

---

## The Legal and Security Aspects of ICT and Industry 4.0 Importance for Financial Industry 4.0 Development

---

Submitted 02/10/21, 1st revision 16/10/21, 2nd revision 03/11/21, accepted 25/11/21

Weronika Jakubczak<sup>1</sup>, Anna Gołębiowska<sup>2</sup>, Dariusz Prokopowicz<sup>3</sup>

### **Abstract:**

**Purpose:** The research aims to characterize legal and security aspects of Information and Communication Technologies (ICT) and Industry 4.0 importance for Financial Industry 4.0 development. The aim of the topic was to demonstrate the growing importance of ICT implementation in analyses of complex research conducted in Financial Industry 4.0 by conducting research on Big Data Analytics.

**Design/Methodology/Approach:** Authors discuss various legal regulations, security aspects - threats and solutions for ICT and Industry 4.0 in order to examine how big of an impact they have for Financial Industry 4.0 development. Article indicates one of the development key directions of analytics conducted on Big Data Analytics analytical platforms, i.e., sentiment analysis use to assess the perception and Internet users awareness in a specific issue, on example of selected issues of ICT, technological revolution, Industry 4.0, various technological and security risk categories and selected economic categories - Financial Industry 4.0. Authors use elements of concept - descriptive and improving functional and modeling as well as diagnostic and functional.

**Findings:** The working hypothesis refers to the assumption that current legal regulations of ICT and Industry 4.0 shall be further adjusted in order to face ever-growing demands of cyberthreats and security measures shall be constantly developed in order to protect critical infrastructure as Financial Industry 4.0. Implementation and lack of transparency with disclosure of number and scale of attacks create additional weak points.

**Practical Implications:** As a result of conducting the research, it is possible to identify threats and present some recommendations for legal and security aspects of ICT and Industry 4.0 so Financial Industry 4.0 can be developed safely as a part of critical infrastructure.

**Originality/Value:** This is a complete research for legal and security aspects of ICT and Industry 4.0 importance for Financial Industry 4.0 development.

**Keywords:** Security, Financial Industry 4.0, ICT, cybersecurity strategy, information security.

**JEL classification:** H56, F52, O33.

**Paper Type:** Research article.

---

<sup>1</sup>The Main School of Fire Service, Institute of Internal Security, Warsaw,  
ORCID ID: 0000-0003-1501-5064 [w.jakubczak@sgsp.edu.pl](mailto:w.jakubczak@sgsp.edu.pl)

<sup>2</sup>The same as in 1, ORCID ID: 0000-0003-0478-5047 [agolebiowska@sgsp.edu.pl](mailto:agolebiowska@sgsp.edu.pl)

<sup>3</sup>Cardinal Stefan Wyszyński University in Warsaw ORCID ID: 0000-0001-6383-916X,  
[d.prokopowicz@uksw.edu.pl](mailto:d.prokopowicz@uksw.edu.pl);

## **1. Introduction**

Globalization accelerates along with common use of internet (Jakubczak, 2018). Interconnectiveness between countries, markets and people is ever-growing. Markets in developed countries require access to rare earth minerals and sophisticated technologies that are used in vast majority of the sectors due to technical development. The trend is also observant withing critical infrastructure sectors as finance.

Entities that do their best to prove that they support economies of countries where they operate may not always follow their official agendas. Huawei officially considers itself as a supporter of EU's strategic autonomy. However, there is an ongoing case in Poland, where Huawei concentrates its sales and marketing activities (Drahokoupi, 2017) of a high rank Huawei manager accused of spying that started in 2019 when the same person – a Huawei Chinese employee accompanied by a former Polish security official were arrested on spying allegations. Poland's internal affairs minister, called for EU and NATO to work on a joint position over whether to exclude Huawei from their markets (Koper, 2019). Minister responsible for special forces was explicit on threats posed by China's policy – *If 5G technology is to be any next civilization leap for mankind, then introducing such subtle, so sensitive technologies of Chinese companies on the basis of their serious entry is a monstrous risk, it is a monstrous irresponsibility* (Wilson Center, 2021).

The US has been open about dangers related to Chinese policy and openly addresses espionage, cyberthreats like hacking, using and manipulating data to influence public opinion. All aforementioned was stated in 2020 by the Director Federal Bureau of Investigation, Christopher Wray (Wray, 2020).

