Vol.1, No.1, 9-18,2023

Legal Research & Analysis

Consumer Protection in The New Digital Decade

Cristina Mihaela Salcă Rotaru

Faculty of Law, Transilvania University of Brasov, Romania.

* *Corresponding Author Email: rotaruc@unitbv.ro*

Abstract: In this article, the effect of digitization, the use of the Internet and the Internet of Things on consumers in the EU in general and in Romania in particular is discussed. The research is linked to the legislation and policies for accelerating the digital transformation and to the concrete digital objectives pursued in the implementation of the Digital Decade at the level of the European Union. Creating new volumes of data through the implementation of digital services and technologies can create new issues related to data protection and therefore maintaining consumer confidence, confidentiality, access to data and their integrity. The right to information and the information of the average consumer are perhaps the most important aspects of consumer protection. These are key elements of the informed decisions that the consumer must make, in and about the digital environment, so that it is protected against risks and possible harm to its health, safety and fundamental rights. The research results reveal the vulnerability of Romanian consumers to the new reality imposed by the acceleration of digitalization at European level and proposes measures to reduce the digital divide in terms of digital skills.

Keywords: Consumer Protection; Digitalization; Digital Skills; European Policies; European Legislation

1. Introduction

The pandemic has caused and determined the use of the online environment for most fields of activity. Not all individuals were prepared for such a sudden transition of social activities and personal actions into the virtual environment. The digital divide can concern any one or even all the aspects necessary for complete digitization: the equipment, the territorial coverage, and the necessary skills. The European Committee of the Regions states in a current document that "digital transformation is radically changing the lives of consumers. It offers them immense possibilities, but also puts them in front of new difficulties"[1]. The specialized literature (Van Deursen & Helsper, 2018; Van Deursen & Mossberge, 2018; Malchenko *et al.,* 2020; Salca Rotaru, 2021; Repanovici *et al.,* 2021), along with various studies and reports that can be found in the Digital Economy and Society Index (DESI)[2] emphasize the lack of personal skills of individuals, necessary to adapt to a sudden digitization, regardless of belonging to a group, professional or social category.

From the perspective of consumer protection, digitization concerns or has effects, not only in terms of their possibility to access goods and services but also their protection in terms of the right to information and the protection of personal data, important aspects/elements in terms of taking informed decisions. Consumer protection issues in the use of the Internet have been intensively and long discussed in specialized literature, but digitalization also concerns the use of the Internet between objects, that is, what is known as the Internet of Things. In 2009 it was stated in a communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions that" One major next step in this development is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an 'Internet of things'

[1] European Committee of the Region 61/2022, "*Opinion of the European Committee of the Regions — New Consumer Agenda — Strengthening consumer resilience for sustainable recovery*", accessed January 20, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IR0407

[2] European Commision 2021, "*Digital Economy and Society Index 2021*", https://digital-strategy.ec.europa.eu/en/policies/desi

(IoT)"[3]. Since then, the Commission anticipated, in the Communication, the possible emergence of some problems that can directly affect consumers, the example being connected to the management of information related to the location of people. The Commission's prediction at the time that the IoT, which at that time was "not yet a tangible reality, but rather a forward-looking vision of a number of technologies that, combined together, could drastically alter in the next 5 to 15 years the way our societies function"[4] is added today to the pandemic reality that facilitated, and in some situations forced society to transition and intensively use the Internet, including between objects.

We emphasize that the article does not cover the IoT production sector or its use in production activity, which can be characterized more as an intranet use, but cover the use of internet from a consumer perspective, as it is defined in European Union legislation. Unfortunately, the first approach was the one that mainly concerned the European Union, it being interested in competition issues in this emerging sector, and less in "the consumer IoT sector that is still developing"[5].

