Polish Political Science Yearbook, **vol. 49(3) (2020), pp. 134–148**
DOI: https://doi.org/10.15804/ppsy2020308 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Natalia Lewandowska
Adam Mickiewicz University, Poland
ORCID: https://orcid.org/0000-0003-2396-3048
email: nanalewandowska@gmail.com

Big Data – A Complex Analysis of Daily Attitudes as a Modern Inevitable Global Danger

Abstract: In the Fourth Industrial Revolution we already have robots, also there are such technologies as genetic sequencing and editing, artificial intelligence, miniaturized sensors, 3D printing and much more. Digital technologies are constantly being developed with new methods and have been implemented worldwide into various processes and automation systems. The article describes modern digitalization components and analyzes its possible threats. Along with an increase in life comfort, modern civilizations must face with cybercrimes based on data collection, including cyber thefts and hacker attacks. Globalization enables exchanging goods and services between countries of the world. It also gives a tool phishing and illegally access vulnerable information of global enterprises to compete unfairly. Although Big Data can be helpful among organizations, it can also be a mark of the inevitable danger worldwide.

Keywords: *Big Data, globalization, the Fourth Industrial Revolution, Industry 4.0, cybercrimes, digitalization, phishing*

Introduction

In the modern world the process of digitalization is highly developed. In the last 27 years the rate of individuals using the Internet (% of population in the world) has increased from 0.049% in 1990 to 48.565% in 2017. It is important to note that this ranking does not only include countries where Internet is being used commonly. In 2017 this was more common in Canada (93%), Denmark (97%), Finland (87), Iceland (98%), Monaco (97%), New Zealand (91%), Norway (97%), etc., then in small countries such as Eritrea (1%), Afghanistan (11%), Burundi (6%), Chad (6%), Liberia (8%), Pakistan (16%), Rwanda (22%)[1]. Within the

[1] Based on World Bank Group: https://data.worldbank.org/

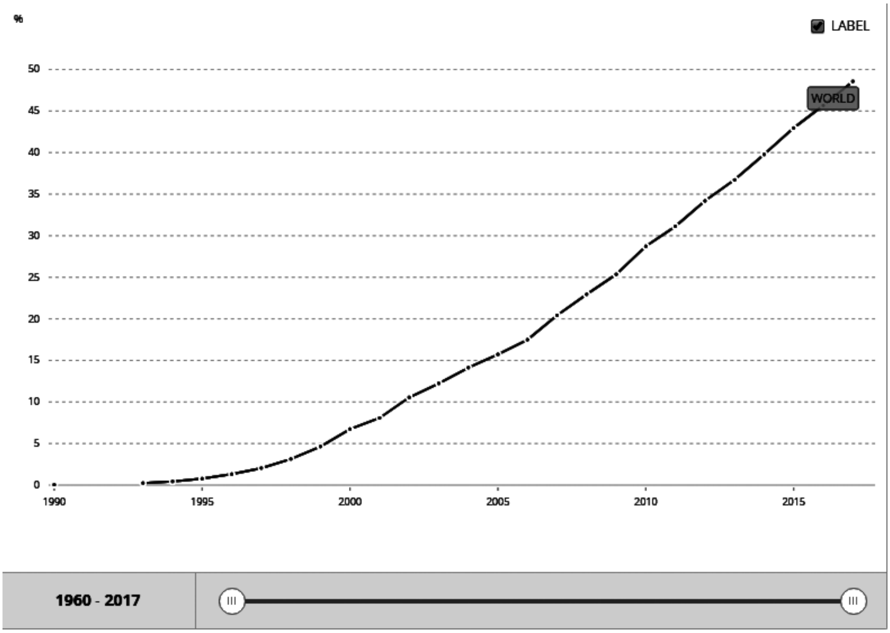


Fig.1. Individuals using the Internet (% of population)
Source: International Telecommunication Union, World Telecommunication/ICT Development Report and database, https://data.worldbank.org

21st century the Internet and Big Data became of utmost importance, which after a wider analysis can appear also as a treacherous challenge for governments.

Globalization is a process of exchanging goods and services between countries of the world, which enables the interaction and integration among people and governments. Globalization, as the word suggests, is not a political creation, but it is created by a developing economic trend. *Collins English Dictionary* refers to it as a "trend toward the existence of a single world market dominated by multinational companies" (*Globalization*, 2008). Due to the globalization process, the labor market is less constrained by national boundaries. As with any other complex process, there are pros and cons. The most obvious pros are the gaining of new technologies and acceleration of development, which maximizes profits. On the contrary an increase in globalization also leads to the loss of local businesses as that are unable to compete with the much larger companies, such us Pizza Huts, McDonald's and Starbucks, unless those are able to adapt.