In 2021 Lithuania National Cyber Security Centre at the Ministry of National Defence has identified 10 instances of increased cybersecurity risk in mobile devices manufactured by Huawei, Xiaomi and OnePlus. (NCSC under the MOND, Innovation and Training Division, 2021). While presenting the outcomes of NCSC report, Lithuania's Vice Minister of National Defence Margiris Abukevičius said that consumers should not purchase phones from Chinese manufacturers – *Our recommendation is to not buy new Chinese phones, and to get rid of those already purchased* (Reuters, 2021).

The aforementioned cases prove that implementation of security policy oriented upon strategic autonomy and invest in our own technology development or buy from our allies especially when addressing needs of critical structure system. With the respect to regulations there are many both on national and international levels. They address to security and economic matters. Authors has decided to mention only most relevant ones, bearing in mind that further research is to be conducted and presented in the future.

As an introduction, it is worth to cite that *The early Green Paper by European Commission on critical infrastructures contains an example list of critical sectors, products and services. For the critical Information and Communication Technologies (ICT) sector, seven products and services are listed.* (Luijff, 2015).

European Programme for Critical Infrastructure Protection explains *European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State* (Commission of the European Communities, 2021).

Directive EC 2008/114 of the European Council (European Council, 2008) explains in Art.2 (a) ‘critical infrastructure’ (...) as an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and disruption or destruction of which would have a significant impact in a Member State as a result of failure to maintain those functions; Further (b) it is stated ‘*European critical infrastructure*’ or ‘*ECI*’ means *critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States and play vital role for the functioning of a society and economy* (Spear Project, 2020). In the Indicative list of ECI sectors Financial sector and Information, Communication Technologies, ICT are mentioned.

EU's Cybersecurity Strategy for the Digital Decade (Strategy) explains: *Cybersecurity is an integral part of Europeans' security. Cybersecurity is therefore essential for building a resilient, green and digital Europe. The malicious targeting of critical infrastructure is a major global risk* (European Commission, 2020). Digital services and finance sector are among the most frequent targets of cyberattacks (...) yet cyber readiness and awareness among businesses and individuals remain low (Ponemon Institute, 2020), and there is a major shortage of cybersecurity skills in the workforce (ENISA, 2020). There were almost 450 cybersecurity incidents in 2019 involving European critical infrastructures like finance and energy (Eurostat, 2019).

On the national level in Poland critical infrastructure *ought to be understood as systems and their functionally related objects, including construction objects, devices, installations, services essential for the security of the state and its citizens, and to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs* (Polish Act on crisis management, 2007). Among other Critical infrastructure in Poland includes communication and financial system as well as ICT networks. Still the problem is the same – growing threats and demands are difficult to address in timely manner. Increasing scale of internet services use in finance and more conducted cyberattacks implies that financial institutions security is crucial. Flexible regulations are to be constantly updated.

Public and local administration ought to be aware of it and can do their security tasks (Gołębiowska, 2017).

## **2. The Scope and Methods of Research**

The study was based on a desk research analysis using quantitative data available for the legal and security aspects of ICT and Industry 4.0 importance for Financial Industry 4.0 and the analysis of available literature. The theoretical issues were determined based on the analysis of available literature and legal regulations. The research methods used in the study included a critical analysis of the literature, legal acts, comparative analysis and secondary data analysis.

## **3. ICT and Industry 4.0 Information Technologies in Analyzes of Multifaceted Economic and Financial Processes Implemented in the Financial Industry 4.0 Formula**

Currently, the prevailing opinion is that all economic entities, including commercial sectors and public sector institutions, must constantly adapt to socio-economic environment changing realities and technological progress in modern IT solutions for secure archiving, storing, processing and sharing of information. This can create a big challenge. Due to growing level of competition on the markets, the effective development of the company is determined by making right decisions i.e. increase in computerization that results in effectiveness of implemented production, business, technological processes, management and reporting (Strang, 2016). Cloud computing techniques are being developed, data sets are collected in Big Data databases, and synergy between various determinants of on-line enterprises functioning in global network is growing (Antkiewicz, 2008).

