донесе исправна одлука.

За значењето на етиката не се зборува само во филозофските кругови, туку и во стопанските и во јавните организации. Низ тие расправи се развиле повеќе модели за етички решенија и тоа:

- утилитарен модел;
- правен модел;
- модел на правичност.

Од аспект на применливост се поставува прашање кој од овие модели е најдобар и најприменуван, кој е најправичен, а секако дали е можна нивна комплементарност и напоредна употреба. Всушност, колку луѓето можат да бидат темелни и совесни да ги извршуваат задачите чесно, совесно со достоинство и знаење, одговорно и во кодекс со сите морални норми.

Социјалната етика ги акцептира стандардите кои укажуваат како индивидуите треба да се однесуваат меѓусебно, но и кон општеството и кои се најголемите човечки вредности во општеството. Социјалните стандарди произлегуваат од актуелните општествени закони, обичаите, практиката, но и од непишаните вредности кои се практикуваат меѓу луѓето во нивната комуникација. Во минатото тие непишани правила се почитувале и вреднувале. Ретки се општествата каде сите начини на комуникација и целото човечко поведение е целосно уредено, па затоа се јавува вакуум од недоречености, па се јавуваат и поведенија кои се спротивни на моралот, на етичките стандарди и норми. Во тие недоречености лежи всушност и замката која често е злоупотребена, па се јавува митото, корупцијата и воопшто девијантните поведенија.

Етичките дилеми често се на разни полиња, но сепак најважни и најризични се во полето на корупцијата, кражбите, шпионажата, конфликтот на интереси, злоупотреба на медиумите и измамите.

Во политиката и во правната теорија под корупција се подразбира злоупотреба на јавните овластувања и довербата со цел за стекнување на лична корист, непотизам, како и митото како придружна појава.

По препораките на OECD се укажува на почитување на одредени стандарди кои се неопходни за сите јавни службеници и вработени во јавни и владини институции. Еден од најважните стандарди е спречување на секаков вид корупција и пред сè подигнување на свеста на луѓето и дефинирање на моралот и моралните стандарди. Не случајно во критериумите за членство во евроатлантските организации на прво место се спомнува борбата со митото, корупцијата, транспарентноста, личната слобода и правата, слободата на медиумите и општите вредности како демократијата. УНЕСКО се залага за изградување на универзална етика која ќе почива на најдлабоките етички и човечки вредности од сите народи и држави.

¹ Sinteza 10-15308 2014-94

² Sinteza 10-15308 2014-94 -100

Етичките кодекси влијаат на работната професионалност, на меѓусебната комуникација на сопственото изградување и надградување, како и на рејтингот на професијата. Од тој аспект лекарската фела најпрво има изградено кодекс и ја прифатила "Хипократовата заклетва" која без сомнение придонела Светското здружение на лекари во Женева во 1948г. да ја донесе и Женевската заклетва. Денес сите професии кои на некој начин сакаат да дадат значење на професионалност, совесност и бренд градат кодекс на својата професија.

Етичкиот кодекс има и свои принципи и тоа:

- принцип на должност;
- принцип на професионалност;
- принцип на совесност, едноставност, ефикасност, уредност и навременост;
- принцип на коректност;
- принцип на доверба и соработка;
- други принципи - непристрасност, самостојност во одлучување.

Влијание на службената етика и службената комуникација

Комуникацијата се остварува врз основа на информации кои можат да се споделат намерно и ненамерно. Знаците се делат на природни и вештачки. Природните знаци се јавуваат како израз на емоционална состојба, а вештачките се збир на гласови, линии се што може да се означи одредена појава која човекот ја конструира.

Сигналите се знаци кои предизвикуваат нечие внимание, додека симболите ги означуваат стварите и појавите. Човечката комуникација може да се подели на повеќе начини и според повеќе критериуми првично на симболичка и сигнална. Комуникацијата може да биде:

- вербална - симболична;
- невербална - сигнална;
- гласовна - негласовна;
- посредна - непосредна;
- еднонасочна - двонасочна;
- преговарање како тип на комуникација.

Секоја човечка комуникација треба да биде одраз на културата на идентитетот на индивидуата, но и почит кон соговорникот и неговата личност.

Етички норми

Хосмер прави разлика меѓу етички правила и етички кодекс. Етичките кодекси се формализирани стандарди или правила кои се темелат врз разбирањето на доброто и лошото, а кои менаџерите и бизнисмените можат да ги употребат во своите постапки кон себе и кон своите соработници или целни групи. Во тие стандарди се содржани гледиштата за етичките вредности како што се правда, слобода, еднаквост, правдина и лојалност. Решенијата во етичкиот кодекс во деловноста произлегуваат од:

- социјалните;
- професионалните;
- индивидуалните вредности.

Со етичкиот кодекс се воспоставуваат високоморални норми и се дефинираат вредностите на кои тие се базираат. Етичките правила ги опфаќаат начините на однесување, на одредени очекувања во однесување или нивно барање на почитување.

Некои од тие правила се, на пример, почитување на законите и начинот на однесување во земјата во која се престојува без оглед на колку време се престојува во неа, значи да се биде достоин посетител.

Неетичко однесување во електронското работење

Во електронското работење, односно со развојот на ИТ, се зголемува и неетичкото однесување, а тоа пред сè се однесува на интелектуалното присвојување, на кражбите, измамите и компјутерскиот тероризам.

Етиката има свој пристап и во компјутерското работење. Етичките кодекси и правила се создадени од Институтот за компјутерска етика во 1992г. и за прв пат се објавени од Рамон Ц. Баркин. Не почитувањето на овој кодекс подлежи на законски казни. Правилата од кодексот биле често мета на дискусии и дебати и од хакерските заедници, но и од академските кругови. Д-р Бен Ферветер од Центарот за сметање и социјална одговорност (Centre for Computing and Social Responsibility) смета дека се многу ограничени. Прекршувањето на принципите од етичкиот кодекс е казнив, а самите прекршувања се случуваат бидејќи компјутерите ги користат луѓе кои се различно едуцирани или неедуцирани, за што и постојат многу дебати во однос на етичното однесување на лицата кои работат со компјутер или пак лицата кои се професионални програмери. Сепак, категоричен е ставот дека без класификација на професионалноста секој што влегува во сајбер општеството мора да ги почитува и правилата. Секое непочитување на истите всушност донесува штета на некој корисник.

Сега во моментот е многу актуелно испитувањето на Марк Цукерберг, точно поради произлегување на податоци и информации од неговата најкористена социјална мрежа – Facebook. Има секако и многу дилеми во однос на етиката која е можна во социјалните мрежи во кои има многу лични податоци и на многу едноставен начин тие се достапни за секого. Поради тоа е битна заштитата на

личните податоци и од друга страна внимателно користење на социјалните мрежи, бидејќи тие се одлична основа за повеќе форми на компјутерски криминал.

Во работата со компјутер некој си наоѓа само полесен и посоодветен начин за извршување на своите работи, но за жал некои лица гледаат начин да создадат вируси, програми со кои ќе им наштетат на другите, или пак кога љубопитноста ги тера луѓето да влегуваат во туѓа е-пошта и да ја читаат. Тоа наштетување, а пред сè и злоупотребување не само што мора да се спречува, туку и самите лица треба да знаат дека треба да ја прифатат одговорноста за своето недолично однесување.

Лицата кои работат со компјутери се свесни за сите можности за инциденти, кражби кои можат да настанат, но тие од своја страна треба да почитуваат одредени правила, односно сами да не го прават тоа што не го сакаат од другите. Треба да се соочат со правилата за:

- приватност на е-поштата;
- да се поседува софтверска лиценца;
- да се почитуваат авторските права над софтверот;
- пристап до хардверот - под кои околности и под кои услови;
- сопственоста на интелектуалната своина - што е и како се определува сопственоста над неа;
- пристап до датотеките - под кои околности користењето на одредени фајлови може да се смета за неморално;
- сопственост над податоците.

Постојат и одредени општи морални императиви според кои на некој начин треба индивидуалците да се однесуваат и да ги почитуваат. Тие императиви или некои правила да ги наречеме би требале да се сметаат за база за сите вработени и се:

- работете да придонесете за развојот на заедницата и човештвото во целина;
- не нанесувајте штета на другите;
- бидете чесни и одговорни;
- бидете правични и не вршете каква било дискриминација - верска, полова или расна;
- почитувајте го правото на сопственост, правото на патент, лиценца или авторско право;
- правилно однесувајте се со интелектуалната сопственост;
- почитувајте ги доверените податоци и информации, односно водете дискреција;
- почитувајте ја туѓата приватност.

Овие основни правила не значи дека треба само тие да се почитуваат, секако дека треба да се работи и однесува со достоинство, да се биде ефикасен и продуктивен, односно својата работа да се извршува максимално професионално со дигнитет и квалитет.

Заклучок

Професионалното работење на многу лица им значи доаѓање на работа, но тоа е всушност многу комплексно и означува пред сè професионално знаење и постојано надградување во областа, темелно проучување на процесот за работа, правење анализа за можни ризици или пак изнаоѓање на полесни начини, а подобри резултати. Почитување на договорите, роковите и термините е многу битен фактор во работата, како и прецизноста. Прифаќање на критика и туѓо мислење не е слабост туку доблест што може да доведе до подобар успех.

Од тој аспект етиката и кодексите на етичко и професионално работење се основа на секој систем на функционирање и од приватен и од професионален аспект. Етиката не е догма, но треба да се прифати како начин на размислување.

Литература

1. Access Data: Forensic Toolkit, <http://www.accessdata.com/>.
2. Analyst's Notebook, <http://www.i2.co.uk/>.
3. Будимик М., П.Пухарик - Компјутерски криминал – БИХ, Сараево 2009
3. Д-р Димитриевиќ Предраг "Компјутерски криминал" – Македонија, Скопје 2010
4. Д-р Лозановски Јован "Компјутерска етика" - Македонија, Скопје 2011
5. <http://www.rtv.rs/sp-lat/evropa/milionska-kraga-lozinki-u-nemackoj-454999html>-10.03.2015

СОВРЕМЕНИ ОБЛИЦИ НА КИБЕРНЕТСКИОТ КРИМИНАЛ

UDC: 343.9:004.49

*Прегледен труд***Марија Трајковска***Европски универзитет Република Македонија - Скопје*

Апстракт

21 век стана синоним на дигитализиран свет како последица на појавата, забрзаниот развој и несопирливото (позитивно и негативно) влијание на глобализацијата, техниката и посебно технологијата. Овие процеси кои, главно, се доминантни движечки сили во овој современ свет се главни причинители за формирање на една нова гранка наречена кибернетика. Паралелно со тоа, тие, освен што придонесоа за појава на голем број откритија и напредоци во оваа новооткриена сфера, придонесоа и за повеќекратен пораст на постојните традиционални закани, а со тоа и до појавување на нови нетрадиционални (кибернетски) закани кои почнаа да се манифестираат во повеќе различни облици и се со различен деструктивен потенцијал, притоа предизвикувајќи директни или индиректни последици на индивидуалната и колективната кибернетска безбедност. Во овој труд предмет на истражување и анализа ќе бидат кибернетскиот криминал и некои од позначајните појавни облици во кој тој се манифестира, таргетите спрема кои тој е насочен, профилот на современиот кибер-криминалец, последиците кои може да настапат и радиусот на нивниот досег, степенот на ранливост на машините како целини и хардверските и софтверските компоненти, вклучително и позначајни примери на извршени кибернетски криминални дела.

Клучни зборови: кибернетски криминал, кибер-криминалци, кибер-безбедност, кибер-закани, кибер-напади, виртуелен простор, интернет.

MODERN FORMS OF CYBERCRIME

Abstract

The 21st century became a synonym of the digitized world as a consequence of the emergence, the accelerated development and the unstoppable (positive and negative) influence of globalization, technology and, in particular, technology. These processes, which are mainly dominant driving forces in this modern world, are the main causes for the formation of a new branch called cybernetics. At the same time, they, in addition to contributing to the great number of discoveries and advancements in this newly discovered sphere, have contributed to the multiple rise of existing traditional threats, and hence the emergence of new non-traditional

(cybernetic) threats that have begun to manifest in many different forms and with destructive potential, while causing direct or indirect consequences for individual and collective cyber security. In this paper, the subject of research and analysis will be cybercrime and some of the more significant manifestations in which it manifests itself, the targets towards which it is directed, the profile of the contemporary cyber criminal, the consequences that may occur and the radius of their reach, the degree the vulnerability of machines as wholes and hardware and software components, including more significant examples of cybercrime crimes committed.

Keywords: cybercrime, cyber criminals, cyber security, cyber threats, cyber attacks, consequences, virtual space, the Internet.

Вовед

За кибернетскиот криминал може да се каже дека слободно го заземе својот примат во рамките на виртуелниот простор. Имено, тоа го потврдуваат повеќе факти. Штетите кои настануваат од овој облик на криминал може да изнесуваат од неколку милиони, па се до неколку милијарди парични единици секојдневно ширум светот. А облиците во кој тој може да се манифестира се многубројни. За кибер-криминалците не претставуваат пречки локацијата на таргетираните цели, ниту пак безбедносните закрпи на оперативните системи, антивирусните и другите специјализирани софтверски безбедносни решенија кои нудат кибер-безбедност и кибер-заштита. Исто така, тие имаат капацитети криминалните операции да ги изведуваат незабележително, без притоа да остават (значителни) дигитални докази, но од друга страна пак да остават значителни последици од различни размери. Сето тоа им го овозможуваат достапноста на знаењето, слободните пазари и крајно пристапните цени на конкретните хардверски, софтверски и друг вид на ИТ-алатки кои (во комбинација со нивниот интелект и талент) се предуслов за успешна реализација на ваквите кибер-криминални операции. Токму поради тоа, шансите да бидат разоткриени и изведени пред лицето на правдата се сведени на најниско можно ниво. Ова го надополнува и нивната способност за (брзо и аналитичко) размислување неколку чекори напред пред да се одлучат конечно да преземат било каква добро пресметана акција.

1. Кибернетски криминал

Кибернетскиот криминал (познат и како кибер-криминал, сајбер криминал, електронски криминал, компјутерски криминал, информатички криминал) е релативно нов облик на криминал, кој има сериозен капацитет да предизвикува последици како во виртуелни рамки, така и во реалноста, притоа предизвикувајќи катастрофални (трајни или привремени) последици за индивидуалната и колективната кибернетска безбедност, изразени во милиони, а ако не и во милијарди парични единици секојдневно низ светот. Типично за овој облик на криминал е тоа што, главно, компјутерот се става во функција како

основна алатка за извршување на кибер-криминални дејствија. Но, опсервирајќи од друг агол, пак, компјутерот истовремено претставува и примарна таргетна цел или, пак, параван со цел да се нанесат штети на крајните корисници или изведуваат други криминални дејствија од (не)кибернетски карактер на сметка на корисниците. Основниот мотив кој ги поттикнува на кибер-криминалците да изведуваат вакви кибер-криминални акции е едноставно потребата за стекнување на противправна материјална корист. За нив не претставуваат пречки нивната (физичка) оддалеченост со таргетите, годишните времиња и временските услови, временските зони, деловите од деноноќијата итн. Исто така, тие зад компјутерските екрани, т.е. зад битовите и бајтовите вешто ги кријат нивните вистински идентитети со цел што е можно повеќе да се анонимизира сè што може (ин)директно да упатува на разоткривање на нивниот пол, раса, боја на кожа, религиските и политичките убедувања, етничката и националната припадност, возраст, нивниот социјален живот, членовите на нивните семејства, нивната локација во моментот на извршување на кибер-нападите итн. Но, покрај тоа, за нив се исто така ирелевантни ваквите определби, посебно кога здружено оперираат во интернет-просторот. Тоа е така затоа што тие знаат да препознаат дека со заеднички сили поверојатно е успешно да ги реализираат кибер-нападите. Односно, поинаку кажано, доколку кибер-криминалците насетат дека на долг рок може да имаат повеќе придобивки отколку загуби и опасности, тие не ризикуваат да ги саботираат таквите предности кои им се нудат со нивното здружено дејствување. Еден од основните мотиви е поради можноста да се помагаат и заштитуваат меѓусебно и побрзо и симултано да ги извршуваат кибер-нападите, а притоа зголемувајќи ги шансите да останат што е можно помалку дигитални траги на местата на настаните. Што се однесува, пак, до облиците, може слободно да се каже дека кибернетскиот криминал денес може да се манифестира во многу појавни облици, од кои поважните ќе бидат предмет на анализа и истражување во овој труд.

2. Појавни облици на кибернетскиот криминал во 21 век

Како што е претходно наведено, кибернетскиот криминал не се манифестира исклучиво во еден и единствен облик. Напротив, се манифестира во многу повеќе, потешки и посложени облици, и токму заради тоа тој е заслужен за појавата на една целосно нова криминална индустрија, која, за жал, стабилно egzистира во современите држави низ светот.

2.1. Хакирање

Во основа, хакерството претставува неовластен пристап до компјутерските и мрежните системи на жртвите со цел да се предизвика (не)контролиран хаос. Генерално, тоа се постигнува со предизвикување на штети и тоа преку изменување на вредностите во системите или вметнување на грешки, блокирање на системите за авторизација, изменување, прибирање, па дури и објавување во

јавност на запишаните и складираните податоци и информации итн. Секако, многу поширок е спектарот на кибер-закани кои извираат од овој појавен облик на кибернетски криминал, додека кибер-криминалците кои практикуваат хакерство се познати како *хакери*, *кракери* и др. За нив постојат многубројни дефиниции. Но, најчесто под хакер се подразбира љубопитен млад познавач на компјутерите и комуникациската технологија, кој неовластено „ора“ по туѓите компјутерски системи, главно без малициозни намери, во желба за стекнување нови знаења, потврда на своето емо или од љубопитност.¹ Тие најчесто се технолошки фанатици кои имаат вештини на експертско ниво во една конкретна софтверска програма или јазик.² Бидејќи во непрекинат континуитет еволуира концептот на хакерството, паралелно со него еволуираат и мотивите и начините на хакерско дејствување на хакерите. Па така, тие сè почесто се забележуваат и како деструктивци кои имаат за цел да нанесуваат штети, да тероризираат, да наметнуваат немир, несигурност, паника и страв; во дадени ситуации и временски околности. А, секако, силно побудени и од мотивите за стекнување на пари на брз и лесен начин, потоа за моќ, одмазда, шпионажа итн. Воедно, со исклучок на нивното индивидуално дејствување, хакерите денес сè почесто се забележуваат како изведуваат и кибер-акции во самоорганизирани тимови, па дури и со поддршка од некакви криминални организации или држави итн. Но, исто така, тоа што е доста поново за нив е тоа што кај истите се забележува дури и т.н. „хакерски клиентелизам“. Односно, поинаку кажано, нивните знаења и искуства почнаа да ги продаваат (во виртуелниот простор и во реалноста преку доверливи посредници) во вид на давање на услуги на „сериозни клиенти“ кои се подготвени да платат повисоки цени. Паралелно со тоа, се појавуваат и како „државни хакери“ кои се ангажираат за потребите на државите и државните служби за борба против кибернетскиот криминал, главно, за прилично високи надоместоци во вид на државни плати. Примери за тоа се САД, Германија, Франција, В. Британија итн.