2. The General Issue

The use of the Internet has gradually brought both benefits, through the development of communication and various industries or services, but also many problems, starting from data protection to health or marginalization/discrimination of some social categories (Colgate *et al.,* 2005; Chadwick *et al.,* 2017; Blank & Lutz, 2018; Livingstone *et al.,* 2024). The evolution in the use of the Internet for personal or economic purposes, being somewhat slower, compared to the evolution of IoT, has also benefited from regulations regarding various aspects of consumer protection, among which we mention:

- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market[6],
- Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market[7],
- Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods[8],

[3] European Commission, 278/2009, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things: an action plan for Europe" /*COM/2009/0278 final */, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0278&qid=1708713804325

[4] European Commission, 278/2009, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Internet of Things: an action plan for Europe" /* COM/2009/0278 final */, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0278&qid=1708713804325

[5] European Commission, 10/2022, COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT "Final report - Sector inquiry into consumer Internet of Things", SWD/2022/10 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52022SC0010&qid=1708714458141

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *JO L 178, 17.7.2000, p. 1-16,* accessed January, 15, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32000L0031&qid=1708716511987

[7] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, *JO L 149, 11.6.2005, p. 22-39,* accessed January, 15, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32005L0029&qid=1708716590178

[8] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, *JO L 136, 22.5.2019, p. 28-50,* accessed January, 15, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019L0771&qid=1708716645153

- Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services[9],
- Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services[10].

The digital transformation determined by new digital technologies has led to the emergence of a new concept, the Digital Decade. It is stated that „the benefits arising from digital technologies do not come without risks and costs. Citizens no longer feel in control over what happens with their personal data and are increasingly overloaded by artificial solicitations of their attention. And malicious cyberactivity may threaten our personal well-being or disrupt our critical infrastructures and wider security interests”[11].

The statement of the Commissioner for the Internal Market, Thierry Breton, is relevant, stating that "Europe, across the continent, must ensure that citizens and businesses have access to a wide range of next-generation technologies that make their lives better, safer and even more ecological - provided that they are able to use the respective technologies. In the post-pandemic world, this is how we will together shape a resilient and digitally sovereign Europe. This is Europe's digital decade." (Breton, 2021).

At this moment, not even the European Union knows or foresees the problems that may arise in the framework of the digital transformation, because it itself recognizes that „Creating a Europe fit for the digital age is a complex puzzle with many interconnected pieces; as with any puzzle, the whole picture cannot be seen without putting all the pieces together”[12]. Consumer protection is in the same situation when it comes to IoT. The literature generally highlights the benefits brought by IoT (Manyika *et al.,* 2015; Anand & Jeyaraj, 2019), it being undeniable that IoT has brought multiple benefits in areas such as health (Nasajpour *et al.,* 2020), industry (Lampropoulos *et al.,* 2019), energy (Hossein Motlagh *et al.,* 2020) or even agriculture (Kour & Arora, 2020). However, along with the mentioned benefits, there are also problems related to security (Ande *et al.,* 2020; Arora *et al.,* 2019; Chu *et al.,* 2019), personal data protection (Finck, 2018; Gkotsopoulou & Quinn, 2021) and ethics (Baldini *et al.,* 2018; Tzafestas, 2018; El-Khoury & Arikan, 2021) or even the exercise or respect of fundamental rights (Wachter, 2018a, 2018b; Fornasier, 2020).

There is already talk of European technological sovereignty (Crespi *et al.,* 2021). It is stated that this „starts from ensuring the integrity and resilience of our data infrastructure, networks and communications” and that „is not defined against anyone else, … focusing on the needs of Europeans and of the European social model”[13], but it does not say where it ends or what are the limits of this sovereignty. It is proposed, also here, the existence of a universally accepted public electronic identity

[9] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, *JO L 186, 11.7.2019, p. 57-79,* accessed January, 15, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019R1150&qid=1708716780314

[10] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *JO L 136, 22.5.2019, p. 1-27,* accessed January, 15, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019L0770&qid=1708716711797

[11] European Commission 67/2020, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Shaping Europe's digital future”, COM(2020) 67 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067&qid=1708717124718

[12] European Commission 67/2020, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Shaping Europe's digital future”, COM(2020) 67 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067&qid=1708717124718

[13] European Commission 67/2020, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Shaping Europe's digital future”, COM(2020) 67 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067&qid=1708717124718

(eID) required for authentication in order to have access to certain online services that would ensure: (i) control over identity in the online environment and require the assumption of greater personal responsibility in this meaning, and (ii) avoiding the use of platforms that require the communication of personal data unnecessarily.