In relation to the developing world conditions, the wider consideration is inevitable, therefore the McKinsey Global Institute provided a "digital globalization" term, which it explains as follows: "like traditional globalization, however, digital globalization is threatened by a number of barriers and protectionist policies, such as data localization requirements, online censorship, market restrictions on digital content providers, and conflicting and overlapping rules on data privacy and protection. Although these policies are often adopted to address legitimate underlying concerns, they threaten to disrupt the flow of data around the world, imposing significant costs to companies and harm to consumers" (Lund & Manyika, 2017). The term 'digital' refers to innovation that connects technology, data, devices, design, and business strategy leading to enhancements in business process or customer experience. In the age of digital disruption, companies face increasing pressure to improve time to market, and deliver best in class solutions. Digital strategy focuses on creating a seamless, immersive, engaging, personalized and cohesive environment for the customers.

To collect, analyze and exchange information globally, Big Data is being using. Based on the online Cambridge Dictionary, the "Big Data" term is defined as very large sets of data that are produced by people using the internet, and that can only be stored, understood, and used with the help of special tools and methods[2]. It is also defined as three V's, which are Volume, Velocity and Value (Laney, 2001). That might be a helpful tool which is used for forecasting trade, manufacturing, healthcare, finance, tourism and even politics. All actions made by Internet users leave "footprints" on servers. That is the reason why each person receives personalized advertisements according to websites which she has visited. It definitely saves time during online research. Electronic device's users can also save time during typing text with smart suggestions, provided in relation to their previous messages. It is also a part of, and closely connected to the Big Data process, and is called Machinery Learning (ML). According to an article in *Journal of Big Data*: "when dealing with data analysis, ML is generally used to create models for prediction and knowledge discovery to enable data-driven decision-making" (Hariri et al., 2019). Taking the Machinery Learning together with Artificial Intelligence, Internet of Things, and eventually the Big Data all together, we can see foremost factors which form global trends in the modern, digitalized world. The question is: could the Big Data be a danger for democracy and social life?

The 4th Industrial Revolution – "Industry 4.0"

The First Industrial Revolution is defined as the age of mechanical production, and beginning around 1760, through the advent of the steam engine. By the early part of the 20th century were the age of science and mass production, the Second Industrial Revolution. Things started to speed up with a number of key inventions, most notably the assembly line, which effectively powered mass production, moreover: gasoline engines, airplanes, chemical fertilizer. Beginning in the 1950s, the Third Industrial Revolution brought semiconductors, mainframe computing, personal computing, and the Internet – the digital revolution. Things that used to be analog moved to digital technologies. The Fourth Industrial Revolution is

[2] Meaning of big data in English, https://dictionary.cambridge.org/dictionary/english/big-data

starting now. Already we have got robots, also there is genetic sequencing and editing, artificial intelligence, miniaturized sensors, and 3D printing, to name a few[3].

Smart manufacturing can improve production processes, increase efficiency and improve safety on the factory floor. The rise of Industry 4.0 has provided manufacturers with the opportunity to utilize advanced manufacturing capabilities and information technology throughout the product lifecycle. Digital technologies are constantly developing with new methods and have been implemented worldwide into manufacturing processes with computerization and automation of industry. In 2011, the German federal government published the high-tech strategy entitled "Industry 4.0", appearing also as the Fourth Technological Revolution. "The fourth technological revolution [Industry 4.0] (the term originated in Germany and can in many ways be labelled as [smart factories], [smart industry] or [advanced manufacturing]) refers to the implementation in production technologies supported by a variety of digital technologies (e.g. 3D printing, Cloud computing, ICT, advanced robotics) and new materials" (Karabegović, 2019). The main reasons supporting the idea of smart adjustment of industrial production by digitalization and automatization are to decrease costs and reduce the time by detecting errors that occur during the process, which becomes possible because of machinery learning. "Finally, the intelligent production can incredibly save the human resource and socially necessary labor time, reducing the consumption on repeating the essential work. The Fourth Industrial Revolution can thus save the resources, improve the production efficiency and eventually benefit the profits in economic growth" (Li et al., 2017). To take human resources in considerations, we should consider the role of robots in manufacturing, which are being developed to aid workers and support the system with their death-and-injuries-proofing, non-exhausting, and quick learning abilities. In the article scientist mentioned about industrial robots by saying: "Intelligent robots will completely replace the workers in the production process, and at the same time workers will work on more effective creative tasks" (Karabegović, 2019). This idea seems to be propitious, unless consider what is supposed to happen with previous employees. Blue-collar workers usually are neither qualified, nor skilled to work on more effective tasks. Production operator position is mostly holding by non-educated people, who do not have inspirations to take up more challenging tasks; and it is relevant to labor migration. Labor migration phenomenon concerns many EU Member States, e.g. in Poland being represented by Ukrainians workers, or in United Kingdom by Polish. Beside transnational examples, the problem exists also in China in the case of immigration of workforce form countryside to urbanized areas. If robots will replace those workers, solutions must be found to motivate people to develop themselves, give them tool to achieve new skills, and find a different job for them.

