THE RISKS OF DIGITIZATION IN THE CONTEXT OF ECONOMIC DEVELOPMENT AND OF ENSURING SOCIAL AND INFORMATIONAL SECURITY

Carmen Valentina RĂDULESCU [a]*, Dumitru Alexandru BODISLAV [a], Mihaela Diana OANCEA NEGESCU [a] Marcela Antoneta MITRIȚĂ [a]

[a]The Bucharest University of Economic Studies

ABSTRACT

The digital revolution, which has taken on a rather active scale in the early nineties, has begun to develop and be increasingly implemented both at the level of national economies at regional and local level and in various priority and complex areas, the banking system, the oil field, the automotive, rail, maritime and aeronautical and aerospace industries, agriculture and rural development, including in the labor market. Although the implementation of many sectors in the Greece sector still leads to the work of various sectors and to the creation of new jobs, it is important to ensure information security and social security at all levels in order to ensure the transparency, information and efficiency of the various economic and social sectors.

KEYWORDS: *digital revolution, social security, informational security*

1. INTRODUCTION

According to the basic document, Strategy 2020, launched on March 3rd, 2010 by the European Commission, titled Europe 2020 – A European strategy for smart, sustainable and inclusion favorable growth, the general purpose of the strategy is to guide the EU economy into the next decade, through a unitary thematic approach of the economic and social reforms, focused on the three priorities of European 2020 Strategy , that define the EU vison on market social economy for the 21st century: Smart Growth, Sustainable Growth, Inclusion Favorable Growth (Profiroiu et al., 2019).

The National Strategy on the Digital Agenda for Romania reflects the needs and implicitly the Romanian vision through the development of the ITC sector. This one concerns mainly three ways of action: public administration and its modernization, the private sector and the indirect support of its competitivity, as well as the large population by ensuring access to resources like ITC and digital inclusion (Burlacu, 2009, 2010, 2011a, b, c, 2014).

The basis of digital economy is the Internet networks, where the main participants are the communities of manufacturers, traders, various consumers of goods and services that online. This new economy will create new markets, new models of business and public and private institutional management (Burlacu, Profiroiu & Vasilache, 2019). People's behavior will change, just like the producers' and the consumers (Ionita et al., 2009 a, b, c). This will trigger radical transformations of the economy. The major components of digital economy are consumers and sellers of digital products, both physical persons and companies with infrastructure, intermediaries, maintenance and support services, web-site creators, platform and various software (Burlacu & Jiroveanu, 2011, 2012).

* Corresponding author. E-mail address: *cv_radulescu@yahoo.com*

With the revolutionary development of the digital economy, the digitization of various areas of activity and the radical change of Paradigm, the nature of information security incidents is changing from the local level to threats that can be national and international, both in the public institutions, financial institutions, but also those in the private sector (Burlacu, Gutu, & Matei, 2018). We note that digital technologies and telecommunication and interconnection technologies, although benefiting and supporting the management of public institutions, financial and banking institutions, as well as the process of digitization of industry, transport, agriculture and many other branches, also bring various vulnerabilities (Rădulescu et al., 2018 a,b).. Authors Mario Spremić, Alen Šimunik, Cyber Security Challenges in Digital Economy, Proceedings of the World Congress on Engineering 2018 Vol I WCE 2018, July 4-6, 2018, London, U.K. "Nowadays, information security is not enough to achieve basic protection against" common "cyber-attacks, in cyber security organizations, organizations need to implement smart, innovative and effective controls to detect and prevent the emergence and advancement cyber-attacks." Cyber security activities should not just be the responsibility of the IT departments or the designated individuals but the efforts of the institutions with the employees. As digital technologies are strategically aligned with business strategy, the same must be done with cyber security.
Andy Phippen and Simon Ashby analyzed the growing problem of digital risk in the workplace and how organizations could respond to the types of problems that could be classified as such. Whereas, at first sight, we might consider that the growth of digital behaviors beyond the traditional limits of Information Assurance is the result of a younger, more digitally employed workforce, we could argue that this is a simplistic interpretation of the blurring between social and workplace effects resulting from the emergence of social media, mobile technology and services easily accessible through the Internet and that digital social behavior with a potential impact on the workplace is not just the youngest workforce. We have to keep in mind that employees of all ages are involved in digital social technologies and their behaviors are adapting as a result of this adoption. Phippen & Ashby (2015, 43) introduce the concept of "risky" digital behaviors in the workplace and the problems that these behaviors introduce to the risk assessment of an organization. The authors introduced issues such as: monitoring internet access and employee rights; the ethical interpretation of practices that are perfectly legal; defining the policy of embracing digital behaviors at work; awareness and on-the-job training to communicate corporate policy; the difference between common sense and required diligence in an organizational setting.