Integration of business processes of entities geographically distant from one another is growing thanks to Internet IT systems and electronic banking. Computerized platforms for conducting business analyzes in the Business Intelligence formula are being created (Surma, 2016). Efficient organization management, analytical and decision-making processes in enterprises based on the current analysis of market, micro and macroeconomic data is increased through use of Business Intelligence IT platforms. Key determinant of its development was reduction of analyzes operating costs related to their time-consuming nature (Grzegorek, 2012).

Strong economy without good security strategy can only attract threats. Following the principles of the free market, economic competition and responding to the newest trends is timely and expected, a sector like finances that is the part of critical infrastructure and must take care of certain level of security reflecting the factual needs of the system. Internet's information resources are doubled approximately every two years. Globally operating Internet companies such as Google or Facebook collect data on Internet users in their Big Data databases to such a wide extent that they themselves are not able to precisely predict what they will use collected

---

information for in 5 years (Roser, 2016). Internet is changing dynamically and Internet libraries and other knowledge bases are gradually increasing.

Therefore, enterprises using Internet should taking into account dynamic nature of collected data variability (Blagov, 2019). The scope of this process, i.e., use of information and technological possibilities of Internet by economic entities, is constantly growing and it is currently impossible to define the limits of this development (Bloem, 2012).

Many enterprises, financial and public institutions see Internet as important and use its capabilities in Business Intelligence formula and management decision making (Radziszewski, 2016). They use its new applications, e.g., conducting business analyses according to the Business Intelligence formula (Gendron, 2014). Large collections of Big Data market information enable real time analyse with account multi-criteria information processing (Fan, 2015). Thanks to cloud computing real-time remote access to current information via mobile devices such as tablets or smartphones is possible. Business Intelligence analytical techniques significantly increase effectiveness of business entities analytics by reducing man-hours number.

Analytics based on Business Intelligence formula is currently interpreted in companies as a business analytics process of transforming multi-criteria data sets into knowledge useful for needs of effective enterprise management. They organize, process and visualize information to extensive reports on economic and financial enterprise situation (Sun, 2016) so managers quicker interpret large data sets processed in real time (Chang, 2018) thanks to IT platforms where generation of Business Intelligence analytical reports is combined with cloud computing and Big Data databases (Olszak, 2014). The concept of Industry 4.0 was introduced in *The Fourth Industrial Revolution* (Schwab, 2016).

As analytical, computerized statistical and econometric instruments and methods are used in the Financial Industry 4.0 (Gandomi, 2015) it is useful for verification and research development of large quantitative data sets describing complex macroeconomic processes, functioning of markets and branches of economy, analysis of public finances of the state and enterprises, financial institutions and other economic entities. It helps in developing prediction models of economic and financial phenomena occurring in economy (Groot, 2012). The Financial Industry 4.0 helps in creating econometric models that facilitate development of models for precise risk estimation, determining the market potential of a company in specific markets, determining the probability of both business success and potential business entity bankruptcy (Lim, 2013).

ICT and Industry 4.0 dynamic development enables multi-criteria analytics researching large data sets popularity, including information downloaded from Internet and then processed on analytical platforms: Business Intelligence, Data Analytics, Data Science, Big Data Analytics, etc. Security rules in data transfer on

Internet and proper handling of data and information collected on internet ought to be maintained (Dolecki, 2016) since they are burdened with high risk of data transfer (Liderman, 2008). High rank data transfer security issues on internet is confirmed by cybercrime cases diagnosed in electronic banking (Prokopowicz, 2009).

In Poland, scale of fraudulent funds based on personal data stolen in IT systems, i.e. so-called identity theft (Wociór, 2016) has been growing. According to Polish Bank Association, in the second quarter of 2021, attempts were made to extort PLN81.8 million. Data from this report shows that over 1.5 thousand cases were detected of using stolen identity in procedure of extorting funds (InfoDOK, 2016).

In order to reduce cybercrime of classified information Internet theft a "Restricted Documents" system was created where stolen documents can be registered (InfoDOK, 2016). Usually successful hacking attacks against financial institutions are not made public since attacked companies are afraid of loss of business (Prokopowicz, 2016). Phishing is still the most popular method of attacks on financial institutions IT systems (Król, 2016).