За тоа колку се присутни хакерите на виртуелната сцена говорат и енормно големиот број на кибер-безбедносни инциденти. Од 2013, па се до 2018 година следуваа серија на кибер-инциденти и тоа со извршени кибер-кражби на милионски кориснички имиња и посебно на лозинки на кориснички профили на најпопуларните социјални мрежи (Фејсбук, Твитер, Цимејл, Јаху, Линкедин, Мајспејс, Снепчет итн.), притоа загрозувајќи ја кибер-безбедноста на милиони корисници низ светот. Се случија и популарните кибер-напади во 2017 г. со злонамерните кодови *Ransomware*, *WannaCry*, *Petya* и др., кои нанесоа непоправливи штети, главно, на индивидуалните интернет-корисници, но не ги поштедија ниту пак приватните компании и некои државни институции на земји од Европа и САД. Големи разбранувања се појавија и со серијата на обвиненија на земјите од западниот свет за сè помасовното инволвирање на руските хакери на виртуелната сцена. Имено, тие се обвинувани за инволвирање во електронскиот избирачки процес на гласање за избор на претседател на САД (во периодот кога се кандидираше Доналд Трамп). Но исто така, обвинувања пристигнуваа и од официјален Лондон за нивно инволвирање во севкупната медиумска, телекомуникациска и електронска мрежа. А не беа поштедени ни од обвинувањата упатувани до нив за нивно можно инволвирање дури и во избирачкиот процес за целосна

¹Христов, Ристо. *Детективска информатика*. (Скопје: Европски Универзитет – Р. Македонија, 2015) 486.

²“The 12 types of Cyber Crime.” *Digit.Web*. 28th June 2018. <<https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>>.

независност на Каталонија. Изминатиот период беше, исто така, запаметен и по серијата на хакерски кибер-напади поврзани со повреда на интелектуалната сопственост, така што загрозени беа повеќето од познатите американски телевизиски куќи кои снимаат серии на документарци, филмови и сл. Хакерите ги преземаа содржините од нивните медиумски сервери и притоа за истите бараа откуп со цел да не бидат предвреме публикувани, односно емитувани во јавност, а од друга страна да се стекнат со противправна финансиска корист. За жал, некои од ваквите телевизиски куќи плаќаа, но и некои одбиваа да платат откуп за нивните содржини и како резултат на тоа истите беа поставувани на пиратските торент-сервери за нивно бесплатно емитување и преземање.

Иако хакерите продолжуваат во непрекинат континуитет, со примена на секакви мерки, да останат анонимни, има и такви исклучоци кои настојуваат да стекнат одреден вид публицитет. Меѓу најпознатите во светската јавност се издвојуваат: Кевин Полсон, Кевин Митник, Алберт Гонзалес, Роберт Тапан Морис, Владимир Левин, Џонатан Џејмс, Адријан Ламо, Џорџ Хоџ, Дејвид Смит, Метју Беван, Гери Мекинон, Ричард Прис, Мајкл Калче, Џонатан Џејмс и др. Некои од наведените имаат издржано дури и казна затвор.

2.2. Дисеминација на злонамерни програми

Малициозна програма е код (потпрограма) кој тајно се уфрлува во друга програма со намера да ги уништи податоците, да се активираат деструктивни програми кои ќе ја компромитираат безбедноста и ја нарушат доверливоста, интегритетот или достапноста на податоците, апликациите или нападниот систем.³ Постои широк спектар на вакви деструктивни програми, од кои најпознати и најраспространети се: вирусите, тројанците, црвите, малверите, адверите, спајверите, спамовите, фишинзите, мобилните кодови, социјалниот инженеринг и така натаму. Во овој труд посебно внимание ќе биде посветено исклучиво на вирусите, тројанците и црвите.

2.2.1. Вирус

Вирусот е најраспространетиот и најзлонамерниот компјутерски штетник во светски рамки. Тој претставува мала програма од неколку килобајта, која има единствена цел да направи штета на заразениот компјутер.⁴ Се размножува на тој начин што се „вгнездува“ во друга програма и со нејзиното активирање брише или менува датотеки на дискот.⁵ Ако заразениот компјутер е дел од мрежа, вирусот може да побара

³Христов, Ристо. *Информациони технологии*. (Скопје: Европски Универзитет – Р. Македонија, 2009) 464.

⁴Христов, Ристо. *Информациони технологии*. (Скопје: Европски Универзитет – Р. Македонија, 2009) 464.

⁵*Ibid.* 465.

друг компјутер, а преку него трет и така да се прошири низ целокупната мрежа и насекаде да направи штета.⁶

2.2.2. Тројанец

Тројанецот е злонамерна програма, чија негова задача е да се инфилтрира како „тројански коњ“, во компјутерот на жртвата и противправно да прибира секаков тип на податоци и информации и истите ги испраќа до неговиот создател. Преку тројанецот, создателот е во можност да ги препознава, чита, пишува, изменува и брише на истите, без притоа жртвата да ги забележи таквите активности.

2.2.3. Црв

Компјутерскиот црв е самостојна малициозна компјутерска програма која се саморазмножува за да се шири на други компјутери.⁷ Тој, главно, се шири преку интернет-мрежата со цел да се одомаќини во компјутерот на жртвата. Неговата задача е бришење, изменување, размножување на запишаните податоци и информации на корисникот. Првиот црв е креиран од страна на Роберт Тапан Морис.

2.3. Кибер-кражба на криптовалути

Кибер-кражбата на криптовалути е најсовремена ширококорастечка криминална индустрија која е во незапирлив подем во виртуелниот свет. Всушност, главна причина за тоа се токму криптовалутите. Тие се електронски парични единици кои се еквивалент на денешните ковани и книжни парични единици на современите земји. Но со единствена разлика што нивната вредност е повеќепати поголема и прилично стабилна во однос на регуларните парични единици кои се во оптек во земјите. Во некои земји овие криптовалути (со задоцнување) се прифатени и легализирани (како на пример, во Јапонија). Додека, пак, во други не се (како на пример, во Р Македонија). Тие се третираат како платежно средство и како средство за тргување на виртуелниот пазар. Тоа што е индикативно е што вредноста на овие криптовалути константно вртоглаво расте, и како резултат на тоа тие почнуваат да ги условуваат состојбите не само на виртуелните, туку и на пазарите во реалниот свет. И покрај тоа што некои од нив одвреме-навреме доживуваат привремени падови на вредноста, тоа сепак не ги спречува да продолжуваат да се движат во нагорна линија. Најдоминантна криптовалута е т.н. „биткоин“, но секако на пазарот постојано се појавуваат нови, од кои позначајни да се споменат се: „биткоин кеш“, „етереум“, „стелар“, „рипл“,

⁶Ibid.465.

⁷“Computer worm.” *Wikipedia: The Free Encyclopedia*. Wikipedia contributors. 28th June 2018. Web. 29th June 2018. <https://en.wikipedia.org/wiki/Computer_worm>.

„лајткоин“, „монеро“, „нео“, „кардано“, „атари“, „деш“, „трон“, „зкеш“, „оилкоин“ итн. Секоја од овие криптовалути има свои предности, но и недостатоци.

Процесот на купување, на одржување стабилна вредност на криптовалути на пазарот и зголемување на крипто-богатството е познат како „рударење“ или „крипто-рударење“. Сопствениците на овие дигитални парични средства потребно е да инвестираат во моќни компјутерски системи и посебно моќни графички картички и, секако, истите да бидат издржливи и подготвени за деноноќна работа, за да го постигнат гореспоменатото. Токму поради сето ова, претставуваше доволен поттик за кибер-криминалците за да почнат да оперираат и во оваа дигитална сфера, па како резултат на тоа се појавија и голем број од нив како „крипто-милијардери“ извршувајќи кибер-кражби од крипто-богатствата на „легалните“ инвеститори на крипто-пазарот. Инаку најголема мета на кибер-криминалците е биткоинот. Но за да реализираат што поголема противправна финансиска добивка, тие, исто така, целат и на други криптовалути (со поголема, но и со помала вредност). Најголема закана за инвеститорите кои „легално“ вложуваат во крипто-пазарот е тоа што и кибер-криминалците учествуваат во легалната купопродажба и друг вид на трговија со криптовалути, така што практично се невидливи за јавноста, односно обичните инвеститори кои се обидуваат да се збогатат и тргуваат со овој вид на дигитални криптовалути, вклучително и за современите кибернетски безбедносни служби на земјите.

2.4. Кибер-кражба на идентитет

Во основа, кибер-кражбата на идентитет претставува противправно анонимно присвојување на лични податоци кои се однесуваат на идентитетите на жртвите, а со крајна цел директно да им се нанесат штети или, пак, во нивно име да се извршуваат (други) кибер-криминални дејствија спрема трети цели. Најчестите операции кои кибер-криминалците ги изведуваат се: празнење на кредитни картички на жртвите, подигнување на енормно големи кредити во кеш од банките, претставувајќи се со идентитетите на жртвите, фалсификување на лични карти, пасоши, возачки дозволи и други патни исправи на жртвите; извршување на кибер-кражби на криптовалути, перење на пари, дисеминација на злонамерни програми, кибер-трговија со идентитети, оружје, дрога, нарачки на убиства и други криминални услуги; претставување со идентитетите на жртвите во моментите на извршување на класични или кибер-криминални акти како превентива за после тоа да не можат да бидат откриени, а вината да биде пренесена на жртвите; осигурителни и даночни измами, профилирање на жртвите преку нивните профили на социјалните мрежи и преку нив извлекување на лични податоци и информации кои се однесуваат на нивните идентитети итн. Доказ за тоа колку е сериозна оваа кибер-закана говорат и следните факти изразени во бројки. Всушност, само во 2016 година биле украдени рекордни 421 милијарди податоци.⁸ Ако тоа не е доволно страшно, 35 податочни записи се изгубени или украдени секоја секунда и над 3

⁸“Identity theft and Cybercrime statistics.” *Global Cyber Alliance*. Rachael Trotman 06th March 2017. Web. 29th June 2018. <<https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html>>.

милиони податоци се изгубени или украдени секој ден.⁹ Оваа проблематика во нашето македонско законодавство е регулирана согласно членовите од Кривичниот законик на РМ: 149, 235, 247, 251, 251-а, 251-б, 274-б, 249, 273 и др.

2.5. Кибер-војна

Кибер-војната е (виртуелна) војна во која кибер-војските машините и програмите ги третираат како борбени оружја за изведување на кибер-офанзивни операции против непријателските кибер-сили во кибер-просторот. Овој современ облик на војување е познат и под други термини, како на пример, кибернетска војна, сајбер-војна, електронска војна, информатичка војна, компјутерска војна и сл. Претставува дел од кибернетскиот криминал, бидејќи во својата основа има кримоногени елементи. Целта на кибер-војските е да предизвикаат што е можно помасовни штети, притоа максимално искористувајќи ги сите расположливи начини и средства за деструктивно дејствување. Тие вклучуваат широк спектар на операции, како на пример, шпионажа, саботажа, диверзија, инфилтрација, кражби итн. Додека нивните мотиви можат, исто така, да бидат од најразлична природа, како на пример, од воена, политичка, религиска, хактивистичка и сл. Но може да бидат и едноставно поради омраза, верска, етничка или национална нетрпеливост; долгогодишно непријателство кое се негува во секоја сфера, потреба за докажување висок дострел во кибернетиката на спротивната страна и друго. Што се однесува до нивните цели тие целат кон предизвикување општа хаварија, не само во виртуелниот, туку и во реалниот свет. Па според тоа, тие може да се забележат како изведуваат операции, како на пример, прекин во снабдувањето и испораката на електрична енергија, нафта, гас, вода до крајните корисници, потоа трајно или времено онеспособување на целокупната национална интернет-мрежа на таргетираната земја, предизвикување катастрофи во работата на хидроцентралите, ветерниците, нафтените и гасните платформи, сончевите колектори за производство и дистрибуција на електрична енергија, атомските центри; предизвикување хаос во копнениот, поморскиот и воздушниот сообраќај; предизвикување колапс на банкарските и берзанските (безбедносни) системи, колапс на одбранбените и безбедносните информатички системи итн. Токму поради сето тоа, кибер-војната е една од најзагрозувачките кибер-закани на сегашноста.

2.6. Кибер-тероризам

Кибер-тероризмот е асиметрична кибер-закана. Во основа, како и кај кибер-војувањето, така и кај кибер-тероризмот се забележуваат очигледните заеднички препознатливи обележја и за двата кибер-криминални облици. Слободно може да се каже дека тие се рамо до рамо кога станува збор за кибер-

⁹*Ibid.*

злосторствата во виртуелниот простор, и дека во некои поедини (изолирани) случаи надлежните институции за борба против нив имаат значителни тешкотии во обидите за квалификација, т.е. дистинкција во однос на тоа дали станува збор за изведени кибер-воени или кибер-терористички злосторства. Паралелно со тоа, исто како кибер-војната, така и кибер-тероризмот има криминогени елементи. Па токму поради тоа, тој претставува составен дел од кибернетскиот криминал. Генерално, мотивите на кибер-терористите за кибер-терористичко дејствување можат да бидат поткрепени од истите причини кои се и за кибер-војските. Целите кои ги таргетираат можат да бидат избрани по случаен или селективен избор, правејќи анализи и истражувања за утврдување која солуција е идеална за предизвикување огромни штети. Најчесто ги таргетираат индивидуалните интернет-корисници и владините институции. Но понекогаш ги земаат предвид и големите приватни компании кои се со стратегиско значење за современите земји. Асортиманот на кибер-терористичко дејствување е мошне широк. Така на пример, тие изведуваат хакерски кибер-напади во вид на DDoS-напади, дисеминација на злонамерни програми, операции со перење на пари, неовластени пристапи и предизвикување штети, кибер-кражби на криптовалути и средства од кредитни картички за финансирање на нивните операции и др. Нивната примарна цел е да предизвикаат хаварија во рамките на информатичко-комуникациската технологија. Но, за нив ќе биде и идеално доколку успеат да предизвикаат и било каков помал степен на штети на таргетираните цели. Но за да постигнат каков било терористички прогрес тие прво мора да ги детектираат и потоа таргетираат потенцијалните критични кибер-безбедносни точки.

Заклучок

Од досега изнесеното во трудот може да се констатираат следните работи. Имено, глобализациските и техничко-технолошките текови придонесоа за појавата на кибернетиката, а со тоа наметнаа и нови безбедносни предизвици. На овој начин, овие текови од корен ги изменија одбранбените и безбедносните стратегии на современите земји. Опасностите од кибернетскиот криминал отидоа до таму така што тој почна да се манифестира во повеќе појавни облици во виртуелниот простор, а каде што последиците почнаа да се пренесуваат и во реалноста. Од овие кибер-закани не се засегнати исклучиво институциите на земјите, туку и нивните населенија, т.е. индивидуалните интернет-корисници. За кибер-криминалците не постојат безбедносни, хардверски, софтверски или кој било друг облик на ограничувања и препреки во нивното кибер-криминогено дејствување. Додека последиците од изведените кибер-напади може да бидат трајни или привремени. Тие може да изнесуваат од неколку милиони, па се до неколку милијарди парични единици на земјите секојдневно или на месечно или годишно ниво. Мотивите на овој вид на кибер-криминалци можат да бидат од најразлична природа. Во поглед пак на целите, тие настојуваат да ги исцрпат сите можни расположливи ресурси (знаења и искуства, ИТ-алатки и др.) со крајна цел да обезбедат сигурна реализација на зацртаните кибер-криминални планови и стратегии за деструктивно дејствување.

Литература

1. Христов, Р. *Детективска информатика*. Скопје: Европски Универзитет – Р. Македонија, 2015. Print.
2. Христов, Р. *Информациони технологии*. Скопје: Европски Универзитет – Р. Македонија, 2009. Print.
3. “Computer worm.” *Wikipedia: The Free Encyclopedia*. Wikipedia contributors. 28th June 2018. Web. 29th June 2018. <https://en.wikipedia.org/wiki/Computer_worm>.
4. “Identity theft and Cybercrime statistics.” *Global Cyber Alliance*. Rachel Trotman. 06th March 2017. Web. 29th June 2018. <<https://www.globalcyberalliance.org/identity-theft-and-cybercrime-statistics.html>>.
5. “The 12 types of Cyber Crime.” *Digit*. Web. 28th June 2018. <<https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>>.

САЈБЕР ТЕРОРИЗМОТ КАКО ЗАКАНА ЗА БЕЗБЕДНОСТА НА ДРЖАВАТА

UDC: 343.9:004.491.056.2

*Стручен труд***Емилија Дамчевска***Министерство за внатрешни работи*

Апстракт

Сајбер тероризмот претставува една од главните глобални закани на современата безбедност. Системи за заштита од ваков вид на напади поседуваат меѓународните организации како НАТО и ЕУ и развиените држави како што се САД, Кина, Русија, Велика Британија и други. НАТО е единствената организација која на систематски и стручен начин се занимава со заштита од овој тип на тероризам и поседува развиен систем на сајбер одбрана.

Развојот на современата технологија ја зголемува одбраната од терористичките закани, но исто така ги зголемува и можностите на терористите за успешно остварување на нивните цели. Терористите денес многу лесно оперираат во кибернетскиот простор така што уништуваат определени податоци, но и манипулираат со значајни податоци.

Клучни зборови: *тероризам, сајбер тероризам, закана, безбедност*

CYBER TERRORISM AS A THREAT TO THE SECURITY OF THE STATE

Abstract

Cyber terrorism is one of the major global threats to modern security. International protection organizations such as NATO and the EU and developed countries such as the United States, China, Russia, the United Kingdom and others have systems of protection against this type of attacks. NATO is the only organization that deals with the protection of this type of terrorism in a systematic and expert way and owns a developed cyber defense system. The development of modern technology increases the defense of terrorist threats, but also increases the capabilities of the terrorists to successfully achieve their goals. Today, terrorists are very easy to operate in cyber space by destroying certain data, but also manipulating significant data.

Keywords: *terrorism, cyber-terrorism, threat, security*

Вовед

Огромните достигнувања и развојот на врвната технологија, софистицираните компјутерски системи го отворија новиот „сајбер простор“, кој постојано ги уништува старите традиционални форми на организација, однесување и верување. Сајбер информациите доведоа до сајбер револуција и до појава на информатичкото општество, во кое доминира трката за информации и за комуникациски технологии, паралелно со светската либерализација и слободна циркулација на луѓе, стоки и идеи.

Денес, триесетина години по воведувањето на терминот, концептот кибернетика, тој неизбежно стана примарна компонента на голем број значајни термини: **сајбер општество, сајбер политика, сајбер економија, сајбер војна, сајбер тероризам, сајбер криминал, во чија суштина најскапоцена круна претставува сајбер информацијата.**

Изградбата на современи и флексибилни компјутерски комуникациски системи и поставување ТСП/IP протоколот како универзален протокол за комуникација овозможува информациите низ светот да се движат со неверојатна брзина, пренесувајќи ги сите настани во една нова димензија на комуникација, наречена сајбер простор.

Новите форми на војување, а и тероризмот како специфична, современа „форма на војување“ ќе коегзистираат во исто време со „сајбер просторните“ напади. Најголемиот проблем можеби лежи и во фактот што интернет просторот од правен аспект се уште не е регулирана материја и според некои експерти е дефиниран како „Ничија земја“.