The mentioned benefits of automatization are also important goals of "Made in China 2025" strategy, which was recently presented in the "Report on the Work of the Government",

[3] New World Encyclopedia: Industrial Revolution, https://www.newworldencyclopedia.org/entry/Industrial_Revolution

delivered by Premier Li Keqiang at the Third Session of the 12th National People's Congress on March 5th, 2015 and adopted on March 15th in 2015. To ensure balancing steady economic growth and structural improvement, the Premier of the State Council formed goals such as increase effective investment in public goods including: projects of rebuilding dilapidated urban areas and renovating deteriorated houses, projects for upgrading traditional industries; also to develop smart cities. By aiming at a medium-high level in industrial structural upgrading, Li mentioned as following: "Manufacturing is traditionally a strong industry for China. We will implement the [Made in China 2025] strategy; seek innovation-driven development; apply smart technologies; strengthen foundations; pursue green development; and redouble our efforts to upgrade China from a manufacturer of quantity to one of quality" (Li, 2015). Afterwards he extends the role of new technologies and digitalization such us "We will ensure the development of some industries while restricting the growth of others, cut overcapacity, support business acquisitions and restructuring, and let market competition determine which business survive. We will promote the extensive application of information technologies in industrialization, develop and utilize networking, digitalization, and smart technologies, and work to develop certain key areas first and make breakthroughs areas" (Li, 2015). Developing production with an artificial intelligence's support is a great opportunity worldwide. With its ability to help alleviate many repetitive tasks, AI is changing the way in which humans approach work. Nevertheless, one of issues which also caused the modern trade war between China and USA is intellectual property, whereby the U.S. accused China of unfair trading practices including stealing intellectual property and favor domestic companies through subsidies (Palumbo, & Nicolaci da Costa, 2019). Robert G. Sutter mentioned in his book about obstacles in economic relations between U.S. and China which involves security, political, sovereignty, and foreign policy issues, and also "Chinese currency policies and practices, U.S. dependence on Chinese financing U.S. government budget deficits, and Chinese lax enforcement of intellectual property rights and wide use of industrial espionage targeting U.S. firms" (Sutter, 2013). The trade war between the world's two largest economies with billions of dollars tariffs imposed of various products effects on global business. The U.S.–China trade war has contributed to losses for investors on the global financial market and launched a great uncertainty all around the world.

Another potential of the Fourth Industrial Revolution are smart-cities technologies, which on the other hand also pose a social risk. Smart-cities use data collection and new technologies, which are orientated on delivery more efficient local services. "Indeed, connected sensors, satellite images, and widespread smartphones produce massive amounts of data that facilitate better mapping by remote sensing, gathering environmental and other city-related data, and citizen behavior data" (Arcila, 2019). The potential of these devices is visible whenever we see intelligent streets cameras that regulate lights according to the traffic and pedestrians' movements, traffic navigation maps, public transportation apps, parking space apps or bike, scooter, and car-sharing platforms. Surveillance cameras improve crime prevention and investigation. Particularly monitoring systems and algorithms pose risk. "Because algorithms that help policing activities often take information about former arrests and crimes to tell police officers where crimes are likely to occur in the future, the algorithms may end up reinforcing existing prejudices, such as that low-income people are more likely to be violent and consume or sell drugs" (Arcila, 2019). System could unfairly indicate and follow citizens from poorer backgrounds. Tracking and surveillance systems follow individuals' private life, collect private data, and provide reports to governments or even media. Therefore, social services and advertisements are adjusted with regard to interests and movement analysis. Thus, it is an obvious interference in individual's lifestyle and preferences.

Beside the fact, that China rapidly develops urban agglomerations, based on the International Telecommunication Union's report, in 2017 only 54% of individuals were using Internet in China. Another strategy relevant to "Made in China 2015" strategy, aims to merge industries and launch new types of businesses. "We will develop the [Internet Plus] action plan to integrate the mobile Internet, cloud computing, big data, and the Internet of Things with modern manufacturing, to encourage the healthy development of e-commerce, industrial networks, and Internet banking, and to guide Internet-based companies to increase their presence in the international market" (Li, 2015).