2. DIGITIZATION IN THE CONTEXT OF ECONOMIC DEVELOPMENT

Considering the magnitude of the digital revolution that we are influenced in society and economy at national, regional and local level, we wonder how much we are prepared for tomorrow's revolution ... in all areas of economic and social life, what are the concrete development opportunities, digital technologies penetrate all the activities of society, have a strong impact on economic growth, social inclusion and sustainable development (Bran, Alpopi & Burlacu, 2018).
"Significant progress in access to telecom services, the use of social media applications and networks, the implementation of eLearning policies and programs, eHealth and the adoption of relevant regulatory frameworks". Therefore, the pace of progress varies greatly between countries and there are large loopholes within countries, even if they continue to stay well beyond the more developed economies (Jianu et al., 2019). Under the current lack of slowdown in current trends, we expect the world to undergo a more dramatic change by 2025: 1. The impact of smart phones brings to the widespread and global use of the Internet and social networks with over 80% of the population. 2. By installing intelligent systems in homes and cars and other devices used by humans, connected objects invade the available time, no matter where we are. 3. The constant evolution of e-commerce will reach an initial stage of maturity (15-25% of the penetration rate) in many industries, and newcomers will cause many inheritances and profits.

2.1. The Digital Agenda

The Digital Agenda includes proposals for action to be taken urgently to bring Europe back on the path of smart, sustainable and inclusive growth. These proposals will form a framework for the long-term transformation of a society and an increasingly digitized economy. The Digital Agenda for Europe is one of the seven Europe 2020 flagship initiatives and aims at defining the key motor role that the use of information and communication technology (ICT) will need to play in achieving Europe's 2020 goals. The objective of this Agenda is to make a journey in order to maximize the social and economic potential of ICT, especially the Internet, which is a vital support of economic and social activities, be it business, work, play, communicate or express us freely. Successful implementation of this Agenda will stimulate innovation and economic growth, while improving the quality of everyday life of citizens and businesses. Wider application and more effective use of digital technologies will enable Europe to address the fundamental challenges it faces and give Europeans better quality of life, thanks to improved healthcare services, more efficient transport solutions, cleaner environment, new opportunities for communication and easier access to public services and cultural content.

According to Ciobanu & Stratulat (2016) "the Romanian IT society faces a number of essential issues, but is also characterized by a good level of experts' training in this area. Romania must approach the huge gap of digital competences". In order to fully develop the digital economy and the digital society, Romania has to develop the citizens' digital skills. Without digitization and production efficiency, the Romanian companies will struggle in vain to become part of the world's digital economy. The Romanian companies also need to take advantage of the possibilities provided by on-line commerce. They go on to assert that "The creation and adoption of a legal framework to support developers and local suppliers of innovative IT&C solutions, granting facilities so as to increase the attractiveness of local entrepreneurs and suppliers of IT&C products and services for the international markets. Although the national educational system has a good potential, it is one of the weak points of the national IT&C industry because of under-financing, the insufficient number of graduates with really effective digital skills and of the small number of IT&C specialists who graduate annually in Romania. Therefore, the trend of the number of graduates over the last years shows that there is rather a decrease compared to the demand on the labor market".