Постоечките норми во меѓународното право и правилата во националните законодавства не можат целосно да ги опфатат сите тие феномени кои се случуваат. Потребни се нови концепти и реформа во однос на инкриминирање на ваков тип на форми на сајбер криминалитет.

1. Сајбер тероризмот како глобална безбедносна закана

Сајбер тероризмот претставува една од главните глобални закани на современата безбедност. Системи за заштита од ваков вид на напади поседуваат меѓународните организации како НАТО и ЕУ и развиените држави како што се САД, Кина, Русија, Велика Британија и други.

НАТО е единствената организација која на систематски и стручен начин се занимава со заштита од овој тип на тероризам и поседува развиен систем на сајбер одбрана. Како би останале во тек со рапидно променливите облици на закана и како би одржале силен ниво на сајбер одбрана, НАТО усвои нова и напредна политика и акционен план кој го поддржаа сојузниците на Самитот во Велс во септември 2014 година.

НАТО силите за одговор на компјутерски инциденти (The NATO Computer Incident Response Capability (NCIRC)) ја штити сопствената мрежа нудејќи 24-часовна поддршка во сајбер одбраната на разни сајтови на НАТО. НАТО Кооперативниот центар за сајбер одбрана (The NATO Cooperative Cyber

Defence Centre of Excellence (CCD CoE)) во Талин во Естонија е најистакната од страна на НАТО акредитирана институција за истражување и обука, која се занимава со образование, консултации, размена на лекции и развој во врска со сајбер одбраната.

Целокупниот овој систем е токму фокусиран и лоциран во Естонија, бидејќи оваа Балтичка држава Естонија во 2007 е нападната од страна на хакери кои ја блокирале буквално целата инфраструктура во земјата на определен период. Тогашните политички односи помеѓу оваа земја и Русија беа затегнати, можеби и поради фактот дека Естонија во 2004 година стана земја членка на НАТО, а се шпекулира и дека сајбер нападот е како резултат на Естонско-Рускиот спор за отстранувањето на бронзена статуа на која бил прикажан советски војник од Втората светска војна во центарот на главниот град на Естонија - Талин.

Доколку пак ги мериме способностите за сајбер војување на определени држави, покрај САД, Кина, Русија, Израел и Франција, според процените на стручњациите постојат помеѓу 20 или 30 држави кои имаат респектабилни способности за сајбер војување (Тајван, Иран, Јужна Кореја, Индија, Пакистан...). Според тоа можеме да заклучиме и дека тие способности можат да бидат злоупотребени.

Сајбер тероризмот е значаен потсистем на сајбер војувањето, и е многу потежок за откривање и спротивставување, бидејќи е скоро неможно да се одреди политичката припадност или спонзорите на неговите извршители. Кога се зборува за поимот сајбер тероризам, според Федералното истражно биро – ФБИ овој феномен се дефинира како: „предумислени, политички мотивирани напади против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од страна на субнационалните групи или тајни агенти“.

Сајбер војувањето е насочено спрема информациите и информативните системи што даваат поддршка на цивилните и воените структури на противникот. Тоа навлегува во сфера која е многу посуптилна од физичките напади и уништувања, односно дејствува врз протокот на информациите во мрежите и манипулира со нив (прекинува, видоизменува, додава и слично). Неговите активности се насочени првенствено кон информациите кои се пресудни за функционирање на цивилните и воените системи како и контролата на авиосообраќајот, стоките берзи, меѓународните финансиски трансакции, логистичките потреби и цели.

Можностите за енормно нарушување на националните компјутерски системи и можноста да го загрозат нормалното пулсирање на општествениот живот, како и опасностите за масовно загрозување на животите на луѓето придонесуваат терминот „сајбер тероризам“ да биде опколен со чувство на страв и завиткан со велот на мистериозност.

Ако војувањето со информации, без сомнение, ќе претставува начин за војување во иднина, тогаш и иднината на тероризмот ќе биде суштински детерминирана со појавата на сајбер тероризмот. Привлечноста на војувањето со информации спонзорирани од државата е толку голема што многу нации не ќе можат да одолеат на овој „предизвик и искушение“. Меѓутоа, сајбер тероризмот во иднина ќе претставува нова „фатална привлечност“, за голем број терористи и терористички организации. Овој тероризам е најјасен пример за глобализацијата на светот, но и истовремено негово „вонбрачно палаво

дете“, кое опасно ќе ги загрозува комуникациите во воената сфера, службите за итна медицинска помош, системите на сообраќај од различен вид, телекомуникациите и другите добра. Исто така, неговите „хакерски игри“ може да предизвикаат хаос и анархија преку нападите на банкарите и други финансиски и компјутерски врски и тотално да го парализираат животот во големите урбани центри на најразвиените држави.

Во нивниот широк дијапазон на активности спаѓаат и користењето на приватните информации во функција на изнудување исти форми на сајбер криминал, преку влегување во мрежите, како и физичко и електронско уништување на дигиталниот информациски систем. Веќе не постои дигитален уред кој не може да стане жртва на компјутерските вандали и терористи. Сите уреди поврзани со компјутерите можат да станат цел на хакерите, кои преку глобалната компјутерска мрежа можат да внесат дигитален код што ќе го наруши нивното регуларно и нормално работење. На секој уред што се поврзува во мрежа можат да му испратат низа дигитални команди што ќе направат уредот да работи онака како што ќе посака креаторот на тие команди. Класичните системи за заштита се речиси беспомошни во поглед на методите што ги користат денешните хакери и сајбер терористите.

Главна опасност денес претставуваат хакерските кодови, кои користејќи ја секоја пригода се имплементираат во некоја затворена компјутерска мрежа, креирани се така што можат самите да се активираат и да биде ефектот уште пострашен, самите да го изнаоѓаат патот за своето размножување, ширејќи го „злостниот код“.

Исто така и принтерите кои стануваат се посоефицирани, надградени со побројни софтверски апликации за поддршка може да бидат искористени за хакерски сајбер терористички упади во мрежите.

Во правна смисла, сајбер тероризмот претставува намерна злоупотреба на дигиталниот информациски систем, мрежа или компонента што ја заокружува или комплетира терористичката борба и активност. Последица од злоупотребата на системот нема да биде директно насилство против луѓето (што не е исклучено, на пример, со паѓање на авиони, хаос во болниците и слично), но сепак ќе може да предизвика страв, зголемување на светскиот криминал со најбрзо темпо, најголема стратешка ранливост на сите витални општествени функции, огромни човечки страдања, но и жртви како „коллатерална штета“.

Во овој контекст, уште пострашен е и фактот што овие суптилни дејства може да иницираат и кибернетичка војна или да „наместат“ определени држави да отпочнат класична војна, како одговор на сајбер дејствата „преземени од друга страна“.

Според определени американски размислувања само е прашање на време кога САД може да го искушат „сајбер Перл Харбур“, кои би имале опустошувачки резултати, кражби на електронски фондови на податоци со кои би се поддржале терористичките информации, препраќање, пренасочување на пратките со оружје и слично. Но веројатно најопасна е евентуалната симулација на „сајбер Чернобил“ хаварија.

2. Методи за извршување на сајбер тероризам

Во општествата на третата технолошка револуција постојат две основни методи преку кои терористите можат да извршат терористички напади.

Првата метода е кога самата информациска технологија претставува цел на терористичките напади. Со изведување на определени саботажи (електронски и физички) врз информацискиот систем, ќе се обидат да го уништат или да извршат прекин во функционирањето на информацискиот систем и информациска инфраструктура, во зависност од самата конкретна цел.

Втората метода е кога информацискиот напад претставува средство - чекор за спроведување на поголема операција. Овој чин имплицира дека терористите ќе прават напори за манипулација и експлоатација на информацискиот систем, кражба на информации како алтернатива или принудување – „програмирање“ на системот да врши функција за која не е наменет.

Под поимот компјутерски вируси се мисли на програми кои несвесни поединци ги пишуваат за да нанесат што поголема штета на многу компјутери врзани во мрежа како на пример на глобалната интернет-мрежа. Нивни основни одлики се: се копираат самите себеси на секој компјутер со кој ќе дојдат во контакт. Не се забележливи, односно најчесто се невидливи за корисникот на компјутерот, посебно ако на компјутерот не е инсталиран специјализиран софтвер за нивна детекција. Автоматски извршуваат одредени команди како бришење на корисни податоци на компјутерот на жртвата, или пак ги испраќаат податоците на одредена друга локација на мрежата без знаење на сопственикот на компјутерот.

Покрај хакерите и групите што тие ги организираат за неовластено навлегување во заштитени системи, на денешно време постојат и специјализирани тајни владини служби кои преку навлегување во компјутерскиот систем на другите држави прибавуваат податоци од разузнавачка природа. Така под поимот компјутерска шпионажа може да се дефинира еден од најмодерните облици на разузнавање, но исто така постои и индустриска шпионажа која е само од комерцијална природа. Компјутерска саботажа имаме во случај кога некој ќе уништи, избрише, промени, прикрие или на друг начин ќе онеспособи податок, програма или ќе го оштети компјутерот кој е од значење за државен орган, институција, јавна служба.

Нападот со информатичката технологија е лесно изводлив, со примена на евтини средства кои лесно се прикриваат и виртуелно се недофатливи. Ако е познато дека терористите „лудуваат“ околу нивната медиумска промоција, ако е познато дека најпосакувана цел на терористите се медиумите, тогаш со сигурност можеме да констатираме дека можностите на терористите за непречен упад во осетливата информациска технологија енорно ги зголемува нивните можности за „информатичко војување“. Тоа е само уште едно совршено оружје во богатиот арсенал на оружје на терористите кои неуморно ги следат сите современи трендови и во оваа значајна сфера.

Мотивациите за извршување на вакви напади се секако добро познатите барања за политички промени, социјални промени или економски промени.

Ако денес постојат огромен број на објективни и субјективни пречки за отпочнување на сајбер војни од поголеми размери (пример меѓународната економска зависност, ескалацијата и одговорот од другата страна со воен конфликт, немање на технолошка подготвеност), тогаш за новите „терористи“ не постојат никакви пречки, нити „црвена линија“ за отпочнување на сајбер тероризмот на глобален план.

Невидливиот непријател вооружен единствено со лаптоп персонален компјутер, конектиран на глобалната компјутерска мрежа, „вооружен“ со огромно човечко знаење трансформирано во дигитален код, кој одлучува со огромна деструктивна енергија и огнена желба да ги оствари своите мрачни цели, вپловува во напад со тешко препознатлив правец, но со единствена цел: електронски атак врз државната информациска мрежа од огромно стратегиско значење за непречено функционирање на сите витални општествени функции.

Тоа е злокобното лице на сајбер терористот и на сајбер тероризмот, опасна закана за националната безбедност на определени држави, смртна закана и за глобалната безбедност во наредниот период. Тоа е опасност блиска до атомска бомба. Инвазијата на сајбер просторот и понатаму продолжува со огромна брзина, со брзината на развојот на моќната офанзивна компјутерска технологија. Светот повторно се наоѓа пред уште еден нов и мошне опасен сериозен безбедносен предизвик од најголемото зло - тероризмот.

3. Цели на напад на сајбер тероризмот

Во денешно време, најсовременото оружје е компјутерот. Секој добро обучен компјутерџија е добар војник. Секое дете кое добро го разбира концептот на компјутерите и начинот на работа на некои програми е потенцијална опасност за целиот свет. Во светот постојат многу примери на компјутерски напади, при што жртви на таквите напади се најразлични компании или владини институции. Се поставува прашањето која е целта на таквите напади? Што се постигнува со тие напади? Во многу случаи со таквите напади се крадат информации од воени институции со кои директно се загрозува безбедноста на одредена земја. Во други случаи се крадат кодови од некои програми кои се во развој, а во трети случаи, пак, нападите се извршуваат едноставно за забава (или пак тренинг). Ова ќе се разгледа преку примери за компјутерски напади во кои се нападнати сервери од една земја од страна на компјутерџији од друга земја.

Во 1997 година ИРА ја шокираше англиската јавност со упатување на закани дека покрај бомби, атентати и други облици на терористички напади ќе почне да користи и електронски напади на службените и владини компјутерски системи.

Искуствата со Ал-каеда и ИСИЛ исто така покажаа дека припадниците на овие терористички организации се служат со софистицирани техники на заштита на своите канали на комуникација преку Интернет, секојдневно поставување на нови веб локации на кои ги пропагираат своите

фундаменталистички идеи, а кај некои од уапсените терористи се пронајдени компјутери со шифрирани фајлови.

Нападот на Светскиот трговски центар во Њујорк знаеме сите добро како заврши. Меѓутоа интересно беше нешто друго. Непосредно со нападите, беше блокиран и официјалниот сајт на Светскиот трговски центар. Тешко е ова да се нарече случајност.

Непосредно по овој напад, во САД се стравуваше од повторен напад, но овој пат компјутерски. Според мислењето на американските стручњаци успешноста на ваквиот напад би ја парализирал целата држава. За нивна среќа, ваков напад не следеше (барем не успешен). Меѓутоа од превентивни мерки, Пентагон беше „откачен“ од Интернет. САД се спремаше за „електронски Перл Харбур“. Штетите од ваквиот напад би биле непроценливи. Имено, пред неколку години во САД, извесен Robert Morris, син на некој од директорите на Агенцијата за национална безбедност, во мрежата уфрлил програм кој во целост ги парализирал компјутерите во некои од најважните федерални и универзитетски институции (за тоа добил казна само од 10.000 долари и 3 години условен затвор).

Изразита „сајбер“ војна се водеше помеѓу Кина и САД во мај 2001 година (причина беше судирот на кинески авион со американски шпионски авион). Веднаш по судирот почнаа напади најпрвин од кинеска страна. Цел на таквите напади беа сервери ширум САД, а страдаше и страницата на Американскиот конгрес. Карактеристично е тоа што при овие напади не се направија некои поголеми штети, туку само се измени содржината на некои страници (најчесто се испишуваа кинески симболи). Меѓутоа и хакерите од САД на овие напади не останаа должни. Тие одговорија со напади на веб-страниците на покраинските власти во некои од покраините во Кина, како и на корејските компании Samsung и Daewoo Telecoma (интересно е тоа што во оваа „сајбер“ војна, на страната на Американците беа хакерите од Саудиска Арабија, Пакистан, Индија, Бразил, Аргентина и Малезија, а на страната на Кинезите хакерите од Јапонија, Кореја и Индонезија). Очигледно беше дека државите ги финансираа ваквите напади, бидејќи двајца „големи“ хакери беа задолжени за подготовка на серверите во САД од можни напади. На 1 јули 2001 година, во Мексико бил уапсен некој мексикански тинејџер кој бил обвинет дека извршил напад врз НАСА. Тој успеал да влезе во серверот, модифицирал некои фајлови и креирал некои нелегални акаунти. Интересно е тоа што во одбраната, мексиканскиот тинејџер се бранел со тоа дека немал никаква врска со компјутери, и дека лажно е обвинет. Дали со тоа државата сака да влее страв помеѓу хакерите за успешно нивно гонење? Дали државата се служи со лажни обвиненија? Зошто се тие лажни обвиненија? Докажувањето на овој тип на криминалитет е многу тежок и секако дека на правосудните органи им е недвосмислено потребна стручна помош од стручни лица кои добро ја разбираат и се упатени во оваа проблематика, особено што заканите во сајбер просторот се во постојана еволутивност.

Заклучок

Развојот на современата технологија ја зголемува одбраната од терористичките закани, но исто така ги зголемува и можностите на терористите за успешно остварување на нивните цели. Терористите

денес многу лесно оперираат во кибернетскиот простор така што уништуваат определени податоци, но и манипулираат со значајни податоци.

Денешните „компјутерски крадци“ со терористичките намени можат да влезат во најбезбедните банки на податоци со цел да извршат кражба на безбедносно осетливи информации и да ги уништат или блокираат. Овие можности ги зголемуваат шансите терористите да манипулираат на берзите во свој интерес, да предизвикаат определен финансиски застој или да го забрзаат процесот на инфлација.

Значајно е да се каже дека сајбер тероризмот во иднина ќе претставува многу опасна форма на политичко насилство. Ниту Македонија не е имуна на овој тип на сајбер напади на инфраструктурата кои би можеле да се случат. Сите надлежни институции во овој контекст како што се МВР, Министерството за информатичко општество, Центарот за управување со кризи и други надлежни органи треба да преземат мерки со цел зајакнување на безбедносниот систем од овој вид на сајбер напади. Со оглед на фактот дека овој тип на тероризам претставува сериозна глобална закана, Република Македонија треба да ја зајакне меѓународната соработка во овој контекст и да преземе соодветни мерки и стратегии за заштита од овој вид на сајбер тероризам. Се наоѓаме во период и во време кога националната безбедност е секојдневно присутна тема во медиумите, па со тоа и во јавноста ширум Европа и светот. Во тој контекст, сајбер безбедноста и градењето на добра и ефикасна стратегија за имплементација на истата претставува можеби и клучен елемент на кои се базира успешноста на одбранбениот систем на една земја. Целокупната, може да се каже, инвазија на сајбер просторот се шири со огромна брзина и во иднина можеме да очекуваме сè повеќе сајбер напади. Тероризмот во иднина или иднината на тероризмот треба да претставува значаен патоказ за современите влади во која насока ќе треба да се организира борбата против тероризмот, а посебно против сајбер тероризмот.

Литература

Stern, Jessica. *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press, 1999. p.204

Hower, Sara; Uradnik, Kathleen (2011). *Cyberterrorism* (1st ed.). Santa Barbara, CA:

Greenwood. pp. 140–149. Retrieved 4 December 2016.

Idem, p. 127-128.

Според Федералното биро за истрага – ФБИ

(http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci771061,00.html)

Митко Котовчевски „Борба против тероризмот“, Македонска цивилизација Скопје. str. 182

Badey, Thomas (ed.). *Violence and Terrorism* 05/06. Dubuque, IA: McGraw-Hill/Dushkin, 2005. p.152

Tuchman, Barbara. *The Proud Tower*. New York: Macmillan, 1967. p.52

White, Jonathan. *Terrorism: An Introduction*. New York: Thompson-Wadsworth, 2003. p.89

www.ict.org.il

Списание, декември 2001: Одбрана бр. 68

<http://www.terrorism.org/>

Богоев Славчо, Колективните системи на безбедност: процес и критериуми на интеграција на Република Македонија во НАТО, Правен факултет, 2010 стр. 63

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА – ЗАКАНА ИЛИ ГАРАНТ НА БЕЗБЕДНОСТА

UDC: 004.89:355.45

*Стручен труд***Доц. д-р Марјан Габеров***Европски Универзитет Република Македонија – Скопје*

Апстракт

Поимот на вештачка интелигенција иако потекнува од порано, сепак во последните неколку години станува многу популарен како резултат на зголемениот обем на податоци, користењето на напредните алгоритми и како резултат на постојаниот напредок и усовршување на компјутерските системи. Особено внимание на полето на вештачката интелигенција предизвикуваат евентуалните ризици кои би можеле да настанат за општеството, посебно за безбедноста како резултат на примената на овие нови технологии.

Постојаниот напредок на технологијата и инсистирањето на концептот на вештачка интелигенција е доволен показател за потребата на итно преземање на соодветни мерки за воспоставување на еден систем на правилно управување со самите системи на вештачката интелигенција.