Contextualizing, the current study highlights the basis of current consumer protection issues in Internet use. Some of the issues can be considered already old, even if their age is no more than a decade, and others fall under current or even emerging issues.

3. Old Problems, New Problems and Emerging Issues

3.1. Old Problems

It is already known and recognized that any citizen, regardless of age, gender or professional experience, must have the opportunity to develop on a personal level, to get involved in society, and in terms of his quality as a consumer to make choices free and safe.

The new agenda for consumer protection starts from an already known problem, namely the vulnerability of certain groups of consumers (especially children, the elderly and the disabled) who require specific protection measures, but adds this vulnerability to a new situation determined by the digital divide[14].

The digital divide, determined by specific equipment, territorial coverage, and individual skills, concerns the entire European Union, Romania being sufficiently affected as well. The existence of this gap and its effects determined the realization of numerous research and publications that share the new expression "digital divide". These aspects have been explored in a previous paper which aims at the need to rethink the importance of IL skills in consumer protection (Salca Rotaru, 2021).

These problems "must" be solved soon, because the Compass for Europe's digital dimension: the European model for the digital decade[15], document developed by the European Commission in 2021 proposes that by 2030:

- at least 80% of adults should have basic digital skills and there should be 20 million specialists employed in the ICT sector in the EU,
- all households in the EU should have gigabit connectivity, and all populated areas should be covered by 5G technology,
- three out of four companies should use cloud computing services, big data systems and artificial intelligence, more than 90% of SMEs should reach at least a basic level of adoption of digital technologies, and the number of EU unicorn start-ups should double,
- all essential public services should be available online, all citizens will have access to their electronic medical records, and 80% of citizens should use an electronic identification solution.

3.2. New problems

Among the topical issues regarding IoT, the one that has a direct impact on consumer protection, from a financial protection perspective, is interoperability at this level. This is a problem of access to the main technological platforms of consumer IoT, which turns into a competition problem in the IoT market, as

[14] European Commision. Communication from the Commission to the European Parliament and the Council. "New Consumer Agenda. Strengthening consumer resilience for sustainable recovery." COM/2020/696 final. accessed February, 10, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0696

[15] European Commision. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions „2030 Digital Compass: The European way for the Digital Decade." COM(2021) 118 final. Accessed February, 10, 2024, https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:52021DC0118

it is related to the main providers of operating systems for smart (mobile) devices and voice assistants (Amazon, Google, and Apple).

Through the IoT, a very large amount of data is collected, of which we distinguish three categories:

- a first category is the data provided directly by users, in order to obtain user access, these being mostly personal data
- a second category is constituted by the data collected by operating the device or accessing the service and which come from monitoring the behavior of users, accepted by them as a way of operating these objects, and
- the third category is made up of data originating from and aimed at the way object's function and the space around them. A conclusive example is that of the data that can be obtained and/or provided by a smart thermostat, in which case it can collect data on the temperature and air quality of the space in which it is located, and data on the arrival and departure of its users spacebar.

Thus, the second problem reported is that of the collected data and its use. If cybersecurity regarding the collection and use of data obtained through IoT is already a subject of specialized literature (Lee, 2020; Fagan *et al.,* 2021) there are other less obvious aspects.

In the Final Report of the European Commission of January 20, 2022, it is stated that "the use of consumer IoT data for digital advertising purposes can be of particular value to key players in the field of consumer IoT that carry out an economic activity of digital advertising"[16]. Even though it is stated that "this business opportunity is not yet very advanced and should comply with data protection rules"[17] economic interest in this industry can create enough consumer protection problems. A control over the future behavior of consumers can be had by the providers of voice assistants by leveraging the obtained data to create and provide other IoT related products and services aimed at consumers, in which sense we can reach the notion of captive users. That is why standardization efforts in IoT are welcome, but probably as late as possible considering that the entry and development of smaller competitors in this market also depends on them.