For Ciobanu et al. (2015, 190) considering: "the lag of economic development at the level of regional development, we believe that an important issue is to ensure the IT of the regions. We will be able to develop the regions if we create national and regional development networks, virtual organizations of different levels and in different areas of activities".

Tabel 1. The main indicators of the information society at national level

	2010	2011	2013	2014	2015	2016	2017
Number of fixed telephone lines per 1000 inhabitants	209.4	219.3	218.4	212,6	197,9	207.8	197.7
Number of mobile subscribers per 1000 inhabitants	1135.6	1091.6	1055.8	1059,1	1071,4	1157.8	1145.9
Number of Internet users per 1000 inhabitants	399.3	440.2	497.6	540,888	557.6	595	637.5
Number of Internet broadband subscribers per 1000 inhabitants	139.6	153.9	174.7	185.2	197.7	225	242.9

Source: www.insse.ro

Tabel 2. Share of enterprises using PC, Internet connection and Investments in hardware products

		2010	2011	2013	2014	2015	2016	2017
	Share of enterprises using PC in total active enterprises in the sector (%)	83.5	81.5	87.5	88.3	87.3	87,0	87,6
	Share of enterprises with Internet connection in total enterprises active in the sector (%)	78.5	79.3	85.0	88.2	86.5	86,1	87,0
	Share of the personnel who used PC in total personnel (%)	33.9	30.6	31.7	32.1	32.7	35,6	37,6
	Share of staff using PC connected to the Internet in total staff (%)	28.8	26.5	28.7	29.7	28.7	32,3	33,8
	Investments in hardware products (mil. lei)	772.6	548	596.2	861.9	684.5	873,7	655,2
	Investments and expenditures for information technology products and services (mil. lei)	3996.3	5363	82.4	84.5	82.6	82,7	83,8
	Share of broadband companies in total active enterprises in the sector (%)	54.3	62.7					
	Share of enterprises that have used a mobile connection to connect to the Internet in total enterprises active in the sector	19.4	25.7					
	Share of enterprises owning their own website in total enterprises active in the sector (%)	33.8	35.8	43.8	43.9	47.6	45,4	45,3
	Share of Internet turnover in the total turnover of enterprises with economic activity in the sector (%)	3,0	4.2					
	Share of Internet turnover in the total turnover of enterprises selling online (%)							
					7.9	7.4	8,4	8,8

Source: www.insse.ro

Tabel 3. Using PC in the Romanian region of development

	Region	**Share of personnel using PC -% -**			Share of staff who used PCs connected to the Internet in total staff -% -		
		2010	**2015**	**2017**	**2010**	**2015**	**2017**
1	North – East	24.8	24.3	27.8	22.2	21.7	24.9
2	South – East	19.9	20.9	22.5	16.8	17.3	19.7
3	South – Muntenia	19.8	27.7	26.3	16.2	24.5	22.3
4	South – Vest Oltenia	17.8	21.2	20.5	15.0	18.0	18.3
5	West	20.4	25.3	26.7	17.3	22.6	23.3
6	North – Vest	23.3	24.7	29.8	19.7	21.6	26.0
7	Center	25.3	26.2	29.0	21.2	21.7	24.8
8	Bucharest – Ilfov	50.1	52. 7	59.1	44.5	45.6	54.6
	Total	30.2	32.7	37.6	26.2	28.7	33.8

Source: www.insse.ro

2.2. Risk of digitization

In the work *managing digital risk Trends, issues and implications for business* the authors consider that: Digital risk must become a board-level concern. Risk managers need to set up ways to regularly monitor digital risks and provide them with an informed view of their businesses. Digital risk assessment requires the input of technology experts and other stakeholders in the company. *As businesses become more technology dependent and the pace of technological change continues repeatedly*, the digital risks faced by companies are likely to grow and become more complex (Costache, 2015). The range, frequency and magnitude of digital attacks on businesses will increase, increasingly sophisticated attackers are rapidly adapting to the ever-changing digital environment. Risk managers need to develop comprehensive risk management strategies involving mitigation measures and risk transfer solutions. Risk managers need to prioritize which of the available IT security options will best reduce the risk to their company. More communication, cooperation and collaboration are needed to combat digital risk. Governments, industries and companies need to work harder to combat cyber-attacks.