Data Collection

In regarding to the statistics about Internet users which were presented, we should mention what people use media for. The Digital Information World published results of its research in this topic for citizens of the United States. "The report explains that on average an American adult spends over three hours every day scrolling through their phone for different reasons. However, the leading reason still remains the use of digital media. This simply means that users are more indulge in social media networks which is the reason social media networks like Facebook are now offering money to the users to describe the usage of their app as well as the online habits of the users" (Saeed, 2019).

Social Media and platforms collect details about its users. "We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. It can also include what you see through features we provide, such as our camera, so we can do things like suggest masks and filters that you might like, or give you tips on using portrait mode. Our systems automatically process content and communications you and others provide to analyze context and what's in them for the purposes described below. Learn more about how you can control who can see the things you share" (*Data Policy*, 2019). Below is a short summary about Data Policy which describes the information they process to support Facebook, Instagram, Messenger and other products and features offered by Facebook:

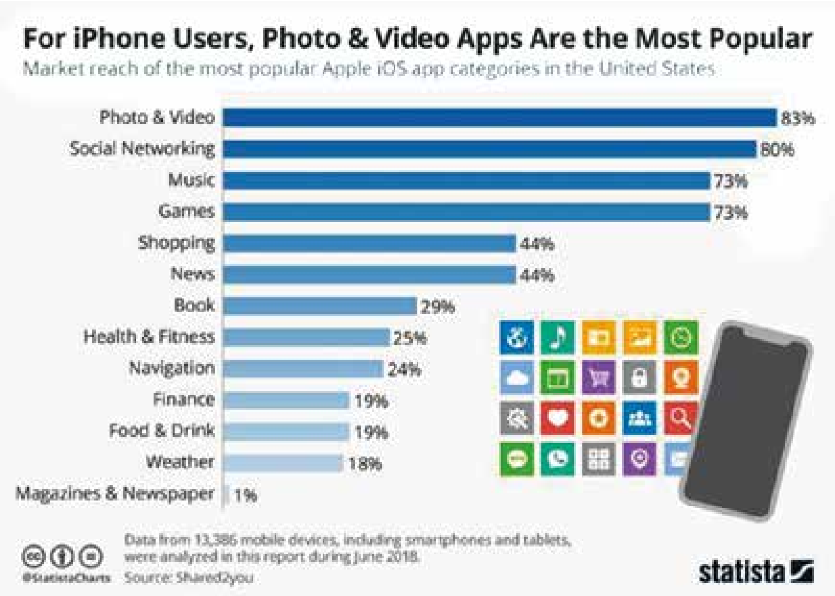


Fig. 2. The most popular app categories in the United States
Source: Digital Information World, 2019.

- Information and content you provide (created or shared content and messages),
- Networks and connections (information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them; s an address book or call log or SMS log history),
- Your usage (the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities),
- Information about transactions made on our Products (information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details),
- Things others do and information they provide about you (when others share or comment on a photo of you, send a message to you, or upload, sync or import your contact information),
- Device attributes (operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins),
- Device operations (whether a window is foregrounded or backgrounded, or mouse movements),

- Identifiers (unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts you use, and Family Device IDs),
- Device signals (Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers),
- Data from device settings (access to your GPS location, camera or photos),
- Network and connections (the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network),
- Cookie data (data from cookies stored on your device),
- Information from partners (information about your device, websites you visit, purchases you make, the ads you see, and how you use their services) (*Data Policy*, 2019).

Nowadays people are granted by unlimited access to scientific studies, economic analysis, and political news and entertainment sites. Available sources bring advantages to society, unless data is generated beyond any control. In fact, the issue is the amount of data we produce globally every single minute, and we have to face the difficulty how to detach the truth from fake news. COVID-19 originated in China in November 2019 spread worldwide within three months. This example gives us an opportunity to verify promises and observe how governments handle pandemic with the use of Big Data, and how media impacts on people's attitude. The European Centre for Disease Prevention and Control (ECDC) is in continuous contact with the European Commission and the World Health Organization regarding the assessment. Scientifics and politicians exchange intimations, research groups around the world are racing to create a vaccine and simultaneously share results of researches to each other. As mentioned on the official website that gathering questions & answers on COVID-19: "To inform the European Commission and the public health authorities in Member States of the ongoing situation, ECDC publishes daily summaries and continuously assesses the risk for EU citizens". Cooperation and sharing data related to the virus is necessary, and on the stage of fighting against the pandemic any action seems to be justified. The European Commission has been leaning on Europe's telecoms operators to share aggregate location data on their users. From the other hand, we have no guarantee that such tools will not be kept for future to track citizens and constrain their freedom. Authorities have a chance to implement sophisticated solutions for their benefits, for example Polish government wants citizens to be able to vote remotely during Presidential Election, which is against the Constitution of the Republic of Poland.