3.3. Emerging Issues

It is obvious that digital transformation cannot take place without the ownership of citizens. It can only be forced up to a point. We believe that digital transformation is imposed both through the economy and through the authorities and public administrations. To reach the full potential of digital transformation, citizens must trust that their applications and products are secure. We find that the more interconnected we are, the more vulnerable we are to malicious cyber activity (Maroz, 2021). It was stated that "feeling safe and secure is not just about cyber security. Citizens must be able to trust the technology itself as well as how it is used"[18].

That's why maybe, the Guiding Digital Principles to be considered in the context of the process stemming from the Commission's Communication "2030 Digital Compass: The European way for the

[16] European Commission, 10/2022, COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT „Final report - Sector inquiry into consumer Internet of Things", SWD/2022/10 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52022SC0010&qid=1708714458141

[17] European Commission, 10/2022, COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT „Final report - Sector inquiry into consumer Internet of Things", SWD/2022/10 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52022SC0010&qid=1708714458141

[18] European Commission 67/2020, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, „Shaping Europe's digital future", COM(2020) 67 final, accessed February, 3, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067&qid=1708717124718

Digital Decade" which can be found in the annex of the Lisbon Declaration – Digital Democracy with a Purpose, from 2021, regarding electronic identity states that:

- Everyone should be able to have a personal digital identity, to fully enjoy citizenship in the digital environment and avail of legal protection against any form of discrimination in the online environment.
- Everyone should be able to use convenient, trusted and secure electronic identification means and trusted services that can be used for accessing public and private online services, including cross-border, where the user can increasingly exercise their rights over their own data[19].

This idea goes further, even to the point that „Everyone should be able to decide over their own digital personal legacy".

These new directions of development will bring with them new problems to be solved, primarily from a legislative point of view. It proves more than ever that consumer protection is a transversal and transdisciplinary field.

4. What Should be Done

4.1. In General

As stated, the pandemic had both negative and positive effects. From the perspective of the transition to digitization, it imposed a very rapid transition to the digital environment, achieving spectacular results but also highlighting social and legal vulnerabilities.

A new direction is that of digitization centered on people, as opposed to digitization centered on the provision of services and goods, an approach also mentioned in the Opinion of the European Committee of the Regions — New Consumer Agenda — Strengthening consumer resilience for sustainable recovery [20].

Thus, the EU legislation regarding:

- Consumer protection must be coherent and correlated with that regarding digital markets. The purpose of this correlation and coherence should aim at both the consumer's right of free access to the domestic and international market, as well as its protection by ensuring a safe digital environment and establishing clear and achievable rules regarding liability in case of non-compliance by suppliers or intermediaries, including those from the online environment.
- The security of the products, needs to be modernized and to provide solutions to the problems regarding the security of connected objects, especially regarding: the protection of personal data; cyber security; interoperability and reliability of systems; transparency of information and, last but not least, informing the consumer.