Cyber threats can lead to a variety of higher business risks, including: 1. Operational risks - the risk of losses from internal processes, inappropriate or defective individuals or systems, or from external events. 2. Intellectual property risks - loss of marketing plans, marketing plans or critical intellectual property to competitors may seriously damage a company's ability to compete. 3. Legal and Regulatory Risks**.** If it is demonstrated that the organization is in breach of regulatory requirements, which are becoming more cumbersome, it may eventually be sanctioned or amended. 4. The reputation risk - the public visibility of incidents can harm the image, brand and reputation of the company.

Connecting them to individuals and connecting individuals to each other. These give rise to new forms of attack, and new risks. This report highlights that: The threat environment is rich and evolving; Organizations are increasingly exposed to cyber-attacks and non-dangerous threats to technology; Technology and how organizations use it evolves quickly; Risk managers need to pay attention to both future threats and future uses of technology.

As technology grows so fast and cyber-attacks are becoming more and more sophisticated, the challenge faced by risk managers is how to manage this increasingly complex digital risk environment. **For risk managers, we have a number of recommendations:** Set up a working group to monitor and review the exposure of the business to digital threats, and to keep the committees informed; To become more involved in IT governance and strategy and major technological transformations. Most mitigation of digital risks is managed through IT governance; Ensure that recommended and applicable standards and frameworks are used to help manage digital risks; Consider risk transfer solutions as part of the global risk management strategy.

2.3 Future trends and implications for business risks

Digital instructions. Crime and Terrorism, it's more and more common to open a newspaper or see a website and read about a new cyber-attack or a company that has lost people's personal data. **International cooperation is critical to fighting cybercrime. The following list of roles, motivations,** and methods illustrate the range of digital threats that today's businesses face.

Sivobrova & Сивоброва И.А. think that this unresolved issue is a challenge: "Developing a technology to identify crisis situations and determine how to solve them. Creating an advanced strategic management model; Management models: the transparency standard for NGO information. In response to global information activity: Open Government; Open Budget; Open Transactions. As a defense against false accusations".

In the Report of OECD Digital Economy Outlook (2017, 22), "Digital transformation is on the global agenda starting with the G20, OECD and G20 ministerial events of 2016 towards the G20 Ministerial in 2017, digital transformation has become firm on the global agenda. The OECD Ministerial on the Digital Economy, which took place in June 2016, was an essential milestone in

this process where ministers from 43 countries concluded that digitization can be the key to a brighter future and calls for a whole government approach to unlocking the benefits for growth and well-being and starting a new era of policy-making as the best way to enable digital transformation for the benefit of all in all countries".

The study *Risk and opportunity in an increasingly digital world Insurance Governance Leadership Network* (2015, 2) addresses the opportunities: "To avoid the risks and opportunities in an increasingly digital world. Increasing digitization of insurance raises issues related to strategy, risk, organizational and market structure, labor and culture - aspects that, in the final analysis, require special attention of the full board." For insurers, the complexity and the way management boards can bring value as insurers making strategic decisions in an increasingly digital world. Despite the advances in digital insurers' strategies, the participants have identified several important areas for the progress, with implications for the allocation of resources, strategy and organizational structure These views are guided by the following questions: How do the board of directors define and think about digital transformation How fast the leaders of insurers adapt and embrace the digital world How can traditional insurers get it redefine bids to remain relevant? What should councils do to lead organizations through digital transformation? How should board directors define and think about digital transformation?

In the study *Europe's Digital Economy at Risk Eight trends why the European digital economy is losing ground – key measures to regain a leading position*: "We would like to mention the following important trends: 1. ICT segments. Companies in America and Asia have global areas. Less than 10% of global ICT revenues are generated by European companies. Former market leaders have been attracted by global competitors (Nokia) or out of the market (Siemens). Many European industries rely increasingly on non-European IT actors. 2. Capitalization of market loss in the EU. The telecommunications market, the trade in telecommunications services in the EU".