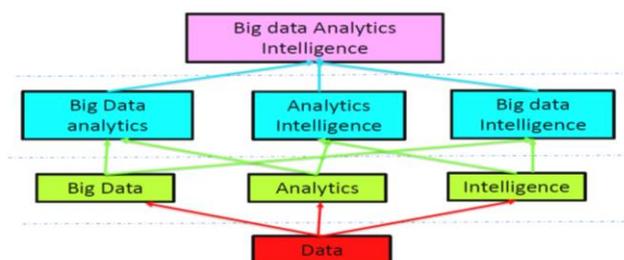
Sensitive informations collected in Big Data database systems are exposed to attacks from cyber criminals. Internet data transfer security is related to data analytics carried out on computerized platforms such as Business Intelligence (Tomczak, 2019), Big Data, Data Science, Data Analytics and analytics conducted there can be used to study the scale of cybercrime (Prokopowicz, 2017). Big Data can be used in fraud prevention by conducting analysis of market risks, threats related to fraud and theft attempts by cybercriminals, i.e. attempts to commit traditional banking fraud. Therefore, share of banks that use Big Data solutions to detect frauds as extorting mortgage loans, payments and financial operations carried out with bank cards, is growing (Dmowski, 2010). Big Data may facilitate analytical processes related to electronic internet banking threats and risks, i.e. analysis of card payments and precise adjustment of banking product offer to behavioral customer profiles developed (Złoch, 2013).

Taking into account ongoing digitization of companies, offices and financial institutions the security of data transfer is becoming a key issue (Gwoździewicz, 2017). Currently, protection of classified data is the area of human existence that should be ensured by entities regulating and operating on internet. According to provisions of the Constitution, the protection of classified data transfer is one of the fundamental rights of every citizen, business entity and public institution. Continuous technological progress, constantly modified technical parameters of electronic banking tele-information systems, development of Big Data, methodologies of analytical processes based on Business Intelligence formula and changing offer of Internet companies' services may result in maladjustment of legal standards to rapidly changing realities of digital age (Gałach, 2013). This can cause large scale political and security problems.

New technologies can be used in The Financial Industry 4.0. Econometric and statistical tools analyzing quantitative data large sets enabled analytics development using advanced data processing (Prokopowicz, 2017). Without use of complex econometric models in verification and analysis of large quantitative data sets, scientific research development would proceed slower (Gwoździewicz, 2017). The Financial Industry 4.0 analytics is helpful in building complex, multi-factor models describing functioning of complex economic organizations (Lim, 2013).

Business management is supported by computerized Business Intelligence platforms facilitating multi-criteria analyses and reporting. Specialized IT companies produce applications helpful in conducting economic analyses, i.e.. Business Intelligence platforms (Grzegorek, 2018). Figure 1 shows organizational structure and relationships between Big Data, Analytics and Intelligence systems.

**Figure 1.** Organizational structure and relations between Big Data, Analytics and Intelligence systems.



*Source:* Z. Sun (2016), *Big Data, Analytics and Intelligence*, (in:) UNITECH Research Committee Seminar, Centre of Big Data Analytics and Intelligence, Department of Business Studies, Papua New Guinea University of Technology, 8 Nov 2016. BAIS No. 16002, p. 14.

Progressive digitization of documents in business entities is conducive to growth of applications of The Financial Industry 4.0 (Lee, 2016). Digitization and internetization of remote communication and economics is accelerated by Covid-19 coronavirus pandemic (Golczak, 2020).

Private enterprises and public institutions are digitizing information. Positive aspects of full digitization are recognized and confirmed by growing capital expenditures of companies (Mayer-Schonberger, 2015). Data processing in cloud computing enables to access, process, analyse and generate reports from anywhere via mobile devices. Databases built on Big Data platforms enable analytical processes to be carried conducted real time on huge data sets, (Libuda, 2016) taking into account multi-criteria processing of information updated on a regular basis. Business Intelligence analytical platforms significantly increase effectiveness of analytical and decision-making processes in business entities by reducing number of man-hours spent on research, multi-criteria processing of information and generating reports according to given criteria (Gendron, 2014).

Increasingly, ICT and Industry 4.0 are being used in predictive analyses of complex economic, financial, natural, geological, climatic processes, etc., (Chen, 2014). Above-mentioned ICT and advanced information processing and analysis technologies Industry 4.0 are used to conduct predictive analyses (Saif, 2012).