New Technologies and Big Data Analyzing

According to the Digital Revolution, basically, there are 10 emerging technologies driving this revolution forward. Technologies Changing the Physical World including: biotechnology, robotics, 3D printing, new materials, Internet of things and energy capture, storage, and transmission. Technologies changing the Digital World including: Artificial Intelligence, blockchain applications, new computational technologies and virtual and augmented reality.

Besides collecting databases based on online activity or personal preferences, it is becoming more and more popular to store measurements of aspects of the human biology. Biometrics involves fingerprints, facial proportions, iris scans, veins traits and characteristics of walking style. Modern devices are also able to provide voiceprint recognition, involving pitch and templates of vocal cords. Fast face detection might be invaluable in violent video scenes by identifying participants and report details to police, nevertheless the use of biometrics by governments and business is rapidly growing, though it is also seen by many as an invasion of citizens privacy and will inevitable cause a degradation of our freedom.

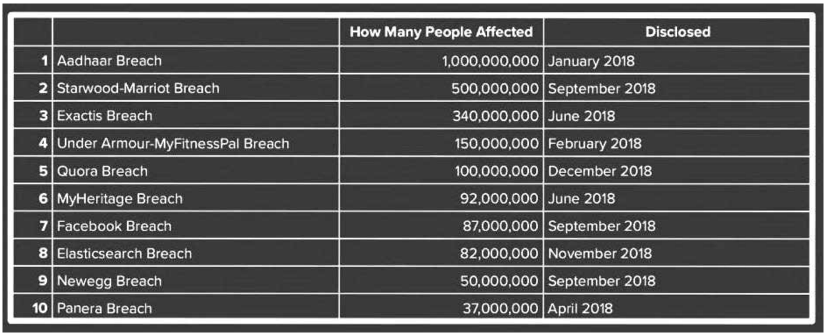
One of the disquieting examples on how private data can be used is the Sesame Credit System implemented in China as conducted by the government, whereby data is downloaded from the Alipay electronic payment scheme. In addition, the data is to be shared by WeChat (multi-purpose messaging, social media and mobile payment app), Tencent Credit (launches its own credit scoring system to rival Alibaba's), and Ant Financial Service Group (operates the world's largest mobile and online payments), which are subjected to the AliPay payment application affiliated with the Alibaba Group. In addition, fingerprinting databases, voice registers, facial biometric data and DNA codes for Chinese citizens are to be developed. Payments made with cards will also be registered in the system. In cases where another method is chosen, one will be required to show an identification, which also aims to record transactions in the system. On this basis, it will be easier to analyze whether a person regularly meets their financial obligations and, therefore, whether he or she will be a reliable borrower.

The street camera systems which have the function of facial recognition will allow it to determine the location of the citizens; and will enable them to be easily connected to the individuals accurately. Such a system will have the capability of facial recognition and will be able to identify with whom individuals are meetings and gathering and such date will be collected and analyzed and possible affect their overall score of such individuals. Such information is also valuable to the authorities. The basic assumption of the surveillance is justified by the use of the mentioned data by the authorities, and then the conversion of data into points. Then, the assessment will determine their chances on the labor market, access to a good school for children, the use of public transport, and even access to dating sites, social networks or internet games, admission to restaurants or theatres – diminishing number of points will be punished by a restriction to prestigious places or making it impossible to leave the city or country. The most painful punishment in the modern world may be slowed or completely blocked from the Internet.

Though the Chinese government is the most obvious at keeping a close eye on its citizens, many other countries such as Saudi Arabia also collect data from anyone buying a SIM card through fingerprints, whereby in European countries like Poland an ID is required. Hungary use eID cards, combining biometric data, an e-signature, social security and tax data. Turkey introduced smart ID cards too, holding fingerprints and in the near future it will be connected to an electronic authentication website. However, we do not know who the authorities share the data with. It is not only governments who are keen interest in collecting, organizing and analyzing biometrics and Big Data. If enterprises use the biometric authentication, it is not always clearly who is responsible for protecting a sensitive information.

Cybercrime

Criminals have shifted their tactics from technological attacks to targeted assaults on employees by manipulating basic human behaviors. More than ever before, every person has an impact on security, regardless of their function or title. Criminals have learned they can exploit typical human emotions and reactions to steal credentials and infiltrate your network. Intruders use fear, trust, curiosity or even morality to manipulate the victim and reach the goal. We can define point methods represent common techniques that cybercriminals use to prey on our humanity and get what they want: phishing and malware, exploit public information, installing devices, data engineering, and even secretly listening in on private conversations (eavesdropping) or collecting information from the recycling or trash that was not appropriately destroyed (Dumpster Diving). The 12th The Verizon Data Breach Investigations Report (DBIR) is built on real-world data from 41,686 security incidents and 2,013 data breaches provided by 73 data sources, both public and private entities, spanning 86 countries worldwide (*2019 Data Breach Investigations Report*, 2019). According to the report 52% of actions are being used are breaches featured Hacking, 33% included Social attacks, 28% involved Malware. Errors were causal events in 21% of breaches (DBIR 2019).