We mention that, first and foremost, US and Asian operators can serve hundreds of millions of customers each in a single consolidated market, the European Commission: the fragmented European market. Secondly, in Europe, remedies against mergers have repeatedly reversed market-based consolidation. Thirdly, the lack of scale prevents investment in European telecoms in the next-generation technology

In the work *Working Party on Security and Privacy in the Digital Economy, Managing digital security and privacy risk, Background report for Ministerial Panel 3.2* we look at the economic and social dimensions of digital security and privacy risks: the evidence of a change in risk understanding and risk management. Digital security incidents undermine innovation, create confidentiality risks and erode confidence (Faggianelli et al., 2018). It is difficult to measure quantitatively, security incidents appear to increase in terms of sophistication, frequency and magnitude of impact. Security incidents may affect the reputation of their organizations, their finances and physical assets, undermine competitiveness, innovation capacity and market positioning.

The OECD Recommendation of 2015 on digital security risk management for economic and social prosperity (the Security Risk Recommendation) sets out a risk management policy framework addressing digital security issues with three messages: 1. It is impossible to completely eliminate the risk digital security when performing digital-based activities. 2. Leaders and decision-makers should focus more on the digital security risk on economic and social activities than on the risk to digital infrastructure; 3. Organizations must integrate digital security risk management into their economic and social decision-making process and overall risk management framework.

Managing privacy risks can improve privacy the 2013 OECD Privacy and Cross-Border Data Flows Guidelines (OECD Privacy Guidelines 2013) recommend the adoption of a risk-based approach to the implementation of confidentiality, principles and the improvement of the protection of privacy. While the concept of risk management is well defined in the digital security space, more work is needed to determine how it can be applied to privacy and there is a debate on how to

implement an approach global risk management to strengthen enforcement, which set out the principles of the OECD Privacy Guidelines. *Effective management of digital security and confidentiality risk* is essential for countries to achieve the full economic and social benefits of the digital economy. Establishing higher levels of trust with users and customers can allow digital services to become more widely accepted and used by individuals and organizations. Governments play a key role in supporting the conditions to build trust and complement the initiatives of the private sector.

In "Privacy Risk Management can enhance Privacy Protection" (OECD, 2013), the Privacy and Cross-Border Data Protection Guidelines recommend the adoption of a risk-based approach to the implementation of confidentiality principles and the improvement of the protection of privacy. Managing privacy risks can contribute to the overall interoperability of privacy protection frameworks. The digital world is not static and continues to have a rapid development. The large-scale changes generated by the digital environment today have significantly widened the scale of digital security and privacy challenges. Effective management of digital security and confidentiality risk is essential for countries to achieve the full economic and social benefits of the digital economy. We want to mention some important moments. Namely, we primarily refer to *the cost of digital security incidents.* The incidence of digital security will have different types of consequences for different institutions: undermining reputation when branding, loss of competitiveness, when there are certain frauds or information theft, financial loss resulting from business loses, business interruption and recovery costs or of legal proceedings and fines. While technical experts and policy makers argue that digitization of security and confidentiality in information security is changing on a scale and requires urgent action by all stakeholders. Concerning *risk understanding and risk management, we mention that* risk management has progressively emerged as a means of addressing digital security and privacy challenges. An important element is also *the components of the risk management cycle that include: 1. Establishment of objectives and context.* We cannot determine the acceptable level of risk in an abstract manner. The first step is understanding the organization's mission, economic and social issues. *2. Risk assessment. This analytical step consists of three distinct tasks:* a) Identification of risk factors: deliberate and unintentional threats, possible vulnerabilities and possible occurrences b) Analysis of risk factors involving consideration of probability or likelihood of an event occurring) Risk evaluation. *3. Risk management,* includes how to address the problem to achieve the goals and benefits anticipated. Involves one or more of the following: a) Acceptance of risk; b) Risk reduction through general information security measures, processes and technologies. c) Sharing the risk or transferring it to another party; d) Avoiding risk by not doing business and thus giving up the potential benefits. *4. Continuous Monitoring and Review Cycle.* We cannot fail to emphasize the fact that National Digital Security Strategies can facilitate the development of safer risk indicators for digital security to better inform public policy makers to assess the effectiveness of public policies. OCDE (2015, 12-15). In this case: Governments and decision-makers in different institutions will address digital security as an economic and social risk, and not just a computer, software, hard, or telecommunication problem. Risk management aims to reduce risk to an acceptable level in light of potential economic and social benefits. Therefore, Governments will have an important leadership mission in promoting digital security risk management by developing national digital security strategies in collaboration with other stakeholders. *Last but not least, the application of risk management to the protection of confidentiality is of major importance.* The challenges of private life in the hyper-connected and intensive digital environment have led decision-makers and other institutions to look for new opportunities, opportunities and effective ways that will apply privacy principles. The concept of confidentiality risk and confidentiality risk management is currently being given increased attention by regulators, academics and policy makers.