Основна цел на трудот е да ја анализира вештачката интелигенција како потенцијална закана или гаранција за безбедноста воопшто, со посебен акцент на различните домени на безбедноста. Како предмет на трудот се поставува анализата на различните домени на безбедноста во контекст на примената на вештачката интелигенција. Преку трудот се очекува да се утврдат заклучоци кои научно би ја оправдале или негирале примената на вештачката интелигенција во делот на безбедноста во рамките на едно општество.

Клучни зборови: вештачка интелигенција, технологија, роботи, безбедност, интернет.

ARTIFICIAL INTELLIGENCE - THREAT OR GUARANTEE OF SECURITY

Abstract

The notion of artificial intelligence, though originated from earlier, has become very popular in the last few years as a result of the increased volume of data, the use of advanced algorithms, and the continuous progress and improvement of computer systems. Particular attention in the field of artificial intelligence causes the possible risks that could arise for society, especially for safety as a result of the application of these new technologies.

The continued advancement of technology and the insistence on the concept of artificial intelligence is a sufficient indication of the need to take immediate steps to establish a system for the proper management of the artificial intelligence systems themselves.

The main goal of the paper is to analyze artificial intelligence as a potential threat or guarantee for security in general, with particular emphasis on different domains of security. The subject of the paper is the analysis of the various domains of security in the context of the application of artificial intelligence. Through paper, it is expected to establish conclusions that would scientifically justify or deny the application of artificial intelligence in the area of security within a society.

Key words: *artificial intelligence, technology, robots, security, internet.*

Вовед

Концептот на вештачка интелигенција, иако потекнува од порано, сепак во изминатите неколку години постојано се актуализира преку бројни научни истражувања и дебати. Иако постојат различни пристапи при изучувањето и објаснувањето на вештачката интелигенција, сепак во една општо прифатена дефиниција, вештачката интелигенција, може да се дефинира како определена способност на дигиталните компјутери или способност на компјутерски управуваните работи да извршуваат некои задачи кои се поврзуваат со извршување од страна на интелигентни битија.¹ Со други зборови, под општиот термин на вештачка интелигенција се подразбираат интелигентните ентитети.²

Се поставува прашањето дали опстојувањето на вештачка интелигенција како концепт е оправдано, односно која е нејзината цел. Секако во севкупното разгледување на овој концепт, неспорно е дека најважната цел се состои во изградбата на интелектуални машини, односно работи кои би можеле да ја користат човечката интелигенција на исто ниво на човекот, но дури и подобро од него. Освен оваа примарна цел на вештачката интелигенција, истата поседува и секундарна цел која се состои во огромните напори на бројни истражувачи да ја сфатат природата на вештачката интелигенција, а со самото тоа да ја потврдат и нејзината оправданост, односно неоправданост.

Во една историска конотација вештачката интелигенција првпат се споменува во 50-тите години на минатиот век, конкретно во текот на 1956 година. Иако овој поим се споменува многу поодамна, истиот добива на постојана актуализација во последните неколку години. Зголемувањето и инсистирањето на концептот на вештачка интелигенција во последните неколку години се должи пред сè на неколку фактори, и тоа: постојаното зголемување на податоците кои циркулираат низ бројните системи за комуникација, создавањето на се посоефицирани и поуспешни програми и алгоритми, како и поради постојаното усовршување на компјутерите и другите машини. Во едно севкупно објаснување на вештачката интелигенција, треба да се подразбере дека овој концепт претпоставува искористување на

¹<http://www.britannica.com/EBchecked/topic/37146/artificial-intelligence-AI> (Aug.19.2018).

²Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach. Harlow: Prentice Hall. 2009.

компјутерските системи за извршување на определени задачи за кое е потребно користење на човечка интелигенција, како што се на пример, можноста за визуализација на определени состојби, препознавање, односно детектирање на говорна комуникација, донесување на определени одлуки слично како и кај донесувањето на одлуки од страна на самиот човек, како и способност за воспоставување на систем кој што би бил користен за обезбедување на превод на определени јазици. Еден од примерите за максимално искористување на концептот на вештачката интелигенција е и платформата која се користи доста многу за преведување од еден на друг јазик, односно платформата <https://translate.google.com/>.³

За значењето на вештачката интелигенција како концепт за целото општество, говори и еден од менаџерите во големата компанија "Google", односно Алек Ицев. Според него постојаното развивање и унапредување на вештачката интелигенција се очекува да придонесе за значајно менување на целокупното живеење во општеството. Според неговите истражувања, вештачката интелигенција својот максимум на развивање, усовршување и искористување би го постигнала најдоцна до 2049 година, година во која се очекува да се направат голем број на промени токму како резултат на ова усовршување на вештачката интелигенција.⁴ Постојаното унапредување на вештачката интелигенција до нејзино совршенство во догледно време може да означува и потполно заменување на човекот со машини, односно потполно заменување на извршување на задачите од страна на човек со определени машини кои би функционирале токму врз принципот на вештачка интелигенција. Постојат и определени размислувања, според кои максимумот на својот развој на вештачката интелигенција може да создаде и услови за постепено приближување на концептот на вештачка интелигенција, до функционалноста на човечкиот мозок.⁵

Вештачката интелигенција и безбедноста

Секоја држава одделно, но и целиот свет постојано е изложен на постојани закани по безбедноста како резултат на бројните стари, односно традиционални начини на загрозување на безбедноста, но и како резултат на современите, односно новите форми на загрозување на безбедноста, како на национален план, така и на меѓународен план. Посебно внимание во светската јавност привлекуваат новите начини и форми на загрозување на безбедноста на државите, од причина што истите до тогаш не биле познати, и како резултат на тоа не постои соодветен систем за нивно превенирање и нивно сузбивање.

Веднаш на почетокот треба да се потенцира фактот дека вештачката интелигенција, освен што има огромен број на придобивки за општеството и за самиот човек, истата има и свои негативни страни. Постојаниот развој и усовршување на вештачката интелигенција предизвикува оправдани стравови кај голем број аналитичари и теоретичари од областа на безбедноста. Се поставува прашањето дали

³<https://translate.google.com/> (Aug.21.2018).

⁴<http://91.222.7.186/vesti/naslovna/tehnologije/aktuelno.236.html:693728-Vestacka-inteligencija-do-2050-preuzima-vecinu-poslova> (Aug. 23.2018).

⁵Nils, N.: Artificial Intelligence – A New Synthesis: Morgan Kaufmann Pub. Inc. 1998.

опстојувањето и усовршувањето на вештачката интелигенција може да бидат искористени од страна на определени поединци или групи на поединци како закана за самата безбедност. Секако дека вештачката интелигенција може да биде искористена, односно може да биде злоупотребена за загрозување на безбедноста. Ова загрозување на безбедноста од страна на вештачката интелигенција може да биде направено намерно и ненамерно. Намерно злоупотребување на вештачката интелигенција за загрозување на безбедноста имаме во ситуација кога постои свест кај лицата кои се користат со вештачката интелигенција дека е можно со нивните дејствија да биде загрозувана безбедноста, токму како резултат на самата вештачка интелигенција. Додека, пак од друга страна, ненамерното загрозување со вештачка интелигенција имаме во ситуациите кога истата се користи за оправдани цели, но нејзиното користење може да предизвика определени загрозувања на безбедноста, односно загрозувања на безбедноста како резултат на некои непредвидени појави и случувања.

Постојат три главни области на безбедноста, кои постојано се изложени на бројни ризици токму како резултат на искористувањето, односно злоупотребувањето на вештачката интелигенција. Првата област ја покрива дигиталната безбедност, односно бројните ризици кои може да настанат како резултат на искористувањето на вештачката интелигенција за сајбер просторот. Токму како резултат на злоупотребување на вештачката интелигенција во оваа област доаѓа до развивање и усовршување на сајбер криминалитетот, односно до постојано извршување и практикување на сајбер напади.

Интернет просторот или како што уште се нарекува во информатичките кругови, сајбер просторот, во моментот претставува најголем ресурс со информации во светот. Истиот е така широко отворен за поставување и преземање на информации. Со употребата на интернетот во секојдневниот живот се подобрува комуникацијата меѓу луѓето, а физичките бариери и пречки што може да се појават се избришани. Влијанието кое го извршува интернетот врз целокупниот живот на човекот е огромно и доста забележително. Интернетот се појавува во секој аспект на човековиот живот, користејќи го како начин за добивање на најнови вести и информации, како начин за барање работа, создавање нови пријателства, користење на разни веб-страници со најразлична содржина, како едукативен медиум и сл.⁶ Имајќи ја предвид оваа присутност на интернетот во секојдневното живеење, како и неговото значење за целокупното општество, потребно е искористување на вештачката интелигенција со голема внимателност токму во делот на сајбер просторот, како би се спречиле можни злоупотреби.

Следната област од безбедноста која може да биде загрозувана како резултат на искористување на вештачката интелигенција е физичката безбедност. Загрозувањето на физичката безбедност како резултат на злоупотребата на вештачката интелигенција најчесто се извршува преку реализација на напади со помош на дронови, како и реализација на напади со останати физички системи. Често се случува токму со помош на дронови да бидат извршени некои терористички напади кои имаат трајни и разорни последици за голем број на жртви, како и последици за самото општество.

Историјата на почеток на искористување на дроновите за војување е од 2001 година, конкретно на 7 октомври кога Соединетите Американски Држави во Авганистан искористуваат беспилотно летало

⁶Prlja, D.: *Pravnainformatika*: Beograd: PravnofakultetUniverziteta Union. 2010.

токму за оваа намена. Веќе од 2001 година па наваму, војувањето со беспилотни летала постојано се проширува. Според некои статистики до 2015 година од страна на Соединетите Американски Држави во Авганистан извршени се преку 200 напади со помош на дронови, односно со помош на беспилотни летала. Во една проекција, до 2019 година се очекува да дојде до зголемување за 50 % на вкупно извршените напади со дронови од страна на Соединетите Американски Држави.⁷ Користењето на дроновите за војување не е проблематично кога се работи за постигнување на оправдано воени цели, но неговото користење за постигнување на неоправдани цели доведува до разорни последици. Типичен пример за злоупотребата на беспилотните летала, односно користењето на дроновите е нивното користење од страна на терористите за постигнување на нивните терористички цели. Тероризмот најдобро се дефинира преку наведувањето на последиците и целите кои настануваат со преземањето на терористичките акти, со преземањето на терористичките напади. Кога се зборува за тероризам во прв план се работи за употреба на насилство, за употреба на агресија, односно за употреба на сила или за заканување за нивна употреба се со цел да се остварат определени цели на терористите, кои во суштина значат остварување на политички промени.⁸ Имајќи ги предвид овие штетни последици како резултат на практикувањето на тероризмот, се добива јасна слика од евентуалната злоупотреба на вештачката интелигенција во областа на физичката безбедност, пред сè на бројните злоупотреби кои се извршуваат за остварување на целите на терористите.

Последната, односно третата област на безбедноста која е изложена на постојан ризик како резултат на практикувањето и усовршувањето на вештачката интелигенција е областа на политичка безбедност. Како најчести дејствија кои се случуваат во рамките на оваа област, а истите се резултат на злоупотребата на вештачката интелигенција, се следните: преземањето на различни мерки за постојано надгледување и опсервација на лица или пак на објекти, преземање на бројни активности во насока на спроведување на определена пропаганда за постигнување на некоја цел, како и дејствија што значат сторување на разни измени со помош на бројни манипулативни видеоматеријали. Иако може да се изгенерализираат овие три посебни области на загрозување на безбедноста како резултат на злоупотребата на вештачката интелигенција, сепак треба да се има во предвид дека полето за загрозување на безбедноста е многу пошироко од овие кои се посочени. Како резултат на усовршување на вештачката интелигенција, постојано се зголемуваат и можностите за нејзино злоупотребување во насока на повредување на различните области на безбедноста.

Заклучок

Од денешен аспект кога се зборува за вештачката интелигенција, генералниот заклучок е дека е се присутна во општеството и дека таа сè повеќе и повеќе се усовршува и ќе се доразвива. Неспорни се

⁷<http://balkans.aljazeera.net/vijesti/sta-je-presuceno-o-dronovima>(Aug. 25.2018).

⁸Jenkins, B.: International terrorism: a new kind of warfare: Santa Monica, California: The Rand Corporation. 1974.

придобивките за општеството од самиот концепт на вештачка интелигенција, но како што видовме постојат и бројни негативности од користењето на вештачката интелигенција, односно истата создава можности и услови за нејзино злоупотребување во различни сфери. Една од тие сфери на можни злоупотреби на вештачката интелигенција е и сферата на безбедноста, како сфера која е од пресудно значење за нормално функционирање на секое општество, на секоја држава. Во сферата на безбедноста, три области се под посебна закана на вештачката интелигенција, односно сајбер просторот, физичката безбедност, како и политичката безбедност. Во секое општество кое е насочено кон развивање на концептот на вештачка интелигенција и кон негово легално употребување за остварување на легитимни цели, потребно е да се преземат низа дејствија како би се спречиле евентуални злоупотреби на овој концепт. Така потребно е постојано истражување и проектирање на вештачката интелигенција, пред се од лицата кои се стручни во областа, за определување и детектирање на можните негативни последици за општеството од развивање и употребување на овој концепт. Истражувањето на вештачката интелигенција, во никој случај не може да биде насочена единствено кон постигнување на нејзините цели, односно истата мора да биде истражувана и во контекст на нејзините веќе посочени негативни страни како би се добила комплетна слика за појавата која е предмет на интерес. Потребно е да бидат искористени најдобрите практики во областа на вештачката интелигенција, како би се добиле конечни решенија кои се одржливи на долг рок и решенија кои претставуваат опасност за општеството. И секако на крај потребен е еден интегративен и мултидисциплинарен пристап во изучувањето на концептот на вештачка интелигенција, од проста причина што целите кои се остваруваат со истиот, како и евентуалните негативни последици не може да се подведат под една научна дисциплина.

Литература

- Jenkins, B.: International terrorism: a new kind of warfare: Santa Monica, California: The Rand Corporation. 1974.
- Nils, N.: Artificial Intelligence – A New Synthesis: Morgan Kaufmann Pub. Inc. 1998.
- Prlja, D.: Pravnainformatika: Beograd: PravnikafakultetUniverziteta Union. 2010.
- Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach. Harlow: Prentice Hall. 2009.
- <http://www.britannica.com/EBchecked/topic/37146/artificial-intelligence-AI> (Aug.19.2018).
- <http://91.222.7.186/vesti/naslovna/tehnologije/aktuelno.236.html:693728-Vestacka-inteligencija-do-2050-preuzima-vecinu-poslova>(Aug. 23.2018).
- <http://balkans.aljazeera.net/vijesti/sta-je-presuceno-o-dronovima>(Aug. 25.2018).
- <https://translate.google.com/>(Aug.21.2018).

КОНЦЕПТОТ НА ПОЗИТИВНА ДИСКРИМИНАЦИЈА ВО СОВРЕМЕНОТО ОПШТЕСТВО

UDC: 316.647.82

*Прегледен труд***Д-р Роза Гурмешевиќ**

Апстракт

Една од главните карактеристики на европските општества е различноста. Таа подразбира индивидуални разлики меѓу луѓето кои бараат прифаќање, почитување, признавање и уважување од страна на другите. Покрај бројните предности кои ги носи богатството на различноста во современото општество, искуството покажува дека разликите меѓу луѓето можат да доведат и до различни искуства, системи на вредности, начини на размислување, однесување, комуникација, па дури и до етнички судири кои обично стојат на патот на општествената интеграција. Со цел да се избегнат таквите ситуации, неопходно е правилно разбирање и вреднување на политиките на различност. Една од таквите политики која има за цел да ја исправи историската неправда и нерамноправна положба на одредени групи на луѓе чии права се систематски ускратувани и кршени е позитивната дискриминација. Иако во суштина се работи за прописи, мерки или практики кои не се неправедни и со кои се остваруваат предности во одредени области за одредена категорија на лица, постојат и негативни размислувања кои одат во насока на нивно укинување и кои ја доведуваат во прашање функционалноста на резултатот кој треба да го постигнат. Во таа смисла, Европската унија и Советот на Европа, пружаат јасни насоки за разбирање на концептот на позитивна дискриминација, како во областа на законодавството, така и во судската пракса.

Клучни зборови: *позитивна дискриминација, афирмативна акција, полна рамноправност, групни права, различен третман*

THE CONCEPT OF POSITIVE DISCRIMINATION IN MODERN SOCIETY

Abstract

One of the main characteristics of European societies is diversity. It involves individual differences among people seeking acceptance, respect, recognition and appreciation of others. Despite the numerous advantages that richness of diversity brings in modern society, experience shows that differences between people can lead to different experiences, value systems, ways of thinking, behavior, communication, and even to ethnic conflicts that usually stand on the way of social integration. In order to avoid such situations, it is necessary to properly

understand and value diversity policies. One of such policies which aim to correct the historical injustice and disadvantage of certain groups of people whose rights are systematically violated and denied is positive discrimination. Although essentially it involves regulations, measures or practices that are not unfair and that accomplish advantages in certain areas for a certain category of people, there are negative opinions that go towards their lifting and calling into question the functionality of the result to be achieved. In this sense, the European Union and the Council of Europe provide clear guidelines for understanding the concept of positive discrimination, both in legislation and in judicial practice.

Keywords: *Positive discrimination, affirmative action, full equality, group rights, different treatment.*

1. Поим на позитивна дискриминација

Позитивната дискриминација претставува пракса на имплементирање на оние постапки чија цел е давање на предност на групите во општеството кои често се дискриминирани.¹ Во таа група најчесто спаѓаат жените, Ромите, лицата со инвалидност, припадниците на етничките групи и многу други чии права се систематски ускратувани и кршени, и тоа често низ вековите. Последиците од таквиот третман се нерамноправна положба во општеството и намалување на нивните можности за уживање на основните права, као што се правото на образование, вработување, социјална и здравствена заштита итн. Затоа постојат посебни прописи, мерки или практики со кои се остварува предност при вработувањето, во образованието и уживањето на поедини права, кои во суштина се дискриминаторни (негативни) спрема останатите членови на општеството, но не и неправедни. Ови прописи, мерки или практики кои ги превземаат владите, организациите или компаниите во правото се познати и како мерки на афирмативна акција. Мерките на афирмативна акција се покренати во САД, под иницијатива на американските претседатели Кенеди и Џонсон, а најголема експанзија и радикализација доживеале за време на владеењето на конзервативниот претседател Ричард Никсон во текот на шеесетите и седумдесетите години на минатиот век. Тие имаат за цел да ги исправат општествените неправди од минатото, да ги намалат постоечките нееднаквости во општеството кои настанале по пат на дискриминација или други облици на насилство и да обезбедат полна и стварна рамноправност, посебно во областа на вработувањето и високото образование.²

2. Предизвиците и последиците на позитивната дискриминација

Во реалноста постојат различни толкувања на концептот на позитивна дискриминација и неговите импликации во општеството. Во тој контекст посебно внимание привлекува дистинкцијата помеѓу

¹ Alexandera, S.: *Legality of Positive Discrimination in the United Kingdom*, Edition 1, Part 1, 2018, p. 1.

² Mesić, M.: „Kontroverzije oko afirmativne akcije“, *Migracijske i etničke teme*, Vol. 21 No. 3, 2005, стр. 187-189.