		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

Fig. 3. Major cyber-attacks in 2018
Source: Avast, 2019.

Cyber-attacks generally are an enormous danger in the modern era. By access to private calls and personnel records, cyber-hackers are able to easily choose which individuals are vulnerable and commit heinous cyber thefts of both identities and properties. However, the real threat occurs when the vulnerable data is intercepted by terrorists. Lastly the BBC news channel reported about global phone networks attack by hackers: "The attack – dubbed Operation Softcell – began in 2017. Cybereason spotted the attacks in 2018 and helped one telecom provider through four more over the next six months. It has now briefed more than a dozen others. None of the targeted firms or people has been named but, according to the report, the hackers collected the call records and geo-location of various individuals from a selection of countries, including those in Europe, the Middle East and Asia" (*Global phone networks attacked by hackers*, 2019). More enlisted cyberterrorists can also use more sophisticated tools to manipulate governments and achieve their goals which may be financially motivated or politically motivated. Eventually, government's or military's database can become a main weapon for international's conflicts and wars. An example of this is when "The US launched a cyber-attack on Iranian weapons systems as President Trump pulled out of air strikes on the country. The cyber-attack disabled computer systems controlling rocket and missile launchers, the Washington Post said. (…) It was aimed at weapons systems used by Iran's Islamic Revolutionary Guard Corps (IRGC), which shot down the US drone last Thursday and which the US says also attacked the tankers" (*US launched cyber-attack on Iran weapons systems*, 2019).

Moreover, another issue of the development of the Internet of Things is the fact that our brains are becoming more dormant; kids do not stimulate their brains as was previously, when the Internet was not popular as yet. The younger generation is more acquainted with Google, Facebook, Instagram, etc. than with books, dictionaries or real-life skills. They do not want to learn and remember, because is easier to search the required phrase in a search engine. To be understood properly: the plight of Internet access is not that we use it, but that we do not verify the content. Let's take as an example the anti-vaccination movement. "In 2014, a large measles outbreak swept through the Disneyland theme park in California, infecting over 50 people. Several of the children who initially spread the disease were intentionally left unvaccinated by their parents. Outbreaks such as the one in the Disneyland theme park are becoming increasingly common due to falling vaccination rates. Undoubtedly, organized anti-vaccination groups have contributed to the drop-in vaccination compliance and anxieties concerning vaccination. These groups often have a strong presence on social media and well-developed websites that attract people to their cause" (Evrony & Caplan, 2017).

Futuristic scientists work to create an immortal humanoid creature. The Human+ project is headed on removal of weak organic bodies to use a brain in post-human frame. "Technologies that intervene with human physiology for curing disease and repairing injury have accelerated to a point in which they also can increase human performance outside the realms of what is considered to be 'normal' for humans. These technologies are referred to as emerging and speculative and include artificial intelligence, nanotechnology, nanomedicine, biotechnology, genetic engineering, stem cell cloning, and transgenesis, for example. Other technologies that could extend and expand human capabilities outside physiology include artificial intelligence, artificial general intelligence, robotics, and brain-computer integration, which form the domain of bionics, uploading, and could be used for developing whole body prosthetics" (*Humanity+ – What We Do*). Because these technologies, and their respective sciences and strategic models, such as blockchain, would take the human beyond the normal state of existence, society, including bioethicists and others who advocate the safe use of technology, have shown concern and uncertainties about the downside of these technologies and possible problematic and dangerous outcomes for our species. Without a doubt it might be an unprecedented achievement, however we cannot predict consequences. The fact is that global technologies exchange and skilled scientist's cooperation is becoming a trend as skills are shared improved amongst the world's leading minds, the world which older generations use to reminiscence will disappear as unchangeable changes are being made.

Summary

in the Fourth Industrial Revolution, key factors driving the incredible changes we are experiencing include the decreasing cost of computing power and connected devices; the ease of using sophisticated algorithms, machine learning, and other forms of artificial intelligence; and the radical drop in the price of genetic sequencing. Smart and connected machines and systems are helping us to build self-driving cars, create virtual assistants, and diagnose disease more precisely- transforming the physical, digital, and biological worlds.