3. CONCLUSIONS

The risk can be managed, that is, it can be reduced to an acceptable level in the light of the interests and benefits concerned and the context; Furthermore, confidentiality risk management can contribute to the overall interoperability of privacy protection frameworks. Like all forms of risk, the risk of confidentiality should not be assessed in isolation, but rather in relation to potential benefits. The digital world is not static and continues to have a rapid development. The widespread changes brought about by the digital environment today have significantly widened the scale of digital security and privacy challenges, indicating the need for an evolution in the way these risks are managed. Creating a risk-free environment without threatening these benefits is impossible. Therefore, all stakeholders need to work together to create an environment that promotes effective digital security management and privacy risk.

The Security Risk Recommendation provides a valuable starting point to explore if and how some of the concepts and methodologies developed to manage digital security risk could be useful for privacy. Co-ordinated national confidentiality strategies will help stimulate cooperation among all stakeholders and reduce uncertainty in data flows.

Vulnerability of SMEs. In particular, start-ups stimulate growth, stimulate competition and innovation and contribute to job creation. The digital economy offers opportunities for improving productivity and transforming their business models. At the same time, it raises special challenges because there is evidence that a large number of SMEs do not have the capacity or do not seem to be aware of how digital risk can affect their business.

Securing digital risk: Compulsory data breach notification rules can play an important role in developing a digital market risk system. As the financial costs to deal with a violation become more expensive, with the added efforts to deal with mandatory disclosure, the option of using digital risk insurance will become more attractive for many small and large businesses.

Public policy can ensure assurance in raising awareness and stimulating the adoption of a good digital model of risk management practices. Although it is business-related, digital assurance is seen primarily as a means of transferring risks outside the firm, its greatest potential is to help businesses, organizations and individuals better understand and assess digital risk and capitalize on best practice risk management practices. The British government, for example, began to work with industry insurance to develop a comprehensive digital security model as the next step to encourage small businesses to adopt Cyber Essentials.

As with notification requirements, ensuring digital risks could generate valuable empirical data that would provide an important evidence base to support digital risk management policy.

In practice, insurance companies have been cautious about covering the risk associated with the widespread use of ICT by businesses or the risk associated with intangible assets such as personal data.

Business development, human relations, communication between people, the society with all its phenomena and the government, are more dependent on information technology than ever before. The future of our global society is indissolubly linked to information technology and the Internet. The trend continues; we will be even more dependent on IT in the future. It is true for the developed world and also developing, where the mobile phone transforms business and lives. There is not going back; nor would anyone be seriously supposed to.

Most of the digital hazards we have described so far share the similarities with the risks we have always faced.

However, in our new cybernetic society, the ways we are now exposed to these fundamentally changed risks. Criminals always have stolen money, used extortion, stolen information, and used terrorism. Natural disasters and mistakes have always led to interruptions and losses. Technology, by making information and processes more accessible by cutting geographies and jurisdictions, changing behaviors and behaviors of people's expectations, and connecting as many resources has

increased the speed with which these risks can occur as well as increasing their impact on our economies and our society.