принципот на еднаков третман, кој претставува водечки принцип не само во европското законодавство и пракса, туку и пошироко, и концептот на позитивна дискриминација. Во последните неколку години актуелни се и дебатите за застапеноста на жените на раководните позиции, имајќи го во вид фактот дека управните одбори во мноштво компании ширум светот претежно се состојат од машки раководители, додека процентот на жени на раководните позиции е сеуште многу мал. Во изминатите децении во законодавствата се превземаат разни иницијативи кои преферираат избор на женски кандидати на работните места како облик на позитивна дискриминација. Такви случаи има и во другите области на општествениот живот, на пример, во здравството и образованието, или кога се во прашање припадниците на осетливите групи во општеството, како што се малцинствата, верските или етничките групи итн. Токму поради таквите иницијативи и импликации врз останатите членови на општеството доаѓа до се почести критики на позитивната дискриминација. Толкувањата на овој концепт во последните години се застапени и во судската пракса на Европскиот суд за човекови права и Европскиот суд на правдата.

Меѓународните инструменти за човекови права, како и националните закони, кои го препознаваат концептот на позитивна дискриминација упатуваат на мерки на позитивна или афирмативна акција кои се понекогаш познати и како посебни или реститутивни мерки. Постојат пет широки категории на позитивна акција: 1) позитивни мерки за искоренување на дискриминацијата (на пример, отстранување на дискриминаторните практики против групите кои со векови биле во нерамноправна положба); 2) фацијално неутрални политики кои имаат за цел пружање на помош на загрозените групи; 3) програми кои се креирани за привлекување на кандидатите од помалку застапените групи; 4) преференцијален третман (на пример, употреба на „квоти“ или „плюс“ фактори); и 5) редефинирање на заслугите со цел забранетиот основ на дискриминација да овозможи квалификација за одредена позиција. Секоја од овие категории има за цел постигнување на стварна еднаквост која бара отстранување на основните структури, како што се историските и културните предрасуди кои ја одржуваат дискриминацијата дури и кога се воспоставени мерки на формална еднаквост. Позитивната акција потврдува дека понекогаш третирањето на поединците на потполно ист начин како што бара формалната еднаквост е недоволно за борба против дискриминацијата на одредени групи на луѓе кои се предмет на латентна или традиционална дискриминација. Затоа на овие групи им е потребен одреден степен на преференцијален третман.³

Покрај аргументите кои одат во корист на позитивната акција, постојат и аргументи против превземањето на такви мерки: 1) затоа што дискриминацијата е дискриминација и не може да биде исправна; 2) затоа што го повредува правото на еднаков третман; 3) затоа што се создава маѓепсан круг во кој секогаш една група е дискриминирана; 4) затоа што преференцијалниот третман треба да биде индивидуален и специфичен, а не глобален; и 5) затоа што се промовира нестручност и пад на квалитетот бидејќи не се гледаат правите критериуми, на пример, критериумите за работа, туку споредните (како што се полот, расата, сексуалната ориентација итн.).⁴ Во овој контекст вреди да се спомене строго формалниот поим на еднаквоста кој ги забранува корективните облици на дискриминација кои се

³ Non-Discrimination in International Law: A Handbook for practitioners, London, 2011, p. 84.

⁴ Kerčević, S.: Pozitivna diskriminacija - Grad Rijeka, 2008.

припишуваат на групите кои се жртви на традиционалната дискриминација. Од друга страна, позитивната акција вообичаено бара привилегирање на групните права над индивидуалните. Како резултат на тоа, концептот на позитивни или афирмативни акции понекогаш се смета за контроверзен.⁵ Позитивната акција треба да се разграничи и од општата обврска на државата да превзема позитивни мерки за обезбедување на еднаквост. Првиот концепт бара државата да превземе мерки со цел да обезбеди преференцијален третман на одредени групи, додека последниот упатува на фактот дека потполната заштита на еднаквоста не само што бара државата да се воздржува од спроведување на дискриминаторни активности, туку и да превзема позитивни мерки (на пример, имплементација на антидискриминационото законодавство) со цел да осигура еднаквост.

3. Позитивната дискриминација и меѓународните инструменти за борба против дискриминација

Меѓународните инструменти, генерално, ја признаваат важноста на мерките на позитивна или афирмативна акција со цел да се надмине дискриминацијата од минатото. Комитетот на ОН за човекови права ја признава потребата за превземање на мерки на позитивна акција во Општиот коментар бр. 18. Општиот коментар бр. 4 на членот 3 на Меѓународниот пакт за граѓански и политички права (МПГПП) утврдува дека член 3, као и член 2, став 1 и член 26 на МПГПП не само што бараат мерки на заштита, туку и мерки на афирмативна акција со цел да се осигура позитивно уживање на загарантираните права. Во Општиот коментар бр. 32 Комитетот за елиминација на расната дискриминација ја појаснува обврската на државата да спроведува посебни мерки во согласност со Конвенцијата. Конвенцијата за елиминација на сите облици на дискриминација на жените упатува на превземање на мерки на афирмативна акција и утврдува дека овие мерки имаат ограничено временско траење, без да ја прецизира нивната временска рамка. Во Општиот коментар бр. 25 Комитетот за елиминација на дискриминацијата на жените ја проширува содржината на Општиот коментар бр. 5 кој се однесува на временски посебни мерки. Комитетот ја појаснува и терминологијата која се користи за означување на мерките на афирмативна акција, обезбедувајќи алтернативни термини како што се „специфични мерки“, „позитивна акција“, „позитивни мерки“, „обратна дискриминација“ и „позитивна дискриминација“ (параграф 17). Комитетот исто така дава објаснување за ограниченото траење на посебните мерки, кое според Комитетот ќе зависи од нивниот функционален резултат како одговор на конкретен проблем, а не од предодредениот проток на време. Овие мерки мораат да бидат прекинати кога ќе биде постигнат саканиот резултат (параграф 20). Мерките на позитивна акција (временски посебни мерки) се признати и во Меѓународниот пакт за економски, социјални и културни права (МПЕСКП), Конвенцијата за правата на лицата со инвалидност и Конвенцијата на Меѓународната организација на трудот бр. 111.⁶

⁵ Non-Discrimination in International Law: A Handbook for practitioners, *loc.cit.*

⁶ *Ibid.*, pp. 90-93.

Членот 14 на Европската конвенција за човекови права (ЕКЧП) утврдува дека уживањето на правата и слободите предвидени во Конвенцијата се обезбедува без дискриминација. Тоа подразбира дека државите членки имаат позитивни обврски спрема членот 14, као и негативни обврски да не превземаат дејства на дискриминација. Рецитал 3 на преамбулата на Протоколот бр. 12 кон ЕКЧП експлицитно ја нагласува важноста на позитивната акција. Иако праксата на Европскиот суд за човекови права нема јасен став по прашањето на спроведување на позитивните акции со цел да се постигне стварна еднаквост, во Белгискиот лингвистички случај (*Belgian Linguistics Case*) Судот експлицитно призна дека „поедини правни нееднаквости имаат за цел единствено да ги исправат фактичките нееднаквости.“⁷

Европската унија во изминатите години имплементирала бројни мерки кои обезбедуваат позитивна акција и кои влијаат на развојот на јуриспруденцијата на ЕУ за превземање на позитивна акција (на пример кога се работи за дискриминација на основа на полот), а посебно на првичната Директива 76/207/ЕЕЗ од 9 февруари 1976 година за примена на принципот на еднаков третман на мажите и жените во поглед на пристапот на вработување, стручно оспособување и напредување и работните услови и членот 157 на Договорот за функционирање на ЕУ. Пред усвојувањето на ревидираната Директива за еднаков третман од 2002 година⁸, во членот 2, став 4 на Директивата за еднаков третман од 1976 година било пропишано дека „мерките за промоција на еднакви можности за жените и мажите, а посебно за отстранување на постоечките нееднаквости кои ги поаѓаат можностите на жените“ нема да се сметаат за дискриминирачки. Ревидираната Директива за еднаков третман ја изменила оваа одредба со цел да овозможи мерките, кои треба да се превземат во согласност со членот 157, став 4 на Договорот за функционирање на ЕУ, да осигураат полна рамноправност помеѓу мажите и жените. Член 157, став 4 на Договорот за функционирање на ЕУ повеќе дозволува отколку што бара од државите членки да превземат позитивна акција со цел да осигураат полна еднаквост во случаите кога недоволно застапениот пол наидува на потешкотии во пристапот на вработување или да ги исправат или спречат недостатоците кои ги претрпел недоволно застапениот пол.⁹ Директивата за еднаквост во вработувањето (член 7, став 1 и 2), како и Директивата за расна еднаквост (член 5), исто така повеќе дозволува отколку што бара од државите членки да превземат мерки на позитивна акција. Сличен пристап во поглед на превземањето на мерки на позитивна акција има и судската пракса на Европскиот суд на правдата.¹⁰

⁷ Вид. The European Court of Human Rights (ECtHR), *Belgian Linguistics Case*, Applications no 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64; para. I (B) (10) и The European Court of Human Rights (ECtHR), *Timishev v. Russia*, Applications nos. 55762/00 and 55974/00, 13 December 2005, para. 44.

⁸ Директива 2002/73/ЕЗ на Европскиот парламент и Советот од 23 септември 2002 година за измена и дополнување на Директивата на Советот ЕУ 76/207/ЕЕЗ за примена на принципот на еднаков третман на мажите и жените во поглед на пристапот на вработување, стручно оспособување и напредување и работните услови.

⁹ *Non-Discrimination in International Law: A Handbook for practitioners*, op.cit., pp. 94-95.

¹⁰ *Ibid.*, p. 96.

4. Позитивната дискриминација во судската пракса на Европскиот суд на правдата

Европските судови ја сметаат директната позитивна дискриминација за незаконита. На пример, во контекст на вработувањето позитивната дискриминација би била незаконита кога работодавачот би вработил кандидат/ка само затоа што тој/таа поседува одредена заштитена карактеристика, а не поради фактот дека се работи за избор на најдобриот кандидат/ка. Исто така незаконито е да се воспостават „квоти“ за вработување или унапредување на одреден број или процент на луѓе со одредена заштитена карактеристика. На пример, позитивната дискриминација се смета за незаконита кога работодавецот објавува оглас за работа кој посебно ја нагласува потребата за вработување на жени. Тоа е потврдено во два клучни случаи на Европскиот суд на правдата.

Во пресудата на германскиот случај Каланке од октомври 1995 година¹¹ Европскиот суд на правдата утврдил дека до примена на позитивна дискриминација може да дојде кога се врши избор на женски и машки кандидати со еднакви квалификации и искуства, при што предноста на жените би се состоела во зголемување на процентот на женска работна сила. Имено, во завршната фаза на избор на кандидати за позицијата менаџер влегле двајца кандидати, господин Каланке и госпоѓа Глиман, кои веќе биле вработени во одделението во кое конкурирале за повисока функција. Раководителите имале намера да го промовираат господин Каланке, но после приговорите од страна на Комитетот на персоналот било одлучено дека мора да се даде предност на женскиот кандидат, госпоѓа Глиман. Тоа било во согласност со параграф 4 на бременскиот Закон за еднаков третман на мажите и жените во јавна служба кој предвидува дека за именувања и унапредувања во службата, жените кои имаат исти квалификации како и мажите кои се пријавени за исто работно место треба да имаат предност во секторите во кои се недоволно застапени, односно кога тие не претставуваат најмалку половина од вработените во поглед на поединечната плата, надоместокот и платата на заработка во релевантната кадровска група во одделението. Против таквата одлука господин Каланке поднел жалба до Судот на трудот во Бремен, а подоцна и до Регионалниот суд на трудот, кои биле безуспешни. На крајот поднел жалба до Сојузниот суд на трудот кој ги прифатил наодите на Регионалниот суд на трудот кои се однесувале на еднаквите квалификации на двата кандидати и недоволната застапеност на жените во одделението. Тој утврдил дека бременскиот Закон за еднаков третман на мажите и жените во јавна служба е во согласност со германските внатрешни законски и уставни прописи, но дека постои сомнеж во врска со ускладеноста со Директивата на Советот 76/207/ЕЕЗ. Во поглед на ова прашање била побарана прелиминарна одлука од страна на Судот на правдата на Европските заедници. Поточно, било поставено прашањето дали членот 2, став 4 на Директивата за еднаков третман од 1976 година може да се толкува во смисла дека ги покрива законските одредби како што се одредбите на бременскиот Закон за еднаков третман кои предвидуваат задолжителна позитивна дискриминација. Доколку не може, тогаш дали член 2, став 1 на Директивата за

¹¹ European Court of Justice: Case C-450/93 (Kalanke v Freie Hansestadt Bremen), Judgement of the Court of October 1995.
174

еднаков третман¹², имајќи го во вид начелото на пропорционалност, може да се толкува во смисла дека не е дозволено да се применува на законски одредби како оние во бременскиот закон.

Европскиот суд на правдата утврдил дека член 2, став 4 на Директивата за еднаков третман мора да се толкува строго. Националните прописи како што се прописите на бременскиот закон кои гарантираат апсолутен и безусловен приоритет на жените за именување или унапредување го надминуваат промовирањето на еднакви можности и ги пречекоруваат границите на исклучоци во член 2, став 4 на Директивата. Од тоа следи дека член 2, став 1 и член 2, став 4 на Директивата за еднаков третман спречуваат национални прописи како што се одредбите на бременскиот закон. Судот утврдил дека националните прописи кои (во случаите кога машките и женските кандидати кои се се еднакво квалификувани и конкурираат за исто унапредување) автоматски предвидуваат приоритет на жените во секторите во кои се недоволно застапени се дискриминирачки со оглед на фактот што вклучуваат дискриминација на основа на полот. Член 2, став 4 на Директивата за еднаков третман кој пропишува дека „мерките за промоција на еднакви можности за жените и мажите, а посебно за отстранување на постоечките нееднаквости кои ги поаѓаат можностите на жените нема да се сметаат за дискриминирачки“ е посебно и исклучиво пропишан со цел да овозможи мерки кои, иако навидум изгледаат дискриминирачки, во суштина имаат за цел да ги елиминираат или намалат стварните случаеви на нееднаквост кои постојат во општествениот живот. На тој начин овој член овозможува превземање на национални мерки во однос на пристапот на вработување, вклучително и унапредување, кои им даваат посебна предност на жените со цел да се подобри нивната способност да се натпреваруваат на пазарот на трудот и да ја продолжат својата кариера на рамноправна основа со мажите. Како што утврдил Советот во третиот рецитал на преамбулата на Препораката 84/635/ЕЕЗ од 13 декември 1984 година за промовирање на позитивна акција за жените „постоечките законски одредби за еднаков третман кои се создадени со цел да се им се овозможат одредени права на поединците се неадекватни за елиминација на сите постоечки нееднаквости, освен ако паралелна акција спроведува владата, компаниите и другите заинтересирани организации, со цел да се спротивстават на штетните ефекти на жените во вработувањето кои произлегуваат од социјалните ставови, однесувања и структури.“¹³

Европскиот суд на правдата завземал сличен став и во пресудата на германскиот случај Маршал од 1997 година во кој утврдил дека позитивната дискриминација во корист на жените била во спротивност со Директивата за еднаков третман 76/207/ЕЕЗ.¹⁴ Господин Хелмут Маршал бил вработен како наставник во средно училиште. Во 1994 година тој аплицирал за унапредување на работното место, но сепак Окружниот орган му соопштил дека унапредувањето било наменето за женски кандидати. Г-дин Маршал безуспешно поднел жалба до Окружниот орган кој утврдил дека во конкретниот случај имало подеднакво квалификувани кандидати, но бидејќи биле вработени помалку женски за разлика од машките кандидати, на жените треба да им се понуди унапредување. Г-дин Маршал започнал постапка против Окружниот

¹² Член 2, став 1 на Директивата за еднаков третман предвидува дека е забранета било каква дискриминација на основа на полот, директна или индиректна.

¹³ European Court of Justice: Case C-450/93 (Kalanke v Freie Hansestadt Bremen), Judgement of the Court of October 1995, para. 11-24.

¹⁴ European Court of Justice: Case C-409/95: Marschall v Land Nordrhein- Westfalen, Judgment of the Court of 11 November 1997.

орган пред локалните судови. Во прв степен било утврдено следното: „со оглед на фактот дека женските кандидати и г-дин Маршал биле подеднакво квалификувани, исходот на случајот ќе зависи од компатибилноста на Директивата за еднаков третман со параграф 25, став 5 на Законот за државни службеници на Северна Рајна-Вестфалија во кој било пропишано следното: „кога во секторот на органот одговорен за унапредување на работното место има помалку жени отколку мажи на жените треба да им се даде предност за унапредување во повисок степен, под услов да постојат подеднакви квалификации на машките и женските кандидати (во однос на нивните подобности, компетенции и професионализам), освен кога постојат причини специфични за поединечни (машки) кандидати кои ја замаглуваат рамнотежата во нивна корист.“

Пред Европскиот суд на правдата било поставено прашањето дали член 2, став 1 и 4 на Директивата за еднаков третман го исклучува правилото на националниот закон, односно Законот за државни службеници на Северна Рајна-Вестфалија, при што Судот утврдил дека „ваквото национално правило не е оневозможено од член 2, став 1 и 4 на Директивата за еднаков третман под услов: а) во секој поединечен случај правилото кое предвидува подеднакво квалификувани машки и женски кандидати да обезбеди гаранција дека кандидатурите ќе бидат предмет на објективна проценка која ќе ги земе во предвид сите критериуми кои се специфични за кандидатите и ќе го премости приоритетот даден на женските кандидати кога еден или повеќе од тие критериуми ја замаглуваат рамнотежата во корист на машките кандидати; и б) таквите критериуми да не се создадени со цел да ги дискриминираат женските кандидати. Повикувајќи се на одлуката во случајот Каланке од 1995 година Европскиот суд на правдата утврдил дека: „приоритетот кој одредбата која е во прашање го дава на жените претставува дискриминација во смисла на член 2, став 1 на Директивата за еднаков третман и таквата дискриминација не се елиминира со можноста за давање на предност на жените, исклучувајќи ги при тоа машките кандидати.“ Судот понатаму утврдил дека „основата за оценување на кандидатите е прекумерно стеснета бидејќи се зема во предвид само нумеричкиот процент на мажите во однос на жените. Покрај тоа, одредбата која е во прашање не ја подобрува способноста на жените да се натпреваруваат на пазарот на трудот и да ја продолжат кариерата на еднаква основа со мажите.“

Во ваквите случаи критичарите на позитивната дискриминација тврдат дека не е фер да се обезбеди вработување на одредено лице само зато што е припадник на одредена група, без да се земат во предвид останатите критериуми кои се поврзани со работното место. Друг аргумент е фактот дека ваквата пракса не влијае добро врз економијата на земјата бидејќи позитивната дискриминација често води кон вработувања на потенцијално неквалификувани и неприкладни кандидати – гледиште кое е застапено и во пресудата на Европскиот суд на правдата во случајот Абрахамсон и Андерсон.¹⁵ Повикувајќи се на член 119 на Договорот од Рим од 1957 година кој пропишува дека жените имаат право на „еднаква плата за еднаква работа“ критичарите на позитивната дискриминација посочуваат дека правните инструменти за човекови права не подразбираат давање на предности на жените кога истите не ги заслужуваат.