#### **4. Conclusions**

This research shows that importance of The Financial Industry 4.0 in business, economic and financial analytics on large sets of quantitative data used in enterprises and institutions in the future, is growing. The development of applications of The Financial Industry 4.0 in economic and financial analysis is one of the features of the development of modern knowledge-based economies. The technological progress taking place in this issue is also an important attribute of the comparative advantage between individual entities operating in the commercial financial sector. The Financial Industry 4.0 is especially helpful in verifying quantitative results of scientific research.

The rapidly developing ICT and Industry 4.0 implementation into economics include Internet electronic banking and e-commerce. The key determinants of the globally developing e-commerce relate primarily to ICT and advanced data processing popularity. Additionally, the use of blockchain for security systems for transactions and data transfer on internet.

During Covid-19 pandemic, internationalization of enterprises commercial activities and offering and sale of products or services on internet increased.

Another important factor in e-commerce development is mobile internet banking (mobile devices) popularization and new solutions related to Internet of Things. Internet banking, development of which is determined by technological progress of information technologies, ICT and Industry 4.0 (Matosek, 2017) is becoming dominant in banking. Informatization is also increasingly applicable to public sector institutions that support business entities tax systems and settlements. Additionally, Business Intelligence analytical platforms have been developed to support e-commerce companies management. Information large sets analytics in Big Data databases is also developing (Gendron, 2014).

Importance of computerized business analytics synergy and use of internet for e-commerce development in other applications is increasing. Big Data Analytics and Data Science analytical systems are used by online commerce economic entities. New Internet marketing instruments used mainly on social media portals have been developed and used by e-commerce companies. Internet technology companies and fin-techs, offering information services on internet to support marketing management are being established. For this purpose, sentiment analyses are used to research opinions of Internet users dominant awareness, recognition, brand image, mission, and offers. This is conducted on large data sets downloaded from various

websites (Chang, 2019). Analytical data collected is very helpful in planning new media advertising campaigns advertising products and services sold online.

Dynamic development of e-commerce taking place is mainly determined by technological progress in ICT, advanced data processing technology Industry 4.0 and new technologies used in securing Internet financial transactions i.e. blockchain. ICT and Industry 4.0 are important factors in economic development, primarily in developing knowledge-based economies. In many countries, investment programs are also financed from public funds in order to stimulate ICT and Industry 4.0 development applications.

ICT and Financial Industry 4.0 are not only elements of critical infrastructure but also an important element of 4th Technological Revolution and to a large extent determine the development of knowledge-based economies. Individual developing countries, whose economies are largely based on such production factors as technology, information, innovation, entrepreneurship and knowledge, build their comparative advantage in this way. Building a comparative advantage in knowledge-based economies takes into account investments in new technologies, including Internet, ICT and Industry 4.0 (Grzegorek, 2017). Investments made in modern forms of aforementioned increase efficiency of production, logistics, management, marketing, risk control, etc. in enterprises operating in various branches of economy (Banafa, 2019).

It is crucial to protect critical infrastructure. Critical ICT are of growing importance and governments regulate national critical infrastructure so telecommunication services and in some cases critical services offered by key Internet Service Providers (ISP) are secured. Still, bearing in mind ever-evolving threats, policy-makers and thus regulations largely overlook to efficiently govern all ICT aspects. In order to properly address financial sector needs constant adjustments have to be made. This would allow to decrease relevant societal and economical risks for elements and services critical to functioning of Poland. Legal and regulatory obligations to increase ICT resilience on EU and country level will encourage this process.

## References:

- Antkiewicz, S. 2008. *Innowacje finansowe*. Warsaw, Publishing house CeDeWu.
- Banafa, A. 2015. *The Future of Big Data and Analytics*. Conference Paper. <https://www.researchgate.net/publication/284826598>.
- Blagov, A., Rytsarev, I., Strelkov, K., Khotilin, M. 2015. *Big data instruments for social media analysis*. Conference Paper, Department of Technical Cybernetics, Samara State Aerospace University, Samara, 445086, Russia. <https://www.researchgate.net/publication/318902625>.
- Bloem, J., Van Doorn, M., Duivestijn, S., Van Ommeren, E. 2012. *Creating clarity with big data*. Sogeti VINT.