Businesses rely heavily on IT and are exposed to these risks. This report shows that the threat environment includes attackers with strong capabilities and diverse motivations and this business operates across multiple jurisdictional jurisdictions on various regulations. Only these factors make it difficult for businesses to manage digital risk. In addition to increasing digital information, improving people and devices connectivity and business virtualization are all set to drive change and increase complexity

For businesses: Attackers will adapt and evolve this new context; taking advantage of safety loses technological change. It will be hard for businesses to keep up.

Businesses respond to these changes and made a series of recommendations to risk managers. Today, most of the digital downturn is happening within the IT department. We advise risk managers should be involved to bring wider business prospects to decision. We also describe the growth of the cyber insurance market and the recommendation that companies pursue and use this market to complement mitigation measures with risk transfer. The real challenge for risk managers is to work out how to monitor digital risk in order to decide how seriously it should be treated. It is suggested that digital risks are a concern at the board level for many companies. We suggest you be regularly intelligent (rather than formal), based on a combination of the threat environment, current technology trends, and the current management risk.

The final conclusion is to remind readers of the need for a balanced approach to risk management. Businesses must strive to take advantage of technology; not doing so will stifle increased opportunities. Business community has a community interest in understanding digital risks, keeping it under the packaging only benefit cyber criminals. The impact of failures and the risks we face will strengthen the ability of businesses to function successfully in cyber society; even in the face of significant and real digital risks.

REFERENCES

Ashby, S. & Phippen, A. (2015). Managing Digital Risk. Retrieved from: www.talanx.com/~/media/Files/T/ Talanx/pdfcontent/karriere/ebooks/managing-digital-risk.pdf.

Baldwin, A., Shiu, S., Sadler , M. & Horne, B. (2010). Lloyd's 360° Risk Insight Managing digital risk Trends, issues and implications for business, London: Lloyd's 2010.

Bran, F., Alpopi, C. & Burlacu, S. (2018). Territorial developement-disparities between the developed and the least developed areas of Romania. *LUMEN Proceedings*, 6(1), 146-155.

Burlacu, S. (2009). Pre-training human resources in Romanian public administration in the new Knowledge-based economy using electronic communication. *Proceedings of the International Conference Public Institutions' Capacity to Implement the Administrative Reform Process*, Bucharest, June (pp. 23-24).

Burlacu, S. (2010). Role of training in the knowledge society. *Proceedings of Administration and Public Management International Conference*, 6(1), 203-208.

Burlacu, S. (2011a). The role of NGOs in awareness of the public private partnership in the social economy in Romania. *Proceedings of Administration and Public Management International Conference*, 7(1), 118-127.

Burlacu, S. (2011b). Characteristics of Knowledge-based economy and the new technologies in education. *Administratie si Management Public*, 16, 114-119.

Burlacu, S. (2011c). Le rôle des ONG pour la prise de conscience de l'importance des partenariats publics-prives dans l'économie sociale en Roumanie. *Administratie si Management Public (RAMP)*, 17, 120-129.

Burlacu, S. (2014). Integrating the e-learning dimension in the EDU-RES master's programme. *Proceedings of Administration and Public Management International* Conference, 10(1), 139-147.

Burlacu, S. & Jiroveanu, D. (2012). The role of support open source systems to improve the quality of decisions in an educational institution in Romania. *Proceedings of the 6th International Management Conference: Approaches in organisational management*, 15th-16th, November, Bucharest, Romania (pp. 641-647).

Burlacu, S. & Jiroveanu, D.C. (2011). The development of software solution for supply chain management. *REVISTA DE MANAGEMENT COMPARAT INTERNATIONAL/REVIEW OF INTERNATIONAL COMPARATIVE MANAGEMENT*, 12(6), 140-145.

Burlacu, S., Gutu, C. & Matei, F.O. (2018). Globalization – Pros and cons. *Quality-Access to Success*, 19.

Burlacu, S., Profiroiu, A. & Vasilache, P.C. (2019). Impact of demography on the public finance of the European Union. *Calitatea*, 20(S2), 136-138.