¹⁵ European Court of Justice: Case C-407/98 - Abrahamsson and Anderson, Judgment of the Court (Fifth Chamber) of 6 July 2000.
176

Заклучок

Иако меѓународните инструменти за човекови права го препознаваат концептот на позитивна дискриминација, во националните законодавства различно се толкува и применува и често се смета за незаконит и контроверзен концепт. Од друга страна, праксата на европските судови потврдува дека нееднаквостите кои се резултат на повеќекратната дискриминација на поедини групи на луѓе не треба да се занемарат. Европскиот суд на правдата не го занемарува фактот дека некои длабоко вкоренети предрасуди и стереотипи за улогата и капацитетот на жените во областа на вработувањето се уште постојат. Од друга страна Судот утврдува дека приоритетот кој им се дава на подеднакво квалификуваните жени со мажите со цел повторно да се воспостави баланс не е во спротивност со правото на Заедницата, под услов таквиот приоритет да има за цел да се вршат објективни проценки на секој кандидат поединечно, без оглед на нивниот пол. Од ваквиот пристап на Европскиот суд на правдата произлегува дека правилната примена на концептот на позитивна дискриминација подразбира хармонизација на националното законодавство со европското и правилно толкување и примена на одредбите на меѓународните инструменти кои предвидуваат мерки на позитивна акција, но и одреден степен на флексибилност во примената на мноштвото пристапи на позитивна акција не само во областа на вработувањето, туку и во другите области на општествениот живот и во однос на другите осетливи групи

Литература

- Milan Mesić: „Kontroverzije oko afirmativne akcije“, Migracijske i etničke teme, Vol. 21 No. 3, 2005;
- Non-Discrimination in International Law: A Handbook for practitioners, London, 2011;
- Solomon Alexandra: Legality of Positive Discrimination in the United Kingdom, Edition 1, Part 1, 2018;
- Srđan Kerčević: Pozitivna diskriminacija - Grad Rijeka, 2008;
- European Court of Justice: Case C-407/98 - Abrahamsson and Anderson, Judgment of the Court (Fifth Chamber) of 6 July 2000.
- European Court of Justice: Case C-450/93 (Kalanke v Freie Hansestadt Bremen), Judgement of the Court of October 1995;
- European Court of Justice: Case C-409/95: Marschall v Land Nordrhein- Westfalen, Judgment of the Court of 11 November 1997.
- The European Court of Human Rights (ECtHR), Belgian Linguistics Case, Applications no 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64;
- The European Court of Human Rights (ECtHR), Timishev v. Russia, Applications nos. 55762/00 and 55974/00, 13 December 2005;

HOW ARTIFICIAL INTELLIGENCE CHANGES HUMAN EXPERIENCE IN ART

UDC: 004.8/9:7

Reviews

Ass. Prof. Blagojche Naumoski, M.A.*European University – Republic of Macedonia, Skopje*

Abstract

Computational art is a creative field that indicates the futuristic idea of artificial intelligence. Despite the common belief that a machine is unable to create art, current developments and examples in computational art present a new form of art. Reaching to a broad variety of artistic dimensions, artificial intelligence programs generate poetry, music, visual art, architecture and design.

This paper introduces artificial intelligence as an artistic phenomenon and analyzes the artifacts that are produced by computer algorithms. Thus, it provides a theoretical framework and a philosophical discussion on the creative abilities of artificial intelligence. Furthermore, it is concerned with the entitlement of artiness, by presenting a reflection on the dynamics between the artwork, the art maker and the art audience.

Innovation in the sciences is always linked to the human experience in a certain way, either directly or indirectly. Of course, human experiences happen through engaging with the arts – for example, listening to music or looking at a piece of art. The arts tend to be ahead of the society when it comes to envisioning the future of technology – for instance, all the science fiction works that have shown us the future before scientists and engineers in reality. Many artists ‘magpie’ new technologies to use within the creative process. Because of technology, the role of the artist and the scientist, as well as their creative processes, is melding and the rigour of the resulting works is unbelievable. Our creativity has allowed our species to thrive, and, now, with machines having their own concepts of aesthetics, perception and creativity, it poses some important questions to artists. Artificial Intelligence (AI) brings the gap between technology and art by challenging creative intelligence and sensorial experiences, integrating networks known as GANs (Generative Adversarial Networks) and cGANs (Conditional Generative Adversarial Network), and changing the manner artists interact with their so-to-speak canvases.

Keywords: *Digital, technology, Artificial Intelligence, arts, social media*

Introduction

Computer music, software-developed works of art, bots that write pop music, schools teaching computational approaches to art and design – robots may not replace humans, but they certainly help and support them, even in their artistic production. Artificial intelligence and machine learning underlie this artistic revolution

– two branches of computer science embraced not only by well-known independent computer programmers/Internet artists such as Darius Kazemi, but also by companies, such as Google, which has launched two initiatives dedicated to the creative applications of AI, as well as institutions, such as the New York based School for Poetic Computation, which have long offered training programmes on the issues.

When the machines started to generate artworks, became creative producers themselves. From being a fictional theme in dystopian/utopian literature and science-fiction movies, intelligent machines have transformed into the writers of those movies and stories.

Therefore, their role in creative industries has been rapidly changing. Even though artificial intelligence and its artistic applications have been important scientific topics for decades, their popularity and recognition have been increased in recent years. Nevertheless, the legitimacy of this art genre and the concept of creativity in the field of artificial intelligence are still controversial subjects that need academic attention. Since the conventional definition of ‘art’ defines this notion as a way of communication between human subjects, new academic research that deals with AI art needs alternative approaches to the concept of art, to be able to put forward a classification for AI art.

Artists also begin to influence more actively and message the results of the artwork they create with their machine learning algorithms – changing their relationship with the AI to be more of an ideation partner, rather than simply a tool for making new tools.

Art and creativity are fundamental features inherent in human intelligence and fundamental signatures of humankind. It is a way through which we express our sentience. Artistic expression is attributed to be a human aspect related to consciousness. Therefore, it is seen as a human experience associated with awareness, will, perception, thought, memory, intelligence, creativity, identity and autonomy ¹.

1.1 Artistic Aspects of Research

In order to answer the research question, the study will contain three sub topics: **AI as an Impersonator**, **AI’s perception as artwork** and **Art + AI tomorrow** which addresses the concept of creativity and the artificial intelligence’s capability of generating creative outputs that have an artistic quality. As a novelty that has been attributed to the human mind, creativity is the main inquiry of the research regarding artificial intelligence.

Magenta is a **Google Brain** project that uses machine learning to create music and art. The initiative unites a network of artists, programmers and researchers who share innovative methods and approaches to create art. One of its first experiments led to the creation of AI Duet, a computerized piano that reacts to sound inputs entered by humans.

One of the most interesting results to come out of Magenta is Nsynth, an audio synthesizer that uses AI to produce new sounds using mathematical algorithms. Nsynth takes simple sounds, such as those of a flute,

¹ King, 2007: 152¹.

organ, violin or a xylophone, and combines them to create new sound effects, as if generated by an instrument that does not exist.

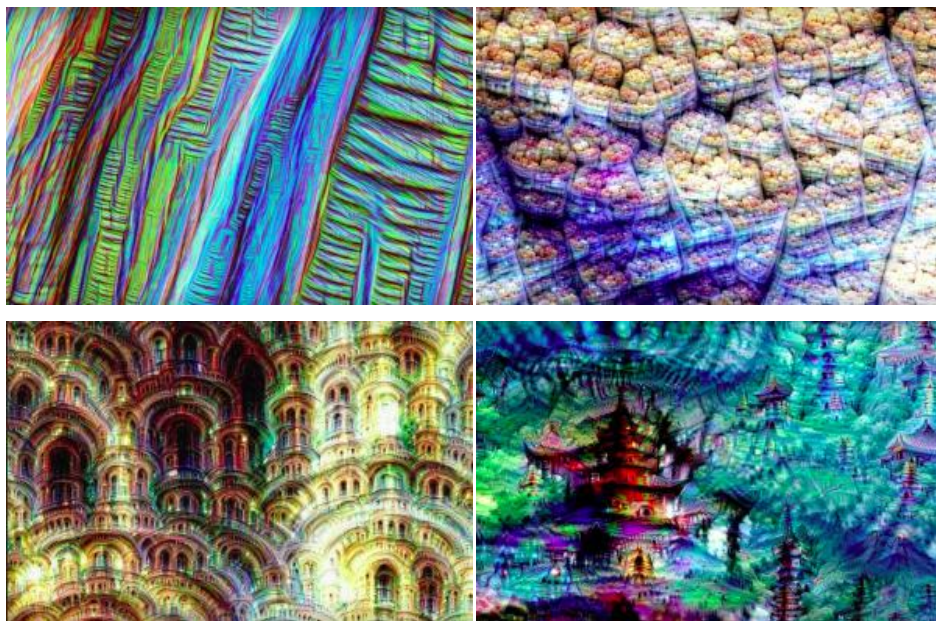
Founded in 2013 in New York to explore the intersections of code, design, hardware and theory, the **School for Poetic Computation**² is a hybrid of a school, residency and a research group, focusing on poetic production through bots and Man-Computer symbiosis.

The artist Darius Kazemi is convinced that artificial intelligence does not necessarily require considerable investments. Kazemi has created dozens of online bots: *Two Headlines* takes two headlines and combines them with amusing results; Museum Bot tweets a random high-res Open Access image from the Metropolitan Museum of Art, four times a day; *Very Old Tweets* retweets some of the earliest posts, when users still used Twitter to describe what they were doing.

Then, there's AI software capable of creating amazing reproductions of original paintings. The algorithm, known as **GAN** (Generative Adversarial Network), consists of two interacting neural networks. One generates, the other evaluates, and the algorithm ploughs on until the desired result is achieved. GAN was trained on 81,500 paintings to tell the difference between images we would class as artworks and those that are mere simple images. The network was also trained to distinguish different styles of art, such as Cubism, Rococo or abstract art.

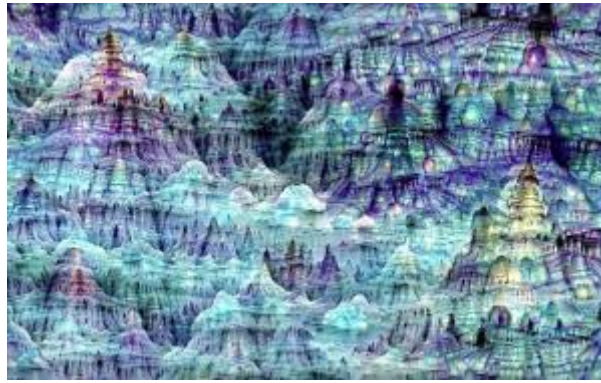
There is also an algorithm that can show a network trained to recognize, let's say, a painting, to run the network forward, and, from what the network have seen, the algorithm adjusts the pixels in the picture according to the interpretation. They observed that early layers cared about simple features, but, as we move through the network, we encounter higher order of features³.

Figure 1. Five successive layers of a network interpreting different features



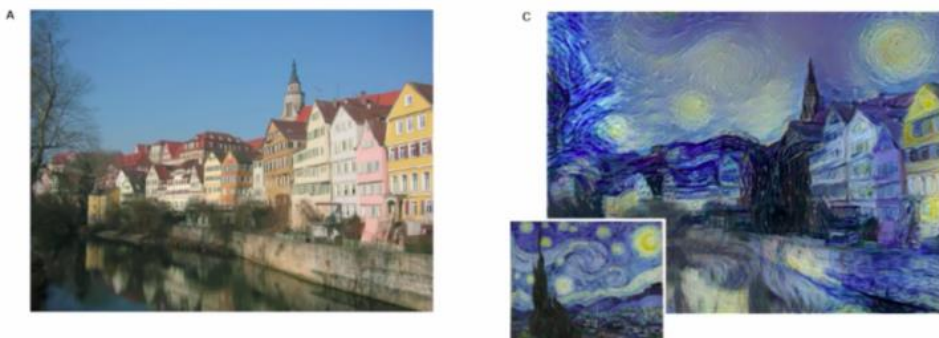
² <http://sfpc.io/> (8 Sept. 2018)

³ <https://artsciblog.wordpress.com/2017/02/25/first-blog-post/> (8 Sept. 2018)



How can these networks be used in arts or how can they inspire arts? With a technique which is an extension of the neural networks, called ‘deep’ neural networks. Deep neural networks is an extension of neural networks where the computer goes one step further and each neuron figures out its own function as well. In an example of treating art with deep networks, the author takes a photograph, chooses a painting style that they would like to interpret and the network applies the artistic style of the painting to the image and transforms it as shown below in Figure 2⁴.

Figure 2. (right) Input painting (left). Output painting which learnt style from inset painting (left bottom).



1.2 AI as an Impersonator

We began using AI to create art by first teaching it to understand and replicate our own art. The technique is called “style transfer” and uses deep neural networks to replicate, recreate and blend styles of artwork. It identifies and combines stylistic elements of one image and applies them to another. No artistic or coding experience required.

⁴ <http://uk.businessinsider.com/ai-makes-photos-look-like-famous-paintings-2015-9/#for-their-experiment-the-scientists-used-a-photo-of-the-neckar-river-in-tuebingen-germany-2> (8 Sept. 2018)

Whether it's applied to paintings, photography, video, or music, the concept is the same: choose a piece of artwork whose style you want to recreate, then let the algorithm apply that style to a different image. Or, choose several styles of art and let the AI produce mash-ups that incrementally blend styles together. In the example below, taken from Google AI, you can see the four original pieces of artwork chosen in each corner. The grid of images between these corners represents the degrees of blending one image into another and applying the resulting style to a new photo. The middle image beings the result of an equal mix of all four pieces.

Figure 3. Google AI's Style Transfer model. Four original pieces of artwork (one in each corner) combined in gradients of proportions to produce a new photograph.

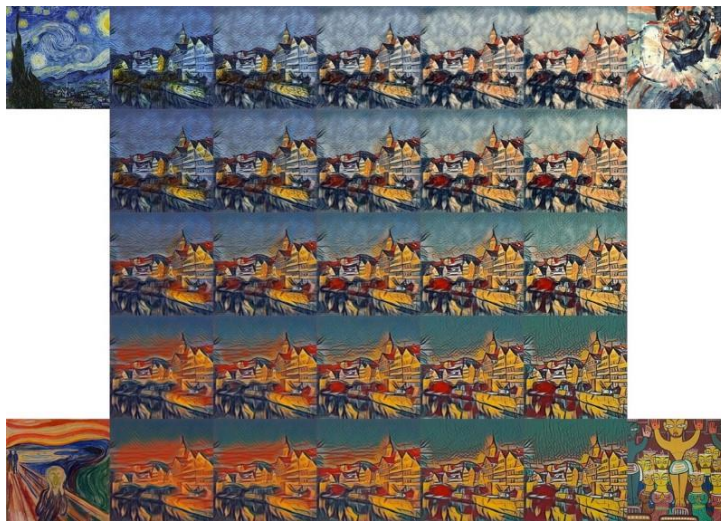


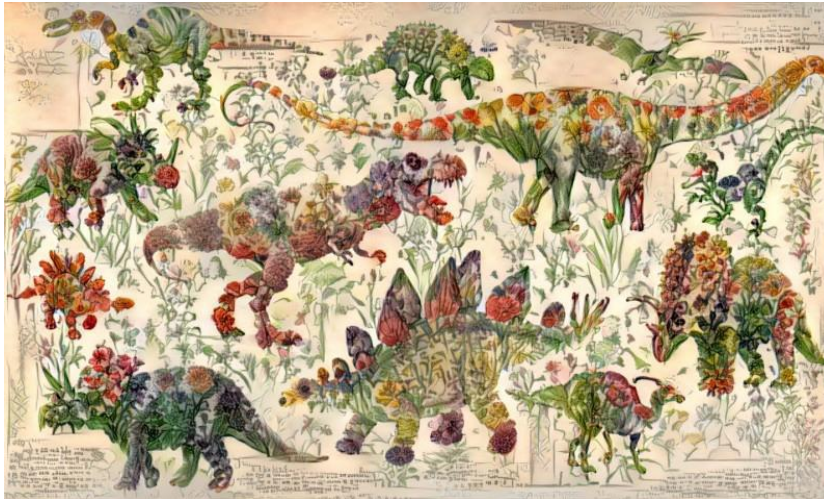
Figure 4. The original photograph of Tübingen Google applied the blended styles to.



The use of AI to impersonate and remix artwork has had varying degrees of "artistic" success, from this "Dinosaur x Flower mash-up" by Chris Rodley that went viral, to the more common psychedelic looking examples can be found all over Reddit⁵.

⁵ https://www.boredpanda.com/dinosaur-flowers-fruits-vegetables-artificial-intelligence-art-chris-rodley/?utm_source=google&utm_medium=organic&utm_campaign=organic (8 Sept. 2018)

Figure 5. Dinosaur x Flower, by Chris Rodley



There are even stunning results of style transfer that begin to be perceived as original art in their own right, like the image below by the Reddit user vic8760, who combined a neoclassical portrait of Napoleon, and a High Renaissance painting of a crowd scene⁶.

Figure 6. Napoleon Bonapart A2 by the Reddit User vic8760



Another form of imitation similar to style transfer is the image-to-image translation, which can completely change the appearance a photo or video, allowing users to edit the image's context, such as time of day, season or weather.

⁶ https://www.reddit.com/r/artwork/comments/8gvyns/napoleon_bonaparte_a2_by_vic8760/ (8 Sept.2018)

Figure 7. Nvidia's image-to-image translator



1.3 AI's Perception as Artwork

What about AI's perception as artwork? A pioneer of AI and art, Tom White from London, will be presenting two provocative series. The first series starts from a simple drawing made by an algorithm. Then, an AI algorithm which was trained on photographs from Image Net, slowly transforms the initial sketch into an abstract representation of a physical object. This painting will not necessarily be recognisable to humans. The second series, a little more provocative, uses the same systems, but, instead, produces images that will generally be categorised as 'inappropriate' or 'having explicit content' by online image analysis AIs.

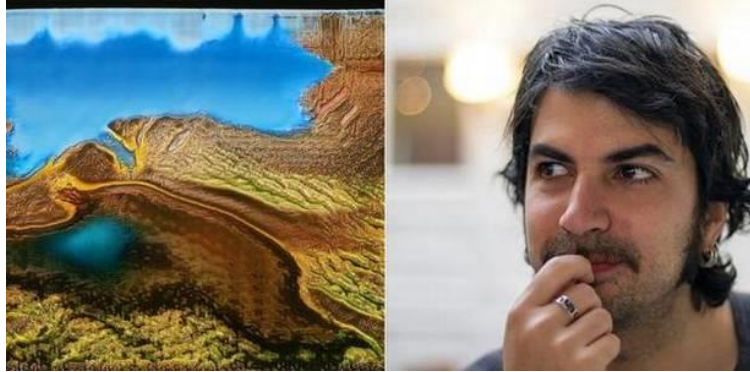
Figure 8. „Perception Engines” by Tom White



Turkish artist Memo Akten takes over the investigation, 'Learning to See', of how the experience or the memory of the machine affects what it sees and how it sees it. He describes it as "an artificial neural network making predictions on live webcam input, trying to make sense of what it sees in context of what it has seen

before.” He is also unveiling ‘Deep Meditations’, an extension of the aforementioned works, using machine-learning algorithms to create a two-hour meditative channel video and sound installation.