The reality is that the trend to replace workforce by machines already exists, which however might seem to be better than development of sweatshops. Enterprises which implement such systems must be aware of computer's errors and imperfections. If machine duplicates incorrect data based on machine learning, and no one supervises the situation properly, the eventual outcome might be wrong. Algorithms and patterns do not include all circumstances, which a regular person could adapt to. They are neither perfect nor infallible. Yet. Digital has reshaped industries across the globe, driven by technology and customer-centricity. Every industry is evolving to harbor specific digital business investment areas and trends. Artificial Intelligence, Machine Learning, Blockchain, Internet of Things, Edge Computing, Extended Reality (AR/VR), Connected Home and Conversational User Interface – all mentioned elements are potential digital disruptors. AI is a way of making computers, computer-controlled robots, or software capable of thinking intelligently, like humans. Definitely there is a great amount of arguments for Big Data and digitalization. McKinsey&Company introduces values of the Internet of Things on its website: "Sensors and ubiquitous connectivity, combined with data and analytics, open up new opportunities to innovate products and services and to increase the efficiency of operations. This digitization of the physical world- or Internet of Things (IoT)- creates new value for our clients and for their customers".[4] The truth is, that

[4] *Internet of Things. We help clients unlock value by digitizing the physical world,* https://www.mckinsey.com.

we have learned how to research the most unusual information; we reached a skill how to type on keyboard without looking at the letters. We are able to travel the world and exchange technologies. But we are forgetting how to handle unexpected situations without Internet. We know patterns, but we will not know the real life and real world, or nature soon.

On CNN Business website we can find Inside the Pentagon's race against deepfake videos, explained as below: "Advances in artificial intelligence could soon make creating convincing fake audio and video – known as "deepfakes"- relatively easy. Making a person appear to say or do something they did not has the potential to take the war of disinformation to a whole new level".[5] In the era of Big Data and Smart-Phones, Smart-Watches, Smart-Homes let's not lose our smartness, integrity nor our humanity. We must remember about it and use our individual's potential. Internet is the best space to publish, and to spread fake news. Unfortunately, we barely verify what we see, and this allows us to trust what authors want us to believe in. Especially being in quarantine during the COVID-19 global pandemic, people more and more are getting accustomed to be isolated from social life. We use online platforms to learn, to meet friends, to workout, to do shopping, to work. It is convenient, easy, and allows us to avoid or at least postpone facing some social issues. The quality of the data gathered, social life, and relationships is not most important anymore. People are able to generate volumes of information, with lack of efficient tool to separate the valuable sources and utilize the rest. Big Data itself would not be a danger for democracy; however, the way how people manage the superintelligence and using sophisticated manipulation technologies to control the economy and society – this is a real, serious danger for humanity. We all are not only being remotely controlled, but we are convinced by recommendation we receive, to believe that we make choices ourselves. We need to stay open-minded and suppress the automation of society and programming people.

References:

Books:

Agnellutti, C. (2014). *Big Data: An Exploration of Opportunities, Values, and Privacy Issues*. New York: Nova Publishers.

Helbing, D. (2015). *The Automation of Society is Next. How to Survive the Digital Revolution*. CreateSpace Independent Publishing Platform.

Helbing, D. (2015). *Thinking Ahead – Essays on Big Data, Digital Revolution, and Participatory Market Society*. Springer International Publishing.

Jules, T. D. (Ed.) (2017). *The Global Educational Policy Environment in the Fourth Industrial Revolution: Gated, Regulated and Governed*. Public Policy and Governance, Volume 26. Bingley: Emerald Group Publishing Limited.

[5] *When seeing is no longer believing,* https://edition.cnn.com, 2019.

Koppelaar, R., & Middelkoop, W. (2017). *The Tesla Revolution: Why Big Oil Has Lost the Energy War*. Amsterdam: Amsterdam University Press B.V.

Marszałek-Kawa, J., Plecka, D. (Eds.). (2019). *The Dictionary of Political Knowledge*. Toruń: Adam Marszałek Publishing House.

Marszałek-Kawa, J., Plecka, D. & Hołub, A. (Eds.). (2018). *Social Security. Selected Aspects*, Toruń: Adam Marszałek Publishing House.

Osburg, T., & Lohrmann, C. (Eds.) (2017). *Sustainability in a Digital World: New Opportunities Through New Technologies*. Cham: Springer International Publishing AG.

Schwab, K. (2018). Czwarta rewolucja przemysłowa, Warsaw: Studio EMKA.

Sutter, R. G. (2013). *U.S.-Chinese Relations. Perilous Past, Pragmatic Present*. Plymouth: Rowman & Littlefield Publishers, Inc.