Burlacu, S. & Jiroveanu, D.C. (2009) IT governance and educational ideal. *Administrație și Management Public*, 13, 73-82.

Ciobanu, G. & Stratulat, O. (2016) Analysis of Romanian companyes activity in the context of building the informational society in Romania. *Calitatea, suppl. Supplement to Quality – Access to Success*, 17(1), 319-326.

Ciobanu, G., Ghinararu, C., Crețu, A.Ș., Davidescu, A.A.M. & Chiriac, B. (2015). *Aspects of the digital economy development in Romania. Theory, measurement techniques, development policies and job generation*, Bucharest: Editura Universitară.

Costache, G., Marinas, C.V., Igret, R. & Burlacu, S. (2015). Internship in the HR department-organizational and individual perspectives. *Proceedings of the INTERNATIONAL MANAGEMENT CONFERENCE*, 9(1), 359-370.

Faggianelli, D., Burlacu, S. & Carra, C. (2018). Victimization of health professionals in Bucharest service relations and social work relationships. *Administrație și Management Public*, 30: 109-126.

Ionita, F., & Burlacu, S. (2009a) Public administration from Romania in the knowledge society and e-learning. *Proceedings of the Fifth Administration and Public Management International Conference: "Public Institutions' Capacity to Implement the Administrative Reform Process"*.

Ionita, F., Ursacescu, M. & Burlacu, S. (2009b). Public services as poles of regional competitiveness in sustainable developement. *Revista de Management Comparat International/Review of International Comparative Management*, 10(3), 552-565.

Ioniță, F., Burlacu, S. & Gaidargi, A. (2009c). Modern approaches of the management of alternative trade systems. *Revista de Management Comparat Internațional/Review of International Comparative Management*, 51, 473-480

Jianu, I., Dobre, I., Bodislav, D.A., Radulescu, C.V. & Burlacu, S. (2019). The implications of institutional specificities on the income inequalities drivers in European Union. *Economic Computation and Economic Cybernetics Studies and Research*, 53(2), 59-76.

OCDE. (2015). *Innovation Strategy 2015 An Agenda for Policy Action*, (pp. 12-15).

OECD. (2013). *Managing privacy risks can improve privacy The 2013 OECD Privacy and Cross-Border Data Flows Guidelines*. Paris

OECD. (2013). *Privacy Risk Management can enhance Privacy Protection*. Paris.

OECD. (2016). *Working Party on Security and Privacy in the Digital Economy, Managing digital security and privacy risk. Background report for Ministerial Panel 3.2 ,DSTI/ICCP/REG(2016)1/FINAL JT03397039*. Paris.

OECD. (2017). *OECD Digital Economy Outlook 2017.* Paris.

Profiroiu, A., Burlacu, S. & Sabie, O. (2019). Reform of the pension system in Romania. *Calitatea,* 20(2), 521-524.

Rădulescu, C.V., Bodislav, D.A. & Burlacu, S. (2018a). Demographic explosion and IT governance in Public institutions. *Managerial Challenges of the Contemporary Society. Proceedings*, 11(1), 18-24.

Rădulescu, C.V., Dobrea, R.C. & Burlacu, S. (2018b) The business management of distress situations. *Proceedings of the 12th INTERNATIONAL MANAGEMENT CONFERENCE "Management Perspectives in the Digital Era"*, 741-747.

Sivobrova, I.A., Сивоброва Ирина Анатольевна, Социальные риски цифровой трансформации общества

Stratulat, O. & Ciobanu, G., (2016) Romanian IT&C industry development in the context of development of the digital economy. *Calitatea, suppl. Supplement to Quality – Access to Success*. 2016, 17(1), 347-352.

*** (2015). *Risk and opportunity in an increasingly digital world Insurance Governance Leadership Network.* Insurance Governance Leadership Network View Points.

***. (2014). *Strategia Nationala privind Agenda Digitala pentru Romania, iulie 2014*. The National Strategy for the Digital Agenda for Romania.