Figure 9. ”Deep Meditations” by Memo Akten



An example of taking AI perception to the next level is the ‘Imaginary Landscape’ by the Japanese artist Nao Tokui. As various objects are manipulated in front of the camera, the machine, trained only on specific sets of images (for instance, of beaches or flames) reinterprets these objects as instances of categories it knows. The eerie effect of seeing a mobile phone power adapter reinterpreted by the algorithm as a cliff by a beach is not one a viewer is likely to forget, perhaps causing them to wonder whether this is all of nature that will be left in the future.

Figure 10. „Imaginary Landscape” by Nao Tokui



1.4 Art + AI Tomorrow

What art has taught us about AI so far

Art is how we explore, who we are and who we want to become, as AI changes the picture of daily life.

Our whole notion of what defines something as "art" is going to change. It can help us understand more deeply what we want to communicate. It can change what we communicate by virtue of how we create it and who we create it with.

The questions we need art to help answer

We need art to imagine what AI can become, and understand its impact on who we are becoming. There's no denying that by giving machines the same abilities that inspired us to create art (memory, language, expression, understanding, reasoning, learning), it may, one day, decide to make art of its own.

Conclusion

Thanks to technology, the roles of the artist and the scientist, as well as their creative processes, are melding and the rigour of the resulting works is unbelievable. Our creativity has allowed our species to thrive, and, now, with machines having their own concepts of aesthetics, perception and creativity, it poses some important questions to artists.

The basis of AI-art can be summed up as generating a new and authentic art form by a computational system which models the human mind and creativity. Thus, in regard to the previous discussions about the authenticity and legitimization of AI-art, the thesis suggests that it is possible to consider AI-art as an 'autonomous art genre'. The autonomous aspect of the genre is due to its modeling of human art and the qualification of human perceptions. The evaluation of AI-art is still bound to human emotions and human taste of aesthetics. Nevertheless, it is a different art form which has computational features. It is a genre that combines the human aesthetic, human culture and analog features of the human mind, with the computational system and digital features of machine intelligence. Hence, while it is based on the model of the human cognitive system of creativity, it presents an idiosyncratic style owing to its computational features.

Therefore, when evaluating AI-art, attributing it as an autonomous art genre would provide a better understanding of AI-art as a concept and a field of research. Furthermore, classifying AI-art as an autonomous genre would make it easier to describe and evaluate the AI artworks. It would also mean endorsing the entitlement of AI-art as a creative industry. AI-art is already a creative industry which has ranged far beyond the computer labs and reached into art galleries, film festivals, music industry, and literature.

Bibliography

1. Leon A. Gatys, Alexander S. Ecker, Matthias Bethge, A Neural Algorithm of Artistic Style, Werner Reichardt Centre for Integrative Neuroscience, 2015
2. Xavier Alameda – Pineda, Elisa Ricci, Yan Yan, Nicy Sebe, Recognizing Emotions from Abstract Paintings using Non–Linear Matrix Completion, The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 5240-5248
3. Divya Kala Bhavani. Gradient Descent: when Artificial Intelligence meets art, 2017
4. Blaise Agüera y Arcas. Art in the Age of Machine Intelligence. In *Arts*, volume 6, page 18. Multidisciplinary Digital Publishing Institute, 2017
5. Ed Burton. Representing Representation: Artificial Intelligence and Drawing. *Computers & Art*, 2007
6. Margaret A Boden. Creativity and Artificial Intelligence. *Artificial Intelligence*, 103(1-2):347–356, 1998.
7. Margaret A Boden. Authenticity and Computer Art. *Digital Creativity*, 18(1):3–10, 2007.
8. Blaise Agüera y Arcas. Art in the Age of Machine Intelligence. In *Arts*, volume 6, page 18. Multidisciplinary Digital Publishing Institute, 2017.
9. Ed Burton. Representing Representation: Artificial Intelligence and Drawing. *Computers & Art*, 2007.

ХОЛОГРАФИЈАТА КАКО ТРОДИМЕНЗИОНАЛНО НИВО НА ФОТОГРАФИЈА

UDC: 535.421:004.946]:77.03

*Прегледен труд***М-р Самоил Крстевски***Европски универзитет – Република Македонија - Скопје*

Апстракт

Холографијата е наука за изработка на холограми односно на напредна форма на фотографија со слика на екранот во три димензии, т.е. методи на репродукција и создавање на тродимензионални слики на фотографската плоча со примена на кохерентна светлина (ласерски).

Холограмите се познати кај нас од научно-фантастичните филмови како што се Свездени патеки, Војна на свездите итн.

Предмет на трудот е целосно запознавање со сите аспекти на холографијата и определување на основите на развој на оваа наука.

Очекувана цел на трудот е да се утврдат придобивките од холографијата во различни сфери на интернет-просторот.

Клучни зборови: холограми, интернет, фотографија, ласер, светлина

THE HOLOGRAPHY AS A TRIDIMENSIONAL LEVEL OF PHOTOGRAPHY

Abstract

Holography is a science of making holograms, that is an advanced form of photography with a screen image in three dimensions, methods of reproduction and creation of three-dimensional images on the photographic plate using coherent light (laser).

Holograms are familiar to us from science fiction films such as Star Trek, Star Wars etc.

The subject of labor is a complete introduction to all aspects of holography and the determination of the foundations for the development of this science.

The expected finish of the work is to determine the benefits of holography in various spheres of the internet space.

Keywords: holograms, internet, photography, laser, light

Вовед

Холографија е наука која се занимава со креирање холограми - понапредно ниво на фотографија која ви овозможува да ја снимите фотографијата во три димензии.

Холографијата е метода за изработка и репродукција на тродимензионална слика. Употребува ласерска светлина за да ги снима моделите на светлосните бранови рефлектирани од објектот на емулзијата на светлосно сензитивниот филм (или стаклена површина).

Кога филмот бил развиен и повторно изложен на ласерско светло (или нормално светло, како повеќето холограми денес), повторно ги креира - во просторот - сите точки од светлото кои првично потекнуваат од објектот.

Како резултат пред или по холографскиот филм, сликата ги има сите димензии на оригиналниот објект и изгледа толку реално што тие со искушение сакаа да посетнат и да го допрат - само за да го најдат таму, но ништо не ја фокусира светлината.

Холографијата потекнува од грчкиот збор **холос** што значи целосен, целосно и **графос** што значи пишувам, да привлече.

Холографијата е техника која овозможува да се фотографира предмет со тоа што еден ласер ќе се раздели на два посебни.

Првиот зрак се одбива од предметот што се снима, а тогаш на вториот му се дозволува да се судри со рефлектираната светлина од првиот.

Тие создаваат интерференциски ефект, кој се снима на парче филм.

Кога низ таквиот објект ќе помине ласерски зрак, се појавува тродимензионална слика на предметот што бил фотографиран, наречена холограм. Тродимензионалноста на таквите слики е застрашувачки уверлива.

Холографот бил измислен во 1948 година од унгарскиот физичар д-р Денис Габор.

Во 1971 Габор доби Нобелова награда за физика. Првите холограмски прикази на 3Д-слики биле направени од Емет Лејт и Хурис Упатијекс во Мичиген, САД, во 1963 година и Јури Денисјук во СССР. Првите холограми биле трансмисииски холограми кои настануваат со помош на ласерски зраци, а подоцна "виножито трансмисија", холограми кои настануваат со помош на белата светлина.

И денес такви примери наоѓаме кај кредитните картички како заштита од фалсификување и при пакување на производи.

Денисјуковиот холограм е вистинскиот холограм на рефлексија на белата светлост кој е произведен така што сликата е реконструирана природно употребувајќи ја светлината од истата страна на холограмот од која е и набљудувачот.

Еден од напредоците кој најмногу ветува во кратката историја на холографите се масовните производства на евтини ласери, најчесто употребувани во милионите ДВД-уреди и во други примери, но понекогаш се корисни во холографијата. Овие евтини, компактни ласери можат многу добро да им конкурираат на големите и скапи ласери.

За разлика од фотографијата, холографијата може да овозможи предмет со целосна димензионална вредност. Холограмот креира со твоите очи да видиш - длабочина, форма, текстура и релативна позиција на многу точки на гледање.

Постојат два типа на холограми - рефлексија и трансмисија. Може да се разликуваат по начинот на кој тие се осветлени.

Рефлексионите холограми се осветлени однапред, рефлектирајќи ја светлината од вас како што вие ја гледате сликата или цртежот обесен на ѕидот. Различни емулзии на филм создаваат слики со различни карактеристики како што се:

-Првата *силвер халиде* е емулзија за повеќето уметници и холографери употребувајќи стаклена површина од сребрен халид за да постигнат највисок квалитет на сликата.

Холограферите исто така употребуваат филм од сребрен халид кој е поевтин, помалку кршлив и полесен за употреба, но не ја дава длабочината, резолуцијата и проекцијата е можна со стаклена плоча.

Како и да е, филмот е успешно употребен да произведува повеќе работи.

-Вториот (*dichromated gelatin DCG*) - *дихроматски желатин* е мешан, исушен желатин кој е обложен со парче од стакло. ДЦГ произведува многу светли слики во златножолта боја.

Сликите имаат минимален степен на длабочина, но тие се видени во нормална собна светлина, без специјални рефлектори. Ова го прави погодно како мал подарок дихроматиден производ за потрошувачот во маркетите, или премијата и за индустријата во пораст.

ДЦГ многу се заменети од страна на поевтините масовно произведувани фотополимерни холограми. Медиумите сèуште работат најдобро за дифрактивна оптика со високи перформанси и најверојатно ќе работат за подолго време. Светлите, чисти ДЦГ сè уште се користат кај фотополимерите за копирање.

Од 1975 до 1984 Рич Ралисон (International Dichromate Corp., Draper, UT), првично го воведо производството на двострани, стаклени дихроматски холограми кои беа употребувани како накит, приврзоци, тежина за хартијата и други производи. Тој ги произведе овие различни величини на дихромати од страна на Џејсон Сапан (Jason Sapan, holographic Studios, NJC in 1978-79.) во 1978-79 година.

-Третите фотополимерни материјали се најновите снимања. Развиени од страна на Полароид и Дупонт, фотопластичните полимери имаат поддршка и се погодни за производство на долги стази.

Длабочината на сликата на фотополимерите е малку помала отколку таа на силверхалидот, но сликите се посветли, со поширок агол на гледање. Трансмисијските холограми се осветлени одзади (како фотографска транспарентност), светлото го подава холограмот во вашите очи за да ја формира сликата.

Првите ласерски трансмисиони холограми се направени со ласери, како и сите холограми, но мора да бидат осветлени од ласерите за да можат да бидат видени. Затоа, сликите кои се појавуваат во бојата на ласерското светло се употребени за да ги видат нив, најчесто во црвена боја (хелиумско-неонски ласер).

Други видови холограми кои користат ласерска трансмисија се оние од кои копиите се направени. Ова е најновата форма на холограм развиен од страна на Leith и Упатникс во 1962.

Вторите трансмисиони холограми со бела светлина се од обично светло (бела светлина) и произведуваат

слики кои содржат спектар на бои од виножито. Ја менуваат бојата како што гледачот се помрдува нагоре и надолу и најчесто се нарекувани “виножито холограми”.

Холограферите развија значајна контрола над боите на екранот на овој тип произведени холографски слики во боја или приближно целосно природна боја.

Одредени поими кои се користат во холографијата

Амплитуда - висина бран или длабочината низ бранот, е мерен од средната точка

Разделувач на зраци - уред кој се користи за да се раздели светлината од ласерот во два посебни снопа - референтен и објективен снап на зраци. Се состои од делумно транспарентно огледало кое рефлектира дел од ласерскиот снап и ги поминува останатите.

Кохерентна светлина - светлина која е со иста фреквенција и во вибрирачка фаза. Ласерот произведува кохерентна светлина.

Филм - дали фотографски или холографски филмот се состои од светли сензитивни хемикалии (за емулзијата) кои се распрскани на површината. Филмската резолуција ја мери способноста за разликување помеѓу деталите. Бидејќи холографските филмови мора да бидат способни да снимаат детални информации, ја имаат моќта да ги решат 50 или повеќе пати отколку фотографскиот филм. Тие бараат или изложување на високопулсирачка јачина или постојано изложување на ласерски долги бранови. Холографскиот филм е развиен на начин сличен на фотографскиот филм со потопување во серија на хемиски агенси.

Холограм - медиум за свиткување или фокусирање на светлина. Го користи мешањето на монохроматски објекти и референтни бранови за да снима и пушта повеќе дводимензионални слики од дводимензионалниот поглед. За разлика од фотографијата која ја снима сликата како што е видена од еден аспект, холограмот е запис на слика која е видена од многу гледишта.

Ласер - акроним за “засилувачка светлина од стимулирана емисија на радијација”. Ласерот е уред кој произведува концентриран снап на кохерентна светлина. Некои, наречени ласери за континуирани бранови, продуцираат континуиран снап на светлина. Други, наречени пулсирачки ласери емитираат повеќе светлина во кратки импулси што се способни да го замрзнат движењето.

Леќи - кои го променуваат правецот на светлината. Во фотографијата леќите се употребуваат за да се фокусира сликата на филмот. Холограферите ги употребуваат леќите за да го издолжат ласерскиот снап за да го осветлат целиот објект кој ќе биде холографиран.

Цел на снопот - светлината од ласерскиот снап која го осветлува објектот и го рефлектира холографскиот филм.

Фаза - позиција на бранот во просторот во конкретен момент на време.

Сноп на ласерска светлина е оптички поделен на два снопа. Едниот референтен зрак е насочен кон парче на холографскиот филм (неговиот дијаметар е зголемен) за светлината да го покрие филмот и потполно

да е еднаков. Вториот сноп на зрак е насочен кон субјектот на композицијата и слично е проширен за да свети. Кога зракот од објектот се одбива, од објектот ја носи со себе информацијата за локацијата, големината, формата и текстурата на објектот. Некој од овие рефлектирани зраци од објектот потоа го сретнуваат референтниот сноп на холографскиот филм, мешајќи го произведениот модел кој е сниман на светла сензитивна емулзија.

Холографите го употребуваат во основа истиот вид на филм и развивач како и фотографите. Стандардниот силверхалиден филм (или стаклена површина) е сличен на тој што го употребуваат фотографите, но е побавен и бара подолго време на изложување, добра резолуција, и е многу осетлив на црвена светлина. Вклучува процесирање на истиот развивач, хипо и фиксатор кој се употребува кај фотографијата. Избелувачот се употребува за да се осветли сликата и други егзотични хемикалии се употребуваат привремено за да се намали или зголеми емулзијата со цел да се контролира бојата на сликата.

Кога ќе се развие филмот, холограмот е осветлен од истиот агол како и референтниот зрак за време на оригиналното изложување за да се открие 3Д-слика.

Холограмот мора да биде осветлен за да произведе слика. Иако се употребува ласерска светлина за да се направи холограм, тие обично се направени од нормални светлечки рефлектори. За да се видат холографските слики, гледачот мора да гледа на филмот, проектираните слики се појавуваат во просторот помеѓу филмот и гледачот.

Не постои моментална технологија која ја дава можноста да се почне со фокусирање на антената или на сликата во отворен простор без ставање на одредени типови на екран како што е чадот, или конкавни огледала. Сликите можат да бидат проектирани од филмот до далечна точка. Холограмот може да продуцира реална или виртуелна слика во просторот, но само кога е погледана низ или рефлектирана од физичкиот филм.

Разликите помеѓу холограм и фотографија ќе ги објасниме ако прво објасниме што е црно-бела слика. Всушност, тоа е точка по точка снимање на интензитетот на светлосниот зрак што ја дава сликата. Секоја точка од фотографијата снима само една работа, а тоа е јачината на светлосниот зрак што ја осветлува една одредена точка.

Кај фотографијата во боја многу повеќе информации се снимаат (во пракса разликата се снима три пати гледана во три различни филтри боја).

Тоа овозможува ограничена реконструкција на должината на светлината, а со тоа и својата боја. Покрај тоа, светлината нема само амплитудна и бранова должина туку има и фаза. Во фотографијата фазата на светлинската е изгубена. На холограмите се забележува и амплитуда и фаза на светлина, конкретно бранова должина.

Кога холограмот е конструиран, како резултат на светлината, светлосното поле е слично на она кое произлегува од оригиналната сцена давајќи совршени тродимензионални слики (иако во повеќето случаи монохроматски, но се можни и холограми во боја).

За снимање на фазата на светлинскиот бран на одредени точки на сликата, холографијата користи

референтни зраци комбинирани со светлинска сцена или објект (објект-светлина). Оптичката интерференција (супер позиција на бран) помеѓу референтниот зрак и објектниот зрак поради супер позицијата на светлосните бранови произведува серија на линии на интензитет, кои можат да бидат снимани на стандардниот фотографски филм. Тие линии формираат еден вид на холограм.

Заклучок

Холографијата е метод за изработка и репродукција на тродимензионална слика која употребува ласерска светлина за да ги снима моделите на светлосните бранови рефлектирани од објектот на емулзијата на светлосно сензитивниот филм (или стаклена површина).

Холографијата може да овозможи целосна димензионална вредност. Холограмот креира со нашите очи да видиме длабочина, големина, форма, текстура и релативна позиција на многу точки на гледање.

Значи, холографијата е наука за иднината, можностите се многу големи и таа зависи од техничките можности.

Холографијата има широка примена, денес таа се применува во забавната индустрија, во уметноста, во музиката, во медицината, со еден збор во секојдневниот живот на човекот.

Литература

1. G. Berger et. al, Digital Data Storage in a phase-encoded holographic memory system: data quality and security, Proceedings of SPIE, Vol. 4988, p. 104-111 (2003)
2. Optical holography: principles, techniques, and applications P. Hariharan, Cambridge University Press; 2 edition (1996), ISBN 978-0521439657
3. Principles of holography H. M. Smith, Wiley (1976)
4. Холографски универзум Мајкл Талбот, Аквариус Пет, Скопје, 2009, ISBN 978-608-4502-18-0
5. E. Hecht, Optics, ISBN 0-201-30425-2
6. <http://mk.wikipedia.org/wiki/>
7. <http://holophile.com>
8. www.holoworld.com
9. www.holoforum.com
10. www.holodisks.com
11. www.foobarsoft.com/holograms/single.html
12. <http://www.caesar.de/holographyandlaser.0.html>

TRANSFORMABLE LIVING UNIT – HOMO–CYBER–SAPIENS – IDENTITY OF PLACE AND ARCHITECTURE OF EMOTIONS

UDC: 728.1.012.183-027.39:004.8/.9

Original scientific paper

Katarzyna Utecht, PhD

Faculty of Visual Arts, Academy of Art, Szczecin | Poland

Abstract

The living space should be open during the daytime and more private and closed off during the evening in order to feel safe there. The domicile should easily adapt to family's needs, it should be dynamic, should enliven and move, and should change like the scenery during the performance. The flat may be adapted to the needs, the age and the lifestyle of occupants and the change of decoration.