- Chang, C.L., McAleer, M., Wong, W.K. 2018. Big Data, Computational Science, Economics, Finance, Marketing, Management and Psychology: Connections. *Journal of Risk and Financial Management*, 11(15). doi:10.3390/jrfm11010015.
- Commission of the European Communities. 2006. COM(2006) Communication From The Commission on a European Programme for Critical Infrastructure Protection, Brussels. <http://eur-lex.europa.eu/legal-content/EN/TXT/PF/?uri=CELEX:52006DC0786&from=EN>.
- Dmowski, A., Prokopowicz, D. 2010. *Rynki finansowe*. Publishing house Centrum Doradztwa i Informacji Difin sp. z o.o., Warsaw.
- Dolecki, S. 2016. Brutalna cyberzeczywistość, Bank. *Miesięcznik Finansowy*, raport specjalny Cyberbezpieczeństwo, 4(276).
- Drahokoupi, J., McCaleb, A., Pawlicki, P., Szunomar, A. 2017. Huawei in Europe: strategic integration of local capabilities in a global production network. In: J. Drahokoupil (eds), *Chinese investment in Europe: corporate strategies and labour relations*, 978-2-87452-454-7, Etui.
- ENISA. 2020. Threat Landscape 2020 <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> Verizon Data Breach Investigations Report 2020 <https://enterprise.verizon.com/resources/reports/dbir/>.
- European Commission. 2020. High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade, Brussels.
- European Council. 2008. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32008L0114>.
- Eurostat. 2019. ICT usage in enterprises in 2019. <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>.
- Fan, S., Lau, R.Y., Zhao, J.L. 2015. Demystifying Big Data Analytics for Business Intelligence Through the Lens of Marketing Mix. *Big Data Research*, 2.
- Gałach, A., Jędruszczak, A., Nowakowski, B. 2013. *Ochrona danych osobowych, informacji najważniejszych i systemów teleinformatycznych w sektorze publicznym*. Warsaw, C.H. Beck.
- Gandomi, A., Haider, M. 2015. Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35.
- Golczak, K., Golinowski, K., Kamycki, J., Lewandowski, K.J., Pająk, K., Płaczek, J., Prokopowicz, D., Wesołowski, Z. 2020. Prognoza globalnego kryzysu finansowo-gospodarczego zdeterminowanego przez pandemię koronawirusa w obszarze gospodarczym, społecznym, politycznym i geopolitycznym. Prognoza kryzysu w obszarze gospodarczym. In: Soroka, P., Skrabacz, A., Wilczyński, P., Golczak, K., Kołodziejczyk, R., Pająk, K., Mitręga, A. (ed.) *Raport zawierający diagnozę i prognozę globalnego kryzysu finansowo-gospodarczego zdeterminowanego przez pandemię koronawirusa w obszarze gospodarczym, społecznym, politycznym i geopolitycznym*. Elipsa, Warsaw.
- Gołębiowska, A., Zientarski, P.B. 2017. Organy administracji rządowej i samorządowej w sferze bezpieczeństwa i porządku publicznego. In: *Administracja publiczna w systemie bezpieczeństwa państwa*. Warsaw.