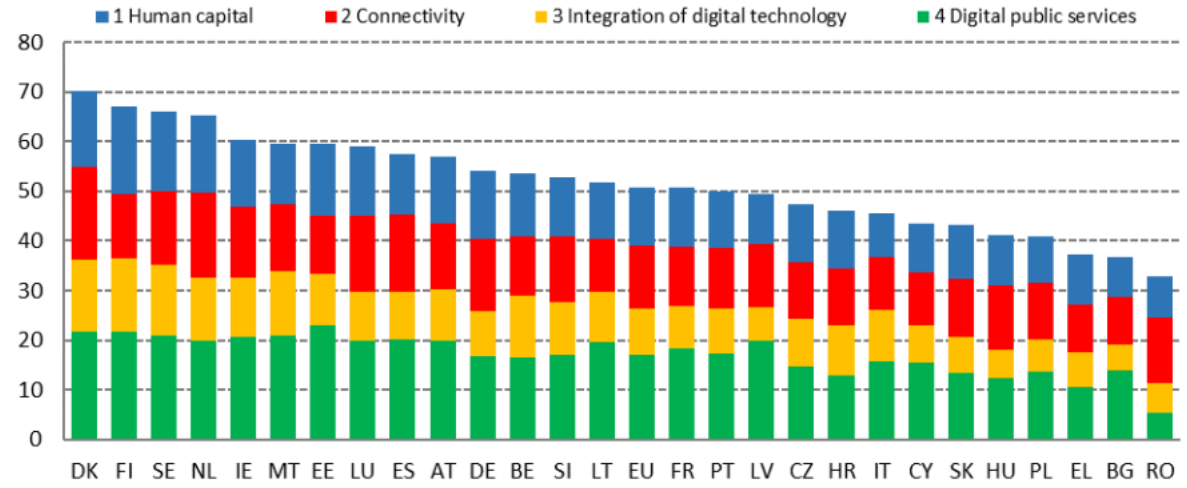
Aspects related to consumer vulnerability and exclusion, in any of the forms and in any category, should be addressed in such a way as to aim at their elimination concentrically and gradually. Concentric because the solutions addressed must start from specific, local problems, which must in turn be contained in the extended macro-level and gradual solutions, because no solution that is not based on successive and logical steps can achieve its finality.

[19] Lisbon Declaration – Digital Democracy with a Purpose. Accessed February 12, 2024, https://www.lisbondeclaration.eu/learn-more/

[20] European Committee of the Region 61/2022, "*Opinion of the European Committee of the Regions — New Consumer Agenda — Strengthening consumer resilience for sustainable recovery*", accessed January 20, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IR0407

4.2. In Romania

The DESI 2021 report shows with regard to Romania that regarding the digital skills of Romanian citizens, they are far behind compared to the EU average. Perhaps this is also the reason why the integration of digital technology by businesses is at one of the lowest percentages in the EU. It is also stated that „Most countries, which are below the EU digitalization average, have not progressed much in the last 5 years. This is the case especially for Bulgaria and Romania"[21]. The most relevant information on these aspects emerges from Figure 1, which presents the comparative percentages between all EU states regarding the digital skills of human capital, connectivity, the integration of digital technologies in the economy and public services.



Source: DESI 2021, European Commission.

Figure 1. Comparative percentage representation (DESI - Full Economical Analysis 2021 p.19).

From the perspective of the previously identified problems and solutions, but also from the perspective of previous research on the national consumer (Salca Rotaru, 2021), we appreciate that the solutions cover the following aspects:

- The real identification of the digital divide, its causes and the spread area. These data allow the establishment of concrete policies and programs/projects for digital literacy or increasing digital skills,
- An effective cooperation between the main national authorities with competences in establishing and implementing these policies, programs, and projects (Ministry of Research, Innovation and Digitization, Ministry of Education and the National Authority for Consumer Protection),
- Creation of digital advisory/information offices/services at local, institutional, organizational level, which offer help and information at individual level, including regarding cyber security,
- The prohibition of the total elimination of face-to-face interaction in terms of the relationship consumer - supplier of products and/or services because there will always be consumers in one of the categories of vulnerable consumers, who are the most likely to be subjected to discrimination from the perspective of the right of access to products and services.

These general recommendations can be developed in further research that identifies concrete implementation elements.

[21] European Commission, "Digital Economy and Society Index 2021 Thematic chapters". (2021): 1-108. Accessed January 25, 2024, DESI - Full Economical Analysis 2021

5. Conclusions

The development of new technologies, which permeate our professional and private lives, calls for even more respect for consumer rights, especially the right to a technology that can be trusted. Distrust and lack of skills can lead to consumer resilience to their use and thus failure to meet the demands of the Digital Decade. Adoption of technologies without having sufficient information or without understanding them can easily be speculated by illegal use of data obtained from consumers. The authorities must be more involved in ensuring the legal and institutional framework in terms of the development and implementation of new instruments to ensure the respect of consumer rights in the new development context. The future of digital technology cannot be known, but it can be predicted. That is why the framework must be created to ensure, also in the digital space, compliance with European values, ethical and social norms.