Articles in Journals:

Hariri, R. H, Fredericks, E. M., & Bowers, K. M. (2019). "Uncertainty in big data analytics: survey, opportunities, and challenges". *Journal of Big Data*, 6(44). DOI: https://doi.org/10.1186/s40537-019-0206-3.

Evrony, A., & Caplan, A. (2017). "The overlooked dangers of anti-vaccination groups' social media presence". *Human vaccines & immunotherapeutics*, 13(6), 1–2. DOI:10.1080/21645515.2017.1283467.

Subroto, A. & Apriyana, A. (2019). "Cyber risk prediction through social media big data analytics and statistical machine learning". *Journal of Big Data*, 6(50). DOI: https://doi.org/10.1186/s40537-019-0216-1.

Sreenu G., Saleem Durai M. A. (2019). "Intelligent video surveillance: a review through deep learning techniques for crowd analysis". *Journal of Big Data*, 6(48). DOI: https://doi.org/10.1186/s40537-019-0212-5.

Dash, S., Shakyawar, S. K., Sharma, M. et al. (2019). "Big data in healthcare: management, analysis and future prospects". *Journal of Big Data*, 6(54). DOI: https://doi.org/10.1186/s40537-019-0217-0.

Nasiri, H., Nasehi, S., Goudarzi, M. (2019). "Evaluation of distributed stream processing frameworks for IoT applications in Smart Cities". *Journal of Big Data*, 6(52). DOI: https://doi.org/10.1186/s40537-019-0215-2.

Lytras, M., & Visvizi, A. (2019). "Big Data and Their Social Impact: Preliminary Study". *Sustainability*, 11(5067). DOI: 10.3390/su11185067.

Paskaleva, K., Evans, J., Martin Ch., et al. (2017). "Data Governance in the Sustainable Smart City". *Informatics*. DOI: https://doi.org/10.3390/informatics4040041.

Electronic sources:

"2019 Data Breach Investigations Report". *Verizon*. Retrieved from: https://enterprise.verizon.com/resources/reports/dbir/.

Dowdy, J., & Taylor, M. (2013). "Defense outlook 2015: A global survey of defense-industry executives". *McKinsey&Company*. Retrieved from: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/defense-outlook-2015.

Ganesan, V., Ji, Y., & Patel, M. (2016). "Video meets the Internet of Things". *McKinsey&Company*. Retrieved from: https://www.mckinsey.com/industries/high-tech/our-insights/video-meets-the-internet-of-things.

"Global phone networks attacked by hackers". (2019). *BBC news*. Retrieved from: https://www.bbc.com/news/technology-48756030.

Helbing, D., Frey, B. S., & Gigerenzer, G. et al. (2017). "Will Democracy Survive Big Data and Artificial

Intelligence?" *Scientificamerican.com*. Retrieved from: https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/?print=true

Laney, D. (2001). "3D data management: controlling data volume, velocity and variety". *META Group Res Note*. Retrieved from: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lomas, N. (2020). "Telco metadata grab is for modelling COVID-19 spread, not tracking citizens, says EC". Retrieved from: echcrunch.com/2020/03/27/telco-metadata-grab-is-for-modelling-covid-19-spread-not-tracking-citizens-says-ec/.

Lund, S., & Manyika, J. (2017). "Defending Digital Globalization. Let the Data Flow". *Foreign Affairs*. Retrieved from: https://www.foreignaffairs.com/articles/world/2017-04-20/defending-digital-globalization.

Matloob, A. (2019). "Shocking report reveals 43% of high-risk vulnerabilities in Android apps and 38% in iOS apps". *Digital Information World*. Retrieved from: https://www.digitalinformationworld.com/2019/06/apple-google-play-store-apps-riddled-with-high-risk-vulnerabilities-study-revealed.html.

O'Neil, C. (2017). "The era of blind faith and big data must end". TED2017. Retrieved from: https://archive.org/details/CathyONeil_2017.

Palumbo, D., & Nicolaci da Costa, A. (2019). "Trade war: US-China trade battle in charts". *BBC news*. Retrieved from: https://www.bbc.com/news/business-48196495.

Rundem, D. (2017). "The Data Revolution in Developing Countries Has a Long Way to Go". *Forbes*. Retrieved from: https://www.forbes.com/sites/danielrunde/2017/02/25/the-data-revolution-in-developing-countries-has-a-long-way-to-go/#64f2fa451bfc.

Saeed, A. (2019). "Interesting Insight on the Typical iPhone Users Preference About Apps". *Digital Information World*. Retrieved from: https://www.digitalinformationworld.com/2019/06/top-iphone-app-apple-categories-chart.html.

"US launched cyber-attack on Iran weapons systems". (2019). *BBC news*. Retrieved from: https://www.bbc.com/news/world-us-canada-48735097.