- Groot, R. 2012. Data mining for tweet sentiment classification, Hortonworks Sandbox tutorial. <http://hortonworks.com/tutorials>.
- Grzegorek, J. 2012. Wizja Przyszłości Polski, Tom II Ekspertyzy. Komitet Prognoz „Polska 2000 plus”. PAN, Warsaw.
- Grzegorek, J., Prokopowicz, D. 2017. The Application of the MS EXCEL Program and the Informalized Business Intelligence Analytics Platforms in the Management of the Enterprises/ In: International Journal of New Economics and Social Sciences. MII „Nauka-Edukacja-Rozwój”, Warsaw, 1(5).
- Grzegorek, J., Prokopowicz, D., Gwoździewicz, S., Dahl, M. 2018. Application of data base systems Big Data and Business Intelligence software in integrated risk management in organization. In: International Journal of New Economics and Social Sciences. MII „Nauka-Edukacja-Rozwój”, 2(8), Warsaw.
- Gwoździewicz, S., Prokopowicz, D. 2017. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27.06.2017 r. In: S. Gwoździewicz, K. Tomaszycy (ed.), Prawne i społeczne aspekty cyberbezpieczeństwa. MII “Nauka – Edukacja – Rozwój”, Warsaw.
- Gwoździewicz, S., Prokopowicz, D. 2017. The Big Data technologies as an important factor of electronic data processing and the development of computerized analytical platforms, Business Intelligence. International Journal of Small and Medium Enterprises and Business Sustainability, 2(4), November, Center for Industry, SME and Business Competition Studies, University of Trisakti in Jakarta, Indonesia. University of Social Sciences, Warsaw, Poland.
- Huawei, Investing in local resources for Europe’s strategic autonomy. <https://huawei.eu/press-release/investing-local-resources-europes-strategic-autonomy>.
- InfoDOK, Raport o dokumentach, II kwartał 2016 r. (26 edycja), Związek Banków Polskich, Warsaw 2016.
- InfoDOK: Niemal 900 tys. zł dziennie próbowano wyłudzić przy pomocy kradzionej tożsamości. In: Witryna internetowa Związku Banków Polskich. <https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/infodok-niemal-900-tys-zl-dziennie-probowano-wyludzic-przy-pomocy-kradzonej-tozsamosci>.
- Jakubczak, W. 2016. Condition of Cybersecurity in Poland–Selected Aspects. *Przedsiębiorczość i Zarządzanie*, 17, 5.1. SAN, Warsaw.
- Koper, A., Pawlak, J. 2017. Poland could limit use of Huawei products after worker arrested. <https://www.reuters.com/article/cnews-us-poland-security-idCAKCN1P70JI-OCATP>.
- Król, A. 2016. Po owocach poznacie, że to atak. *Bank. Miesięcznik Finansowy*, 4(276), Kwiecień.
- Lee, H., Sohn, I. 2016. Big Data w przemyśle. Jak wykorzystać analizę danych do optymalizacji kosztów procesów? Warsaw, Naukowe PWN.
- Libuda, L. 2016. Era Big Data - zarządzanie ryzykiem z dopalaczem. *Bank. Miesięcznik Finansowy*, 6(278), June.
- Liderman, K. 2008. Analiza ryzyka i ochrona informacji w systemach komputerowych. Naukowe PWN, Warsaw.
- Lim, E., Chen, H., Chen, G. 2013. Business Intelligence and Analytics: Research Directions. *ACM Transactions on Management Information Systems*, No. 3(4), 2013.