The spaces easy to transform and change are the future of the housing. We should be in control of the flats we live in and they ought to respond to our needs and feelings. All mentioned in the research features and functions of the floor surface are particularly emphasized in the flats with limited space and floor surface (micro-domicile). In this research work, it should be emphasized that the multi functionality of the living quarters shows the complexity of the functions and the processes that lead to comfort in the domicile. The consciousness of the existence of these processes is the mirror of the social dimension – the logic of the mechanisms in the flat; as the primary indicator of internal designing is the human. All these qualities served to design a domicile module with the minimum floor surface, but, with the remaining, all needed normal development and existence functions, including the division into zones.

The subject work is an attempt to collect and order the processes that occur in the flat with the reference to small domiciles simultaneously with the merging and the mutual relations of the zones in the space. The above deliberations find the reference to the changes of the modern human behavior.

The research is an attempt to collect and order the processes that occur in a flat with reference to small domiciles simultaneously with merging and mutual relations of the zones in the space. The above considerations find a reference to changes in the modern human behaviour. It should be emphasized that the multi functionality of the specific living quarters shows the complexity of functions and processes that lead to the comfort in the domicile. The consciousness that these processes exist is the mirror of the social dimension – the logic of the mechanisms in the flat; as the primary indicator of the interior design is human. All these qualities served to design a domicile module with the minimum floor space but with all the remaining functions needed for normal development and existence including the division into zones. An attempt has been made to focus on the psychological aspect of the influence of the limited domicile space (the floor area); this means introducing the issues concerning improvement of the design of minimum interiors so that they should suit the physiological, psychological and social needs of human beings.

Keywords: *emotions, housing, human needs, living unit, module, transformation, multifunctionality.*

MODULE – MULTIFUNCTIONALITY

Fig. 1. Habitation module of homo cyber sapiens

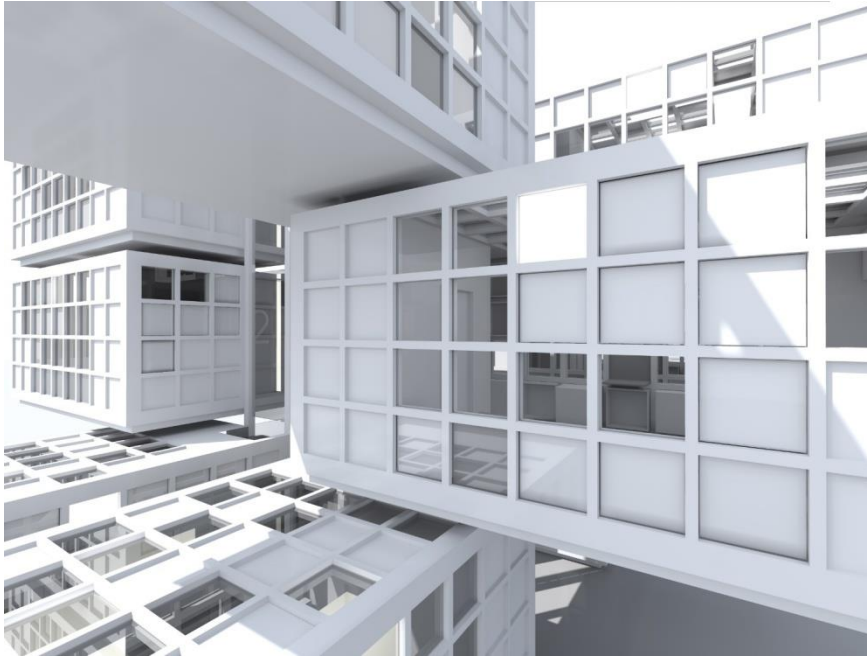
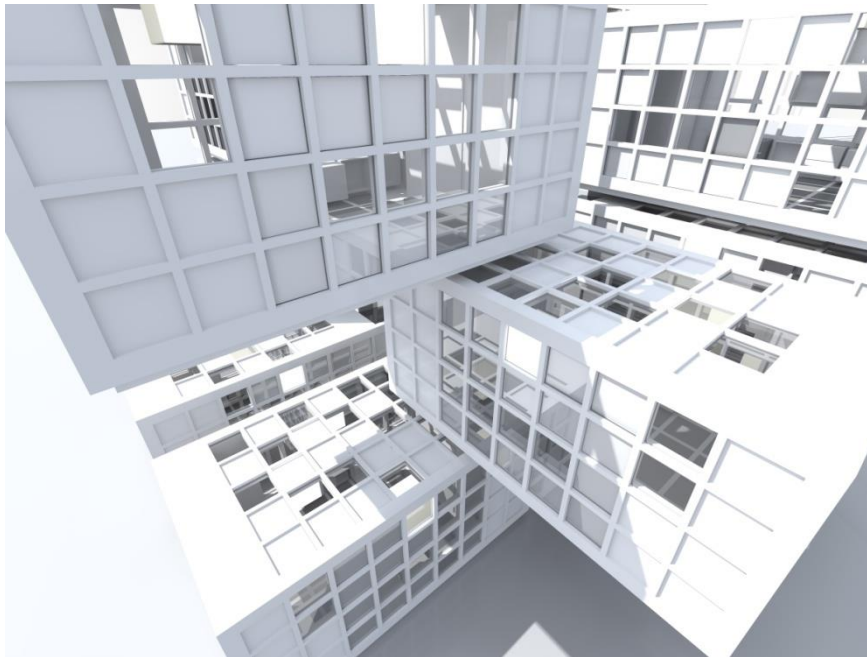


Fig. 2. Habitation module of homo cyber sapiens



The evolution of the psychophysical and sociological human needs has the greatest impact on the function of the dwelling and its individual zones. Therefore, we should allow recipients of the minimum housing area to

choose of the modules that perform various functions, as well as to transform them. Since everybody is different, it can be assumed that needs concerning lifestyle, work and rest are different, too. Transformation and awareness that functions can be changed when a need arises give the user a sense of comfort. This facility, as well as the selection of modules needed, will allow users to perform the synthesis and analysis of what they expect from the apartment. It will make them think about their needs. The size of a given space does not depend on the multiplicity of functions contained therein, but on the type of the user's needs. By enabling a change of the arrangement, com-binatorics and composition, we leave it to the recipient to decide on the destination of the space. Each module will be designed universally, taking into account the ergonomics and meeting the needs of users. By that, we also allow the user to invent or add new values to multifunctional modules. Moreover, the user who creates his or her own set of furniture designs a new spatial and compositional value and is able to match the set of furniture to his or her needs, and with their transformation, change their layout.

Fig. 3. Habitation module of homo cyber sapiens

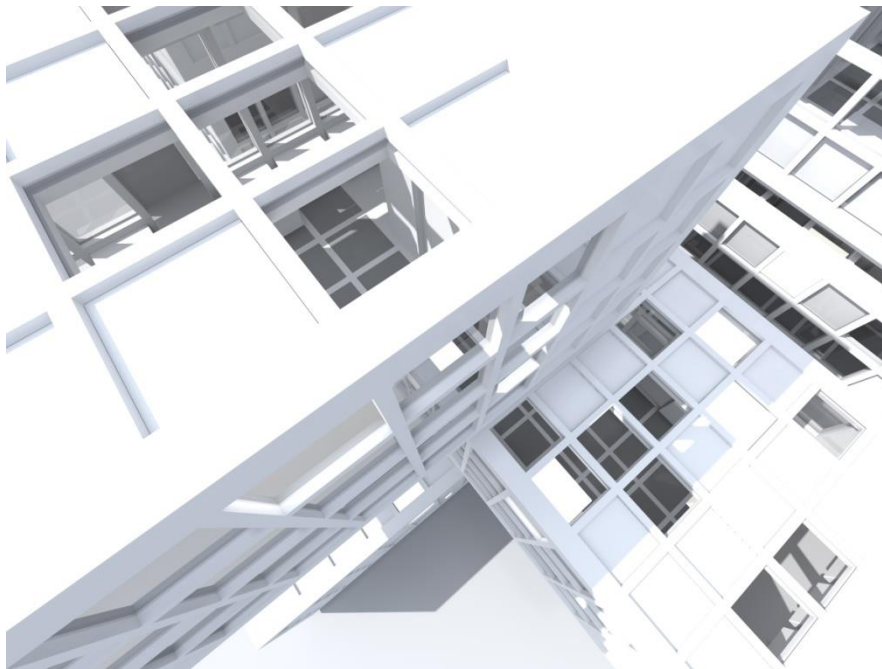


Fig. 4. Habitation module of homo cyber sapiens



MATERIALS – PERCEPTION

Human senses – as the main determinant of the perception of the interior – the knowledge and the way in which they function, as well as learning about the fields in which they operate, are an important condition for the design and dimensioning of all spatial forms in the living area. The factor that is fundamental in designing living units is the natural reception of the interior, which is done through visual, tactile and auditory stimuli. This is related to the most common type of social activity. To understand all forms of spatial and human perception and the reception of dimensions, we need to learn about senses, which is a necessary condition for planning the living area. Organization and interpretation of sensory impressions in order to understand and learn about environment, as the factors of subjective perception of the interior, become very important. Perception is a conscious sensory response to the external stimulus, the way of reacting and receiving sensations. The sense of awareness of the surroundings is related to imagination and intelligence. Human perceptual systems allow the reception of living space, as well as the materials used in it, such as furniture or walls. Their sensory reception allows us to understand response mechanisms and reactions to stimuli. Sensory perception, selecting, organizing and interpreting are the stages in the process of perception. It is not just about the colors or about them lacking, but also, about the structure and texture of the object. The user should intuitively sense the purpose of the module thanks to the used materials and their colors.

Fig. 5. Habitation module of homo cyber sapiens

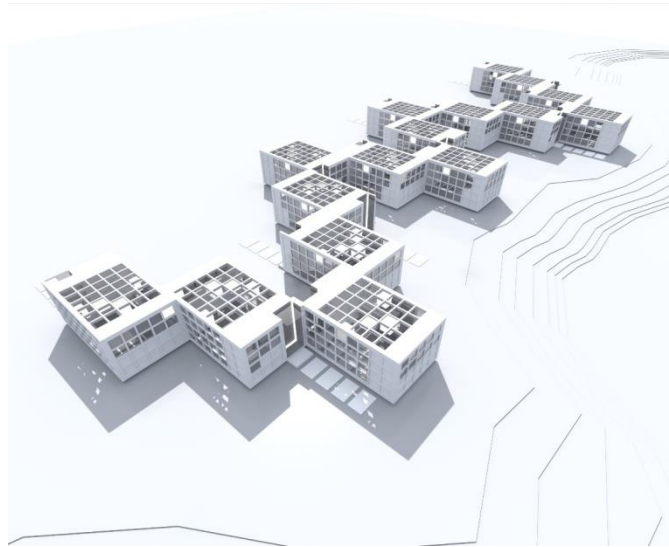
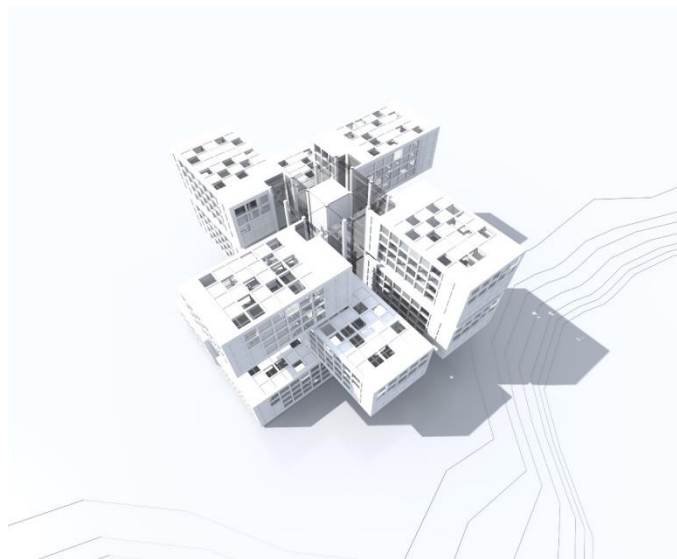


Fig. 6. Habitation module of homo cyber sapiens



MOBILITY – TRANSFORMATION

The functional layout of an apartment should change with the development, age and life of users, transforming their structure to meet the needs and preferences of the people living there. The proper layout of the apartment allows far-reaching changes in the functional layout, as well as their transformation in order to meet the needs of the family. Transformation takes place within the space of the unit; it is the individual modules and the possibility of their transformation that shape the interior of the dwelling unit. The ability to swap, shift or unfold a given module gives the prospect of a surplus surface. What we have in mind is the reserve of the living space that the recipient of such an apartment can, at any moment, obtain in an easy and inexpensive way. There are situations where the reserve space has been used and we feel overwhelmed in the apartment; we can change

this by changing the individual modules. In this context, it is reasonable to define the fundamentals of creating a residential module. In my opinion, looking from the perspective of interior architecture, the size of the module should be a reference to the furnishing of the dwelling, namely, the accepted and widespread norms and dimensions of furniture, kitchenware and other interior fittings, which generally are a basis of dimensions of 60 cm in width, which is, actually, multiplied. Using such multiples of the number allows one to create modules based on that, which, on the one hand, allows to unify the living space, but on the other hand, what is more important, allows for it to be freely adjusted.

Fig. 7. Habitation module of homo cyber sapiens

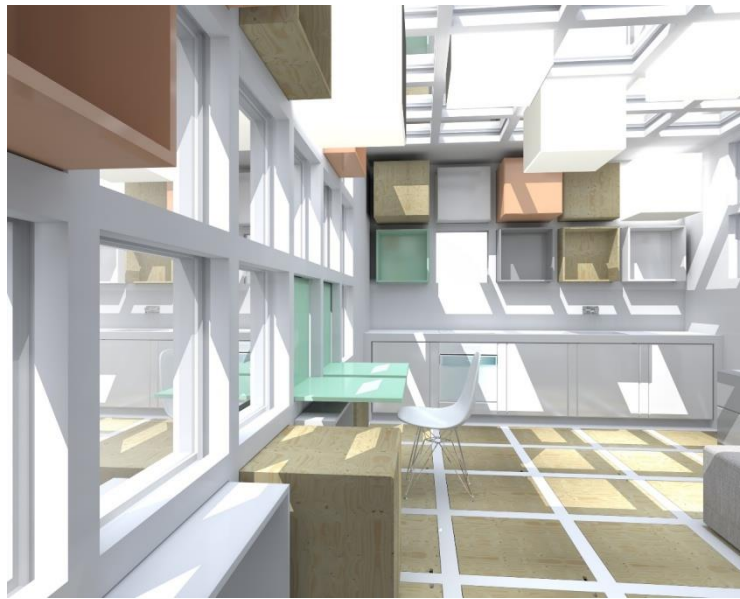
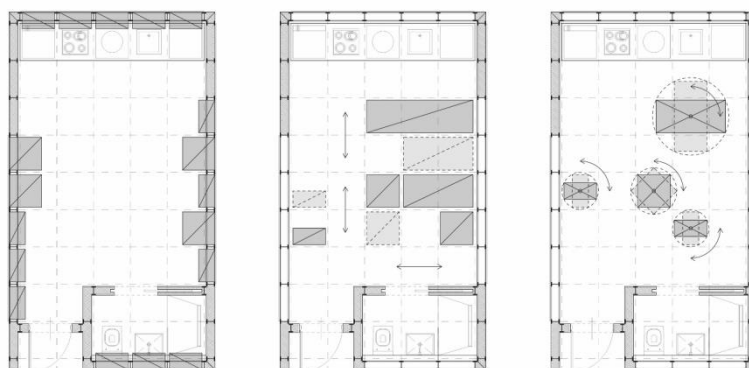


Fig. 8. Projection of the habitation module



HUMAN NEEDS – MOTIVES

The human relation to living space can be considered on two levels; purely utilitarian, where it serves as a means of satisfying the daily needs that have been described extensively in the second chapter of the paper, and

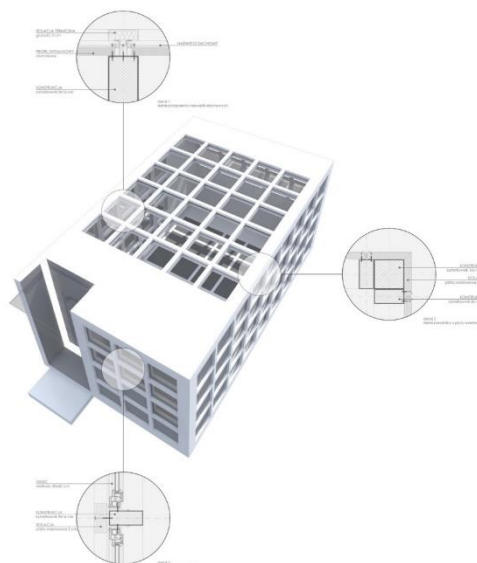
in terms of emotional sphere, where the dwelling is a micro-environment for the user and is shaped according to his or her preferences, tastes, and likes, becoming a part of the personality and an important element of the person's life. The role of housing is the reciprocal proportion of these two meanings; it is a variable and depends on the degree of fulfilling user's needs with respect to the dwelling. With minimal living space, the options of flexibility, adjustability to human needs, and changeability create a desirable direction in the process of shaping living spaces.

In today's world, we can observe a tendency to change the structure of the character and function of the interior into one that will allow the user to transform it quickly and, thus, change its functions in a relatively short time without any extra work. This is due to the fast pace of life, lack of time and the frequent changes in the human needs during the day. Within the minimal living space, where space, or rather its lack, plays an important role, it is obvious that every surface should be designed with special respect in order to be useful. When designing microflats, we should prevent situations when given space is misused and consequently wasted. The change in the aspect of space gives its users a prospect of modifications. It gives the user not only the sense of security in the form of the option of finding another way of using the space, but also a sense of sensible use of space.

In the process of shaping a private space, there are four directions a designer should consider when designing a space with a minimum surface area – human needs and motives, that is a factor that motivates a person to be active, furniture modules which can offer many functions, materials, or rather their differentiation helping in their perception and influence on a person, and finally mobility with transformation, i.e. the possibility to introduce changes and adaptations.

The subtle relation between human behavior and the surrounding spatial arrangement of the interiors and processes that take place between them influences the later reception of the space in which we live. Not only does space have a significant impact on us, but also location and innovative architectural solutions consciously affect recipients and their various behaviors, and the transformation of individual modules gives the user the option to introduce any adaptation within the living space.

Fig. 9. Detail of the habitation module



BIBLIOGRAPHY

- Arnheim R., *Sztuka i percepcja wzrokowa*, trans. J. Mach, pub. słowo/obraz terytoria, Warszawa 2005.
- Brucka B., *Zasady społeczne projektowania osiedli mieszkaniowych*, Publishing of the Ministry of Reconstruction, Warszawa 1948.
- Gehl J., *Życie między budynkami. Użytkowanie przestrzeni publicznych*, Pub. RAM, Kraków 2013.
- Goryński J., *Mieszkanie wczoraj, dziś i jutro*, pub. Wiedza Powszechna, Warszawa 1975.
- Gropius W., *Pełnia architektury*, trans. K. Kopczyńska, pub. Karakter, Kraków 2014.
- Hildner C., *Contemporary Japanese Dwellings – Small houses*, Birkhäuser GmbH, Basel 2011.
- Starska M., Wiener D., Klawiter A., Hridegger M., *Komunikacja. Pogłębienie poczucia przestrzeni*, pub. Fundacja Bęc Zmiana, Warszawa 2009.