The creation of a digital culture is inevitable. Therefore, citizens need to be sensitized and educated about the new social requirements regarding digital skills, which will be useful both in everyday life and in terms of accessing a job. From the perspective of the consumer, we believe that he needs these specific knowledge and skills because he uses the Internet and digital technology not only in the relationship between people, but between people and objects, and especially because it allows the use of the Internet, on his behalf, between objects or between his objects and other people.

References

Abbasi, M., Yaghmaee, M.H., & Rahnama, F. "Internet of Things in agriculture: A survey" . *2019 3rd International Conference on Internet of Things and Applications (IoT)*. IEEE, (2019): 1-12. DOI: 10.1109/IICITA.2019.8808839.

Anand, P., & Jeyaraj, R. "Internet of Things: A primer". *Human Behavior and Emerging Technologies*, 1 no. 1 (2019): 37-47. https://doi.org/10.1002/hbe2.133

Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. "Internet of Things: Evolution and technologies from a security perspective". *Sustainable Cities and Society*, *54*, 101728. (2020). https://doi.org/10.1016/j.scs.2019.101728.

Arora, A., Kaur, A., Bhushan, B., & Saini, H. Security concerns and future trends of internet of things". *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies* 1, (2019): 891-896.

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. "Ethical design in the internet of things". *Science and engineering ethics*, 24 no. 3 (2018): 905-925. https://doi.org/10.1007/s11948-016-9754-5.

Blank, G., & Lutz, C. "Benefits and harms from Internet use: A differentiated analysis of Great Britain". *New media & society*, *20, no. 2* (2018): 618-640. https://doi.org/10.1177/1461444816667135.

Breton, T. March 9, 2021, press release, https://ec.europa.eu/commission/presscorner/detail/ro/IP_21_983.

Chadwick, D. D., Quinn, S., & Fullwood, C. "Perceptions of the risks and benefits of Internet access and use by people with intellectual disabilities" . *British Journal of Learning Disabilities* 45, no.1 (2017): 21-31. 10.1111/bld.12170.

Chu, G., Apthorpe, N., & Feamster, N. "Security and privacy analyses of internet of things children's toys". *IEEE Internet of Things Journal* 6, no. 1 (2018): 978-985. 10.1109/JIOT.2018.2866423.

Colgate, M., Buchanan-Oliver, M., & Elmsly, R. "Relationship benefits in an internet environment". *Managing Service Quality* 15, no. 5 (2005):426-436. 10.1108/09604520510617284.

Crespi, F., Caravella, S., Menghini M., & Salvatori, C. "European technological sovereignty: an emerging framework for policy strategy". *Intereconomics*, 56, no.6 (2021): 348–354, 10.1007/s10272-021-1013-6.

El-Khoury, M., & Arikan, C. L. "From the internet of things toward the internet of bodies: Ethical and legal considerations". *Strategic Change,* 30, no. 3 (2021): 307-314. https://doi.org/10.1002/jsc.2411.

Fagan, M., Marron, J., Brady Jr, K. G., Cuthill, B. B., Megas, K. N., Herold, R., & Hoehn, B. "IoT device cybersecurity guidance for the Federal Government". *NIST Special Publication*, (2021):800 -213. https://doi.org/10.6028/NIST.SP.800-213.Finck, M. "Blockchains and data protection in the European Union". *European Data Protection Law Review* 4, no. 1 (2018):17-35. https://doi.org/10.21552/edpl/2018/1/6.

Fornasier, M.D.O. "The applicability of the Internet of Things (IoT) between fundamental rights to health and to privacy". *Revista de Investigações Constitucionais* 6, no. 2 (2020): 297-321. https://doi.org/10.5380/rinc.v6i2.67592.