- Luijff, E., Klaver, M. 2015. Governing Critical ICT: Elements that Require Attention. *European Journal of Risk Regulation*, 6(2). Cambridge University Press.
- Matosek, M., Prokopowicz, D. 2017. Importance and Security of Information Provided by internet in the Context of the Development of Economic Entities in Poland. *International Journal of New Economics and Social Sciences*, MII „Nauka-Edukacja-Rozwój”, 2(6), Warsaw.
- Mayer-Schonberger, V. 2015. Big Data. Rewolucja, która zmieni nasze myślenie, pracę i życie. Warsaw, MT Biznes.
- NCSC under the MOND, Innovation and Training Division. 2021. Assessment of cybersecurity of mobile devices supporting 5G technology sold in Lithuania, Analysis of Products Made By Huawei, Xiaomi and OnePlus. [https://www.nksc.lt/doc/en/analysis/2021-08-23\\_5G-CN-analysis\\_env3.pdf](https://www.nksc.lt/doc/en/analysis/2021-08-23_5G-CN-analysis_env3.pdf).
- NCSC under the MOND, Innovation and Training Division. 2021. Cybersecurity assessment of 5G-enabled mobile devices sold in Lithuania , Product Analysis of Manufacturers Huawei, Xiaomi and OnePlus. [https://www.nksc.lt/doc/en/analysis/2021-09-27\\_Amendment-EN-full.pdf](https://www.nksc.lt/doc/en/analysis/2021-09-27_Amendment-EN-full.pdf).
- Olszak, C.M. 2014. Business Intelligence in cloud. *Polish Journal of Management Studies*, (10).
- Polish Act of April 26th 2007 on crisis management Dz.U.2020.1856.
- Ponemon Institute, Annual Cost of a Data Breach Report, <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>.
- Prokopowicz, D. 2017. Wzrost znaczenia bezpieczeństwa elektronicznego transferu danych w Internecie w kontekście bezpieczeństwa administracji publicznej państwa. In: A. Gołębiowska, P. Zientarski, „Administracja publiczna w systemie bezpieczeństwa państwa”, Kancelaria Senatu, Senat RP, Warsaw.
- Prokopowicz, D. 2017. Zastosowanie zintegrovaných platform analitycznych Business Intelligence w procesach zintegrowanego zarządzania ryzykiem w organizacji. In: "Zeszyty Naukowe UKSW. Ekonomia i Zarządzanie", UKSW Warsaw, 2(2).
- Prokopowicz, D. 2009. Zagrożenia rozwoju i bezpieczeństwo bankowości elektronicznej. In: *Zeszyty Naukowe WSZiP, Rok XIV. No. 1(30)*.
- Prokopowicz, D., Gwoździewicz, S. 2016. Prawo do ochrony informacji i danych osobowych w cyberprzestrzeni w dobie rozwoju bankowości internetowej - The Right to Protection of Information and Personal Data in the Cyberspace in the Age of internet Banking Development. In: D. Gałuszka, G. Ptaszek, D. Żuchowska-Skiba (ed.), *Technologiczno-społeczne oblicza XXI wieku*. LIBRON Filip Lohner, Kraków.
- Prokopowicz, D., Gwoździewicz, S. 2017. Rozwiązania technologiczne Big Data a znaczenie analiz biznesowych według formuły Business Intelligence. In: M. Oziębło, (ed.) *Zarządzanie - nowe perspektywy z udziałem e-technologii*, "Przedsiębiorczość i zarządzanie", 18(10), part II, SAN, Łódź, Warsaw.
- Radziszewski, P. 2016. Business Intelligence. Moda, wybawienie czy problem dla firm? *Biblioteka Nowoczesnego Menedżera*. Warsaw, Poltext.
- Reuters. 2021. Throw away your Chinese phone' says Lithuania, after new report reveals built-in censorship tech. <https://www.euronews.com/next/2021/09/22/throw-away-your-chinese-phone-says-lithuania-after-new-report-reveals-built-in-censorship>.

- Roser, M. 2016. Internet, Empirical View, Growth of internet. In: Website: OurWorldInData.org, <https://ourworldindata.org/internet> (za:) Internet users are people with access to the worldwide network, World Bank. <http://data.worldbank.org/data-catalog/world-development-indicators>.
- Saif, H., Alani, Y., He, H. 2012. Alleviating data sparsity for twitter sentiment analysis. CEUR Workshop Proceedings, CEUR-WS.org.
- Schwab, K. 2016. The Fourth Industrial Revolution, ISBN 9781524758868. World Economic Forum, Geneva.
- Spear Project. 2020. A Review of Critical Infrastructure Domains in Europe. <https://www.spear2020.eu/News/Details?id=120>.
- Strang, K., Sun, Z. 2016. Meta-Analysis of Big Data Security and Privacy, Scholarly Literature Gaps. IEEE Big Data, Washington DC, USA. IEEE Press.
- Such-Pyrgiel, M. 2019. Człowiek w dobie cyfrowej transformacji. Studium socjologiczne, Adam Marszałek, Toruń.
- Sun, Z. 2016. Big Data, Analytics and Intelligence. UNITECH Research Committee Seminar, Centre of Big Data Analytics and Intelligence, Department of Business Studies, Papua New Guinea University of Technology, 8, BAIS No. 16002.
- Surma, J. 2016. Business Intelligence. Systemy wspomaganie decyzji biznesowych. Warsaw, Naukowe PWN.
- Tomczak, J. 2019. Nowoczesne Systemy Business Intelligence w rozwoju przedsiębiorstw sektora MŚP. In: A. Opolska-Bielańska, (ed.), Logistyka i administrowanie w mediach. Zarządzanie Big Data, "Media początku XXI wieku". UW, Warsaw.
- Wilson Center. 2019. The Collapse of Communism in Eastern Europe: A 30-Year Legacy. <https://www.wilsoncenter.org/event/the-collapse-communism-eastern-europe-30-year-legacy>.
- Wociór, D. 2016. Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego. Warsaw, Publishing house C.H. Beck.
- World Economic Forum. 2021. The Fourth Industrial Revolution, by Klaus Schwab. <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab>.
- Wray, C. 2020. The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States. <https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states>.