Gkotsopoulou, O. & Quinn, P. *Data protection and privacy issues of the internet of things*. In: *Internet of Things, Threats, Landscape, and Countermeasures*, Ed.: Shiaeles, S., & Kolokotronis, N. (Boca Raton: CRC Press, 2021): 1-46. https://www.taylorfrancis.com/books/edit/10.1201/9781003006152/internet-things-threats-landscape-countermeasures-stavros-shiaeles-nicholas-kolokotronis .

Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. "Internet of Things (IoT) and the energy sector". *Energies*, *13*, no. 2 (2020): 494. https://doi.org/10.3390/en13020494.

Kour, V. P., & Arora, S. "Recent developments of the internet of things in agriculture: a survey". *IEEE Access* 8, no. 99 (2020): 129924-129957. 10.1109/ACCESS.2020.3009298.

Lampropoulos, G., Kerstin, S., & Theofylaktos, A.. "Internet of things in the context of industry 4.0: an overview". *International Journal of Entrepreneurial Knowledge,* 7 no. 1 (2019): 4-19. https://doi.org/10.37335/ijek.v7i1.84.

Lee, I. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." *Future Internet* 12, no. 9 (2020): 157. https://doi.org/10.3390/fi12090157.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K., "Risks and safety on the internet. The perspective of European children. Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries". EU Kids Online, Deliverable D4. EU Kids Online Network, London, UK, (2021), accessed January, 13, 2024, https://eprints.lse.ac.uk/33731/.

Malchenko, Y., Gogua, M., Golovacheva, K., Smirnova, M., & Alkanova, O. "A critical review of digital capability frameworks: a consumer perspective". *Digital Policy, Regulation and Governance* 22, no. 4 (2020): 269-288.https://doi.org/10.1108/DPRG-02-2020-0028.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. "The Internet of Things: Maping the value beyond the hype". *McKinsey Global Institute* 1, (2015).

Maroz, N. "A critical analysis of the need for a stronger international legal framework for cyber ethics in times of pandemic". *Ethics and Deontology Journal* 1, no. 01 (2021): 60–73. https://doi.org/10.52744/RED.2021.01.08.

Nasajpour, M., Pouriyeh, S., Parizi, R. M., Dorodchi, M., Valero, M., & Arabnia, H. R. "Internet of Things for current COVID-19 and future pandemics: An exploratory study". *Journal of Healthcare Informatics Research,* 4, no. 4 (2020): 325-364. https://doi.org/10.1007/s41666-020-00080-6.

Repanovici, A., Salcă Rotaru, C.M., Murzea, C. "Development of Sustainable Thinking by Information Literacy". *Sustainability*, 13, no. 1287 (2021): 1-21. https://doi.org/10.3390/su13031287.

Salcă Rotaru, C.M. "After COVID19, is it necessary to rethink the importance of IL skills in consumer protection?". 11th International Conference on Information Science and Information Literacy. *Sciendo*, (2021): 120-129. https://doi.org/10.2478/9788395815065-012.

Tzafestas, S. G. "Ethics and law in the internet of things world". *Smart Cities* 1, no. 1 (2018): 98-120. https://doi.org/10.3390/smartcities1010006.

Van Deursen, A. J., & Helsper, E. J. "Collateral benefits of internet use: explaining the diverse outcomes of engaging with the internet". *New Media & Society,* 20, no. 7 (2018): 2333-2351. https://doi.org/10.1177/1461444817715282.

Van Deursen, A. J., & Mossberger, K. "Any Thing for anyone? A new digital divide in internet-of-things skills". *Policy & Internet,* 10, no. 2 (2018): 122-140. https://doi.org/10.1002/poi3.171.

Wachter, S. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR". *Computer Law & Security Review,* 34, no. 3 (2018): 436-449. http://dx.doi.org/10.2139/ssrn.3083554.

Wachter, S. "The GDPR and the Internet of Things: a three-step transparency model". *Law, Innovation and Technology,* 10, no. 2 (2018): 266-294. http://dx.doi.org/10.2139/ssrn.3130392.